ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Ασφάλεια πληροφοριών στα Ευφυή Δίκτυα ΗΕ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Αναστάσιος-Διονύσιος Καραγιάννης

Επιβλέπων καθηγητής: Παναγιώτης Κωττής, Καθηγητής Ε.Μ.Π

Αθήνα, Ιούνιος 2015

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Ασφάλεια πληροφοριών στα Ευφυή Δίκτυα ΗΕ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Αναστάσιος-Διονύσιος Καραγιάννης

Επιβλέπων καθηγητής: Παναγιώτης Κωττής, Καθηγητής Ε.Μ.Π

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή:

…….	…….	…….
Παναγιώτης Κωττής	Χρήστος Καψάλης	Γεώργιος Φικιώρης
Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π	Αναπληρωτής Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούνιος 2015

……..
Αναστάσιος-Διονύσιος Ι. Καραγιάννης

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Η/Υ Ε.Μ.Π.

Περιεχόμενα

Πίνακας αντιστοίχησης συντομογραφιών

ΑΡΚΤΙΚΟΛΕΞΟ	ΣΥΝΘΕΤΗ ΟΝΟΜΑΣΙΑ	ΕΠΕΞΗΓΗΣΗ
ACL	Access Control List	Κατάλογος ελέγχου πρόσβασης
AES	Advanced Encryption Standard	Σύγχρονο πρωτόκολλο κρυπτογράφησης
ANSI	American National Standards Institute	Αμερικανικό Ινστιτούτο Προτύπων
ARP	Address Resolution Protocol	Πρωτόκολλο αντιχτοίχισης διευθύνσεων στο τοπικό δίκτυο
BYOD	Bring Your Own Device	Πολιτική εταιριών που επιτρέπει στο προσωπικό να χρησιμοποιεί προσωπικές συσκευές στο εταιρικό πληροφοριακό δίκτυο
CIP	Common Industrial Protocol	Δικτυακό πρωτόκολλο που χρησιμοποιείται σε βιομηχανικά πληροφοριακά δίκτυα
CPU	Central Processing Unit	Κεντρική μονάδα επεξεργασίας
CRC	Cyclic Redundancy Check	Πεδίο ορισμένων bit επαλήθευσης ενός μηνύματος ώστε να ανιχνεύονται λάθη κατά τη μεταφορά.
DDOS	Distributed Denial of Service	Κατανεμημένη επίθεση άρνησης διαθεσιμότητας
DHCP	Dynamic Host Configuration Protocol	Δικτυακό πρωτόκολλο αυτόματης διανομής διευθύνσεων IP στο τοπικό δίκτυο.
DMZ	De-Militarized Zones	Αποστρατιωτικοποιημένες ζώνες – Δικτυακές ζώνες στις οποίες τοποθετούνται συστήματα προσβάσιμα από το Διαδίκτυο ώστε να προστατεύεται το υπόλοιπο δίκτυο
DNP3	Distributed Network Protocol 3	Δικτυακό πρωτόκολλο που χρησιμοποιείται σε βιομηχανικά πληροφοριακά δίκτυα
DNS	Domain Name System	Πρωτόκολλο του Διαδικτύου που αντιστοιχεί δικτυακά ονόματα σε διευθύνσεις IP
DRAM	Dynamic Random Access Memory	Κατηγορία μνήμης RAM που κατασκευάζεται με πυκνωτές
EEPROM	Electrically Erasable Programmable Read-Only Memory	Τύπος μνήμης μόνο για ανάγνωση που μπορεί να επανεγγραφεί χωρίς αφαίρεση
FEC	Forward Error Correction	Μέθοδος ελέγχου και δίορθωσης λαθών κατά την μετάδοση

FLASH		Τύπος επανεγγράψιμης μη πτητικής μνήμης
FPGA	Field-Programmable Gate Array	Παραμετροποιήσιμα ολοκληρωμένα κυκλώματα
FTP	File Transfer Protocol	Δικτυακό πρωτόκολλο μεταφοράς αρχείων
FTPS	File Transfer Protocol Secure	Παραλλαγή του πρωτοκόλλου FTP που περιλαμβάνει μηχανισμούς ασφάλειας πληροφοριών
GPRS	General Packet Radio Service	Πρωτόκολλο μετάδοσης δεδομένων πάνω από δίκτυα κινητής τηλεφωνίας
GPS	Global Positioning System	Πρωτόκολλο εντοπισμού γεωγραφικής θέσης
GSM	Global System for Mobile communications	Πρότυπο δικτύων κινητής τηλεφωνίας
HAN	Home Area Network	Οικιακό τοπικό δίκτυο
HMI	Human-Machine Interface	Συστήματα αλληλεπίδρασης ανθρώπου-μηχανής
HSPA+	Evolved High-Speed Packet Access	Πρότυπο μεταφοράς δεδομένων μέσω δικτύων κινητής τηλεφωνίας
HTML	Hyper-Text Markup Language	Γλώσσα περιγραφής ιστοσελίδων
HTTP	Hyper-Text Transfer Protocol	Πρωτόκολλο μεταφοράς ιστοσελίδων – Βασικό πρωτόκολλο του διαδικτύου
HTTPS	Hyper-Text Transfer Protocol Secure	Παραλλαγή του HTTP που περιλαμβάνει μηχανισμούς ασφάλειας πληροφοριών
ICANN	Internet Corporation for Assigned Names and Numbers	Οργανισμός υπεύθυνος για την ονοματοδοσία στο Διαδίκτυο
ICCP	Inter-Control Center Communications Protocol	Πρωτόκολλο επικοινωνίας ελεγκτικών σταθμών SCADA με τις υπό έλεγχο διατάξεις
ICMP	Internet Control Message Protocol	Πρωτόκολλο του Διαδικτύου για σήματα ελέγχου
IDS	Intrusion Detection System	Μηχανισμός ανίχνευσης πιθανής παραβίασης
IEC	International Electrotechnical Commision	Διεθνής οργανισμών προτύπων ηλεκτρολογικών και ηλεκτρονικών τεχνολογιών
IEEE	Institute of Electrical and Electronics Engineers	Διεθνής σύνδεσμων ηλεκτρολόγων και ηλεκτρονικών μηχανικών
IP	Internet Protocol	Πρωτόκολλο διευθυνσιοδότησης στο Διαδίκτυο
IPS	Intrusion Prevention System	Μηχανισμός αποτροπής παραβιάσεων

ISO	International Organization for Standardization	Διεθνής οργανισμός τυποποίησης
ISP	Internet Service Provider	Πάροχος υπηρεσιών διαδικτύου
IT	Information Technology	Η τεχνολογία χρήσης υπολογιστών για αποθήκευση, επεργασία και μετάδοση πληροφοριών
JTAG	Joint Test Action Group	Πρότυπο ελέγχου ορθής λειτουργίας ολοκληρωμένων κυκλωμάτων
LAN	Local Area Network	Τοπικό Δίκτυο
LTE	Long-Time Evolution	Πρότυπο μεταφοράς δεδομένων μέσω δικτύων κινητής τηλεφωνίας
MAC address	Media Access Control address	Διεύθυνσης κάθε δικτυακής συσκευής στο τοπικό δίκτυο
NIST	National Institute of Standards and Technology	Αμερικανικό ινστιτούτο προτύπων και τεχνολογίας
OPC	OLE (Object Linking and Embedding) for Process Control	Πρωτόκολλο διασύνδεσης βιομηχανικών διατάξεων και συστημάτων Windows
PFU	Physically Unclonable Function	Κυκλώματα παραγωγής απρόβλεπτων αριθμών βάσει ενδογενούς αταξίας.
PLC	Power Line Communication	Πρότυπο μεταφοράς δεδομένο μέσω γραμμών μεταφοράς ΗΕ
PLC	Programmable Logic Controller	Ελεγκτής που περιλαμβάνει ρουτίνες αυτομάτου ελέγχου βιομηχανικών διατάξεων
PMU	Phasor Measurement Unit	Βιομηχανική διάταξη μέτρηση φασιθετών του ηλεκτρικού ρεύματος σε πραγματικό χρόνο
PTP	Precision Time Protocol	Πρωτόκολλο χρονικού συγχρονισμού μέσω πληροφοριακών δικτύων
RAM	Random Access Memory	Πτητική μνήμη ενός υπολογιστικού συστήματος
RSA	Rivest Shamir Adleman	Αλγόριθμος κρυπτογράφησης δημοσίου κλειδιού
SCADA	Supervisory Control And Data Acquisition	Σύστημα αυτομάτου ελέγχου βιομηχανικών διατάξεων
SHA	Secure Hash Algorithm	Κρυπτογραφικός αλγόριθμος κατακερματισμού
SNMP	Simple Network Management Protocol	Βασικό πρωτόκολλο διαχείρισης δικτύων
SNR	Signal-to-Noise Ratio	Λόγος σήματος προς θόρυβο
SRAM	Static Random Access Memory	Κατηγορία μνήμης RAM που κατασκευάζεται με transistor
SSH	Secure Shell	Πρωτόκολλο απομακρυσμένου ελέγχου πληροφοριακών συστημάτων UNIX

SSL	Secure Socket Layer	Ξεπερασμένη μέθοδος κρυπτογράφησης
TCP	Transmition Control Protocol	Βασικό πρωτόκολλο στρώματος μεταφοράς στο Διαδίκτυο
TLS	Transport Layer Security	Απόγονος του SSL. Μέθοδος κρυπτογράφησης στο στρώμα μεταφοράς
UDP	User Datagram Protocol	Πρωτόκολλο στρώματος μεταφοράς
UNIX		Οικογένεια λειτουργικών συστημάτων
USB	Universal Serial Bus	Πρότυπο σύνδεσης περιφερειακών διατάξεων σε υπολογιστικά συστήματα
VPN	Virtual Private Network	Πρωτόκολλο ασφαλούς απομακρυσμένης σύνδεσης σε πληροφοριακό δίκτυο

Περίληψη

Σκοπός της παρούσας εργασίας είναι η μελέτη ζητημάτων ασφάλειας πληροφοριών που προκύπτουν κατά τη μετάβαση από τα παραδοσιακά δίκτυα ηλεκτρικής ενέργειας (ΗΕ) στα Ευφυή Δίκτυα. Το Ευφυές Δίκτυο βασίζεται σε πληροφοριακά συστήματα για την επεξεργασία δεδομένων παραγωγής και κατανάλωσης σε πραγματικό χρόνο. Για να υποστηριχτεί η λειτουργικότητα αυτή, το Ευφυές Δίκτυο βασίζεται σε πληροφοριακά συστήματα τα οποία πραγματοποιούν τη μετάδοση και επεξεργασία των δεδομένων. Η χρήση των συστημάτων αυτών έχει εισαγάγει ένα μεγάλο αριθμό νέων απειλών στα δίκτυα ΗΕ. Στην παρούσα εργασία γίνεται ανάλυση των απειλών αυτών και εξετάζονται τρόποι αντιμετώπισης πιθανών επιθέσεων. Για να γίνει περισσότερο συστηματική, η ανωτέρω ανάλυση διαχωρίστηκε στους τρεις μεγάλους τομείς του Ευφυούς Δικτύου.

Αρχικά, γίνεται ανάλυση των απειλών που προκύπτουν εναντίον των ευφυών μετρητών. Αναλύονται επιθέσεις εναντίον του λογισμικού και του υλικού ενός ευφυούς μετρητή και προτείνονται μέθοδοι για την αντιμετώπισή τους. Στη συνέχεια, η ίδια ανάλυση πραγματοποιείται ως προς ό,τι αφορά τα συστήματα εντός των εταιρικών πληροφοριακών δικτύων του διαχειριστή του δικτύου ΗΕ και των παρόχων ΗΕ. Τέλος, πραγματοποιείται ανάλυση των απειλών εναντίον των συστημάτων ελέγχου και των διατάξεων παραγωγής και μεταφοράς ΗΕ που βρίσκονται εντός του βιομηχανικού πληροφοριακού δικτύου του διαχειριστή του δικτύου ΗΕ, και προτείνονται αντίστοιχες μέθοδοι ασφάλειας.

Στο πρώτο κεφάλαιο γίνεται μια εισαγωγική αναφορά στο Ευφυές Δίκτυο, τις επιμέρους λειτουργίες του, τα τμήματα που το απαρτίζουν και τις τεχνολογίες επικοινωνιών που χρησιμοποιούνται στο βιομηχανικό τμήμα του δικτύου. Στο δεύτερο κεφάλαιο, παρουσιάζονται βασικές πληροφορίες για τα πληροφοριακά δίκτυα και την ασφάλεια πληροφοριών. Στο τρίτο κεφάλαιο, αναλύονται τα κίνητρα και οι μέθοδοι επίθεσης εναντίον των υποδομών του Ευφυούς Δικτύου στην πλευρά του καταναλωτή ΗΕ, όπως οι ευφυείς μετρητές. Ακολούθως, προτείνονται και αναλύονται μέθοδοι ασφάλειας για τις υποδομές αυτές. Στο τέταρτο κεφάλαιο, γίνεται αναφορά στα εταιρικά πληροφοριακά δίκτυα του διαχειριστή του δικτύου και των παρόχων ΗΕ. Επισημαίνονται τα κρίσιμα συστήματα για το Ευφυές Δίκτυο που βρίσκονται εντός των εταιρικών πληροφοριακών δικτύων, και αναλύεται ο ρόλος τους στο Ευφυές Δίκτυο. Στη συνέχεια, αναφέρονται κίνητρα κακόβουλων επιθέσεων και αναλύεται η μεθοδολογία που ακολουθείται από επίδοξους εισβολείς εναντίον των συστημάτων αυτών. Για κάθε βήμα της ανωτέρω μεθοδολογίας, αναλύονται τεχνικές άμυνας εναντίον των αντίστοιχων μεθόδων επίθεσης. Τέλος, στο πέμπτο κεφάλαιο, γίνεται αναφορά στα συστήματα που βρίσκονται στο βιομηχανικό τμήμα του Ευφυούς Δικτύου και στα πρωτόκολλα επικοινωνίας που χρησιμοποιούνται. Πραγματοποιείται ανάλυση των μεθόδων επίθεσης εναντίον διατάξεων του βιομηχανικού πληροφοριακού δικτύου και, στη συνέχεια, προτείνονται τεχνικές και μηχανισμοί που μπορούν να διασφαλίσουν τις διατάξεις αυτές έναντι κακόβουλων επιθέσεων.

Λέξεις Κλειδιά

Smart Grid, ασφάλεια πληροφοριών, ευφυείς μετρητές, πληροφοριακά δίκτυα, βιομηχανικά δίκτυα ΗΕ, SCADA.

Abstract

The purpose of this diploma thesis is the study of issues regarding information security that will arize during the transition from legacy electrical networks to the Smart Grid. The Smart Grid is based on computing systems for real-time processing of electricity generation, delivery and consumption. In order to support the this functionality, the Smart Grid relies on information systems for transmitting and processing the data. The use of information systems introduces a wide range of threats to electrical networks. Throughout the diploma thesis such threats are identified and analyzed in order to propose mitigation techniques. To support the systematic analysis of information security threats, the Smart Grid has been divided into three areas.

Initially, an analysis regarding threats agains smart meters is given. Attacks agains the firmware and the hardware of a smart meter are studied leading to the proposal of mitigation techniques. Subsequently, a similar analysis is performed on the information systems belonging to the corporate networks of major players in the electrical energy sector such as the electrical network administrator and electrical energy suppliers. Finally, a study and analysis of the threats against control systems and electricity generation systems that belong to the industial network is given, followed by mitigation techniques.

The first chapter provides an introduction to the Smart Grid, its functionality, the subsection comprising it as well as the information techologies used in the industrial network. In the second chapter, introductory information regarfing computer networks and information security is presented. The third chapter, contains an analysis of motives and attacks against the advanced metering infrastructure of the Smart Grid plus techniques for defending against the attacks presented. The fourth chapter refers to the corporate networks of the administrator of the electrical network and electricity suppliers. Critical infrastructure of the Smart Grid that reside in these networks are indentified. Motives and attacks against this infrastructure are studied followed by techniques for defending against the presented attacks. Finally, the fifth chapter, provides insight on the critical systems belonging to the industrial network and the communication protocols used. An analysis is performed concerning the motives and attacks against these systems, as well as the methods for defending against the attacks presented in the chapter.

Key words

Smart Grid, information security, smart meters, computer networks, industrial networks, SCADA.

Κεφάλαιο 1. Ευφυές Δίκτυο

1.1. Εισαγωγή

Το Ευφυές Δίκτυο (Smart Grid) αποτελεί την τεχνολογική εξέλιξη του παραδοσιακού δικτύου ηλεκτρικής ενέργειας (ΗΕ) που χρησιμοποιείται με μικρές αλλαγές εδώ και αρκετές δεκαετίες. Το Ευφυές Δίκτυο συνδυάζει την υποδομή του δικτύου ΗΕ με υποδομές επικοινωνιακών και πληροφοριακών συστημάτων, επιτρέποντας την είσοδο τεχνολογιών πληροφορικής στα δίκτυα ΗΕ. Τα νέα αυτά συστήματα προσδίδουν στο Ευφυές Δίκτυο τη δυνατότητα συλλογής και επεξεργασίας δεδομένων που αφορούν την λειτουργία του. Έτσι, το σύστημα της παραγωγής, μεταφοράς, διανομής και κατανάλωσης ΗΕ μπορεί να προσαρμόζει τη λειτουργία του με σκοπό τη βελτιστοποίηση ορισμένων από τις παραμέτρους λειτουργίας του. Ενδεικτικά, σε αυτές περιλαμβάνονται το κόστος πρώτων υλών, το είδος των πρώτων υλών και το ενεργειακό τους αποτύπωμα, η διακύμανση της ζήτησης ΗΕ, η μέγιστη τιμή της ζητούμενης ισχύος και το μέγεθος της παραγόμενης ΗΕ. Η αυτόματη λήψη αποφάσεων για τη λειτουργία του δικτύου ΗΕ από τα ίδια τα συστήματά του, αποτελεί το θεμέλιο πάνω στο οποίο βασίζονται πολλά από τα πλεονεκτήματα που προσφέρει.

1.2. Πλεονεκτήματα του Ευφυούς Δικτύου

Οι νέες δυνατότητες που παρέχει το Ευφυές Δίκτυο αποφέρουν πολλαπλά οφέλη σε όλους τους εμπλεκόμενους στην αγορά ΗΕ, από τους παραγωγούς ΗΕ μέχρι τους καταναλωτές. Τα σημαντικότερα από αυτά παρουσιάζονται στη συνέχεια.

1.2.1. Βελτίωση της αξιοπιστίας

Το Ευφυές Δίκτυο αποτελεί αιτία για πολλές εξελίξεις στο ζήτημα της αξιοπιστίας των υποδομών παραγωγής, μεταφοράς και διανομής ΗΕ. Σε συνδυασμό με την ανάπτυξη στους τομείς των ηλεκτρονικών αισθητήρων και των μικροελεγκτών παρέχεται πλέον η δυνατότητα παρακολούθησης σε πραγματικό χρόνο των παραμέτρων λειτουργίας συστημάτων όπως γεννήτριες και μετασχηματιστές. Τα δεδομένα υπόκεινται σε επεξεργασία για την ανακάλυψη ενδείξεων που καταδεικνύουν υπάρχουσες ή επικείμενες βλάβες. Έτσι πλέον, πολλές από τις βλάβες μπορούν να προλαμβάνονται ή ακόμη και να διορθώνονται αυτόματα με νέες ρυθμίσεις της συσκευής, με αποτέλεσμα ο χρόνος ζωής των συστημάτων αυξάνεται σημαντικά. Επίσης, αυξάνεται η αξιοπιστία των συστημάτων ΗΕ και το ποσοστό διαθεσιμότητας των υπηρεσιών που παρέχει το Ευφυές Δίκτυο.

1.2.2. Δυναμική Ανταπόκριση στη ζήτηση ΗΕ

Η ζήτηση ΗΕ συμπεριφέρεται ως τυχαία διαδικασία που επηρεάζεται από πληθώρα διαφορετικών παραγόντων, εμφανίζοντας συχνά αιχμές κατά τις ώρες υψηλής κατανάλωσης. Μέχρι σήμερα, η ανταπόκριση στη ζήτηση γινόταν με παραγωγή ισχύος σε ένα επίπεδο ασφαλείας υψηλότερο από το αναμενόμενο ύψος των αιχμών στη ζήτηση. Το Ευφυές Δίκτυο, όμως, διαθέτει υποδομές ώστε να μπορεί να προβλέπει τις αιχμές στη ζήτηση ΗΕ και να προσαρμόζει την παραγωγή ΗΕ. Επιπλέον, μέσω της υποδομής των αυτόματων μετρητών παρέχονται κίνητρα σε καταναλωτές ΗΕ ώστε να μεταθέσουν ενεργοβόρες διαδικασίες σε ώρες χαμηλότερης ζήτησης ΗΕ. Συνδυάζοντας τις δύο αυτές λειτουργίες, το Ευφυές Δίκτυο μπορεί από τη μια μεριά να εξομαλύνει τις αιχμές της ζήτησης ΗΕ, προσαρμόζοντας παράλληλα τη λειτουργία των υποδομών παραγωγής, και από την άλλη πλευρά να μειώσει το περιθώριο της περίσσειας ισχύος. Το αποτέλεσμα είναι η συνεχής λειτουργία του δικτύου ΗΕ με σημαντικά μικρότερη κατανάλωση καύσιμης πρώτης ύλης και η εξοικονόμηση πόρων από επενδύσεις σε νέους σταθμούς που πλέον δεν θα είναι αναγκαίες.

1.2.3. Χρήση Ανανεώσιμων Πηγών Ενέργειας

Με την είσοδο των κατανεμημένων και των ανανεώσιμων πηγών ενέργειας στις υποδομές παραγωγής ΗΕ, η τοπολογία των υποδομών παραγωγής γίνεται κατανεμημένη. Από το μοντέλο των λίγων μεγάλων σταθμών παραγωγής γίνεται μετάβαση στο υβριδικό μοντέλο με ενσωμάτωση πολλών μικρών σταθμών παραγωγής, συχνά με χρήση συστοιχιών ΑΠΕ. Επειδή, όμως, η παραγόμενη ισχύς των ΑΠΕ είναι μια τυχαία διαδικασία που εξαρτάται δραστικά από τις καιρικές συνθήκες, δεν μπορεί να γίνει στατική σχεδίαση της ροής ισχύος. Το Ευφυές Δίκτυο παρέχει την υποδομή ώστε να λαμβάνονται συνεχώς μετρήσεις της παραγόμενης ισχύος από τις συστοιχίες ΑΠΕ ώστε σε συσχέτιση με τις αντίστοιχες μετρήσεις για τη ζητούμενη ισχύ, να μεταβάλλεται δυναμικά η τοπολογία του δικτύου, με την εισαγωγή ή εξαγωγή κόμβων, και η ροή ισχύος. Από τη στιγμή όπου αυτή η λειτουργία μπορεί να υποστηρίζεται αυτόματα από το Ευφυές Δίκτυο, αναμένεται να διευκολυνθεί σημαντικά η είσοδος των ΑΠΕ στην παραγωγή ΗΕ.

1.3. Βιομηχανικές λειτουργίες του Ευφυούς Δικτύου

Το Ευφυές Δίκτυο αποτελεί αιτία για πολλές καινοτομίες στο δίκτυο ΗΕ οι οποίες βασίζονται σε καινοτομίες στη βιομηχανική υποδομή του.

Το Ευφυές Δίκτυο αποτελεί τον φορέα μέσω του οποίου εισάγονται πολλές καινοτομίες στο δίκτυο ΗΕ. Οι καινοτομίες αυτές βασίζονται σε μεγάλο βαθμό στις αυξημένες δυνατότητες που προσφέρει η βιομηχανική υποδομή του Ευφυούς Δικτύου, δηλαδή οι σταθμοί παραγωγής και διανομής ΗΕ. Οι σύνθετες και αυτοματοποιημένες ενέργειες που πραγματοποιεί το Ευφυές Δίκτυο είναι αποτέλεσμα της συνέργειας των νέων τεχνολογιών μετάδοσης πληροφοριών και των νέων δυνατοτήτων των βιομηχανικών συστημάτων που απαρτίζουν το Ευφυές Δίκτυο. Αυτές οι νέες τεχνολογίες και η υιοθέτησή τους είναι η βάση όπου στηρίζεται το Ευφυές Δίκτυο.

1.3.1. Μέτρηση παραμέτρων σε πραγματικό χρόνο

Η δυνατότητα του ηλεκτρικού δικτύου να μετρά σε πραγματικό χρόνο παραμέτρους σχετικές με την ηλεκτρική είναι θεμελιώδης για το Ευφυές Δίκτυο. Το ηλεκτρικό δίκτυο μπορεί να πραγματοποιεί μετρήσεις σε πραγματικό χρόνο της τάσης, της παραγόμενης και καταναλισκόμενης ισχύος, της συχνότητας και της φάσης του ηλεκτρικού ρεύματος, είτε συγκεντρωτικά, είτε μεμονωμένα ανά τμήματα ή διατάξεις. Για την ολοκληρωμένη λήψη και χρήση των μετρήσεων συνεργάζονται τρεις κατηγορίες συστημάτων. Αρχικά, εξελιγμένοι μετρητές σε κάθε κόμβο του ηλεκτρικού μετρούν συνεχώς κρίσιμα μεγέθη του ηλεκτρικού δικτύου. Στη συνέχεια, τα αντίστοιχα δεδομένα αποστέλλονται μέσω της υποδομής επικοινωνιών του Ευφυούς Δικτύου σε συστήματα επεξεργασίας. Στο τελικό στάδιο, το μεγάλο πλήθος μετρήσεων από όλους τους κόμβους του δικτύου συγκεντρώνεται σε συστήματα υψηλής επεξεργαστικής ισχύος ώστε να προκύψουν συγκεντρωτικά στοιχεία και σύνθετα μεγέθη που στη συνέχεια να χρησιμοποιούνται από προσαρμοστικούς αλγόριθμους με σκοπό τη βέλτιστη λειτουργία του Ευφυούς Δικτύου.

Η υψηλή συχνότητα με την οποία είναι δυνατό να πραγματοποιείται ο ανωτέρω κύκλος λήψης και επεξεργασίας των μετρήσεων παρέχει τη δυνατότητα παρακολούθησης της κατάστασης του δικτύου σε πραγματικό χρόνο, και την εξαγωγή αξιοποιήσιμων συμπερασμάτων ως προς τη δυναμική των μεταβολών αυτών. Τα δεδομένα αυτά, στη συνέχεια, χρησιμοποιούνται για την αξιολόγηση της επίδοσης των υποδομών του ηλεκτρικού δικτύου και τη διόρθωση, εφόσον κριθεί αναγκαίο, ορισμένων παραμέτρων.

1.3.2. Αυτόματη ανίχνευση και αντιμετώπιση προβλημάτων στο δίκτυο

Μία από τις σημαντικότερες καινοτομίες του Ευφυούς Δικτύου είναι η ικανότητά του διορθώνει αυτόματα ορισμένα προβλήματα που μπορεί να εμφανιστούν σε διατάξεις του ηλεκτρικού δικτύου. Αυτό είναι ένα μεγάλο βήμα προόδου σε σύγκριση με την τρέχουσα κατάσταση όπου πολλά προβλήματα γίνονται αντιληπτά όταν μια διάταξη έχει πληγεί ανεπανόρθωτα και χρήζει αντικατάστασης. Και στην περίπτωση αυτή, οι νέες δυνατότητες βασίζονται στα συστήματα επικοινωνίας και επεξεργασίας δεδομένων που διαθέτει το Ευφυές Δίκτυο.

Πλέον, όλες οι κρίσιμες υποδομές του ηλεκτρικού δικτύου υποστηρίζονται από μετρητές, συστήματα επικοινωνίας και μικροεπεξεργαστικές μονάδες. Οι μετρητές λαμβάνουν συνεχώς μετρήσεις των σημαντικότερων μεγεθών που σχετίζονται με τη λειτουργία κάθε διάταξης και τις αποστέλλουν στο κέντρο επεξεργασίας το οποίο τις επεξεργάζεται. Στο κέντρο επεξεργασίας υπάρχουν συστήματα μηχανικής μάθησης τα οποία με αυτόματο τρόπο ανιχνεύουν προβλήματα με βάση τα δεδομένα των συσκευών.

Αντίστοιχα με το πρόβλημα που ανιχνεύεται, υπάρχει η προβλεπόμενη αντιμετώπιση. Όταν από το σύστημα μηχανικής μάθησης το πρόβλημα λειτουργίας κριθεί σοβαρό ειδοποιείται το αντίστοιχο τμήμα του συστήματος ΗΕ ώστε να επιληφθεί του προβλήματος. Στην περίπτωση, ωστόσο, όπου το πρόβλημα εντοπίζεται σε αρχικό στάδιο και είναι αντιμετωπίσιμο, το κέντρο επεξεργασίας αποστέλλει εντολές στη διάταξη για αυτόματη επιδιόρθωση. Έτσι, τα συστήματα λειτουργούν εντός των προδιαγραφών λειτουργίας τους και δίχως προβλήματα, χαρακτηριστικό που βελτιώνει τη λειτουργική επίδοσή τους και αυξάνει σημαντικά το χρόνο ζωής τους.

1.3.3. Αυτόματος έλεγχος πηγών ισχύος

Όπως αναφέρθηκε και προηγουμένως, με την διείσδυση των ΑΠΕ στην παραγωγή ΗΕ παρατηρείται τα τελευταία χρόνια μια στροφή προς την κατανεμημένη παραγωγή ΗΕ. Αυτό, σε συνδυασμό με το μεταβλητό μέγεθος της ΗΕ που παράγεται από τις ΑΠΕ, έχει δημιουργήσει την ανάγκη αυτόματης διαχείρισης των πηγών ισχύος που είναι διαθέσιμες σε κάθε περιοχή. Η διαχείριση αυτή επιτυγχάνεται μέσω των βιομηχανικών υποδομών αυτομάτου ελέγχου που διαθέτει το Ευφυές Δίκτυο.

Τα συστήματα επικοινωνίας του Ευφυούς Δικτύου μεταφέρουν δεδομένα ζήτησης ΗΕ για κάθε περιοχή σε τοπικό κέντρο ελέγχου που είναι υπεύθυνο για τον έλεγχο των μονάδων παραγωγής. Ταυτόχρονα, τα συστήματα αυτά μεταφέρουν και δεδομένα διαθέσιμης ισχύος από τις μονάδες παραγωγής. Στο κέντρο ελέγχου συνδυάζονται τα ανωτέρω δεδομένα και ύστερα από κατάλληλη επεξεργασία προκύπτει το βέλτιστο μέγεθος παραγόμενης ΗΕ για κάθε μονάδα. Στη συνέχεια, ανάλογα με τη ζήτηση, μέσω του βιομηχανικού πληροφοριακού δικτύου και των υποδομών αυτομάτου ελέγχου, διαβιβάζονται στις μονάδες παραγωγής ΗΕ εντολές για είσοδό τους στο δίκτυο ΗΕ ή για έξοδό τους από αυτό.

Η συχνότητα με την οποία λειτουργεί ο ανωτέρω βρόχος αυτομάτου ελέγχου είναι τέτοια ώστε να υπερβαίνει κατά πολύ τη συχνότητα με την οποία μεταβάλλεται η παραγόμενη ισχύς των συστοιχιών ΑΠΕ. Αυτό είναι απαραίτητο ώστε να το σύστημα ελέγχου προλαμβάνει τις μεταβολές στην ισχύ που υπεισέρχονται από την μεταβλητότητα της παραγόμενης ΗΕ από συστοιχίες ΑΠΕ.

1.4. Συστήματα και υποδομές του Ευφυούς Δικτύου

Το Ευφυές Δίκτυο απαρτίζεται από ένα σύνολο συστατικών τμημάτων που αποτελούν την υλικοτεχνική υποδομή του. Κάθε τέτοιο τμήμα είναι επιφορτισμένο με συγκεκριμένες επιμέρους λειτουργίες που υποστηρίζουν άλλες, περισσότερο σύνθετες λειτουργίες του Ευφυούς Δικτύου. Στο σημείο αυτό, θα αναφερθούν τα σημαντικότερα τμήματα της υποδομής του Ευφυούς Δικτύου και οι βασικές λειτουργίες τις οποίες επιτελούν.

1.4.1. Ευφυείς μετρητές

Οι ευφυείς μετρητές είναι νέας γενιάς μετρητές που μετρούν την καταναλισκόμενη ΗΕ και βασικά μεγέθη του ΗΕ. Με την είσοδο των ΑΠΕ στην αγορά ΗΕ πολλοί ιδιώτες, και ανάλογα με τις εκάστοτε καιρικές συνθήκες, είτε πωλούν είτε καταναλώνουν ΗΕ. Ανάλογα με την περίπτωση, ο ευφυής μετρητής έχει τη δυνατότητα να μετρήσει είτε την παραγόμενη είτε την καταναλισκόμενη ΗΕ μιας εγκατάστασης. Σε αντίθεση με τους σημερινούς μετρητές οι έξυπνοι μετρητές διαθέτουν πρόσθετες δυνατότητες μέτρησης και επικοινωνίας. Οι καινοτομίες που διαθέτουν οι ευφυείς μετρητές στους δύο ανωτέρω τομείς επιτρέπουν την πραγματοποίηση περισσότερο σύνθετων και προηγμένων λειτουργιών. Οι σημαντικότερες από τις καινοτομίες των ευφυών μετρητών περιγράφονται στη συνέχεια.

I.1.i. Δυνατότητες μέτρησης

Η μεγάλη καινοτομία των ευφυών μετρητών στον τομέα των μετρήσεων είναι η δυνατότητά τους να μετρούν σε πραγματικό χρόνο την παραγόμενη ή καταναλισκόμενη ΗΕ. Συγχρόνως, αναγνωρίζουν το ποσοστό κατά το οποίο συμβάλει κάθε ηλεκτρική συσκευή στη διαμόρφωση της συνολικής κατανάλωσης ΗΕ. Το ότι η μέτρηση ΗΕ γίνεται σε συνεχώς επιτρέπει στους προμηθευτές ΗΕ να υιοθετούν περισσότερο ευέλικτες πολιτικές τιμολόγησης, διαφοροποιώντας τις χρεώσεις ανάλογα με την ώρα της κατανάλωσης, τη χρονική διάρκειά της και το μέγεθός της.

I.1.ii. Δυνατότητες επικοινωνίας

Άλλη καινοτομία των ευφυών μετρητών είναι η δυνατότητά τους να επικοινωνούν με κεντρικούς σταθμούς τιμολόγησης των παρόχων ΗΕ, όπου μεταδίδουν σε πραγματικό χρόνο τα δεδομένα κατανάλωσης και παραγωγής ΗΕ. Συγχρόνως, όμως, δέχονται πληροφορίες που αποσκοπούν στην υλοποίηση της δυναμικής πολιτικής των παρόχων ΗΕ για αναπρογραμματισμό των ενεργοβόρων εργασιών με αντάλλαγμα μειωμένες τιμές. Επιπλέον, οι ευφυείς μετρητές ενημερώνουν αυτόματα τα τεχνικά τμήματα του διαχειριστή του δικτύου ΗΕ στις περιπτώσεις όπου εμφανίζονται προβλήματα ή έκτακτες καταστάσεις. Μέσω του ίδιου διαύλου επικοινωνίας επιτρέπεται η απομακρυσμένη σύνδεση στο μετρητή προς υλοποίηση απομακρυσμένων ρυθμίσεων στη λειτουργία του. Με αυτό τον τρόπο επιλύονται προβλήματα από απόσταση και εξοικονομούνται πόροι αφού αποφεύγεται η φυσική παρουσία του τεχνικού προσωπικού.

I.1.iii. Πλατφόρμες επικοινωνίας

Τα πρωτόκολλα που χρησιμοποιούνται από τους μετρητές για τη σύνδεσή τους στο δίκτυο του διαχειριστή του δικτύου ΗΕ ή και των προμηθευτών ΗΕ ποικίλλουν αντίστοιχα με τη διαθέσιμη τηλεπικοινωνιακή υποδομή στην περιοχή του μετρητή. τα σημαντικότερα πρωτόκολλα επικοινωνίας είναι τα εξής:

1.1. Διαδίκτυο

Καίτοι δεν αποτελεί πρωτόκολλο αλλά περιλαμβάνει ένα σύνολο πρωτοκόλλων, το Διαδίκτυο μπορεί να χρησιμοποιηθεί για να μεταδίδονται τα δεδομένα από και προς το κέντρο τιμολόγησης. Δεδομένης της σύνδεσης στο Διαδίκτυο, τα κύρια πλεονεκτήματά του είναι: (i) ότι δεν απαιτείται νέος τηλεπικοινωνιακός εξοπλισμός για τους καταναλωτές και τους προμηθευτές ΗΕ και (ii) η μεγάλη αξιοπιστία του. Το μειονέκτημα είναι ότι το Διαδίκτυο περιλαμβάνει τεράστιο πλήθος ανεξάρτητων υποδικτύων, οπότε οι πληροφορίες διέρχονται από δίκτυα στα οποία είναι δυνατό να γίνει υποκλοπή τους. Συνεπώς, για να χρησιμοποιηθεί το Διαδίκτυο πρέπει να υπάρξει εξασφάλιση της ασφάλειας των πληροφοριών και των συστημάτων που επικοινωνούν.

1.2. Δίκτυα GSM/3G

Η τηλεπικοινωνιακή διασύνδεση των ευφυών μετρητών με τους ενδιάμεσους κόμβους και το κέντρο επεξεργασίας δεδομένων μπορεί να γίνει και μέσω των δικτύων κινητής τηλεφωνίας. Συγκριτικό πλεονέκτημα του ανωτέρω τρόπου μετάδοσης πληροφοριών είναι ότι τα τηλεπικοινωνιακά δίκτυα είναι ήδη εγκατεστημένα και παρουσιάζουν πολλή υψηλή γεωγραφική κάλυψη. Στον αντίποδα, ωστόσο, πρέπει να ληφθούν υπόψη και παράγοντες που υποβαθμίζουν την ποιότητα του δικτύου, όπως είναι η πιθανότητα απόρριψης κλήσης που εμφανίζεται συχνά σε πυκνοκατοικημένες περιοχές, ιδιαίτερα στις ώρες αιχμής. Ακόμη, τέλος, ο συγκεκριμένος τρόπος μετάδοσης πληροφοριών είναι αρκετά δαπανηρός ενεργειακά συγκριτικά με άλλους τρόπους που ακολουθούν.

1.3. Τηλεπικοινωνίες μέσω των γραμμών μεταφοράς ΗΕ (PLC)

Η τεχνολογία Power Line Communications (PLC) προσφέρει ένα σύγχρονα πρωτόκολλα φυσικού στρώματος και χρησιμοποιεί τις γραμμές μεταφοράς ΗΕ αξιοποιώντας το φάσμα συχνοτήτων από 1-100MHz. Τα βασικά του πλεονεκτήματα : (i) ότι δεν απαιτείται πρόσφατη τηλεπικοινωνιακή υποδομή και (i) ότι, καθώς χρησιμοποιεί το δίκτυο ΗΕ, προσφέρει καθολική παρουσία και ανεξαρτησία από τρίτα μέρη.

1.4. Ασύρματες επικοινωνίες μικρής εμβέλειας

Βασίζονται στο πρωτόκολλο φυσικό στρώματος IEEE 802.15 με κύριο εκπρόσωπο το πρωτόκολλο ZigBee (802.15.4). και μπορούν να υλοποιούν δίκτυα μετρητών κυρίως σε αστικές περιοχές τοπολογίας πλέγματος, όπου οι επικοινωνίες είναι ασύρματες και χαρακτηρίζονται από μικρές ενεργειακές απαιτήσεις. Στα πλεονεκτήματά τους συγκαταλέγεται η ικανότητα αυτοοργάνωσης και δυναμικής δρομολόγησης που διαθέτουν η οποία προσφέρει υψηλή κλιμακωσιμότητα με μικρή πολυπλοκότητα. Το μειονέκτημα τους είναι η μικρή εμβέλειά τους. Ως εκ τούτου, μπορούν να χρησιμοποιηθούν μόνο σε αστικές περιοχές όπου η πυκνότητα των μετρητών είναι μεγάλη.

1.4.2. Διακομιστές Web και mobile εφαρμογών

Οι ευφυείς μετρητές λαμβάνουν συνεχώς μετρήσεις της κατανάλωσης κάθε ηλεκτρικής συσκευής που τροφοδοτείται από την εγκατάσταση. Ο ρόλος των διακομιστών Web και mobile εφαρμογών είναι να διευκολύνουν την πρόσβαση στα δεδομένα κατανάλωσης ΗΕ από ηλεκτρονικές συσκευές των καταναλωτών, όπως κινητά τηλέφωνα και Η/Υ, ανεξαρτήτως πλατφόρμας. Με αυτό τον τρόπο, διαρκώς ανανεωμένα δεδομένα κατανάλωσης είναι άμεσα προσβάσιμα από των καταναλωτών.

Ουσιαστικά, οι διακομιστές αυτοί υλοποιούν τη σύνδεση των καταναλωτών με την κεντρική βάση δεδομένων και τα στοιχεία κατανάλωσής τους. Οι εφαρμογές, είτε είναι web είτε mobile, επικοινωνούν με τους διακομιστές και λαμβάνουν τα στοιχεία κατανάλωσης και τις ενδεχόμενες προτάσεις για τη μείωση του κόστους ΗΕ. Έτσι, οι καταναλωτές έχουν ενοποιημένη και εύκολη πρόσβαση στα δεδομένα του λογαριασμού τους.

1.4.3. Κέντρο τιμολόγησης

Το κέντρο τιμολόγησης αποτελεί το τμήμα του Ευφυούς Δικτύου όπου συγκεντρώνονται τα στοιχεία κατανάλωσης και παραγωγής ΗΕ από τους ιδιώτες πελάτες του προμηθευτή ΗΕ. Εκεί πραγματοποιείται η επεξεργασία των μετρήσεων ώστε να γίνεται η τιμολόγηση της ΗΕ που καταναλώνεται ή παράγεται. Επιπλέον, τα επεξεργαστικά συστήματα του κέντρου τιμολόγησης αναλύουν το προφίλ της κατανάλωσης κάθε καταναλωτή ώστε να προτείνουν τρόπους μείωσης του κόστους ΗΕ. Μια τέτοια υποδομή είναι αναγκαία ώστε να υπάρχει ένα κεντρικό σημείο ρύθμισης των παραμέτρων χρέωσης και ρύθμισης της κατανάλωσης. Οι αλλαγές των παραμέτρων αυτών πραγματοποιούνται από ένα μοναδικό σημείο, από όπου ενημερώνονται όλοι οι ευφυείς μετρητές ώστε να γίνεται η τιμολόγηση και ο έλεγχος της κατανάλωσης.

Αξίζει εδώ να σημειωθεί ότι παραμένει ανοιχτό ερώτημα το πόσο συγκεντρωτική ή κατανεμημένη θα είναι η αρχιτεκτονική των συστημάτων τιμολόγησης. Για παράδειγμα, θα να είναι ένα το κέντρο τιμολόγησης σε όλη την επικράτεια ή θα υπάρχουν πολλά οργανωμένη σε τοπολογία δέντρου ή αστέρα ώστε κάθε επιμέρους σύστημα να είναι υπεύθυνο για συγκεκριμένο αριθμό ευφυών μετρητών; Κάθε υλοποίηση έχει αντίστοιχα πλεονεκτήματα και μειονεκτήματα, ωστόσο η ανάλυση της ασφάλειας του συστήματος τιμολόγησης και των ευφυών μετρητών δεν επηρεάζεται σημαντικά από την εκάστοτε αρχιτεκτονική του συστήματος τιμολόγησης.

1.4.4. Βάση δεδομένων πελατών

Οι κεντρικές βάσεις δεδομένων των πελατών του διαχειριστή του συστήματος ΗΕ (ΔΕΔΔΗΕ για την Ελλάδα) αλλά και των προμηθευτών ΗΕ αποτελούν κρίσιμες υποδομές για το Ευφυές Δίκτυο διότι λειτουργούν ως κεντρικά σημεία φύλαξης όλων των πληροφοριών που αφορούν τους καταναλωτές ΗΕ. Σε αυτές τις βάσεις δεδομένων αποθηκεύονται πληροφορίες όπως το ιστορικό κατανάλωσης κάθε πελάτη και το ύψος των οφειλών του. Ακόμη, διατηρούνται πληροφορίες που αφορούν το προφίλ κάθε πελάτη, όπως, για παράδειγμα, πόσες φορές έχει υιοθετήσει προτάσεις του διαχειριστή σχετικά με την κατανάλωση ΗΕ ή το ύψος των εκπτώσεων που εφαρμόζονται στο λογαριασμό του.

Στις πληροφορίες αυτές βασίζονται πολλά συστήματα επεξεργασίας και ελέγχου του Ευφυούς Δικτύου. Αρχικά, οι διακομιστές web και mobile εφαρμογών συνδέονται με τις βάσεις δεδομένων ώστε να παρουσιάσουν τα δεδομένα του λογαριασμού σε κάθε καταναλωτή. Τα συστήματα ελέγχου του Ευφυούς Δικτύου υλοποιούν σύνθετες λειτουργίες βασιζόμενα στο δεδομένα καταναλωτών. Για παράδειγμα, τα συστήματα πρόβλεψης της ζήτησης ΗΕ εκτελούν μεθόδους εξόρυξης δεδομένων στα δεδομένα καταναλωτών ώστε να επιτύχουν την όσο το δυνατό καλύτερη πρόβλεψη της ζήτησης ΗΕ για το επόμενο χρονικό διάστημα. Τα συστήματα που προτείνουν την μετάθεση ενεργοβόρων διαδικασιών σε ώρες μικρότερης ζήτησης ελέγχουν τα δεδομένα υιοθέτησης των προτάσεων από τους καταναλωτές ώστε να εκτιμήσουν καλύτερα το μέγεθος της μείωσης της ζήτησης και να ενημερώσουν με ακρίβεια τα συστήματα ελέγχου παραγωγής ΗΕ. Είναι φανερό, επομένως, ότι οι κεντρικές βάσεις δεδομένων είναι θεμελιώδης υποδομή για το Ευφυές Δίκτυο.

1.4.5. Συστήματα SCADA (Supervisory Control And Data Acquisition)

Τα συστήματα SCADA αποτελούν κρίσιμη υποδομή για το βιομηχανικό τμήμα του Ευφυούς Δικτύου καθώς είναι επιφορτισμένα με τον αυτόματο έλεγχο των διατάξεων του βιομηχανικού πληροφοριακού δικτύου. Όλα τα συστήματα που συμμετέχουν στην παραγωγή, μεταφορά και διανομή ΗΕ συνδέονται με συστήματα SCADA που είναι υπεύθυνα για τον έλεγχο, την παρακολούθηση και τη ρύθμιση της λειτουργίας τους. Τα συστήματα SCADA περιλαμβάνουν επιμέρους συστήματα τα σημαντικότερα των οποίων είναι:

1.1. Εποπτικός σταθμός

Είναι το κεντρικό σύστημα κάθε ομάδας συστημάτων του βιομηχανικού πληροφοριακού δικτύου με το οποίο είναι επιφορτισμένο με τον έλεγχο των διατάξεων PLC (Programmable Logic Controller) που υπάγονται σε αυτό.. Στον εποπτικό σταθμό μεταδίδονται τα δεδομένα για την κατάσταση λειτουργίας όλων των βιομηχανικών διατάξεων του Ευφυούς Δικτύου. Αντίστοιχα, από τον εποπτικό σταθμό αποστέλλονται εντολές ελέγχου προς αυτές τις διατάξεις, όπως, για παράδειγμα εντολές αλλαγής των ρυθμίσεων λειτουργίας μιας διάταξης.

1.2. Κατανεμημένα συστήματα ελέγχου

Κατανεμημένα συστήματα ελέγχου υφίστανται σε αρχιτεκτονικές όπου χρησιμοποιούνται περισσότεροι του ενός ελεγκτές. Συγκεκριμένα, ένας εποπτικός σταθμός είναι υπεύθυνος για ένα σύνολο ελεγκτών καθένας από τους οποίους είναι με τη σειρά του υπεύθυνος για ένα σύνολο διατάξεων PLC. Έτσι, μπορούν να δημιουργηθούν δενδρικές τοπολογίες στο βιομηχανικό πληροφοριακό δίκτυο.

Κάθε ελεγκτής στα κατανεμημένα συστήματα ελέγχου είναι επιφορτισμένος με τον έλεγχο μίας ή περισσότερων βιομηχανικών διατάξεων PLC χωρίς την ανάγκη άμεσης επικοινωνίας με τον εποπτικό σταθμό. Ακόμη, τα κατανεμημένα συστήματα ελέγχου είναι υπεύθυνα για τη συλλογή δεδομένων από αισθητήρες, μετασχηματιστές και γεννήτριες και την αποστολή τους στον εποπτικό σταθμό.

1.3. Συστήματα αλληλεπίδρασης ανθρώπου-μηχανής (Human machine interaction - HMI)

Τα συστήματα HMI είναι υπεύθυνα για τη συγκεντρωτική παρουσίαση των δεδομένων λειτουργίας των βιομηχανικών συσκευών υπό κατανοητή για τον άνθρωπο μορφή. Είναι συνήθως Η/Υ που διαθέτουν εμπορικά λειτουργικά συστήματα στα οποία εγκαθίσταται το πρόγραμμα που αναλαμβάνει χρέη HMI για ένα ή περισσότερα συστήματα SCADA. Τα συστήματα HMI είναι υπεύθυνα για την παρουσίαση στο υπεύθυνο ανθρώπινο δυναμικό των δεδομένων λειτουργίας των βιομηχανικών υποδομών που ελέγχονται από το σύστημα SCADA. Επιπλέον, σε αυτά τα συστήματα εισάγονται, από το χρήστη, εντολές ελέγχου και αλλαγές στις ρυθμίσεις λειτουργίας των βιομηχανικών διατάξεων.

1.4.6. Συστήματα παρακολούθησης και διατήρησης ιστορικού

Τα συστήματα αυτής της κατηγορίας είναι επιφορτισμένα αρχικά με την παρακολούθηση και καταγραφή της κίνησης (traffic) του δικτύου επικοινωνίας και των ενεργειών που πραγματοποιούν τα συστήματα του Ευφυούς Δικτύου. Σε περίπτωση κάποιου σφάλματος ή απειλής για κάποιο σύστημα του Ευφυούς Δικτύου τα τεχνικά κλιμάκια του διαχειριστή του δικτύου μπορούν να ανατρέξουν στο λεπτομερές ιστορικό των όσων συνέβησαν ώστε να γίνει αντιληπτό τι ακριβώς συνέβη και να διορθωθεί. Αν και δεν είναι απαραίτητο σύστημα για τις λειτουργίες του Ευφυούς Δικτύου, είναι πολύ σημαντικό για ζητήματα ασφάλειας και αποκατάστασης της λειτουργίας του συστήματος ΗΕ μετά από σφάλματα ή διακοπές.

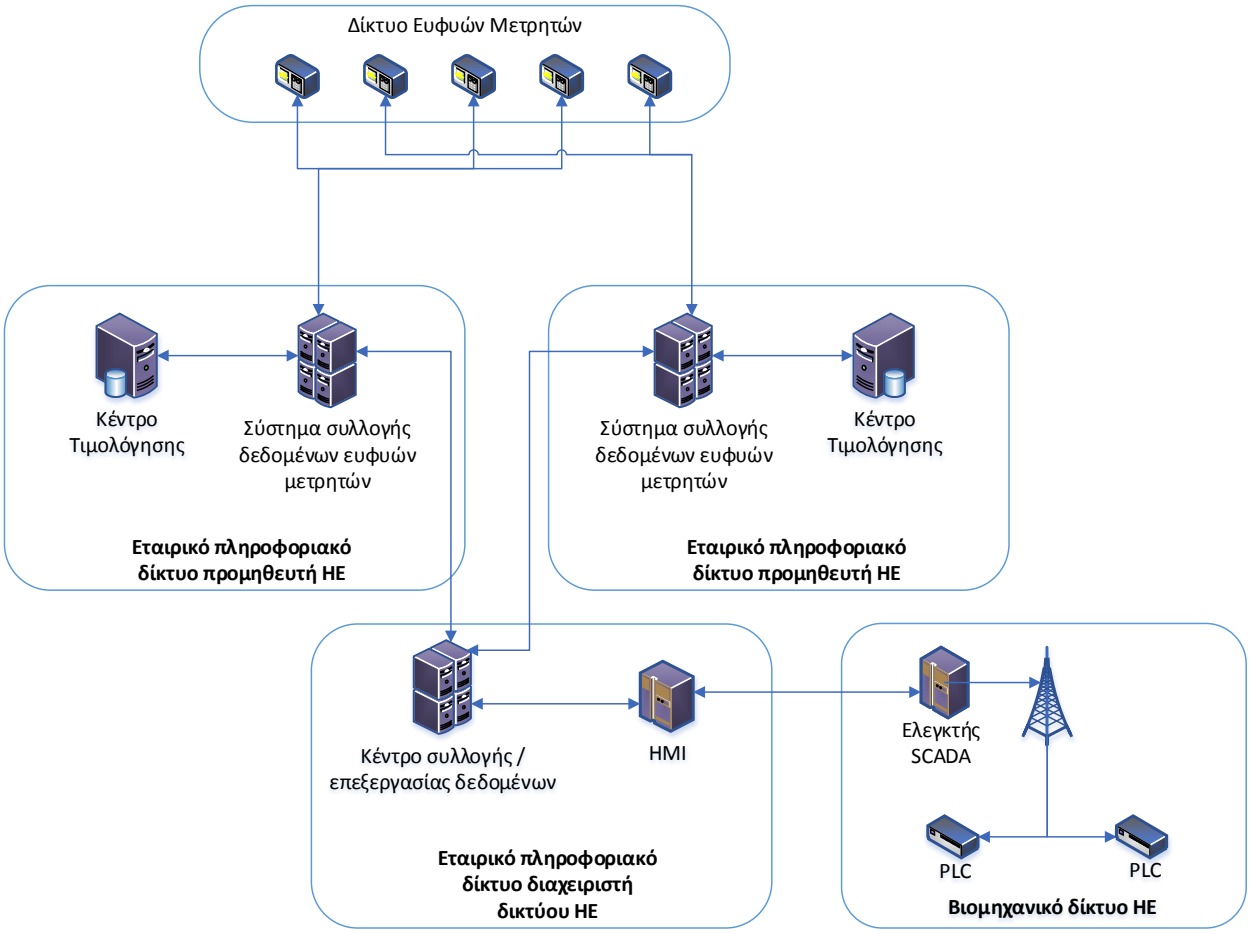
1.4.7. Συστήματα μέτρησης phasors (PMU)

Τα συστήματα αυτά έχουν κεντρικό ρόλο στις καινοτομίες του Ευφυούς Δικτύου ως προς τον έλεγχο της κατάστασης των δικτύων μεταφοράς και διανομής ΗΕ. Τα συστήματα PMU μετρούν σε πραγματικό χρόνο τις τιμές σημαντικών μεγεθών που έχουν σχέση με την ποιότητα ηλεκτρικής ισχύος. Μια τυπική συχνότητα μέτρησης είναι 2400 Hz, που μεταφράζεται σε 48 μετρήσεις ανά κύκλο εναλλασσόμενου ρεύματος συχνότητας 50Hz. Τα δεδομένα των μετρήσεων που λαμβάνονται είναι χρήσιμα για την παρακολούθηση της κατάστασης και τον έλεγχο των υποδομών του ηλεκτρικού δικτύου.

Για τη σωστή λειτουργία των συστημάτων μέτρησης PMU είναι απαραίτητος ο ακριβής χρονικός συγχρονισμός τους ώστε οι μετρήσεις που προέρχονται από διαφορετικά PMUs μέσω του τηλεπικοινωνιακού δικτύου να αναγράφουν την ακριβή χρονική στιγμή της μέτρησης και να μπορούν να ταξινομηθούν σωστά οι μετρήσεις στο κέντρο ελέγχου. Ο ακριβής χρονικός συγχρονισμός των λαμβανόμενων μετρήσεων γίνεται με χρήση δεκτών GPS με σφάλμα της τάξης του 1μs.

1.5. Μοντέλο Smart Grid

Καθ' όλη την έκταση της διπλωματικής εργασίας ακολουθείται ένα μοντέλο της αρχιτεκτονικής του Smart Grid, το οποίο απεικονίζεται στο Σχήμα. Το μοντέλο του Smart Grid χωρίζεται σε τρεις τομείς σε ότι αφορά την ανάλυση της ασφάλειάς του. Πρώτος τομέας είναι το δίκτυο ευφυών μετρητών. Αφορά όλους τους ευφυείς μετρητές που είναι εγκατεστημένοι σε καταναλωτές και ιδιώτες παραγωγούς ΗΕ. Δεύτερος τομέας είναι τα εταιρικά πληροφοριακά δίκτυα των προμηθευτών ΗΕ και του διαχειριστή του δικτύου ΗΕ. Τα εταιρικά πληροφοριακά δίκτυα είναι τα δίκτυα υπολογιστών μέσω των οποίων διασυνδέονται τα πληροφοριακά συστήματα που είναι θεμελιώδη για τη λειτουργία του Smart Grid. Τρίτος τομέας είναι το βιομηχανικό δίκτυο ΗΕ. Εκεί περιλαμβάνονται όλες οι διατάξεις που είναι υπεύθυνες για την παραγωγή μεταφορά και διανομή ΗΕ. Περιλαμβάνει και όλα τα συστήματα που είναι επιφορτισμένα με τον αυτόματο έλεγχο των διατάξεων αυτών. Ακόμη, στο σχήμα φαίνονται και οι διασυνδέσεις μεταξύ των συστημάτων, μέσω των οποίων οι απαραίτητες πληροφορίες διοχετεύονται στα διάφορα τμήματα του Smart Grid.



Σχήμα 1.1. Σχηματική απεικόνιση του μοντέλου του Smart Grid.

Κεφάλαιο 2. Πληροφοριακά Δίκτυα και Ασφάλεια Πληροφοριών

2.1. Εισαγωγή

Το Ευφυές Δίκτυο αποτελεί ένα δίκτυο πληροφοριακών συστημάτων που διασυνδέει τα διάφορα τμήματα της υποδομής του Ευφυούς Δικτύου. Οι πληροφορίες που ανταλλάσσονται μεταξύ αυτών των τμημάτων υποδομής είναι μεγάλης σημασίας για την αξιόπιστη λειτουργία του Ευφυούς Δικτύου. Είναι πολύ σημαντικό, επομένως, να εξασφαλιστεί η αξιόπιστη μετάδοση αυτών των πληροφοριών.

Η σωστή σχεδίαση και υλοποίηση μηχανισμών για την ασφάλεια των πληροφοριών απαιτούν ενδελεχή μελέτη των χαρακτηριστικών των συστημάτων που επικοινωνούν και των πληροφοριών που ανταλλάσσουν. Αυτές είναι:

1. Το είδος των συστημάτων που επικοινωνούν και οι δικτυακές απαιτήσεις τους. Για παράδειγμα, αν ένα σύστημα υλοποιεί μια λειτουργία πραγματικού χρόνου, οι απαιτήσεις του από το δίκτυο ανταλλαγής πληροφοριών είναι για ελάχιστη καθυστέρηση και ελάχιστη διακύμανση της καθυστέρησης, χαρακτηριστικά που είναι θεμελιώδη για τη σχεδίαση και υλοποίηση των μηχανισμών ασφάλειας.
2. Την αρχιτεκτονική του δικτύου μέσω του οποίου θα γίνει η επικοινωνία μεταξύ των συστημάτων.
3. Τις απαιτήσεις ασφάλειας για κάθε είδος διακινούμενης πληροφορίας ως προς εμπιστευτικότητα και την ακεραιότητα.
4. Τα πρωτόκολλα δικτύου που θα χρησιμοποιηθούν κατά την ανταλλαγή πληροφοριών.

Τα ανωτέρω χαρακτηριστικά διαμορφώνουν μια δενδρική δομή ταξινόμησης των πληροφοριακών συστημάτων. Βάσει της δομής αυτής, πραγματοποιείται στη συνέχεια η ανάλυση των προαναφερθέντων χαρακτηριστικών.

2.2. Ομάδες συστημάτων στο Ευφυές Δίκτυο

Το Smart Grid (SG) απαρτίζεται από πληθώρα συστημάτων που επιτελούν τις διάφορες λειτουργίες που είναι αναγκαίες για την παροχή των SG υπηρεσιών. Τα SG συστήματα οργανώνονται σε ομάδες, καθεμία από τις οποίες συγκροτεί ένα τοπικό δίκτυο μέσω του οποίου επικοινωνούν οι διατάξεις που ανήκουν στην ομάδα. εφόσον κριθεί αναγκαίο από τη σχεδίαση του συνολικού δικτύου τα τοπικά δίκτυα ομάδων που πρέπει να επικοινωνούν μεταξύ τους συνδέονται διαμορφώνοντας μεγαλύτερα δίκτυα. Οι λειτουργίες που επιτελούνται από τα συστήματα είναι συχνά πολύ διαφορετικές μεταξύ τους, χαρακτηριστικό που οδηγεί σε πολύ διαφοροποιημένες προδιαγραφές για τις δικτυακές εγκαταστάσεις και έχει ως άμεση συνέπεια να διαφέρουν

τα δίκτυα μιας ομάδας από τα δίκτυα μιας άλλης. Αυτό οδηγεί σε διατύπωση διαφορετικών πρωτοκόλλων και σε υιοθέτηση διαφορετικών μεθόδων ασφάλειας των πληροφοριών στο SG.

2.2.1. Εταιρικά πληροφοριακά δίκτυα

Ως πληροφοριακό δίκτυο μιας εταιρίας ορίζεται το δίκτυο υπολογιστών που διασυνδέει όλα τα επιμέρους συστήματα που παράγουν δεδομένα, τόσο μεταξύ τους όσο και με διάφορες οντότητες της εταιρίας. Περιλαμβάνει βάσεις δεδομένων, συστήματα αρχειοθέτησης, web servers, και τους Η/Υ εργασίας των υπαλλήλων και διευθυντικών στελεχών. Στο εταιρικό πληροφοριακό δίκτυο οι επικοινωνίες βασίζονται στη συλλογή πρωτοκόλλων του Διαδικτύου (TCP/IP), που υποστηρίζεται από την πλειοψηφία των διαφορετικών συστημάτων που πρέπει να επικοινωνούν μέσω του πληροφοριακού δικτύου.

2.2.2. Βιομηχανικό πληροφοριακό δίκτυο

Το βιομηχανικό πληροφοριακό δίκτυο περιλαμβάνει όλα τα συστήματα και τις διατάξεις που υλοποιούν τις λειτουργίες και τον αυτόματο έλεγχο των κρίσιμων υποδομών στα δίκτυα παραγωγής, μεταφοράς και διανομής ΗΕ. Μέσω του βιομηχανικού πληροφοριακού δικτύου πραγματοποιούνται όλες οι απαραίτητες επικοινωνίες μεταξύ των ανωτέρω διατάξεων ώστε να υποστηριχθούν οι νέες τεχνολογίες του Ευφυούς Δικτύου. Τα πρωτόκολλα βιομηχανικών πληροφοριακών δικτύων είναι ειδικά σχεδιασμένα για να παρέχουν μετάδοση πληροφοριών με ανεκτή καθυστέρηση στη μεταφορά δεδομένων για υπηρεσίες πραγματικού χρόνου. Λόγω της ανωτέρω ικανότητάς τους, τα βιομηχανικά πρωτόκολλα επικοινωνιών προτιμώνται έναντι των πληροφοριακών στο δίκτυο βιομηχανικών διατάξεων του Ευφυούς Δικτύου.

2.3. Συλλογή πρωτοκόλλων του Διαδικτύου – TCP/IP

Η συλλογή πρωτοκόλλων του Διαδικτύου περιλαμβάνει όλα τα πρωτόκολλα επικοινωνίας που χρησιμοποιούνται στο Διαδίκτυο. Η συλλογή διαθέτει 5 επίπεδα, καθένα από το οποίο είναι υπεύθυνο για την υλοποίηση μιας συγκεκριμένης λειτουργίας και τη απόκρυψη των λεπτομερειών υλοποίησης από τα πρωτόκολλα των ανώτερων επιπέδων. Στη συνέχεια, για κάθε επίπεδο της συλλογής πρωτοκόλλων του Διαδικτύου αναφέρονται τα πλέον διαδεδομένα πρωτόκολλα.

2.3.1. Πρωτόκολλα φυσικού στρώματος

Τα πρωτόκολλα φυσικού στρώματος είναι υπεύθυνα για την τηλεπικοινωνιακή σύνδεση δύο κόμβων προκειμένου να γίνει ανταλλαγή δεδομένων. Σε πρωτόκολλα αυτά καθορίζονται τα εξής:

1. Το φυσικό μέσο επικοινωνίας.
2. Το φάσμα συχνοτήτων που χρησιμοποιείται.
3. Τα σχήματα διαμόρφωσης και κωδικοποίησης FEC (Forward Error Correction) που χρησιμοποιούνται.

4. Οι μέθοδοι πολλαπλής πρόσβασης και ελέγχου συγκρούσεων.

Το κατάλληλο πρωτόκολλο φυσικού στρώματος επιλέγεται με κριτήριο τις προδιαγραφές των διατάξεων που επικοινωνούν και τα φυσικά μέσα επικοινωνίας που είναι διαθέσιμα. Τα πλέον διαδεδομένα πρωτόκολλα είναι τα εξής:

1. **IEEE 802.3**

   Είναι το παραδοσιακό πρωτόκολλο σύνδεσης μέσω καλωδίων συνεστραμμένων ζευγών που υιοθετείται στην περίπτωση των ενσύρματων τοπικών δικτύων. Το πρωτόκολλο εξελίσσεται συνεχώς και σήμερα υποστηρίζει ταχύτητες μετάδοσης μέχρι 10 Gbps σε αποστάσεις μέχρι 100m από το πρότυπο 10GBASE-T.

   Στην ίδια οικογένεια προτύπων ανήκουν και τα πρωτόκολλα επικοινωνίας μέσω καλωδίων οπτικών ινών. Με χρήση του πρωτοκόλλου οπτικών ινών 10GBASE-PR αυξάνεται η μέγιστη απόσταση επικοινωνίας στα 20km, επιτρέποντας τη σύνδεση κόμβων σε μεγάλες αποστάσεις με πολύ υψηλούς ρυθμούς μετάδοσης.

   Το πρωτόκολλο αυτό συναντάται πολύ συχνά στα εταιρικά πληροφοριακά δίκτυα του διαχειριστή του δικτύου ΗΕ και των προμηθευτών ΗΕ. Ακόμη, εμφανίζεται και σε βιομηχανικά πληροφοριακά δίκτυα.

2. **IEEE 802.11**

   Η οικογένεια πρωτοκόλλων 802.11 αφορά το ευρύτατα γνωστό και χρησιμοποιούμενο Wi-Fi που επιτρέπει τη λειτουργία ασφαλών ασύρματων τοπικών δικτύων. Αυτή τη στιγμή το πρωτόκολλο λειτουργεί με ρυθμούς μετάδοσης μέχρι 1 Gbps, αναμένεται, ωστόσο, να φθάσει σύντομα τα 7 Gbps [1].

3. **IEEE 1901**

   Αφορά τη χρήση των γραμμών μεταφοράς ηλεκτρικής ενέργειας για τη μετάδοση τηλεπικοινωνιακών σημάτων. Αξιοποιεί τμήματα του φάσματος στη ζώνη συχνοτήτων 1-100 MHz και επιτυγχάνει ταχύτητες μετάδοσης μέχρι 500 Mbps.

4. **IEEE 802.15.4**

   Το συγκεκριμένο πρότυπο αφορά ασύρματη επικοινωνία χαμηλού ρυθμού μετάδοσης. Χαρακτηρίζεται από τις μικρές ενεργειακές του ανάγκες και επιτρέπει τη μετάδοση πληροφορίας με ρυθμό μέχρι 250 Kbps σε μέγιστη απόσταση 10m.

5. **Δίκτυα GPRS / 3G / 4G (LTE)**

   Το πρότυπα GPRS, 3G, 4G προτυποποιούν τη μετάδοση δεδομένων μέσω του δικτύου κινητής τηλεφωνίας. Επιτυγχάνουν πολύ υψηλούς ρυθμούς μετάδοσης που φτάνουν μέχρι τα 500 Mbps στις περιπτώσεις του πρωτοκόλλου HSPA+ και LTE.

2.3.2. Πρωτόκολλα ζεύξης δεδομένων

Τα πρωτόκολλα του στρώματος μεταφοράς είναι αρμόδια για τη λογική σύνδεση μεταξύ γειτονικών κόμβων ενός τοπικού δικτύου. Το καθολικά χρησιμοποιούμενο πρωτόκολλο στρώματος μεταφοράς είναι το Ethernet ή IEEE 802.3. Η διευθυνσιοδότηση των κόμβων γίνεται μέσω των διευθύνσεων MAC που διαθέτει κάθε συσκευή δικτύου.

2.3.3. Πρωτόκολλα στρώματος δικτύου

Τα πρωτόκολλα του στρώματος αυτού είναι υπεύθυνα για την υποστήριξη της επικοινωνίας μεταξύ διαφορετικών δικτύων. Στο στρώμα αυτό χρησιμοποιούνται διάφορα πρωτόκολλα για να επιτελούν αντίστοιχες λειτουργίες, τα σημαντικότερα των οποίων είναι τα εξής:

1. **Internet Protocol (IP)**

   Το πρωτόκολλο IP είναι το βασικό πρωτόκολλο του στρώματος δικτύου. Προβλέπει τη μοναδική διευθυνσιοδότηση κάθε συσκευής ώστε να επιτρέπεται η επικοινωνία με συσκευές που δεν ανήκουν στο ίδιο τοπικό δίκτυο. Μέσω της IP διευθυνσιοδότησης γίνεται η δρομολόγηση των πακέτων μέσω διαφόρων δικτύων, μέχρι αυτά να φθάσουν στον προορισμό τους. Τα τελευταία χρόνια, ωστόσο, το πλήθος των συσκευών με δυνατότητες διαδικτύωσης έχει πλησιάσει το μέγιστο πλήθος IP διευθύνσεων που προέβλεπε η έκδοση IPv4 του πρωτοκόλλου IP. Για το λόγο αυτό, προωθείται η νέα έκδοση IPv6 όπου αυξήθηκαν τα bits διευθυνσιοδότησης από 32 σε 128, ώστε να αυξηθεί το πλήθος των διαφορετικών IP διευθύνσεων.

2. **Internet Control Message Protocol (ICMP)**

   Το ICMP είναι το πρωτόκολλο μέσω του οποίου μεταφέρονται μηνύματα ελέγχου μεταξύ κόμβων του Διαδικτύου. Αποσκοπεί, επίσης, στο να ειδοποιείται ο αποστολέα ενός πακέτου σε περίπτωση κάποιου λάθος κατά την αποστολή του πακέτου.

3. **Address Resolution Protocol (ARP)**

   Το πρωτόκολλο ARP είναι ο συνδετικός κρίκος με το πρωτόκολλο Ethernet που λειτουργεί στο αμέσως χαμηλότερο επίπεδο. Είναι αρμόδιο για την αντιστοίχιση της διεύθυνσης IP μιας συσκευής με τη διεύθυνση MAC που η ίδια χρησιμοποιεί στο πρωτόκολλο Ethernet και λειτουργεί με το μοντέλο ερώτησης-απάντησης. Ωστόσο, το πρωτόκολλο ARP υποστηρίζει και τη λειτουργία gratuitous ARP, μέσω της οποίας ένας κόμβος μπορεί να ανακοινώσει τη διεύθυνση IP του στο τοπικό δίκτυο, δίχως να έχει προηγηθεί ερώτηση, με στόχο να ενημερωθούν οι γειτονικοί κόμβοι. Είναι φανερό ότι η λειτουργία αυτή εγείρει σημαντικά ζητήματα ασφαλείας.

2.3.4. Πρωτόκολλα στρώματος μεταφοράς

Τα πρωτόκολλα του στρώματος μεταφοράς είναι υπεύθυνα για τη διαχείριση της από άκρο σε άκρο σύνδεσης δύο συσκευών, παρακάμπτοντας τις ανομοιογένειες των δικτύων μέσω των οποίων γίνεται η μεταφορά πακέτων. Η σύνδεση γίνεται μέσω αντίστοιχων θυρών στον αποστολέα και στον παραλήπτη. Οι

θύρες είναι αριθμοί 16-bit που χρησιμοποιούνται για την ταυτοποίηση της εφαρμογής η οποία χρησιμοποιεί την σύνδεση. Ο αποστολέας φροντίζει ώστε τα πακέτα να περιέχουν τη θύρα του παραλήπτη για την οποία προορίζονται. Στον παραλήπτη, το λειτουργικό σύστημα μεταφέρει τα πακέτα στο λογισμικό που έχει δεσμεύσει τη συγκεκριμένη θύρα. Τα πρωτόκολλα που χρησιμοποιούνται για το σκοπό αυτό είναι τα εξής:

1. **Transmission Control Protocol (TCP)**

   Το πρωτόκολλο TCP είναι το πλέον συνηθισμένο πρωτόκολλο στρώματος μεταφοράς στο Διαδίκτυο. Προσφέρει αξιόπιστη μεταφορά δεδομένων, επιβεβαιώνοντας την ορθή άφιξη κάθε πακέτου. Επιπλέον, αποτρέπει τη συμφόρηση του δικτύου με ρύθμιση του ρυθμού μετάδοσης πακέτων ανάλογα με τις κατάλληλες ενδείξεις ως προς τη συμφόρηση του δικτύου.

2. **User Datagram Protocol (UDP)**

   Το UDP είναι το άλλο πρωτόκολλο στρώματος μεταφοράς που λειτουργεί με απλούστερο μηχανισμό από το TCP. Δεν παρέχει καμία εγγύηση για την ορθή μετάδοση δεδομένων. Όμως, λόγω του σημαντικά μικρότερου φόρτου επεξεργασίας πακέτων σε σύγκριση με το TCP, χρησιμοποιείται από εφαρμογές για μεταφορά δεδομένων που απαιτούν ελάχιστη καθυστέρηση, όπως οι εφαρμογές πραγματικού χρόνου.

2.3.5. Πρωτόκολλα στρώματος εφαρμογής

Στο υψηλότερο επίπεδο της στοίβας πρωτοκόλλων του Διαδικτύου συγκαταλέγονται τα συγκεκριμένα πρωτόκολλα που ορίζονται από κάθε εφαρμογή που χρησιμοποιείται στο Διαδίκτυο. Ενδεικτικά θα αναφερθούν οι συχνότερα χρησιμοποιούμενες εφαρμογές και ο συνδυασμός θύρας και πρωτοκόλλου μεταφοράς που χρησιμοποιούν. Συγκεκριμένα:

1. **HTTP** (Θύρα 80 TCP)

   Το HTTP είναι το πρωτόκολλο το οποίο χρησιμοποιεί το World Wide Web.
2. **DNS** (Θύρα 53 TCP/UDP)

   Το πρωτόκολλο DNS είναι υπεύθυνο για την αντιστοίχιση των ονομάτων των ιστοσελίδων με τις διευθύνσεις IP των διακομιστών τους.
3. **FTP** (Θύρα 21 TCP)

   Το FTP είναι το δημοφιλέστερο πρωτόκολλο μεταφοράς αρχείων.
4. **SSH** (Θύρα 22 TCP/UDP)

   Ασφαλές πρωτόκολλο απομακρυσμένης σύνδεσης. Διαβιβάζει στο χρήστη μια γραμμή εντολών μέσω της οποίας μπορεί να αποστέλλει εντολές στο απομακρυσμένο σύστημα και να λαμβάνει τα αποτελέσματά τους.
5. **DHCP** (Θύρες 67-68 UDP)

   Είναι υπεύθυνο για τη δυναμική απόδοση IP διευθύνσεων σε συσκευές που συνδέονται στο τοπικό δίκτυο για το οποίο είναι υπεύθυνη η συσκευή που υλοποιεί τη συγκεκριμένη υπηρεσία.
6. **SNMP** (Θύρες 161-162 UDP)

   Είναι το βασικό πρωτόκολλο διαχείρισης δικτύου.

7. **OpenVPN** (Θύρα 1194 TCP/UDP)

   Ασφαλές πρωτόκολλο ανοικτού κώδικα που επιτρέπει τη σύνδεση μιας συσκευής σε κάποιο απομακρυσμένο τοπικό δίκτυο.

2.4. Πρωτόκολλα βιομηχανικών πληροφοριακών δικτύων

Παραδοσιακά, τα βιομηχανικά πληροφοριακά δίκτυα επικοινωνούν μέσω σειριακών διαύλων επικοινωνίας. Τα τελευταία χρόνια, ωστόσο, έχουν αναπτυχθεί παραλλαγές των πρωτοκόλλων βιομηχανικών πληροφοριακών δικτύων ώστε να είναι δυνατή η επικοινωνία των διατάξεων χρησιμοποιώντας τα πρωτόκολλα TCP/IP και το Ethernet. Τα βιομηχανικά πρωτόκολλα επικοινωνίας τα οποία, χρησιμοποιούνται συχνότερα στα βιομηχανικά πληροφοριακά δίκτυα είναι τα εξής:

1. **Modbus – Modbus TCP**

   Το Modbus είναι το πρώτο, χρονικά, και δημοφιλέστερο βιομηχανικό πρωτόκολλο επικοινωνίας. Είναι πρωτόκολλο του στρώματος εφαρμογής, με αποτέλεσμα να μπορεί να λειτουργήσει ανεξαρτήτως από τα δικτυακά πρωτόκολλα των χαμηλότερων στρωμάτων.
2. **ICCP**

   Το πρωτόκολλο αυτό χρησιμοποιείται στη βιομηχανία ΗΕ ως πρότυπο για την επικοινωνία του κέντρου ελέγχου με τα συστήματα παραγωγής και διανομής ΗΕ. Χρησιμοποιεί το μοντέλο client/server για την επικοινωνία, και μπορεί να εγκατασταθεί πάνω σε διάφορους συνδυασμούς πρωτοκόλλων φυσικού στρώματος, στρώματος δικτύου και στρώματος μεταφοράς. Ωστόσο, η επικοινωνία πραγματοποιείται συνήθως μέσω της θύρας 102 του πρωτοκόλλου TCP.
3. **DNP3**

   Το DNP3 είναι το πλέον σύγχρονο βιομηχανικό πρωτόκολλο επικοινωνίας. Το πρότυπο ορίζει δικά του πρωτόκολλα στρώματος ζεύξης δεδομένων, μεταφοράς και εφαρμογής. Επεκτάθηκε, ωστόσο, ώστε να μπορεί να χρησιμοποιηθεί και σε δίκτυα TCP/IP. Είναι από τα πλέον αξιόπιστα βιομηχανικά πρωτόκολλα επικοινωνίας καθώς πραγματοποιεί ευρεία χρήση των ελέγχων CRC σε διάφορα τμήματα του πακέτου, με στόχο να ανακαλύπτονται ενδεχόμενα λάθη κατά τη μετάδοση των αντίστοιχων δεδομένων του πακέτου.
4. **OPC**

   Πρωτόκολλο το οποίο διευκολύνει την επικοινωνία βιομηχανικών συσκευών με συστήματα λειτουργικού συστήματος Windows.
5. **Ethernet/IP**

   Χρησιμοποιεί το πρότυπο CIP (Common Industrial Protocol) πάνω από δίκτυα τύπου Ethernet για την επικοινωνία με βιομηχανικές συσκευές.
6. **Profibus**

   Πρωτόκολλο το οποίο αναπτύχθηκε στη Γερμανία και επιτρέπει την επικοινωνία βιομηχανικών συσκευών ακολουθώντας το μοντέλο master/slave σε δίκτυα μοιραζόμενης σκυτάλης (token sharing).

2.5. Προδιαγραφές ασφάλειας πληροφοριών

Οι πληροφορίες που διακινούνται σε ένα δίκτυο προέρχονται από εφαρμογές που εκτελούνται στα πληροφοριακά συστήματα του δικτύου. Συχνά, μεγάλο μέρος των πληροφοριών αυτών είναι κρίσιμο για την ορθή λειτουργία των συστημάτων του δικτύου. Είναι, λοιπόν, απαραίτητο να διασφαλιστεί η ασφάλεια των πληροφοριών από κάθε ενέργεια που μπορεί να οδηγήσει σε δυσλειτουργία των συστημάτων του δικτύου. Κάθε εφαρμογή, με κριτήριο το είδος των πληροφοριών που ανταλλάσσει, θέτει προδιαγραφές για την ασφάλειά τους. Αυτές οι προδιαγραφές αφορούν τομείς όπως:

1. Η εμπιστευτικότητα των πληροφοριών.
2. Η ακεραιότητα των πληροφοριών.
3. Η πιστοποίηση της ταυτότητας των οντοτήτων που ανταλλάσσουν τις πληροφορίες.

Για παράδειγμα, ένα σύστημα που ανταλλάσσει εμπιστευτικές πληροφορίες, έχει ανάγκη από μηχανισμούς που εγγυώνται την εμπιστευτικότητα αυτή. Αντίστοιχα, ένα σύστημα ελέγχου μιας γεννήτριας, είναι αναγκαίο να διαθέτει, τουλάχιστον, μηχανισμούς που εξασφαλίζουν την ακεραιότητα των δεδομένων ελέγχου καθώς το παραμικρό λάθος στις εντολές μπορεί να δημιουργήσει σοβαρά προβλήματα.

2.5.1. Πρωτόκολλα ασφάλειας πληροφοριών

Οι ανάγκες ασφάλειας των μεταδιδόμενων πληροφοριών που αναφέρθηκαν προηγουμένως ώθησαν την κοινότητα της πληροφορικής στην ανάπτυξη των σχετικών πρωτοκόλλων. Τα πρωτόκολλα αυτά είναι σχεδιασμένα ώστε να παρέχουν ταυτόχρονα εμπιστευτικότητα και ακεραιότητα των δεδομένων καθώς και πιστοποίηση της ταυτότητας των συστημάτων που επικοινωνούν.

1. IPsec

Όπως δηλώνει και η ονομασία του, το IPsec είναι ένα πρωτόκολλο ασφάλειας πληροφοριών που λειτουργεί στο στρώμα διαδικτύου της συλλογής πρωτοκόλλων του Διαδικτύου. Αναλαμβάνει την προστασία των πακέτων IP που αποστέλλονται μεταξύ δύο κόμβων. Αρχικά, προβλέπει την αμοιβαία ταυτοποίηση των δύο οντοτήτων που επικοινωνούν μέσω της σύνδεσης. Στην συνέχεια, ανταλλάσσονται τα κλειδιά κρυπτογράφησης που θα χρησιμοποιηθούν στη συγκεκριμένη σύνδεση και συμφωνείται ο αλγόριθμος κρυπτογράφησης. Τέλος, κάθε πακέτο IP ενθυλακώνεται σε ένα πακέτο IPsec. Στο τελευταίο εισάγεται μία τιμή επαλήθευσης της ακεραιότητας, και στη συνέχεια γίνεται κρυπτογράφηση και αποστολή. Η ανωτέρω διαδικασία εγγυάται την τήρηση των προδιαγραφών εμπιστευτικότητας, ακεραιότητας και πιστοποίησης που παρέχει το πρωτόκολλο.

2. Transport Layer Security (TLS)

Το πρωτόκολλο TLS είναι αυτή τη στιγμή το δημοφιλέστερο πρωτόκολλο ασφάλειας επικοινωνιών στο Διαδίκτυο καθώς χρησιμοποιείται στις ασφαλείς εκδόσεις δημοφιλών πρωτοκόλλων όπως τα HTTPS και FTPS. Το TLS προέρχεται από το πρωτόκολλο SSL (Secure Socket Layer) και εγγυάται εμπιστευτικότητα, ακεραιότητα και πιστοποίηση.

Σε αντίθεση με το IPsec, το πρωτόκολλο TLS λειτουργεί ενδιάμεσα στο στρώμα μεταφοράς και το στρώμα εφαρμογής της συλλογής πρωτοκόλλων του Διαδικτύου. Αρχικά, η πιστοποίηση των οντοτήτων που επικοινωνούν γίνεται με χρήση πιστοποιητικών X.509 που εκδίδονται από ανεξάρτητες αρχές και περιέχουν το δημόσιο κλειδί κρυπτογράφησης που χρησιμοποιεί κάθε οντότητα. Ακολούθως, αποκαθίσταται η σύνδεση με ασύμμετρη κρυπτογράφηση κατά την οποία συμφωνείται ο αλγόριθμος συμμετρικής κρυπτογράφησης και το τυχαίο συμμετρικό κλειδί που θα χρησιμοποιηθούν στη συνέχεια. Από το σημείο -και μετά, η επικοινωνία πραγματοποιείται με συμμετρική κρυπτογράφηση των πακέτων TCP στα οποία έχει προστεθεί μια τιμή ελέγχου της ακεραιότητας των δεδομένων.

2.5.2. Ασφάλεια πληροφοριών σε βιομηχανικά πληροφοριακά δίκτυα

Στην περίπτωση των βιομηχανικών πρωτοκόλλων η ύπαρξη ή όχι μέριμνας για την ασφάλεια των μεταδιδόμενων πληροφοριών εμπίπτει στο ίδιο το πρωτόκολλο. Για παράδειγμα, πρωτόκολλα όπως το ICCP και το DNP3 διαθέτουν εκδόσεις που περιλαμβάνουν μηχανισμούς για την ασφάλεια των δεδομένων, σε αντίθεση με το πρωτόκολλο Modbus. Ακόμη υπάρχουν προτάσεις για χρήση πρωτοκόλλων διαχείρισης διατάξεων στο βιομηχανικά πληροφοριακά δίκτυα που πληρούν υψηλές προδιαγραφές ασφάλειας πληροφορικών [2]. Τα τελευταία χρόνια, όμως, αναπτύσσονται εκδόσεις των ανωτέρω πρωτοκόλλων που λειτουργούν επί δικτύων που χρησιμοποιούν τα πρωτόκολλα TCP/IP. Σε αυτές τις περιπτώσεις και υπό ορισμένες προϋποθέσεις, μπορούν να χρησιμοποιηθούν τα πρωτόκολλα ασφάλειας IPsec και TLS που αναφέρθηκαν προηγουμένως. Έτσι, χωρίς να υπάρξει αλλαγή των βιομηχανικών πρωτοκόλλων τηρούνται όλες οι προδιαγραφές για την ασφάλεια των διακινούμενων πληροφοριών.

Κεφάλαιο 3. Ευφυείς Μετρητές

3.1. Εισαγωγή

Οι ευφυείς μετρητές είναι μία θεμελιώδης κατηγορία διατάξεων για το σύστημα του Ευφυές Δίκτυο. Ο ρόλος των ευφυών μετρητών στο Smart Grid είναι διπλός. Αρχικά, σε αντίθεση με τους σημερινούς μετρητές, είναι ευφυείς ψηφιακοί μετρητές που μετρούν σε πραγματικό χρόνο πολλά μεγέθη που αφορούν την κατανάλωση ΗΕ μιας εγκατάστασης, και το ηλεκτρικό ρεύμα. Επιπλέον, διαθέτουν τη δυνατότητα αμφίδρομης επικοινωνίας με το διαχειριστή του δικτύου ΗΕ καθώς και με τις ηλεκτρικές και ηλεκτρονικές συσκευές μέσα στο Οικιακό Τοπικό Δίκτυο (Home Area Network – HAN).

Στα δύο βασικά χαρακτηριστικά του ευφυούς μετρητή, δηλαδή της συνεχούς μέτρησης μεγεθών του ηλεκτρικού ρεύματος και της επικοινωνίας με άλλες συσκευές, βασίζονται όλες οι υπηρεσίες που προσφέρονται μέσω του ευφυούς μετρητή στους καταναλωτές. Ενδεικτικά, ανάλογα με τα τρέχοντα στοιχεία κατανάλωσης, οι προμηθευτές ΗΕ μπορούν να προτείνουν τρόπους μείωσης του κόστους ΗΕ στους καταναλωτές. Επιπλέον, οι ευφυείς μετρητές έχουν τη δυνατότητα να αποτελέσουν τον κεντρικό κόμβο αυτόματης διαχείρισης και απομακρυσμένου ελέγχου όλων των συσκευών που είναι συνδεδεμένα στο HAN.

Η αναβάθμιση των μετρητών ΗΕ ώστε να μπορούν να παρέχουν εξελιγμένες υπηρεσίες δημιουργεί διάφορες προκλήσεις. Αυτές προκύπτουν κυρίως από το ότι ο ευφυής μετρητής είναι πλέον, μια υπολογιστική συνδεδεμένη με το Διαδίκτυο, διάταξη όπου εκτελείται ένα λειτουργικό σύστημα. Αυτό καθιστά τον ευφυή μετρητή ενδεχόμενο στόχο κακόβουλων επιθέσεων είτε για ατομικό όφελος του επιτιθέμενου είτε ως το πρώτο βήμα μιας ευρύτερης επίθεσης εναντίον του διαχειριστή του δικτύου ΗΕ και των προμηθευτών ΗΕ.

3.2. Κίνητρα κακόβουλων επιθέσεων

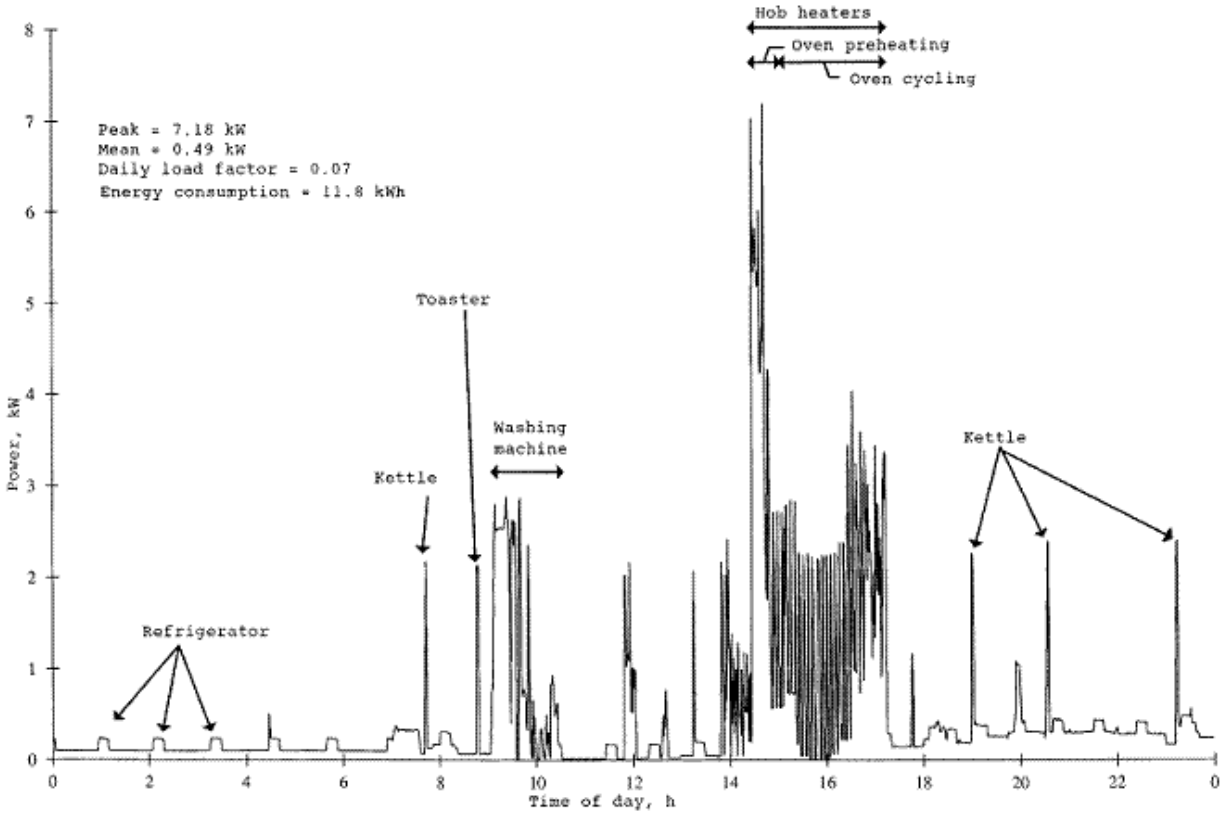
3.2.1. Υποκλοπή προσωπικών δεδομένων κατανάλωσης ΗΕ

Οι ευφυείς μετρητές μετρούν σε πραγματικό χρόνο την κατανάλωση ισχύος και αποστέλλουν χρήσιμα στοιχεία στο κέντρο ελέγχου του διαχειριστή του δικτύου ΗΕ. Τα στοιχεία κατανάλωσης επιτρέπουν στο διαχειριστή του δικτύου ΗΕ να διαχειρίζεται σε πραγματικό χρόνο το συνολικό φορτίο και στους προμηθευτές ΗΕ να προσφέρουν κίνητρα στους καταναλωτές για να μειώσουν την κατανάλωση σε ώρες αιχμής.

Ωστόσο, τα δεδομένα κατανάλωσης ισχύος αποτελούν προσωπικά δεδομένα, μέσω της επεξεργασίας των οποίων μπορούν προκύπτουν σημαντικές πληροφορίες για την προσωπική ζωή των καταναλωτών. Ενδεικτικά, όπως φαίνεται και στο σχήμα που ακολουθεί, είναι πολύ εύκολο από τη μέτρηση της κατανάλωσης ΗΕ να εξακριβωθεί ποιές συσκευές λειτουργούν, σε ποιές ώρες και με ποιό προγραμματισμό [3]. Επομένως, με απλό τρόπο μπορούν να εξαχθούν πληροφορίες σχετικά με το πρόγραμμα κάθε καταναλωτή, τον τρόπο ζωής του, τις συνήθειές του, ακόμα και το πότε βρίσκεται στην οικία του.

Πληροφορίες όπως οι ανωτέρω είναι περιζήτητες από εταιρίες διαφημίσεων και στοχευμένου marketing ώστε να παράγουν εξατομικευμένες διαφημίσεις στους καταναλωτές προσαρμοσμένες στον τρόπο ζωής τους. Η υψηλή διεισδυτικότητα αυτού του είδους marketing θα ωθήσει πολλές εταιρίες να προσφέρουν αδρές αμοιβές για να λαμβάνουν τέτοιου είδους πληροφορίες. Οι αμοιβές αυτές θα αποτελέσουν σημαντικό κίνητρο

για κακόβουλους χρήστες να επιτεθούν είτε στους ευφυείς μετρητές είτε στη ψηφιακή πλατφόρμα μέσω της οποίας γίνεται η διαχείριση του λογαριασμού κάθε καταναλωτή και των συνδεδεμένων ηλεκτρικών συσκευών.



Σχήμα 3.1. Αντιστοίχιση δεδομένων κατανάλωσης σε δραστηριότητα οικιακών συσκευών

3.2.2. Κλοπή ρεύματος – Απάτη

Ένα από τα μεγαλύτερα προβλήματα των σημερινών δικτύων ΗΕ αποτελεί η κλοπή ρεύματος. Παγκοσμίως, η ζημιά από την κλοπή ρεύματος για τους προμηθευτές ΗΕ είναι πολύ μεγάλη. Ως εκ τούτου, η αντιμετώπισή της αποτελεί έναν από τους λόγους ανάπτυξης του Smart Grid [4]. Η υποδομή των ευφυών μετρητών επιτρέπει στους προμηθευτές ΗΕ να συγκρίνουν τα δεδομένα κατανάλωσης με τα δεδομένα διάθεσης ΗΕ ανά περιοχή και καταναλωτή. Έτσι, με άμεσο τρόπο ανακαλύπτονται οι διάφορες περιπτώσεις κλοπής ΗΕ. Με αυτό τον τρόπο επιλύεται σε μεγάλο βαθμό το πρόβλημα της διαπίστωσης της κλοπής ΗΕ, κάτι που αποτελεί ένα σημαντικό βήμα προς την αντιμετώπιση του φαινομένου.

Το ολοένα και αυξανόμενο κόστος ΗΕ θα ωθήσει αρκετούς καταναλωτές να αναζητήσουν νέους τρόπους κλοπής ρεύματος. Οι προσπάθειες αυτές θα έχουν ως κύριο στόχο τους ευφυείς μετρητές με σκοπό την παραβίασή τους και την αποστολή εσφαλμένων στοιχείων στο διαχειριστή του δικτύου ΗΕ. Οι κακόβουλοι καταναλωτές θα μπορούν να αποστέλλουν ψευδή δεδομένα που θα είναι σε θέση να τους εμφανίζουν μέχρι και ως ιδιώτες παραγωγούς ΗΕ. Σε κάθε περίπτωση, οι ευφυείς μετρητές θα αποτελέσουν τον πρώτο στόχο όσων επιδιώκουν κλοπή ρεύματος.

3.2.3. Πρόσβαση στο δίκτυο της εταιρίας ΗΕ

Οι ευφυείς μετρητές αποστέλλουν τις μετρήσεις τους στο κέντρο διαχείρισης δεδομένων του διαχειριστή του δικτύου ΗΕ και πιθανώς και στους προμηθευτές ΗΕ. Ένας επίδοξος εισβολέας που στοχεύει το εσωτερικό δίκτυο του διαχειριστή του δικτύου ΗΕ μπορεί να επιχειρήσει να χρησιμοποιήσει τον ίδιο τον ευφυή μετρητή και τη σύνδεσή του με το κέντρο διαχείρισης δεδομένων ώστε να αποκτήσει πρόσβαση. Στην περίπτωση αυτή, η παραβίαση του μετρητή αποτελεί αρχικό βήμα μιας μεγαλύτερης επίθεσης εναντίον δικτυακών στόχων του διαχειριστή του δικτύου ΗΕ.

3.3. Μέθοδοι επίθεσης στη διαδικτυακή πλατφόρμα διαχείρισης και αντίμετρα

3.3.1. Μέθοδοι επίθεσης

Η διαδικτυακή πλατφόρμα διαχείρισης είναι το εργαλείο με το οποίο ο καταναλωτής σε θέση κάθε στιγμή να διαχειρίζεται το λογαριασμό του στην εταιρία ΗΕ. Εκεί παρουσιάζονται τα στοιχεία κατανάλωσης, οι ενδεχόμενες οφειλές, και οι επιλογές απομακρυσμένης διαχείρισης συσκευών που είναι συνδεδεμένες με τον ευφυή μετρητή. Στην πλατφόρμα αυτή ο καταναλωτής συνδέεται χρησιμοποιώντας ένα username και ένα password που είναι συνδεδεμένα με το συγκεκριμένο λογαριασμό. Λόγω της πληθώρας των πληροφοριών που είναι προσβάσιμες από τη συγκεκριμένη πλατφόρμα, αυτή αποτελεί ένα από τους πιθανότερους στόχους επίθεσης.

1. Παραβίαση Η/Υ και έξυπνων κινητών συσκευών

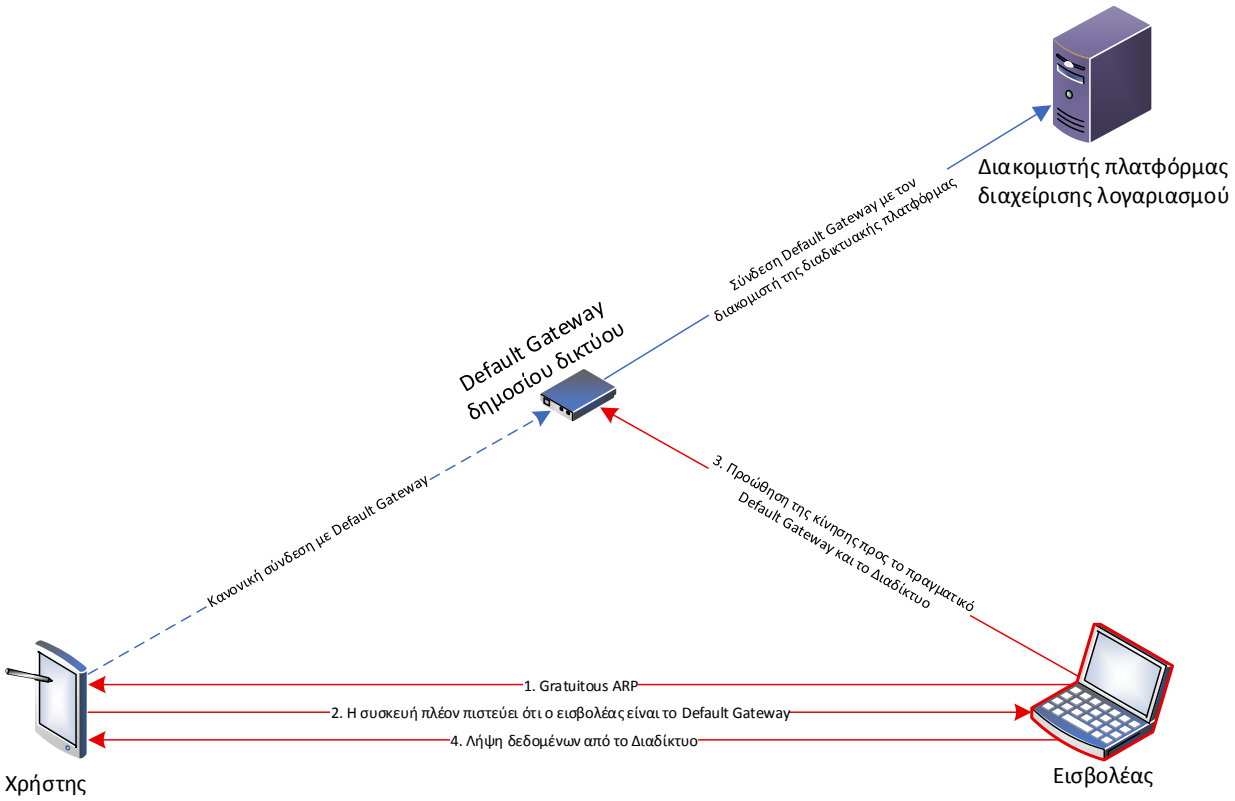
Τα τελευταία χρόνια παρατηρείται στροφή των εταιριών πληροφορικής και των καταναλωτών προς κινητές συσκευές. Συσκευές όπως smartphones και tablets αποκτούν, πλέον, εξέχουσα θέση στις προτιμήσεις των καταναλωτών, με αποτέλεσμα πολλοί καταναλωτές να επιλέξουν να συνδέονται μέσω αυτών στη διαδικτυακή πλατφόρμα ΗΕ. Επομένως, κατά την σύνδεση στην πλατφόρμα διαχείρισης λογαριασμού, η ασφάλεια των συσκευών αυτών, όπως και των Η/Υ, πρέπει να είναι εξασφαλισμένη. Ανάλογη αύξηση με τις πωλήσεις συσκευών πληροφορικής έχουν και τα κακόβουλα λογισμικά που συνεχώς ανακαλύπτονται [5] λόγω της στροφής προς την ανάπτυξη κακόβουλου λογισμικού με στόχο έξυπνες κινητές συσκευές. Το κακόβουλο αυτό λογισμικό εμφανίζεται υπό τη μορφή εκτελέσιμων αρχείων σε υπολογιστές και υπό τη μορφή εφαρμογών στις έξυπνες κινητές συσκευές. Και στις δύο περιπτώσεις, στόχος είναι η απόκτηση πρόσβασης στο λογαριασμό του χρήστη ή και η υποκλοπή των στοιχείων ταυτοποίησης του χρήστη.

Ως προς τους Η/Υ, το είδος του κακόβουλου λογισμικού που χρησιμοποιείται για την απόσπαση στοιχείων ταυτοποίησης χρηστών είναι τα λεγόμενα keyloggers. Τα κακόβουλα αυτά εργαλεία καταγράφουν όλες τις πληκτρολογήσεις και στη συνέχεια αποστέλλουν τις καταγραφές μέσω Διαδικτύου στον επίδοξο εισβολέα. Ο τελευταίος πρέπει να αναζητήσει μέσα στις καταγραφές αυτές, τις εγγραφές εκείνες που αποτελούν πιθανούς κωδικούς πρόσβασης. Όταν ανακαλυφθούν οι κωδικοί πρόσβασης ο επίδοξος εισβολέας έχει στη διάθεσή του τα στοιχεία με τα οποία ταυτοποιείται ο χρήστης στη διαδικτυακή πλατφόρμα διαχείρισης λογαριασμού και μπορεί να αποκτήσει πρόσβαση σε αυτή.

Στην περίπτωση των κινητών τηλεφώνων τα κακόβουλα λογισμικά εμφανίζονται κυρίως υπό τη μορφή εφαρμογών. Η ευκολία με την οποία μια τέτοια εφαρμογή είναι σε θέση να υποκλέψει τα στοιχεία σύνδεσης του χρήστη εξαρτάται κατά πολύ από τα δικαιώματα τα οποία έχουν δοθεί σε αυτή από το χρήστη. Για παράδειγμα, μία εφαρμογή που διαθέτει τα προεπιλεγμένα δικαιώματα δεν μπορεί να έχει πρόσβαση σε δεδομένα που δεν της ανήκουν. Στην περίπτωση αυτή η κακόβουλη εφαρμογή μπορεί να έχει εμφάνιση και λειτουργία που προσομοιάζει σε μία εφαρμογή-εργαλείο σύνδεσης στη διαδικτυακή πλατφόρμα, ώστε να εξαπατήσει το χρήστη, ενώ ταυτόχρονα στο παρασκήνιο να αποστέλλει τα στοιχεία σύνδεσης στον κακόβουλο χρήστη. Όμως, στην περίπτωση όπου από το χρήστη της συσκευής έχουν δοθεί στην εφαρμογή δικαιώματα root ή Administrator, η εφαρμογή έχει απεριόριστη πρόσβαση στα δεδομένα της συσκευής και μπορεί να διαβάσει τους αποθηκευμένους κωδικούς από τα αρχεία συστήματος στα οποία φυλάσσονται και να τους αποστείλει στον επίδοξο εισβολέα.

2. *Είσοδος από δημόσια ασύρματα δίκτυα*

Η τεχνολογία Wi-Fi έχει αναπτυχθεί ραγδαία τα τελευταία χρόνια, με αποτέλεσμα να είναι, πλέον, ευρέως διαδεδομένη. Ενδεικτικά, σε πολλούς δημόσιους και ιδιωτικούς χώρους είναι εγκατεστημένα ελεύθερης πρόσβασης δίκτυα Wi-Fi. Πολλοί χρήστες επιλέγουν να πραγματοποιούν εργασίες σε προσωπικούς τους λογαριασμούς ή αγορές μέσα από τέτοια δημόσια ασύρματα δίκτυα. Όπως και στην περίπτωση του e-banking, για το οποίο προτείνεται η αποφυγή χρήσης του από δημόσια δίκτυα, έτσι πρέπει να συμβαίνει και με υπηρεσίες που αφορούν το λογαριασμό ΗΕ των καταναλωτών. Ο λόγος είναι ότι υπάρχει μια πολύ αποτελεσματική και απλή στην εφαρμογή της επίθεση που έχει ως στόχο την υποκλοπή όλων των δεδομένων της σύνδεσης μιας συσκευής με το Διαδίκτυο μέσα από τα τοπικά δίκτυα Wi-Fi. Η επίθεση αυτή είναι γνωστή με την ονομασία Man-In-The-Middle. Στόχος της επίθεσης αυτής είναι να εισαχθεί ο εισβολέας ως ενδιάμεσος κόμβος μεταξύ της σύνδεσης του χρήστη με τον διακομιστή και να καταγράφει όλα τα δεδομένα που ανταλλάσσονται μέσω της σύνδεσης. Στο Σχ. 3.2, φαίνεται πώς πραγματοποιείται μια επίθεση τέτοιου τύπου. Το πρώτο βήμα είναι η αποστολή από τον εισβολέα ενός πακέτου gratuitous ARP ώστε μέσω του πρωτοκόλλου ARP να ειδοποιήσει ότι η συσκευή του εισβολέα βρίσκεται στην IP του Default Gateway. Η τεχνική αυτή ονομάζεται ARP cache poisoning. Στο σημείο αυτό, η εξαπατηθείσα συσκευή του χρήστη έχει καταχωρήσει ως Default Gateway τη συσκευή του εισβολέα και προωθεί σε αυτήν όλη την κίνηση προς το Διαδίκτυο. Ο εισβολέας την προωθεί με την σειρά του στον πραγματικό Default Gateway αλλά και λαμβάνει τα δεδομένα από το διακομιστή τα οποία αποστέλλει στη συσκευή του χρήστη.



Σχήμα 3.2. Σχηματική απεικόνιση των βημάτων της επίθεσης Man-In-The-Middle

Μετά από την επιτυχία της ανωτέρω διαδικασίας, η κίνηση του χρήστη προς το Διαδίκτυο διέρχεται από τον εισβολέα, με αποτέλεσμα ο τελευταίος να υποκλέπτει όλη την κίνηση και να έχει πρόσβαση σε όλες τις πληροφορίες που εμπεριέχονται στα δεδομένα κίνησης. Στην περίπτωση επίθεσης εναντίον της διαδικτυακής πλατφόρμας διαχείρισης λογαριασμού, τα δεδομένα που ενδιαφέρουν είναι οι κωδικοί ασφαλείας και τα δεδομένα που αυτή επιστρέφει στο χρήστη.

3. Ηλεκτρονική «αλιεία» - Phishing

Η ονομασία αυτή έχει προκύψει λόγω της ομοιότητας της διαδικασίας υποκλοπής με τη διαδικασία μέσω της οποίας κάποιος προσπαθεί να αλιεύσει πληροφορίες από κάποιον που τις διαθέτει αλλά δεν επιθυμεί να τις μοιραστεί. Η ηλεκτρονική «αλιεία» βασίζεται στην εξαπάτηση του χρήστη, εκμεταλλευόμενη κυρίως την εκ μέρους του έλλειψη προσοχής και παρατηρητικότητας με σκοπό και πάλι ο κακόβουλος χρήστης να αποσπάσει τα στοιχεία πρόσβασης του θύματος.

Το πρώτο βήμα που πραγματοποιεί ο κακόβουλος χρήστης είναι να στήσει ένα διακομιστή ορίζοντας ως όνομα της ιστοσελίδας ένα σχεδόν όμοιο με αυτό της ιστοσελίδας στόχου, δηλαδή της διαδικτυακής πλατφόρμας. Στη συνέχεια, μεταβαίνει στην πραγματική ιστοσελίδα και αντιγράφει τον κώδικα HTML της πραγματικής ιστοσελίδας, ώστε και η ψευδής να είναι ίδια εμφανισιακά με την πραγματική. Αφού συμβεί αυτό, είτε περιμένει τα θύματα να πληκτρολογήσουν κατά λάθος το όνομα της δικής του ιστοσελίδας είτε αποστέλλει “phishing email” στα οποία να περιέχει το σύνδεσμο προς την ιστοσελίδα του, ώστε χρήστες που δεν παρατηρούν το ελαφρώς αλλαγμένο όνομα της σελίδας να συνδεθούν σε αυτή. Όταν ένας χρήστης-θύμα

συνδεθεί στην κακόβουλη ιστοσελίδα, εισάγει τα στοιχεία σύνδεσης που χρησιμοποιεί για την πραγματική ιστοσελίδα, τα οποία λαμβάνει ο διακομιστής του κακόβουλου χρήστη και τα αποθηκεύει. Το τελευταίο βήμα πραγματοποιείται μόλις ολοκληρωθεί η εισαγωγή των στοιχείων σύνδεσης του χρήστη. Τότε, η κακόβουλη ιστοσελίδα προωθεί το θύμα στην πραγματική ιστοσελίδα. Κατ' αυτό τον τρόπο, και ειδικά αν το θύμα δεν είναι πολύ έμπειρο στη χρήση του Διαδικτύου, η επίθεση δεν γίνεται αντιληπτή.

Η επίθεση ηλεκτρονικής «αλιείας» είναι ιδιαίτερα αποτελεσματική σε θύματα που έχουν μόνο περιστασιακή σχέση με τους Η/Υ και το Διαδίκτυο. Τις περισσότερες φορές δεν γίνεται αντιληπτή από τα θύματα που, εφόσον δεν γνωρίζουν ότι έπεσαν θύματα επίθεσης, δεν έχουν λόγο να αλλάξουν τους κωδικούς πρόσβασης. Επομένως, ο κακόβουλος χρήστης δημιουργεί σταδιακά μια βάση δεδομένων στην οποία διατηρεί στοιχεία πρόσβασης όλο και περισσότερων χρηστών. Τη βάση αυτή μπορεί να τη διαθέσει στην αντίστοιχη παράνομη αγορά.

4. Ανεύρεση – «Σπάσιμο» κωδικών πρόσβασης

Η μέθοδος του «σπασίματος» κωδικών πρόσβασης, δηλαδή της χρήσης εργαλείων για την εξεύρεση του κωδικού πρόσβασης του χρήστη-θύματος είναι από τις πλέον διαδεδομένες μεθόδους επίθεσης. Βασίζεται στην αδυναμία του ανθρώπινου παράγοντα να διαλέξει κωδικούς πρόσβασης που είναι πραγματικά τυχαίοι. Σχεδόν σε όλες τις περιπτώσεις, οι κωδικοί πρόσβασης σημαίνουν κάτι για τον χρήστη και βασίζονται σε λέξεις. Ακόμη, ο ανθρώπινος παράγοντας υπάρχει σε μεγάλο βαθμό και στις απαντήσεις των ερωτήσεων ασφαλείας. Αυτά τα χαρακτηριστικά εκμεταλλεύονται οι κακόβουλοι χρήστες ώστε να μαντέψουν τον κωδικό πρόσβασης του θύματος ή τις απαντήσεις στις ερωτήσεις ασφαλείας του λογαριασμού του.

4.1. Εύκολοι κωδικοί πρόσβασης

Το πρώτο χαρακτηριστικό που εκμεταλλεύονται τα εργαλεία ανεύρεσης κωδικών πρόσβασης είναι το γεγονός ότι παρά το μεγάλο μήκος του, ο κωδικός πρόσβασης αποτελείται συχνά από λέξεις και αριθμούς. Σε μια τέτοια περίπτωση, το εργαλείο ανεύρεσης κωδικών πρόσβασης έχει ως πηγή πιθανών κωδικών μια μηχανή κατασκευής κωδικών που παράγει πιθανές λύσεις συνδυάζοντας λέξεις ενός λεξικού. Το μέγεθος του χώρου λύσεων που παράγεται από αυτή τη μέθοδο είναι αρκετά μικρό ώστε να μπορεί να ελεγχθεί σε μικρό χρονικό διάστημα. Καίτοι δεν εγγυάται την εύρεση του κωδικού, σε περίπτωση αποτυχίας συμφέρει τον επιτιθέμενο να αναζητήσει νέο θύμα που μπορεί να έχει εύκολο κωδικό πρόσβασης.

4.2. Κωδικοί μικρού μήκους – Εξαντλητική αναζήτηση

Ένα δεύτερο χαρακτηριστικό που καθιστά εύκολη την ανεύρεση ενός κωδικού πρόσβασης είναι το μικρό μήκος του. Το όριο μήκους από το οποίο ένας κωδικός πρόσβασης θεωρείται ασφαλής είναι ένα σχετικό μέγεθος που εξαρτάται από την τάξη μεγέθους της υπολογιστικής ισχύος που διαθέτουν οι σύγχρονες υπολογιστικές μηχανές. Σήμερα, το όριο αυτό βρίσκεται στους 8 χαρακτήρες. Ωστόσο, πολλές φορές παρατηρούνται χρήστες με κωδικούς ασφαλείας μήκους μέχρι και 5 ή 6 χαρακτήρων. Όταν ο κωδικός είναι τόσο μικρός, ο χώρος λύσεων όλων των πιθανών κωδικών μήκους 6 χαρακτήρων είναι αρκετά μικρός ώστε σε μικρό χρονικό διάστημα να μπορεί να ελεγχθεί εξαντλητικά. Επομένως, με εξαντλητική αναζήτηση ένας μικρός κωδικός πρόσβασης θα ανευρεθεί σίγουρα.

4.3. Εύκολες ερωτήσεις ασφαλείας

Άλλο ένα σημείο που αναδεικνύει την αδυναμία που οφείλεται στον ανθρώπινο παράγοντα είναι οι ερωτήσεις ασφαλείας. Σε κάθε λογαριασμό της διαδικτυακής πλατφόρμας, ο χρήστης ορίζει μία ή δύο ερωτήσεις προσωπικές που αφορούν συνήθως τον τόπο γέννησης, το όνομα του πρώτου κατοικίδιου και άλλα, για την περίπτωση ανάκτησης της πρόσβασης. Συχνά, όμως, επιλέγονται ερωτήσεις την απάντηση των οποίων γνωρίζουν αρκετά άτομα και εκτός του στενού κύκλου του χρήστη. Έτσι, κάποιος που γνωρίζει απλώς το θύμα, πιθανώς να γνωρίζει τις απαντήσεις στις ερωτήσεις ασφαλείας και να μπορεί να αποκτήσει πρόσβαση στο λογαριασμό, να μάθει τον κωδικό πρόσβασης, ακόμα και να τον αλλάξει.

5. Κοινωνική Μηχανική – Social Engineering

Η τελευταία μέθοδος επίθεσης εναντίον των λογαριασμών χρηστών της διαδικτυακής πλατφόρμας διαχείρισης βασίζεται στην εξαπάτηση του θύματος από τον επιτιθέμενο. Είναι μία από τις παλαιότερες αλλά και πλέον αποτελεσματικές επιθέσεις. Δεν χρησιμοποιεί υπολογιστικά εργαλεία αλλά βασίζεται εξολοκλήρου στις ικανότητες εξαπάτησης του επιτιθέμενου. Στην πλειονότητα των περιπτώσεων, γίνεται ένα τηλεφώνημα ή αποστέλλεται ένα email στο θύμα, στο οποίο ο θύτης εμφανίζεται ως υπεύθυνος ασφάλειας της διαδικτυακής πλατφόρμα, ζητεί να πραγματοποιήσει εργασίες συντήρησης στο λογαριασμό του χρήστη και, για τις οποίες χρειάζεται τα στοιχεία σύνδεσης του θύματος. Το θύμα πολύ συχνά εξαπατάται από την επικοινωνία και παρέχει τα στοιχεία στον επιτιθέμενο. Έτσι, πολύ εύκολα, ο επιτιθέμενος μπορεί να αποκτήσει τις πληροφορίες από το θύμα χωρίς τη χρήση υπολογιστικών εργαλείων ή εξειδικευμένων μεθόδων.

3.3.2. Τρόποι αντιμετώπισης

Οι επιθέσεις εναντίον των χρηστών της διαδικτυακής πλατφόρμας διαχείρισης λογαριασμού που αναλύθηκαν προηγουμένως μπορούν να αντιμετωπιστούν με χρήση κατάλληλων εργαλείων προστασίας σε συνδυασμό με ενημέρωση των τελικών χρηστών της υπηρεσίας. Στη συνέχεια, παρουσιάζονται όλα τα εργαλεία που βοηθούν στην άμυνα εναντίον τέτοιων επιθέσεων, καθώς και οι σωστές πρακτικές χρήσης των λογισμικών που χρησιμοποιούνται ήδη.

1. Χρήση σύγχρονων εκδόσεων λειτουργικού συστήματος και λογισμικού

Η ασφάλεια υπολογιστικών συστημάτων συχνά καταλήγει σε έναν αγώνα δρόμου ανάμεσα σε ομάδες κακόβουλων χρηστών, οι οποίοι ανακαλύπτουν ευπάθειες σε λογισμικά και λειτουργικά συστήματα, και σε προγραμματιστές που προσπαθούν το ταχύτερο δυνατό να διορθώσουν τα σφάλματα που οδηγούν στην ευπάθεια. Με την πάροδο του χρόνου, πολλές ευπάθειες γίνονται ευρέως γνωστές ενώ εργαλεία εκμετάλλευσής τους κυκλοφορούν ελεύθερα στο Διαδίκτυο. Έτσι, η παραβίαση του απαρχαιωμένου λογισμικού γίνεται τετριμμένη διαδικασία. Παράλληλα, όμως, οι προγραμματιστές λογισμικού διορθώνουν

τις ευπάθειες και αναβαθμίζουν το λογισμικό ενισχύοντας την ασφάλειά του. Επομένως, είναι πολύ σημαντικό οι χρήστες να χρησιμοποιούν τις τελευταίες εκδόσεις των λειτουργικών συστημάτων και των εφαρμογών που χρησιμοποιούν ώστε να διασφαλίζεται η μέγιστη ασφάλεια του συστήματός τους.

2. Χρήση εργαλείων anti-malware

Σε συνδυασμό με τη συνεχή ενημέρωση του λογισμικού που χρησιμοποιούν, οι χρήστες πρέπει χρησιμοποιούν εργαλεία που ενισχύουν την ασφάλεια του συστήματος στο οποίο εγκαθίστανται. Τέτοια εργαλεία είναι τα anti-malware, τα οποία προστατεύουν το σύστημα από όλα τα είδη κακόβουλου λογισμικού. Τα εργαλεία anti-malware παρακολουθούν σε πραγματικό χρόνο τις εργασίες του συστήματος ελέγχοντας τις διεργασίες που τρέχουν και τα προγράμματα που επιχειρούν να εγκατασταθούν. Στην περίπτωση όπου κάποιο από αυτά είναι ένα αναγνωρισμένο κακόβουλο λογισμικό, το εργαλείο αποτρέπει την εκτέλεση και εγκατάστασή του και το διαγράφει.

Επιπλέον, ένα εργαλείο anti-malware διαθέτει μηχανισμούς με τους οποίους ανιχνεύει ύποπτες αλληλουχίες κλήσεων συστήματος (system calls) από διεργασίες που εκτελούνται εκείνη τη στιγμή στο σύστημα ώστε να αναγνωρίζει πρότυπα δράσης κακόβουλων λογισμικών που δεν έχουν αναγνωριστεί προηγουμένως αλλά εμφανίζονται για πρώτη φορά. Προς αυτή την κατεύθυνση διατηρούν λεπτομερείς καταγραφές της συμπεριφοράς των διεργασιών που εκτελούνται τις οποίες, σε περίπτωση αναγνώρισης κακόβουλων ενεργειών από μια διεργασία, αποστέλλουν σε ειδικά εργαστήρια προκειμένου να ελεγχθεί το ύποπτο λογισμικό. Ακόμη, ένα λογισμικό anti-malware μπορεί να εγκατασταθεί σε ένα μολυσμένο σύστημα και να επιχειρήσει να εκκαθαρίσει το σύστημα από το κακόβουλο λογισμικό και από τυχόν μηχανισμούς που έχουν εισαχθεί στο λειτουργικό σύστημα με σκοπό την απόκρυψή του.

Τα εργαλεία anti-malware προστατεύουν το σύστημα ενός τελικού χρήστη, είτε είναι Η/Υ είτε κινητή συσκευή, ασφαλίζοντας όλα τα υποσυστήματά του που είναι πιθανοί στόχοι παραβίασης. Αυτό το πετυχαίνουν με τρόπο απόλυτα αυτοματοποιημένο και πλήρως ανεξάρτητο από τις γνώσεις του τελικού χρήστη σε θέματα ασφάλειας. Τα δύο αυτά χαρακτηριστικά καθιστούν τα anti-malware απαραίτητα εργαλεία για την ασφάλεια του τελικού χρήστη και των προσωπικών του δεδομένων.

3. Χρήση ασφαλών πρωτοκόλλων επικοινωνίας στο Διαδίκτυο

Η ραγδαία ανάπτυξη της πληροφορικής οδήγησε σε παράλληλη ανάπτυξη και τον τομέα της κρυπτογραφίας. Η επιστήμη της κρυπτογραφίας παρέχει εργαλεία με τα οποία μπορεί να διασφαλιστεί η επικοινωνία μεταξύ δύο κόμβων. Ως προς το Διαδίκτυο, σχεδόν όλα τα χρησιμοποιούμενα πρωτόκολλα του Διαδικτύου έχουν ασφαλείς εκδόσεις στις οποίες γίνεται χρήση κρυπτογραφικών μηχανισμών. Στην περίπτωση της διαδικτυακής πλατφόρμας διαχείρισης λογαριασμού ΗΕ, το βασικό πρωτόκολλο προς χρήση είναι το HTTPS που κάνει χρήση του πρωτοκόλλου ασφάλειας πληροφοριών TLS με στόχο να κρυπτογραφήσει και ασφαλίσει τις μεταδιδόμενες πληροφορίες. Χρησιμοποιώντας αλγορίθμους κρυπτογράφησης δημοσίου κλειδιού, το πρωτόκολλο HTTPS εγγυάται την εμπιστευτικότητα και ακεραιότητα των πληροφοριών. Ταυτόχρονα, μέσω της χρήσης ψηφιακών πιστοποιητικών, υπογεγραμμένων από ανεξάρτητη αρχή, εγγυάται στους χρήστες την πραγματική ταυτότητα του διακομιστή με τον οποίο επικοινωνούν.

Από τα προηγούμενα προκύπτει ότι εφόσον χρησιμοποιείται το πρωτόκολλο HTTPS και το ψηφιακό πιστοποιητικό είναι όντως υπογεγραμμένο από ανεξάρτητη αρχή και δηλώνει τον προβλεπόμενο παραλήπτη,

μια σύνδεση είναι ασφαλής έναντι επιθέσεων τύπου Man-In-The-Middle. Συχνά κατά την υλοποίηση επιθέσεων τέτοιου τύπου, ο επιτιθέμενος μπορεί να παρέμβει στη διαδικασία ανταλλαγής πιστοποιητικών και κλειδιών, επιστρέφοντας στο χρήστη-θύμα ένα πλαστό ψηφιακό πιστοποιητικό. Στην περίπτωση αυτή, το πιστοποιητικό δεν είναι υπογεγραμμένο από ανεξάρτητη αρχή αλλά υπογεγραμμένο από τον ίδιο τον επιτιθέμενο και εμφανίζεται από λογισμικά περιήγησης ως self-signed. Οι σύγχρονοι περιηγητές ελέγχουν τα πιστοποιητικά και σε περίπτωση self-signed πιστοποιητικού εμφανίζεται μήνυμα ειδοποίησης στο χρήστη. Σε κάθε περίπτωση, το πρωτόκολλο ασφάλειας HTTPS παρέχει ασφάλεια εναντίον επιθέσεων Man-In-The-Middle.

Ακριβώς με τον ίδιο τρόπο, κάνοντας δηλαδή χρήση των πιστοποιητικών, το πρωτόκολλο HTTPS προστατεύει από επιθέσεις ηλεκτρονικής «αλιείας» από ιστοσελίδες. Η ιστοσελίδα διαχείρισης λογαριασμού ΗΕ οφείλει να χρησιμοποιεί το πρωτόκολλο HTTPS για προστασία των δεδομένων. Μία ιστοσελίδα phishing που την μιμείται, είτε θα διαθέτει πλαστό πιστοποιητικό είτε θα χρησιμοποιεί το πρότυπο HTTP. Αν διαθέτει πλαστό πιστοποιητικό, τότε ο περιηγητής θα ειδοποιήσει το θύμα. Αν όμως χρησιμοποιείται το πρωτόκολλο HTTP δεν θα υπάρξει ειδοποίηση καθώς θεωρείται κανονική συμπεριφορά μιας ιστοσελίδας. Για να προστατευθεί από επιθέσεις ο χρήστης κάθε φορά πρέπει είτε να ελέγχει αν χρησιμοποιείται το πρωτόκολλο HTTPS είτε να εγκαταστήσει επέκταση στον περιηγητή η οποία επιβάλλει τη χρήση μόνο του πρωτοκόλλου HTTPS στο Διαδίκτυο. Η δεύτερη επιλογή προκρίνεται λόγω της αυτοματοποίησης και των πρόσθετων ειδοποιήσεων που προσφέρει στο χρήστη, καθώς θεωρεί ύποπτη τη συμπεριφορά μιας ιστοσελίδα που δεν επικοινωνεί μέσω HTTPS και ενημερώνει το χρήστη για το γεγονός αυτό.

4. Διαχείριση κωδικών πρόσβασης

Όπως έχει ήδη αναφερθεί, οι κωδικοί πρόσβασης αποτελούν σημαντική απειλή για την ασφάλεια του λογαριασμού ενός χρήστη καθώς σε αυτούς βασίζεται ο έλεγχος πρόσβασης σε όλες τις πληροφορίες που αποθηκεύονται στην πλατφόρμα διαχείρισης. Είναι απαραίτητο, λοιπόν, να προσδιοριστούν και υλοποιηθούν μέθοδοι ενίσχυσης της ασφάλειας που παρέχουν οι κωδικοί πρόσβασης.

4.1. Πολιτική αντικατάστασης κωδικών πρόσβασης

Ένας τρόπος ώστε να ενισχύεται ο βαθμός ασφάλειας που προσφέρει ο κωδικός πρόσβασης είναι να υλοποιηθεί μία πολιτική αντικατάστασής του ανά τακτά χρονικά διαστήματα. Συνήθως, η πολιτική αυτή επιβάλλεται από το διακομιστή ώστε να αναγκάζει το χρήστη να αλλάξει τον κωδικό που χρησιμοποιεί στο λογαριασμό του. Η μέθοδος αυτή συμβάλλει στην αντιμετώπιση επιθέσεων εξαντλητικής αναζήτησης, αφού ο κωδικός πρόσβασης αλλάζει ταχύτερα από το χρονικό διάστημα που χρειάζεται ο επιτιθέμενος για την εύρεση του κωδικού πρόσβασης.

Η συγκριμένη μέθοδος, όμως, θεωρείται πλέον ξεπερασμένη και χρησιμοποιείται μόνο συμπληρωματικά προς άλλες αποτελεσματικότερες μεθόδους ενίσχυσης της ασφάλειας των κωδικών πρόσβασης. Ο λόγος είναι ότι, πολύ συχνά οι χρήστες αλλάζουν τον κωδικό πρόσβασης, σε κάποιο σχεδόν όμοιο με τον προηγούμενο. Έτσι, αν ο επιτιθέμενος έχει υποκλέψει τον προηγούμενο κωδικό του χρήστη, είναι πολύ πιθανό να είναι σε θέση να προσδιορίσει αμέσως και το νέο κωδικό, αφού αυτός έχει ελάχιστες αλλαγές σε σχέση με τον προηγούμενο. Ακόμη, η συγκεκριμένη μέθοδος είναι αρκετά ενοχλητική για τους χρήστες, οι οποίοι καταλήγουν συχνά να θυμούνται τους παλαιούς κωδικούς και όχι τους νέους.

4.2. Εργαλεία διαχείρισης κωδικών πρόσβασης

Η χρήση εργαλείων διαχείρισης κωδικών πρόσβασης είναι ένας από τους πλέον ενδεδειγμένους τρόπους ενίσχυσης της ασφάλειας των κωδικών πρόσβασης. Η χρήση τους είναι αυτοματοποιημένη και προσφέρουν μέγιστο επίπεδο ασφάλειας. Η λειτουργία τους είναι απλή και ταυτόχρονα πολύ αποτελεσματική. Δημιουργούν στο σύστημα του χρήστη ένα κρυπτογραφημένο τμήμα όπου φυλάσσονται οι κωδικοί πρόσβασης για κάθε λογαριασμό που διαθέτει ο χρήστης σε υπηρεσίες του Διαδικτύου. Η πρόσβαση στο τμήμα αυτό απαιτεί τη χρήση ενός βασικού κωδικού πρόσβασης που ονομάζεται master password και εισάγεται στο λογισμικό ως κλειδί κρυπτογράφησης του τμήματος φύλαξης. Ο κωδικός αυτός πρέπει να είναι επαρκής σε μήκος, συνήθως πάνω από 10 χαρακτήρες, και να περιέχει τουλάχιστον έναν αριθμό και 1 ειδικό χαρακτήρα, ώστε να μην είναι δυνατό να παραβιαστεί από εργαλεία εξαντλητικής αναζήτησης. Στη συνέχεια, σε κάθε νέο λογαριασμό του χρήστη, το εργαλείο αναλαμβάνει να παραγάγει έναν πραγματικά τυχαίο κωδικό πρόσβασης, τον οποίο συνδέει με το λογαριασμό. Ο χρήστης χρειάζεται να θυμάται μόνο το master password. Κατ' αυτό τον τρόπο, οι κωδικοί πρόσβασης που χρησιμοποιούνται είναι εντελώς τυχαίοι και συνεπώς ασφαλείς απέναντι σε επιθέσεις εξαντλητικής αναζήτησης και λεξικού, και ταυτόχρονα ο χρήστης πρέπει να θυμάται μόνο ένα κωδικό πρόσβασης, αυτόν του εργαλείου διαχείρισης κωδικών.

4.3. Ταυτοποίηση δύο παραγόντων - Two-factor authorization

Η τελευταία μέθοδος ενίσχυσης της ασφάλειας των κωδικών είναι η two-factor authorization. Χρησιμοποιήθηκε αρχικά από τραπεζικά ιδρύματα για να ενισχύσουν την ασφάλεια στους λογαριασμούς e-banking. Και αυτή η μέθοδος αυξάνει σημαντικά την ασφάλεια με ελάχιστη επιβάρυνση του χρήστη. Το μόνο μικρό μειονέκτημα της μεθόδου σε σχέση με τους διαχειριστές κωδικών είναι ότι η συγκεκριμένη μέθοδος πρέπει να υποστηρίζεται από το διακομιστή της υπηρεσίας όπου διαθέτει λογαριασμό ο χρήστης.

Η λειτουργία του two-factor authorization είναι πολύ απλή. Αμέσως μετά την επιτυχή είσοδο του κωδικού πρόσβασης, η πλατφόρμα της υπηρεσίας ζητεί και ένα, συνήθως 6-ψήφιο, κωδικό από το χρήστη. Αυτός ο κωδικός αλλάζει ανά τακτά χρονικά διαστήματα της τάξης των 20s. Ο χρήστης μπορεί να λάβει αυτό τον κωδικό είτε από ειδική συσκευή που του έχει διατεθεί είτε από ειδική εφαρμογή στην έξυπνη κινητή του συσκευή. Έτσι, ακόμα και αν ένας κακόβουλος χρήστης έχει με επιτυχία υποκλέψει τον κωδικό πρόσβασης του θύματος, δεν μπορεί να γνωρίζει τον κωδικό του δεύτερου βήματος του two-factor authorization, και δεν προλαβαίνει να τον αναζητήσει εξαντλητικά μέχρι να παρέλθει η διάρκεια ισχύος του συγκεκριμένου κωδικού. Αυτή η μέθοδος είναι πολύ αποτελεσματική και διαδίδεται σταδιακά σε υπηρεσίες του Διαδικτύου, καθώς με επιτυχία εφαρμόζει το δόγμα της ασφάλειας πληροφοριών, σύμφωνα με το οποίο, για ασφαλή ταυτοποίηση ενός χρήστη, πρέπει να ζητείται κάτι που γνωρίζει ο χρήστης και κάτι που διαθέτει. Στη συγκεκριμένη περίπτωση, ο χρήστης γνωρίζει τον κωδικό πρόσβασης και διαθέτει τη συσκευή που αναγράφει τον κωδικό του two-factor authorization.

3.4. Μέθοδοι επίθεσης στο hardware των ευφυών μετρητών και αντίμετρα

Οι ευφυείς μετρητές διαθέτουν πληθώρα θυρών επικοινωνίας για όλα τα υποστηριζόμενα πρωτόκολλα. Διαθέτουν θύρες επικοινωνίας τοπικού δικτύου (LAN) ώστε να επικοινωνούν με άλλες συσκευές στο οικιακό τοπικό δίκτυο ακόμα και για να συνδέονται με το Default Gateway των οικιών ώστε να αποκτούν πρόσβαση στο Διαδίκτυο και να συνδέονται με το κέντρο διαχείρισης δεδομένων του διαχειριστή του δικτύου ΗΕ. Επιπλέον, διαθέτουν θύρες για φυσική πρόσβαση στο υλικό των μετρητών εκ μέρους των τεχνικών κλιμακίων της εταιρίας που διαχειρίζεται τους ευφυείς μετρητές, είτε σε περιπτώσεις βλάβης είτε σε περιπτώσεις τακτικής συντήρησης. Μέσω των θυρών, αυτών οι τεχνικοί έχουν τη δυνατότητα να ελέγξουν τις παραμέτρους λειτουργίας, να ανιχνεύσουν και να διορθώσουν ενδεχόμενα σφάλματα που δεν μπορούν να διορθωθούν μέσω απομακρυσμένης σύνδεσης.

Οι φυσικές θύρες, ωστόσο, παρέχουν έναν δίαυλο επικοινωνίας με τη συσκευή, τον οποίο συχνά εκμεταλλεύονται κακόβουλοι χρήστες για να παραβιάσουν τους ευφυείς μετρητές. Στη συνέχεια του κεφαλαίου παρουσιάζονται μέθοδοι επιθέσεων εναντίον ευφυών μετρητών μέσω των φυσικών θυρών και του υλικού τους, οι συνέπειές τους και τρόποι αντιμετώπισής τους.

3.4.1. Επίθεση στα πρωτόκολλα επικοινωνίας φυσικών θυρών των ευφυών μετρητών

Τα πρωτόκολλα επικοινωνίας που υλοποιούνται στις φυσικές θύρες των ευφυών μετρητών διαφέρουν μεταξύ Ευρώπης και Αμερικής. Στην Ευρώπη χρησιμοποιείται το πρωτόκολλο IEC 62056 [6], που προτυποποιεί την επικοινωνία φορητών συσκευών με τον ευφυή μετρητή μέσω σειριακής θύρας. Το πρωτόκολλο υποστηρίζει ημι-αμφίδρομη μετάδοση δεδομένων (half-duplex), πάνω από φυσικό στρώμα μετάδοσης που μπορεί να είναι είτε οπτική θύρα υπερύθρων είτε καλώδιο τύπου TP (Twisted Pair).

Στην Αμερική χρησιμοποιούνται τα πρωτόκολλα της οικογένειας ANSI C12. Σε αυτήν περιλαμβάνονται τα πρωτόκολλα C12.18, C12.19, C12.21, C12.22. Τα προαναφερθέντα πρωτόκολλα υποστηρίζουν τη μετάδοση δεδομένων, η δομή των οποίων ορίζεται στο πρωτόκολλο C12.19, μέσω της οπτικής θύρας υπερύθρων του αυτόματου μετρητή (C12.18) και της τηλεφωνικής γραμμής μέσω modem (C12.21). Ειδικότερα, το πρωτόκολλο C12.21 χρησιμοποιείται για απομακρυσμένη σύνδεση με τον ευφυή μετρητή μέσω των τηλεφωνικών γραμμών για τεχνικούς λόγους και για επικοινωνία με το κέντρο τιμολόγησης. Το πρωτόκολλο C12.22 εισάγει ένα επίπεδο αφαίρεσης πάνω από το φυσικό στρώμα διαχωρίζοντάς το από τα ανώτερα στρώματα του πρωτοκόλλου επιτρέποντας τη μετάδοση των δεδομένων πάνω από πολλούς τύπους δικτύων. Το πρωτόκολλο C12.22 είναι το μόνο από πρωτόκολλα της οικογένειας C12 που διαθέτει ολοκληρωμένη σχεδίαση ασφάλειας καθώς υλοποιεί κρυπτογράφηση AES.

Τα πρωτόκολλα C12.18 και C12.21 εμφανίζουν αρκετά κενά ασφαλείας τα οποία μπορούν πολύ εύκολα να εκμεταλλευτούν κακόβουλοι χρήστες. Επιπλέον, επειδή τα ανωτέρω πρωτόκολλα χρησιμοποιούνται από τις πρώτες γενιές ευφυών μετρητών που εγκαταστάθηκαν στις ΗΠΑ, υπάρχει ήδη μεγάλο σύνολο από πιθανούς στόχους για επιθέσεις ενάντια στα συγκεκριμένα πρωτόκολλα.

1. Ευπάθειες και επιθέσεις στο πρωτόκολλο C12.18

Το πρωτόκολλο C12.18 δεν περιλαμβάνει μηχανισμούς ασφάλειας των πληροφοριών που μεταδίδονται. Το μοναδικό στοιχείο που, ενδεχομένως, λειτουργεί αποτρεπτικά για τον κακόβουλο χρήστη είναι το ότι, λόγω της επικοινωνίας μέσω υπέρυθρων, πομπός και δέκτης βρίσκονται σε απόσταση περίπου 1m. Ωστόσο, αυτό σε καμία περίπτωση δεν είναι αρκετό ώστε το συγκεκριμένο πρωτόκολλο να θεωρείται ασφαλές προς χρήση και εγκατάσταση.

Στο C12.18, ο μόνος μηχανισμός που έχει εισαχθεί για την ταυτοποίηση του τεχνικού προσωπικού που επικοινωνεί με τον ευφυή μετρητή είναι ένας κωδικός πρόσβασης. Ο κωδικός πρόσβασης, όμως, δεν κρυπτογραφείται κατά τη μετάδοση αλλά μεταδίδεται αυτούσιος. Έτσι, ένας κακόβουλος χρήστης μπορεί να υποκλέψει με ένα δέκτη υπέρυθρων τη μετάδοση του κωδικού και να τον επαναλάβει στη συνέχεια, ώστε να αποκτήσει πρόσβαση στο μετρητή. Με τον ίδιο ακριβώς τρόπο μπορούν να υποκλαπούν και οι πληροφορίες που μεταδίδονται μεταξύ της συσκευής του τεχνικού προσωπικού και του μετρητή καθώς και αυτές μεταδίδονται αυτούσιες χωρίς κρυπτογράφηση.

Τα προαναφερθέντα συνηγορούν στο ότι το πρωτόκολλο C12.18 δεν πρέπει πλέον να χρησιμοποιείται από τους κατασκευαστές ευφυών μετρητών. Η παντελής έλλειψη μηχανισμών ασφάλειας οδήγησε στην ανάπτυξη νέων προτύπων όπως το C12.22. Ωστόσο, το γεγονός ότι το C12.22 δεν υποστηρίζει οπτικές θύρες, ωθεί κατασκευαστές να εγκαθιστούν το C12.18 σε ευφυείς μετρητές με οπτικές θύρες.

2. Ευπάθειες στο πρωτόκολλο C12.21

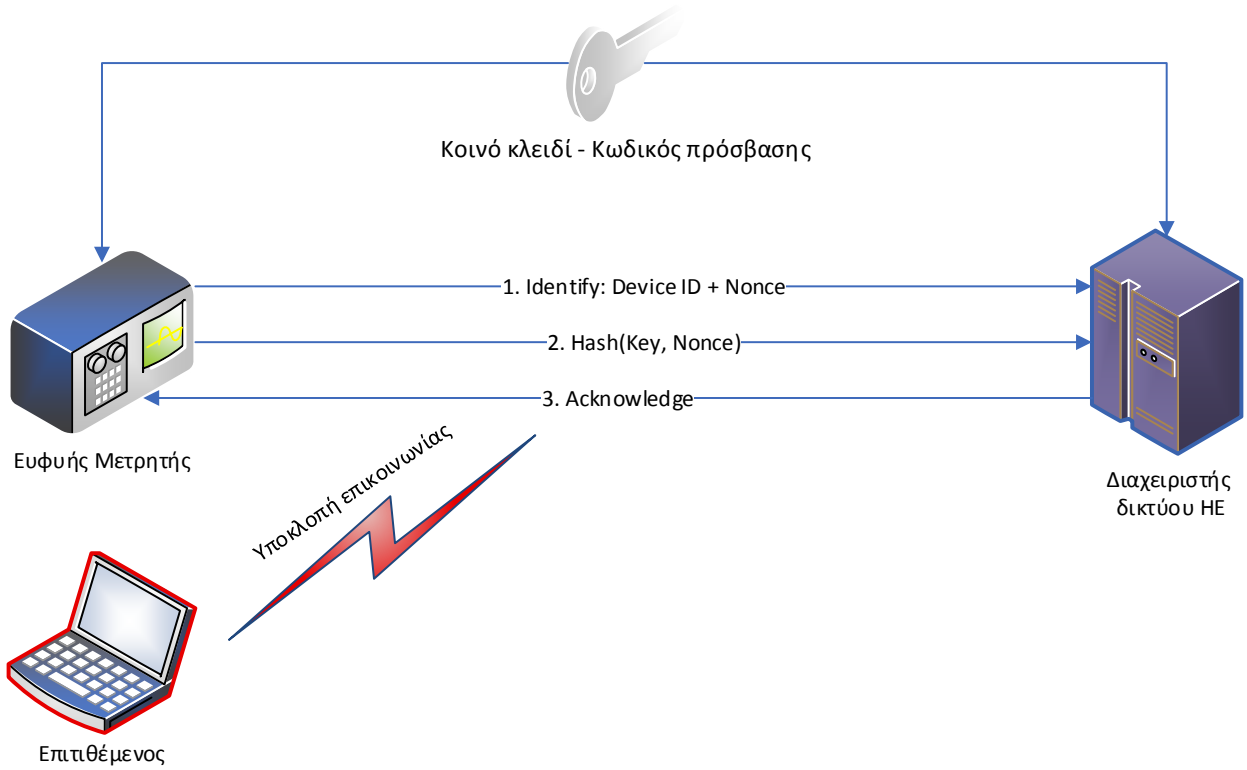
Καίτοι είναι μεταγενέστερο του C12.18, το πρωτόκολλο C12.21 έχει και αυτό αρκετές ελλείψεις σε θέματα ασφάλειας, με αποτέλεσμα και αυτό να μη θεωρείται ασφαλές. Ωστόσο, και αυτό το πρωτόκολλο με τη σειρά του είναι εγκατεστημένο στις πρώτες γενιές ευφυών μετρητών, ιδιαίτερα σε όσους μετρητές κατασκευάστηκαν πριν την υιοθέτηση του πρωτοκόλλου C12.22.

Στο πρωτόκολλο C12.21 η ταυτοποίηση του χρήστη που επικοινωνεί με τη συσκευή του μετρητή γίνεται με χρήση κωδικού πρόσβασης. Ο κωδικός πρόσβασης μεταδίδεται κρυπτογραφημένος, οπότε δεν μπορεί να υποκλαπεί κατά τη διαδρομή από τη συσκευή χρήστη στον ευφυή μετρητή. Ωστόσο, τα δεδομένα που ανταλλάσσονται στη συνέχεια ούτε είναι κρυπτογραφημένα ούτε προστατεύονται από μηχανισμούς που προστατεύουν από την αλλοίωση των δεδομένων. Αυτό έχει ως συνέπεια ένας επιτιθέμενος που παρακολουθεί την τηλεφωνική γραμμή να μπορεί να υποκλέψει τα δεδομένα. Ακόμη, εφόσον καταφέρει να παρευρεθεί στην τοπολογία του δικτύου ανάμεσα στη συσκευή του τεχνικού προσωπικού και τον ευφυή μετρητή, αποκτά τη δυνατότητα να αλλοιώνει τα δεδομένα που ανταλλάσσονται.

Ωστόσο, το σημαντικότερο, ίσως, κενό ασφαλείας του πρωτοκόλλου C12.21 βρίσκεται στη διαδικασία ταυτοποίησης του μετρητή στο διαχειριστή του δικτύου HE. Αυτό το κενό ασφαλείας καθιστά τη διαδικασία ευάλωτη σε επίθεση επανάληψης. Η διαδικασία αυτή έχει χρησιμοποιηθεί για να ταυτοποιηθεί ξένη συσκευή στο δίκτυο της εταιρίας HE, προσποιούμενη το μετρητή, και να μεταδώσει ψευδή στοιχεία κατανάλωσης [7] [8]. Στα Σχ. 3.3 και 3.4 φαίνεται η μεθοδολογία της συγκεκριμένης επίθεσης.

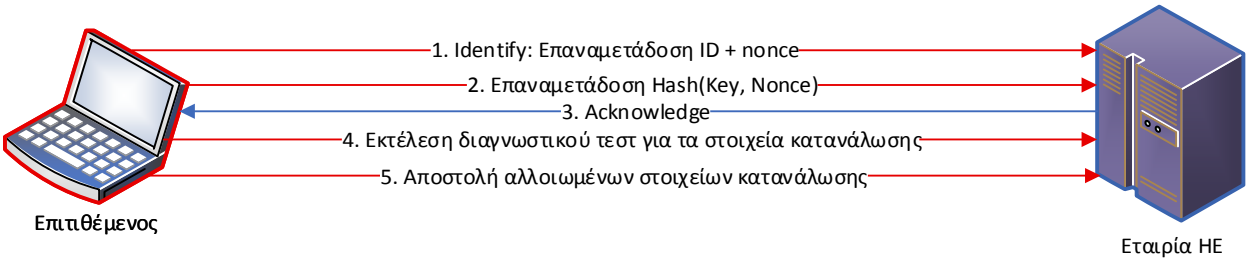
Το πρώτο βήμα είναι η υποκλοπή μιας αυθεντικής επικοινωνίας ταυτοποίησης μεταξύ μετρητή και διαχειριστή δικτύου HE από τον επιτιθέμενο. Σε μια τέτοια επικοινωνία, το πρώτο βήμα είναι η έναρξη της διαδικασίας ταυτοποίησης από τον ευφυή μετρητή. Σε αυτό το βήμα, ο μετρητής μεταδίδει το Device ID και ένα nonce (**n**umber used **once –** τυχαίος αριθμός που πρέπει να χρησιμοποιείται μόνο μία φορά). Στο δεύτερο βήμα, ο μετρητής αποστέλλει το nonce κρυπτογραφημένο με κλειδί κρυπτογράφησης που προέρχεται από

τον κωδικό πρόσβασης. Εφόσον όλα τα δεδομένα είναι ορθά ο διακομιστής του διαχειριστή του δικτύου ΗΕ απαντά με ένα μήνυμα acknowledge ώστε να ενημερώσει το μετρητή ότι έχει πλέον αποκατασταθεί η μεταξύ τους σύνδεση.



Σχήμα 3.3. Σχηματική απεικόνιση μιας αυθεντικής ταυτοποίησης του μετρητή με το διακομιστή του διαχειριστή του δικτύου ΗΕ και των δεδομένων που ανταλλάσσονται.

Το επόμενο βήμα βασίζεται στην αναμετάδοση από την πλευρά του επιτιθέμενου των πληροφοριών του μετρητή. Στο Σχήμα 3.3 φαίνεται η υλοποίηση της επίθεσης. Ο επιτιθέμενος εκκινεί τη διαδικασία ταυτοποίησής του με το διακομιστή του διαχειριστή του δικτύου ΗΕ. Επαναλαμβάνει το μήνυμα που έχει υποκλέψει από την προηγούμενη αυθεντική συνομιλία και το οποίο περιέχει αρχικά το Device ID και το ίδιο nonce. Στην συνέχεια, χωρίς να γνωρίζει τον κωδικό πρόσβασης άρα και το κλειδί κρυπτογράφησης, απλώς αναμεταδίδει το κρυπτογραφημένο μήνυμα που υπέκλεψε από την αυθεντική συνομιλία. Το κενό ασφαλείας που επιτρέπει το πρώτο σκέλος της επίθεσης είναι ότι το πρωτόκολλο δεν προβλέπει τον έλεγχο της μοναδικότητας του nonce που χρησιμοποιείται κάθε φορά που γίνεται ταυτοποίηση. Η χρησιμοποιούμενη μέθοδος ταυτοποίησης είναι ασφαλής μόνο όταν κάθε φορά χρησιμοποιείται διαφορετικό nonce από αυτά που έχουν χρησιμοποιηθεί σε όλες τις προηγούμενες. Στη συγκεκριμένη περίπτωση, δεν γίνεται έλεγχος για αυτό, οπότε ο επιτιθέμενος μπορεί να ταυτοποιηθεί με ένα ήδη χρησιμοποιημένο nonce. Τέλος, ο επιτιθέμενος ενεργοποιεί το διαγνωστικό εργαλείο που είναι προτυποποιημένο από το πρωτόκολλο ώστε να μπορέσει να αλλοιώσει τα στοιχεία κατανάλωσης. Αποστέλλει τα αλλοιωμένα στοιχεία στο κέντρο τιμολόγησης ολοκληρώνοντας την επίθεση. Το δεύτερο μέρος της επίθεσης που περιλαμβάνει την αποστολή ψευδών στοιχείων κατανάλωσης είναι εφικτό λόγω της απουσίας μηχανισμού εξασφάλισης της ακεραιότητας στα μηνύματα του πρωτοκόλλου.



Σχήμα 3.4. Σχηματική απεικόνιση των βημάτων μιας επιτυχημένης επίθεσης επανάληψης και αλλοίωσης στοιχείων με το πρωτόκολλο ANSI C12.21.

3.4.2. Επίθεση υποκλοπής από το δίαυλο δεδομένων της μητρικής πλακέτας (Data Bus Snooping)

Τα δεδομένα τα οποία εισάγονται μέσω των θυρών I/O της συσκευής μεταφέρονται στη μνήμη ή σε buffers της συσκευής για περαιτέρω χρήση από το λειτουργικό σύστημα. Η μεταφορά αυτή γίνεται μέσω του διαύλου δεδομένων. Συχνά, ο δίαυλος δεδομένων είναι σε τέτοια θέση επί της μητρικής πλακέτα ώστε ένας κακόβουλος χρήστης να είναι σε θέση με χρήση ειδικών ηλεκτρονικών συσκευών ή probes να ανιχνεύσει το σήμα και τα δεδομένα που μεταδίδονται [7]. Όμως, πρέπει να σημειωθεί ότι πρόκειται για μια δύσκολη στην υλοποίησή της επίθεση, καθώς απαιτεί άριστες γνώσεις ηλεκτρονικής, τη δυνατότητα να επέμβει ο επιτιθέμενος στο εσωτερικό της συσκευής του μετρητή και τη χρήση εξειδικευμένων probes. Ωστόσο, το δυνατό σημείο της επίθεσης αυτού του τύπου είναι το γεγονός ότι μπορεί σε αρκετές περιπτώσεις να καταρρίψει τη χρήση κρυπτογράφησης κατά τη μεταφορά δεδομένων από τις θύρες I/O προς τη μνήμη. Για παράδειγμα, το πρωτόκολλο ANSI C12.22 χρησιμοποιεί κρυπτογράφηση AES 256-bit. Για την αποκρυπτογράφηση των δεδομένων αυτά οδηγούνται πρώτα στο εξειδικευμένο chip αποκρυπτογράφησης AES και στη συνέχεια μεταφέρονται αποκρυπτογραφημένα στη μνήμη του συστήματος. Η μεταφορά από το chip αποκρυπτογράφησης στους buffers της συσκευής γίνεται μέσω του διαύλου δεδομένων. Συνεπώς, ο επιτιθέμενος μπορεί να υποκλέψει τα δεδομένα παρά το ότι η μετάδοσή τους προς τη συσκευή έγινε με χρήση δυνατής κρυπτογράφησης.

3.4.3. Επίθεση μέσω της θύρας JTAG (Joint Test Action Group)

Η θύρα JTAG (Joint Test Action Group) χρησιμοποιείται από τους κατασκευαστές ηλεκτρονικών συσκευών για να παρέχει μία διεπαφή με όλα τα υποσυστήματα της μητρικής πλακέτας. Χρησιμεύει ιδιαίτερα στη φάση του debugging των κυκλωμάτων που χρησιμοποιούνται στην πλακέτα και κατά τον ποιοτικό έλεγχο ηλεκτρονικών συσκευών. Η θύρα δεν έχει ακροδέκτες στο περίβλημα της συσκευής αλλά μόνο πάνω στην μητρική πλακέτα, κάτι που καθιστά δύσκολη την πρόσβαση σε αυτή. Επιπλέον, για τη χρήση της διεπαφής απαιτείται ειδικός ελεγκτής JTAG ώστε επιτευχθεί η επικοινωνία και η ανταλλαγή δεδομένων με τη συσκευή.

Η θύρα JTAG χρησιμοποιείται συχνά και από κακόβουλους χρήστες με σκοπό να ανακαλυφθούν τα επιμέρους συστήματα και κυκλώματα που απαρτίζουν τον μετρητή. Ο λόγος που επιλέγεται η συγκεκριμένη

διεπαφή είναι οι πολλές δυνατότητες που προσφέρει, από τις οποίες οι πλέον ενδιαφέρουσες για λόγους επίθεσης είναι οι εξής:

1. Παρέχει πρόσβαση στις λειτουργίες των επιμέρους κυκλωμάτων της μητρικής πλακέτας.
2. Επιτρέπει την ανάγνωση και αλλαγή των δεδομένων της μνήμης RAM.
3. Επιτρέπει την ανάγνωση και αλλαγή δεδομένων στη μη-πτητική μνήμη του μετρητή.

Οι ανωτέρω δυνατότητες που παρέχει η διεπαφή JTAG είναι πολύ χρήσιμες και για ενδεχόμενους κακόβουλους χρήστες. Για παράδειγμα, κάποιος μπορεί να αναγνωρίσει τα κυκλώματα που έχουν υλοποιηθεί στην πλακέτα από την λειτουργικότητά τους και να εξαγάγει πληροφορίες για επιμέρους διεργασίες που εκτελούνται από το υλικό. Ακόμη, μπορεί να εξερευνήσει τη λειτουργία των επιμέρους κυκλωμάτων με σκοπό να ανακαλύψει κάποια ευπάθεια, της οποίας η εκμετάλλευση να είναι επωφελής.

Ωστόσο, ακόμη σημαντικότερη για έναν κακόβουλο χρήστη είναι η λειτουργία της διεπαφής JTAG με την οποία πραγματοποιείται επέμβαση στις μνήμες του μετρητή. Ανάλογα με το είδος της μνήμης στην οποία επιχειρείται η επέμβαση προκύπτουν και τα αντίστοιχα αποτελέσματα. Μία ανάγνωση από τη μνήμη RAM επιτρέπει την εξαγωγή δεδομένων αποθηκευμένων από τις εφαρμογές που τρέχουν στον μετρητή. Ο κακόβουλος χρήστης μπορεί να αλλάξει τις τιμές σε επιλεγμένες θέσεις μνήμης και να διαπιστώσει πως επηρεάζεται η λειτουργία των εφαρμογών ώστε να ανακαλύψει το αποτύπωμά τους στην μνήμη RAM. Αυτή η διαδικασία μπορεί να οδηγήσει στην αλλαγή επιμέρους λειτουργιών του μετρητή. Για παράδειγμα, με την αλλαγή των δεδομένων σε ορισμένες θέσεις μνήμης του μετρητή ενδέχεται να αλλάξουν τα δεδομένα κατανάλωσης που στέλνει ο μετρητής στο κέντρο διαχείρισης δεδομένων. Ωστόσο, για να γίνει μια αλλαγή των δεδομένων της μνήμης RAM, με τη συσκευή σε λειτουργία, πρέπει να το επιτρέπει ο ελεγκτής του κυκλώματος της CPU.

Η πρόσβαση στα δεδομένα της μη-πτητικής μνήμης της συσκευής προσφέρει εναλλακτικές δυνατότητες σε έναν κακόβουλο χρήστη. Στη μη-πτητική μνήμη φυλάσσονται δεδομένα που αλλάζουν πολύ σπάνια και που είναι απαραίτητο να διατηρούνται στη συσκευή σε περιπτώσεις επανεκκίνησης. Παράδειγμα τέτοιων δεδομένων είναι το λειτουργικό σύστημα και το firmware του ευφυούς μετρητή. Επιπλέον, στη μη-πτητική μνήμη φυλάσσονται και δεδομένα ταυτοποίησης της συσκευής με το διαχειριστή του δικτύου ΗΕ αλλά και ταυτοποίησης των χρηστών στο σύστημα του μετρητή. Τέτοια δεδομένα είναι οι κωδικοί πρόσβασης των χρηστών και τα πιστοποιητικά ασφαλείας ή κλειδιά κρυπτογράφησης που χρησιμοποιούνται για την κρυπτογραφημένη και ασφαλή αποστολή δεδομένων στο διαχειριστή του δικτύου ΗΕ.

Μέσω της θύρας JTAG, ένας κακόβουλος χρήστης μπορεί να διαβάσει τα δεδομένα της μη-πτητικής μνήμης και να τα αποθηκεύσει σε εξωτερική συσκευή. Επίσης, είναι δυνατή η εγγραφή δεδομένων στη μη-πτητική μνήμη μέσω της διεπαφής JTAG. Αυτές οι δύο ενέργειες χρησιμοποιούνται από τους κακόβουλους χρήστες για δύο βασικούς λόγους. Αρχικά, γίνεται η μεταφορά των δεδομένων (dump) σε εξωτερική συσκευή και γίνεται reverse engineering στον κώδικα του firmware. Μόλις ανιχνευθεί η λειτουργία του firmware, επιχειρείται η αλλαγή τμημάτων του κώδικα προς όφελος του κακόβουλου χρήστη και η αλλαγμένη έκδοση εγγράφεται στη μη-πτητική μνήμη του μετρητή. Ακόμη, ο κακόβουλος χρήστης μπορεί μέσω reverse engineering να ανακαλύψει τις θέσεις στη μη-πτητική μνήμη όπου φυλάσσονται κωδικοί ασφαλείας και κλειδιά κρυπτογράφησης, να τα εξαγάγει και να τα χρησιμοποιήσει ώστε να συνδέεται με το διαχειριστή του δικτύου ΗΕ προσποιούμενος τον ευφυή μετρητή.

3.4.4. Επίθεση ψυχρής εκκίνησης (cold-boot)

Η επίθεση ψυχρής εκκίνησης είναι μία ακόμη μέθοδος απόσπασης των δεδομένων που είναι αποθηκευμένα στη μνήμη RAM. Μπορεί να εφαρμοστεί και σε μνήμες τεχνολογίας DRAM και σε μνήμες SRAM. Καίτοι οι δύο τύποι μνημών λειτουργούν με διαφορετικούς τρόπους, το κοινό βασικό τους χαρακτηριστικό είναι ότι με την απουσία τροφοδοσίας χάνονται τα δεδομένα που φυλάσσονται στη μνήμη. Εσφαλμένα θεωρείται ότι κρίσιμα δεδομένα μπορούν να κρατούνται στη RAM καθώς σε περίπτωση παραβίασης μπορεί να διακοπεί η τροφοδοσία και αυτά να χαθούν και επομένως να μην υποκλαπούν.

Ο λόγος είναι ότι η απώλεια των δεδομένων δεν συμβαίνει ακαριαία. Ο χρόνος διατήρησης των δεδομένων απουσία τροφοδοσίας επηρεάζεται από τις συνθήκες θερμοκρασίας που επικρατούν και τον τύπο της μνήμης. Συγκεκριμένα, με βαθιά ψύξη των κυκλωμάτων της μνήμης είναι δυνατή η διατήρηση των δεδομένων τους για αρκετό χρονικό διάστημα ώστε οι μνήμες να εισαχθούν σε ξεχωριστό σύστημα και να υποκλαπούν αποθηκευμένα δεδομένα, όπως κλειδιά κρυπτογράφησης που χρησιμοποιούνται από το μετρητή [9]. Ακόμη, μπορούν να αποσπαστούν τμήματα κώδικα τα οποία είναι αποθηκευμένα στη μνήμη RAM για λόγους instruction caching (διατήρηση στη μνήμη cache των εντολών προς εκτέλεση).

Η συγκεκριμένη μέθοδος, όμως, δεν είναι πάντα δυνατή και είναι δύσκολη στην υλοποίησή της καθώς ένας κακόβουλος χρήστης πρέπει να διαθέτει εξοπλισμό βαθιάς ψύξης για να την υλοποιήσει και να έχει πρόσβαση στο ολοκληρωμένο κύκλωμα της μνήμης RAM. Επιπλέον, η επίθεση ψυχρής εκκίνησης είναι αρκετά δυσκολότερο να υλοποιηθεί σε μικροελεγκτές. Ο λόγος είναι ότι στα συστήματα μικροελεγκτών η μνήμη RAM βρίσκεται στο ίδιο SoC (System on a Chip) με τη μονάδα επεξεργασίας και δε μπορεί να αποσπαστεί. Στην περίπτωση αυτή, μόνη επιλογή είναι η εκκίνηση από boot sector το οποίο έχει εισαχθεί στη μη-πτητική μνήμη ως αποτέλεσμα άλλης μεθόδου επίθεσης, ώστε να εκκινηθεί το σύστημα εκτελώντας κώδικα του κακόβουλου χρήστη. Κάτι τέτοιο όμως είναι ιδιαίτερα δύσκολο, ενώ είναι πολύ πιθανό ο κακόβουλος χρήστης να έχει απλούστερες εναλλακτικές για να αποσπάσει τα δεδομένα που στοχεύει.

3.4.5. Επιθέσεις πλευρικών καναλιών (side-channel attacks)

Η συγκεκριμένη ομάδα επιθέσεων στοχοποιεί τους αλγόριθμους κρυπτογράφησης που υλοποιούνται στον ευφυή μετρητή. Οι επιθέσεις αυτού του τύπου παρακάμπτουν τη θεωρητική ασφάλεια των αλγορίθμων κρυπτογράφησης και στοχεύουν σε ευπάθειες των υλοποιήσεων αυτών των αλγορίθμων στο hardware. Αυτό πραγματοποιείται μελετώντας τη μεταβολή πλευρικών σημάτων εισόδου και εξόδου από το ολοκληρωμένο κύκλωμα που πραγματοποιεί την κρυπτογράφηση. Πλευρικά σήματα ονομάζονται τα σήματα μεγεθών που επηρεάζονται από την ενέργεια που πραγματοποιείται στο ολοκληρωμένο κύκλωμα αλλά τα οποία δε χρησιμοποιούνται από αυτό για να μεταφέρουν κάποια πληροφορία. Τέτοια σήματα μπορούν να είναι η ισχύς που καταναλώνεται, οι εκπομπές ΗΜ κυμάτων, η χρονική καθυστέρηση στην απόκριση του ολοκληρωμένου κυκλώματος, ακόμα και ηχητικά κύματα που προέρχονται από αυτό.

Οι πρώτες υλοποιήσεις αυτού του είδους επίθεσης έγιναν με παρατήρηση της χρονικής καθυστέρησης στην απόκριση του αλγορίθμου RSA [10]. Συγκεκριμένα, ανάλογα με την τιμή σε κάθε bit του κλειδιού εκτελείται διαφορετικό τμήμα κώδικα με διαφορετική χρονική καθυστέρηση. Η σύγκριση πολλών εκτελέσεων του αλγορίθμου και των αντίστοιχων τιμών της καθυστέρησης της απόκρισης μπορεί να αποκαλύψει το κλειδί κρυπτογράφησης. Παρόμοια δεδομένα μπορούν να εξαχθούν μέσω ανάλυσης του ρεύματος που καταναλώνεται από το ολοκληρωμένο κύκλωμα κατά τους υπολογισμούς του αλγορίθμου [11], της ΗΜ

ενέργειας που εκπέμπεται από το ολοκληρωμένο κύκλωμα [12], και των ηχητικών κυμάτων που παράγονται αυτό [13].

Για την υλοποίηση των ανωτέρω επιθέσεων χρειάζεται εξοπλισμός ανίχνευσης των σημάτων των πλευρικών καναλιών, ο οποίος ανάλογα με την ευαισθησία που απαιτείται ενδέχεται να έχει υψηλό κόστος. Ωστόσο, μέθοδοι όπως η [13] μπορούν να πραγματοποιηθούν ακόμη και με μία έξυπνη κινητή συσκευή σε απόσταση 30cm από τη συσκευή-στόχο. Επομένως, τέτοιες επιθέσεις είναι αποτελεσματικές για την εξακρίβωση στοιχείων της εκτέλεσης του αλγορίθμου κρυπτογράφησης και σε αρκετές περιπτώσεις μπορούν να οδηγήσουν μέχρι και στην υποκλοπή του κλειδιού του αλγορίθμου RSA, που είναι θεμελιώδης για τους αλγόριθμους κρυπτογράφησης δημοσίου κλειδιού. Μία επιτυχημένη επίθεση τέτοιου είδους εναντίον των ευφυών μετρητών επιτρέπει στον επιτιθέμενο να παραβιάσει την κρυπτογράφηση που χρησιμοποιείται στην επικοινωνία με το κέντρο διαχείρισης δεδομένων, να «υφαρπάξει» την επικοινωνία, μέχρι και να εισάγει δικά του πακέτα στη σύνδεση χωρίς να γίνει αντιληπτός. Τέλος, είναι μια κατηγορία μεθόδων ιδιαίτερα διαδεδομένη λόγω του μικρού κόστους υλοποίησης, και στην οποία ανακαλύπτονται συνεχώς νέες επιθέσεις εναντίον συστημάτων που θεωρούνται ασφαλή [14].

3.4.6. Επιθέσεις έγχυσης σφαλμάτων (Fault Injection Attacks)

Οι επιθέσεις αυτής της κατηγορίας βασίζονται στην πρόκληση δυσλειτουργιών στη διάταξη του ευφυούς μετρητή μέσω επιβολής ακραίων συνθηκών περιβάλλοντος οι οποίες δημιουργούν σφάλματα που διαδίδονται μέσω της αλυσίδας υπολογισμών που πραγματοποιείται από το hardware, με σκοπό το τελικό αποτέλεσμα να είναι προς όφελος του επιτιθέμενου. Η διαφοροποίηση στις επιμέρους επιθέσεις γίνεται κυρίως με βάση τον τρόπο εισαγωγής των σφαλμάτων στην αλυσίδα υπολογισμών.

1. Επιθέσεις τύπου clock glitching και power glitching

Χαρακτηριστικά παραδείγματα τέτοιων επιθέσεων είναι οι επιθέσεις clock glitching και power glitching. Στην πρώτη, αλλοιώνεται το σήμα ρολογιού ώστε να δίνεται στο υλικό σήμα μεγαλύτερης συχνότητας από αυτό στο οποίο λειτουργεί κανονικά. Αυτό έχει ως συνέπεια να επέρχεται νέος κτύπος ρολογιού πριν ορισμένα κυκλώματα ολοκληρώσουν τη λειτουργία του τρέχοντος κύκλου. Με τον τρόπο αυτό αλλοιώνονται αρκετές από τις λειτουργίες του συστήματος, συχνά προς όφελος του επιτιθέμενου. Για παράδειγμα, αν στον επεξεργαστή σε αυτό τον κύκλο ρολογιού πρέπει να εκτελεστεί μια εντολή conditional jump, λόγω της αυξημένης συχνότητας ρολογιού, ενδέχεται μόνο να αυξηθεί ο program counter αλλά να μην πραγματοποιηθεί το jump οδηγώντας σε συνέχιση της ροής του προγράμματος σαν να είχαν ικανοποιηθεί οι προϋποθέσεις του conditional jump. Μπορεί, επομένως, ο επιτιθέμενος να παρακάμψει τμήματα κώδικα που εκτελούνται μετά από εντολές conditional jump, όπως η διαδικασία ταυτοποίησής του, απλά επηρεάζοντας το εσωτερικό ρολόι της μονάδας επεξεργασίας της διάταξης.

Το δεύτερο είδος τέτοιων επιθέσεων αφορά έγχυση λαθών μέσω της αλλοίωσης της ισχύος τροφοδοσίας του συστήματος. Συνήθως εφαρμόζονται ως αυξήσεις ή μειώσεις της ισχύος για μια χρονική διάρκεια έως 10 κύκλους ρολογιού. Η συγκεκριμένη μέθοδος επηρεάζει το κατώφλι των transistor του συστήματος με αποτέλεσμα ορισμένα από τα flip-flops να αλλάζουν κατάσταση εισάγοντας έτσι τα λάθη στο σύστημα. Η μέθοδος power glitching μπορεί να επηρεάσει και τη ροή εντολών σε ένα μικροεπεξεργαστή ή μικροελεγκτή

οδηγώντας σε σφάλματα στον κώδικα που εκτελείται. Ωστόσο, είναι δυσκολότερη στην εκτέλεσή της από την μέθοδο clock glitching καθώς είναι περισσότερες οι παράμετροι οι οποίες επηρεάζουν την επίθεση. Ενδεικτικά, οι παράμετροι που επηρεάζουν την έκβαση μιας επίθεσης με τη μέθοδο power glitching είναι το μέγεθος της ισχύος τροφοδοσίας, το χρονικό διάστημα εφαρμογής της έγχυσης λαθών στην ισχύ τροφοδοσίας και ο ρυθμός της αυξομείωσης της ισχύος ώστε να προκληθούν τα λάθη.

2. Επιθέσεις οπτικής έγχυσης λαθών (Optical fault induction attacks)

Οι επιθέσεις οπτικής έγχυσης λαθών αποτελούν ομάδα επιθέσεων που βασίζεται στο ότι αν ένα transistor φωτοεγχυθεί τότε οδηγείται σε αγωγή (κατάσταση on) [15]. Αυτό μπορεί να οδηγήσει σε λάθη κατά την εκτέλεση εντολών σε ολοκληρωμένα κυκλώματα στα οποία πραγματοποιείται η επίθεση. Ενδεικτικά, μπορούν να αλλαχθούν τα δεδομένα σε μνήμες τύπου SRAM [15], σε μνήμες EEPROM και FLASH [16], και να διαταραχθεί η ροή ελέγχου (control flow) σε κάποιους επεξεργαστές [15]. Ακόμη, επιθέσεις τέτοιου είδους μπορούν να πραγματοποιηθούν εναντίον ασφαλών ενσωματωμένων μνημών όπου φυλάσσονται κλειδιά κρυπτογράφησης, κρίσιμα τμήματα κώδικα και ευαίσθητα δεδομένα, με αποτέλεσμα την υποκλοπή των δεδομένων αυτών [17]. Με τον τρόπο αυτό, οι επιθέσεις έγχυσης λαθών είναι αποτελεσματικές εναντίον κρυπτογραφικών υπολογισμών που πραγματοποιούνται στο σύστημα.

3.5. Τρόποι αντιμετώπισης επιθέσεων στο hardware του ευφυούς μετρητή

Στο προηγούμενο εδάφιο αναλύθηκαν οι τρόποι με τους οποίους κακόβουλοι χρήστες μπορούν να παραβιάσουν έναν ευφυή μετρητή. Πολλές από τις επιθέσεις αυτές είναι ιδιαιτέρως επικίνδυνες καθώς μπορεί να οδηγήσουν στην υλοποίηση προγραμματιστικών εργαλείων για αυτόματη παραβίαση των ευφυών μετρητών. Τα εργαλεία αυτά είναι εύκολα στη χρήση ακόμη και από άτομα χωρίς ιδιαίτερες γνώσεις πληροφορικής. Για να εξασφαλιστεί, επομένως, η σωστή και εύρυθμη λειτουργία του Smart Grid, πρέπει το άκρο που αφορά στους καταναλωτές να είναι ασφαλισμένο. Η επιδίωξη για ασφάλεια των ευφυών μετρητών παρουσιάζει δυσκολίες οι περισσότερες των οποίων οφείλονται (i) στις διαφορετικές προδιαγραφές λειτουργίας και ασφάλειας των μοντέλων μετρητών που διατίθενται από τους κατασκευαστές και (ii) στο ότι ο ίδιος ο κάτοχος της συσκευής πρέπει να θεωρείται πιθανός κακόβουλος χρήστης. Στη συνέχεια, περιγράφονται μέθοδοι που είναι αποτελεσματικές για την προστασία των ευφυών μετρητών από επιθέσεις όπως αυτές που αναλύθηκαν προηγουμένως.

3.5.1. Διαχείριση πρωτοκόλλων επικοινωνίας ευφυών μετρητών

Στο προηγούμενο εδάφιο παρουσιάστηκαν κενά ασφαλείας που οφείλονται στον ελλιπή σχεδιασμό των πρωτοκόλλων επικοινωνίας και από κακές υλοποιήσεις αυτών. Χαρακτηριστικά παραδείγματα είναι τα

πρωτόκολλα ANSI C12.18 και C12.21. Τα προβλήματα αυτά μπορούν να αντιμετωπιστούν μέσω ενός κεντρικού σχεδιασμού για τα πρωτόκολλα που υλοποιούνται στους ευφυείς μετρητές.

Αρχικά, πρέπει να γίνει μελέτη του υπό σχεδιασμό πρωτοκόλλου και να δοθούν οι προδιαγραφές επιδόσεων και ασφάλειας για το πρωτόκολλο από τους διαχειριστές δικτύων ΗΕ. Στη συνέχεια, πρέπει να ακολουθήσει ένας ανοικτός διαγωνισμός όπου θα υποβληθούν όσες προτάσεις πληρούν τις προδιαγραφές που έχουν τεθεί, υπό την προϋπόθεση ο κώδικάς τους να είναι ανοικτός και προσβάσιμος σε όσους ενδιαφέρονται για τα πρωτόκολλα ευφυών μετρητών, όπως εταιρίες κατασκευής, διαχειριστές δικτύων ΗΕ, προμηθευτές ΗΕ και ιδιώτες, για έλεγχο. Στο τελευταίο μέρος αυτής της διαδικασίας οι χρήστες που συμμετέχουν σε αυτή την κοινότητα μπορούν να συγκρίνουν τον κώδικα των πρωτοκόλλων που έχουν υποβληθεί και στη συνέχεια να καταλήξουν στις επικρατέστερες προτάσεις. Τα πρωτόκολλα που πέρασαν τον πρώτο γύρο ελέγχων πρέπει εκ νέου να ελεγχθούν εξονυχιστικά για κενά ασφαλείας πριν καταλήξει ο διαγωνισμός στο τελικό πρωτόκολλο που θα υιοθετηθεί από όλες τις εταιρίες κατασκευής ευφυών μετρητών.

Η διαδικασία αυτή έχει ήδη πραγματοποιηθεί με επιτυχία κατά την προτυποποίηση του πρωτοκόλλου κρυπτογράφησης AES. Παρουσιάζει σημαντικά πλεονεκτήματα σε σχέση με τη σημερινή πολιτική κατά την οποία κάθε εταιρία κατασκευής διαθέτει ιδιόκτητη, κλειστού κώδικα, υλοποίηση του πρωτοκόλλου επικοινωνίας, που συχνά δεν είναι συμβατή με συσκευές άλλων εταιριών. Με μία διαδικασία όπως η προηγούμενη, οι εταιρίες δεν μπορούν να επιβάλλουν, μέσω του μεριδίου αγοράς τους, το δικό τους πρωτόκολλο αφού κριτές στο διαγωνισμό είναι όλα τα ενδιαφερόμενα μέρη και η διαδικτυακή κοινότητα. Το τελικό πρωτόκολλο στο τέλος της ανωτέρω διαδικασίας θα έχει περάσει τουλάχιστον δύο κύκλους ελέγχων από ειδικούς ασφάλειας, σχεδιαστές ανταγωνιστικών πρωτοκόλλων και μέλη της διαδικτυακής κοινότητας. Στόχος τους αποτελεί η εύρεση κενών ασφάλειας και ελαττωμάτων στο πρωτόκολλο. Κατά τη διάρκεια των ανωτέρω ελέγχων, όσα ελαττώματα εμφανιστούν διορθώνονται πριν το πρωτόκολλο επιλεχθεί. Με τον τρόπο αυτό, όταν γίνει η τελική επιλογή, το πρωτόκολλο θα είναι όσο το δυνατόν πιο ασφαλές.. Τέλος, το πρωτόκολλο θα υποστηρίζεται από όλες τις εταιρίες της αγοράς και όλες οι συσκευές θα είναι συμβατές μεταξύ τους.

Μέσω της διαδικασίας αυτής θα προκύψει ένα ασφαλές πρωτόκολλο, ελεγμένο σε πολύ μεγαλύτερο βαθμό σε σχέση με το αν ελεγχόταν στο πλαίσιο του σχεδιασμού του από μία μόνο εταιρία. Ακόμη και μετά την χρήση του σε πραγματικούς μετρητές, ο χρόνος που μεσολαβεί μέχρι την ανακάλυψη ενδεχόμενων νέων κενών ασφαλείας αναμένεται να είναι αισθητά μικρότερος λόγω του μεγαλύτερου αριθμού χρηστών του πρωτοκόλλου και ο χρόνος διόρθωσης να είναι αντίστοιχα μικρότερος διότι λόγω του ανοικτού κώδικα του πρωτοκόλλου, προτείνονται πολύ γρήγορα λύσεις και από τη διαδικτυακή κοινότητα. Όλα τα προαναφερθέντα αποτελούν βήματα προόδου συγκριτικά με το σημερινό καθεστώς των πρωτοκόλλων ευφυών μετρητών και συμβάλουν στη ταχεία και επαρκώς ελεγμένη υιοθέτηση τεχνολογιών του Smart Grid στα δίκτυα ΗΕ.

3.5.2. Φυσικό κλείδωμα και προστασία ευφυών μετρητών

Η πλειονότητα των επιθέσεων που αναλύθηκαν προηγουμένως προϋπέθεταν φυσική πρόσβαση στο εσωτερικό του ευφυούς μετρητή. Ακολουθώντας την ίδια λογική, ένα από τα πρώτα βήματα για την ασφάλεια έναντι επιθέσεων τέτοιου τύπου είναι η υλοποίηση μηχανισμών φυσικής ασφάλειας των μετρητών.

Ένα απλοϊκό παράδειγμα είναι αυτό μιας κλειδαριάς. Ωστόσο, σε περιπτώσεις όπως αυτή των ευφυών μετρητών, είναι απαραίτητοι περισσότερο σύνθετοι μηχανισμοί ασφάλειας. Αρχικά, θεωρείται δεδομένο ότι ο καταναλωτής σε καμία περίπτωση δεν θα χρειαστεί να αφαιρέσει το περίβλημα του μετρητή. Για το λόγο

αυτό, το περίβλημα δεν πρέπει να διαθέτει κανένα εμφανές σημείο αποσυναρμολόγησης. Ακόμη, κάθε ανίχνευση προσπάθειας αφαίρεσης του περιβλήματος πρέπει να θεωρείται επιθετική ενέργεια εναντίον του μετρητή με στόχο την παραβίασή του, και να υλοποιούνται από το λογισμικό του ευφυούς μετρητή ενέργειες για να προστατευτούν οι πληροφορίες που διαθέτει από ενδεχόμενη παραβίαση.

Τα προαναφερθέντα συνηγορούν στο ότι οι ευφυείς μετρητές χρειάζονται προστασία από ειδικό περίβλημα το οποίο, εκτός από φυσική προστασία, πρέπει να παρέχει και ανίχνευση φυσικών επιθέσεων. Τέτοια περιβλήματα έχουν στο εσωτερικό τους πολλά επικαλυπτόμενα ηλεκτρικά κυκλώματα. Μόλις ο επιτιθέμενος επιχειρήσει να ανοίξει ή να τρυπήσει το περίβλημα, προκαλούνται βραχυκυκλώματα καθώς κάποιοι αγωγοί πλέον εφάπτονται λόγω της παραμόρφωσης του περιβλήματος. Η ύπαρξη ενός βραχυκυκλώματος είναι αρκετή για να προειδοποιήσει επίθεση εναντίον της συσκευής. Το λογισμικού του ευφυούς μετρητή πρέπει συνεχώς να ελέγχει το συγκεκριμένο σήμα. Σε περίπτωση ενεργοποίησης, πρέπει (i) να ειδοποιούνται τα αντίστοιχα συστήματα του ευφυούς μετρητή και (ii) να ενεργοποιούνται οι μηχανισμοί ασφαλούς διαγραφής των ευαίσθητων πληροφοριών που φυλάσσονται στη συσκευή.

Περιβλήματα με τα χαρακτηριστικά που αναφέρθηκαν προηγουμένως μειώνουν σημαντικά την πιθανότητα μιας επιτυχημένης επίθεσης εναντίον του υλικού ενός ευφυούς μετρητή. Επίσης, λειτουργούν αποτρεπτικά για την πλειονότητα των κακόβουλων χρηστών που δεν διαθέτουν εξειδικευμένο εξοπλισμό που να επιτυγχάνει την παράκαμψη αυτών των μηχανισμών ασφάλειας. Ωστόσο, η φυσική προστασία ενός ευφυή μετρητή δεν μπορεί από μόνη της να εγγυηθεί την ασφάλειά του. Σε συνδυασμό με την φυσική ασφάλεια είναι αναγκαίο να υλοποιηθούν και μηχανισμοί ασφάλειας ίδιο το hardware του ευφυούς μετρητή ώστε να εξασφαλίζεται ο μέγιστος βαθμός ασφάλειας.

3.5.3. Ασφάλεια πρωτοκόλλου JTAG

Το πρωτόκολλο JTAG αποτελεί μια δίοδο εισόδου σε ένα σύστημα, η οποία αρκετά συχνά επιλέγεται από κακόβουλους χρήστες με σκοπό να αποσπάσουν πληροφορίες για το υλικό του μετρητή. Αυτού του είδους η εκμετάλλευση, όμως, δεν οφείλεται σε κενά ασφαλείας ή ευπάθειες του πρωτοκόλλου JTAG αλλά στην κανονική του λειτουργία. Προκειμένου να γίνει με ασφαλή τρόπο η τοποθέτηση της θύρας JTAG στους ευφυείς μετρητές, είναι αναγκαίο να υπάρξουν ορισμένες προσθήκες στο υλικό και ενδεχομένως να αφαιρεθούν κάποιες από τις λειτουργίες του πρωτοκόλλου.

Αρχικά, πρέπει να γίνεται έλεγχος κάθε χρήστη που επιχειρεί να χρησιμοποιήσει το πρωτόκολλο JTAG στη συσκευή του μετρητή. Για να γίνει αυτό είναι απαραίτητος ένας μηχανισμός ταυτοποίησης χρηστών, δηλαδή ένας μηχανισμός κρυπτογράφησης των δεδομένων που μεταφέρονται μεταξύ χρήστη και ελεγκτή JTAG, μία συνάρτηση κατακερματισμού για την ακεραιότητα των δεδομένων, όπως επίσης και ένα μυστικό κλειδί το οποίο χρησιμοποιείται για την ταυτοποίηση του χρήστη με τη συσκευή. Εφόσον ο χρήστης διαθέτει το μυστικό κλειδί, μπορεί να συνδεθεί με τον ελεγκτή JTAG και να χρησιμοποιήσει το πρωτόκολλο. Το κεντρικό chip του μηχανισμού ασφάλειας για το JTAG είναι το κύκλωμα κρυπτογράφησης. Για λόγους εξοικονόμησης χώρου, και συμμόρφωσης με τις προδιαγραφές χρονισμού του JTAG, δεν μπορούν να χρησιμοποιηθούν block αλγόριθμοι κρυπτογράφησης. Αντ’ αυτού προτιμώνται αλγόριθμοι κρυπτογράφησης ροής (stream ciphers) [18].

Με τη χρήση ενός μηχανισμού όπως ο προηγούμενος, προκειμένου να χρησιμοποιήσει τη θύρα JTAG κάποιος χρήστης είναι απαραίτητο να γνωρίζει το μυστικό κλειδί κρυπτογράφησης που χρησιμοποιείται από τον ελεγκτή JTAG. Το μειονέκτημα του ανωτέρω μηχανισμού είναι το αυξημένο κόστος του ελεγκτή JTAG και ο επιπλέον χώρος που θα καταλάβουν τα κυκλώματα κρυπτογράφησης και κατακερματισμού στην πλακέτα.

3.5.4. Ασφάλεια συσκευής έναντι επιθέσεων υποκλοπής στο δίαυλο δεδομένων

Η υποκλοπή δεδομένων από το δίαυλο δεδομένων μιας συσκευής είναι μία από τις πλέον δύσκολες μεθόδους απόσπασης δεδομένων από έναν ευφυή μετρητή αφού προϋποθέτει πλήρη πρόσβαση στο εσωτερικό του και χρήση εξειδικευμένων αισθητήρων για την ανίχνευση των σημάτων στο δίαυλο δεδομένων. Οι βασικές μέθοδοι προστασίας έναντι τέτοιων επιθέσεων είναι δύο. Η πρώτη μέθοδος είναι να μην είναι ο δίαυλος δεδομένων προσβάσιμος από τους αισθητήρες. Η δεύτερη μέθοδος είναι η κρυπτογράφηση των δεδομένων που μεταφέρονται μέσω του διαύλου δεδομένων. Κάθε μία από τις μεθόδους εμφανίζει πλεονεκτήματα και μειονεκτήματα, οπότε η τελική επιλογή είναι ζήτημα πολιτικής του κατασκευαστή του υλικού.

Ο αποτελεσματικότερος τρόπος να γίνει η απόκρυψη του διαύλου δεδομένων είναι να χρησιμοποιηθεί αρχιτεκτονική μικροελεγκτή. Σε αυτή την περίπτωση, όλες οι επιμέρους διατάξεις του κυκλώματος όπως η μονάδα επεξεργασίας, οι μνήμες και οι θύρες εισόδου/εξόδου είναι όλες στο ίδιο chip. Υπάρχει απευθείας εσωτερική σύνδεση των κυκλωμάτων χωρίς τη χρήση διαύλου δεδομένων. Αυτό έχει ως συνέπεια στο εξωτερικό του ολοκληρωμένου κυκλώματος να μην είναι ορατοί και προσβάσιμοι κόμβοι από όπου ένας αισθητήρας να μπορεί να ανιχνεύσει το σήμα. Με αυτό το δομικό τρόπο, η αρχιτεκτονική μικροελεγκτή προστατεύει από επιθέσεις υποκλοπής δεδομένων από τον κεντρικό δίαυλο.

Η δεύτερη μέθοδος βασίζεται στην κρυπτογράφηση των δεδομένων που μεταδίδονται στο δίαυλο. Οι περισσότερες προτάσεις για τέτοιου είδους μηχανισμούς προϋπέθεταν εξειδικευμένο κύκλωμα στο υλικό, με αυξητική επίπτωση στο κόστος κατασκευής των μετρητών. Ωστόσο, έχουν προταθεί και μέθοδοι υλοποίησης της τεχνικής αυτής στο επίπεδο του λειτουργικού συστήματος [19]. Συγκεκριμένα, ορίζονται στο λειτουργικό σύστημα οι διεργασίες για τις οποίες απαιτείται ασφαλής μεταφορά δεδομένων. Με τις κατάλληλες προσθήκες στους μηχανισμούς εικονικής μνήμης και σελιδοποίησης του λειτουργικού συστήματος, όσα δεδομένα οδηγούνται από την cache στην μνήμη οδηγούνται πρώτα στον επεξεργαστή για κρυπτογράφηση και στη συνέχεια αποθηκεύονται. Ο συγκεκριμένος μηχανισμός δεν απαιτεί επιπλέον hardware καθώς η κρυπτογράφηση γίνεται σε ειδικού σκοπού κυκλώματα που διαθέτουν όλοι οι σύγχρονοι επεξεργαστές. Μόνη προϋπόθεση είναι ορισμένες εξειδικευμένες λειτουργίες του ελεγκτή της μνήμης cache οι οποίες, ωστόσο, υλοποιούνται από τα περισσότερα μοντέλα επεξεργαστών. Σημαντικό πλεονέκτημα της μεθόδου αποτελεί το μηδενικό επεξεργαστικό overhead για απλές διεργασίες καθώς για αυτές δεν γίνεται κρυπτογράφηση δεδομένων, ενώ ακόμα και για τις ασφαλείς διεργασίες το overhead που προκαλεί η κρυπτογράφηση είναι της τάξης του 37% [19].

3.5.5. Μέθοδοι ασφάλειας εναντίον επιθέσεων πλευρικών καναλιών

Οι επιθέσεις πλευρικών καναλιών βασίζονται στην ανάλυση σημάτων του συστήματος που επηρεάζονται εμμέσως από τους υπολογισμούς πάνω σε ευαίσθητα δεδομένα. Παραδείγματα είναι η ανάλυση της κατανάλωσης ισχύος κατά τη λειτουργία του μηχανισμού κρυπτογράφησης, τη μελέτη της χρονικής

καθυστέρησης των κυκλωμάτων καθώς και τη μελέτη των ακουστικών κυμάτων που εκπέμπονται κατά την λειτουργία συγκεκριμένων ολοκληρωμένων κυκλωμάτων.

Οι μέθοδοι για την αντιμετώπιση των συγκεκριμένων επιθέσεων κινούνται σε δύο άξονες. Ο πρώτος είναι η όσο το δυνατό μεγαλύτερη ανεξαρτητοποίηση του σήματος των πλευρικών καναλιών από τα δεδομένα που διαχειρίζεται το κύκλωμα. Συγκεκριμένα, σε ό,τι αφορά τη μελέτη χρονικής καθυστέρησης, τα σύγχρονα σχέδια ολοκληρωμένων κυκλωμάτων, όπως ο μηχανισμός κρυπτογράφησης, υλοποιούνται με σχεδίαση που προβλέπει την ίδια χρονική καθυστέρηση ανεξάρτητα από τα δεδομένα εισόδου.

Ως προς το πλευρικό κανάλι της ισχύος που καταναλώνεται από το κύκλωμα, έχουν προταθεί συνδεσμολογίες πυλών που εισάγουν πρόσθετες φάσεις σε ένα κύκλο ρολογιού ώστε η κατανάλωση ισχύος να είναι ανεξάρτητη των δεδομένων υπολογισμού. [20] [21]. Αυτό έχει ως συνέπεια να αυξάνεται ραγδαία το μέγεθος του δείγματος σημάτων που απαιτείται για να πραγματοποιηθεί μια επίθεση σε επίπεδα που την καθιστούν αδύνατη. Ωστόσο, πρέπει να σημειωθεί ότι το κόστος σε χώρο στην πλακέτα, σε απαιτήσεις ισχύος και σε καθυστέρηση είναι της τάξης του 3x, κάτι που καθιστά ιδιαίτερα ακριβή λύση τις συνδεσμολογίες αυτές. Για το λόγο αυτό, οι συνδεσμολογίες τέτοιου είδους χρησιμοποιούνται μόνο σε επιλεγμένα κυκλώματα τα οποία αποτελούν τους συχνότερους στόχους επίθεσης σε ένα σύστημα.

Ο δεύτερος άξονας στον οποίο κινούνται οι μέθοδοι αντιμετώπισης των επιθέσεων πλευρικών καναλιών είναι η απόκρυψη είτε του ίδιου του σήματος του πλευρικού καναλιού είτε των δεδομένων εισόδου, ώστε είτε ο επιτιθέμενος να μην μπορεί να το ανιχνεύσει είτε, αν το ανιχνεύσει, αυτό να μην έχει προκύψει από τα δεδομένα εισόδου. Η απλούστερη εφαρμογή της ανωτέρω στρατηγικής είναι στα ακουστικά πλευρικά κανάλια όπου τις περισσότερες φορές χρησιμοποιείται ειδικό ηχομονωτικό περίβλημα ώστε να μην είναι δυνατή η ανίχνευση όποιου ηχητικού σήματος παράγεται. Επίσης, μπορούν να χρησιμοποιηθούν κυκλώματα παραγωγής θορύβου ώστε να μειωθεί το SNR του σήματος του πλευρικού καναλιού σε επίπεδο που επιτιθέμενος να μη μπορεί να ανιχνεύσει το πραγματικό ηχητικό σήμα.

3.5.6. Ακεραιότητα της μνήμης

Οι τεχνικές που αναλύονται στη συνέχεια αφορούν την ακεραιότητα των δεδομένων που φυλάσσονται στις μνήμες ενός ευφυούς μετρητή. Είναι μηχανισμοί που αποσκοπούν στο να εξασφαλίσουν ότι τα δεδομένα που εγγράφονται και διαβάζονται από και προς τις μνήμες του μετρητή δεν έχουν αλλοιωθεί ως αποτέλεσμα κάποια παραβίασης της συσκευής. Τέτοιες παραβιάσεις μπορούν να προκύψουν είτε από επιθέσεις στο υλικό της συσκευής, όπως οι επιθέσεις έγχυσης λαθών, είτε από επιθέσεις στο λογισμικό του μετρητή, όπως μια trojan διεργασία (δούρειος ίππος) που αλλοιώνει τα δεδομένα άλλων διεργασιών στο σύστημα.

Τα κεντρικά εργαλεία που χρησιμοποιούνται από τους μηχανισμούς ακεραιότητας της μνήμης είναι οι συναρτήσεις κατακερματισμού (hash functions). Η κεντρική ιδέα πίσω από τους μηχανισμούς αυτούς είναι ότι για κάθε block δεδομένων στη μνήμη αποθηκεύεται και ένας κωδικός MAC (Message Authentication Code) που προκύπτει από τον κατακερματισμό του block από μία συνάρτηση κατακερματισμού που δέχεται ως είσοδο και ένα μυστικό κλειδί. Έτσι, αν ο επιτιθέμενος επιχειρήσει να αλλάξει τα δεδομένα, δεν γνωρίζει το μυστικό κλειδί και ως εκ τούτου δε μπορεί να υπολογίσει το νέο κωδικό MAC, παρά μόνο να τον μαντέψει. Έτσι, όταν ο επεξεργαστής ζητήσει τα δεδομένα και ελέγξει τον κωδικό MAC και διαπιστώσει ότι δεν είναι ο σωστός συμπεραίνει ότι τα δεδομένα έχουν αλλοιωθεί και τα απορρίπτει. Όμως το αλγοριθμικό κόστος των αναγκαίων κρυπτογραφικών υπολογισμών είναι αρκετά υψηλό.

Για το λόγο αυτό γίνεται χρήση ειδικών συναρτήσεων κατακερματισμού όπως οι multi-set hash functions [22] και ιδιοτήτων όπως η αυξησιμότητα (incrementality) [23]. Ο λόγος χρήσης των ανωτέρω εργαλείων είναι

να μειωθεί ο φόρτος από τον κατακερματισμό των δεδομένων, ώστε, από ανάλογος του όγκου των δεδομένων που κατακερματίζονται, να γίνει ανάλογος της διαφοράς μεταξύ των νέων δεδομένων και των προηγούμενων. Αυτό μειώνει αισθητά το χρόνο υπολογισμού της τιμής κατακερματισμού. Ως αποτέλεσμα, έχουν δημιουργηθεί μηχανισμοί με βάση τα ανωτέρω εργαλεία [24] [25] [26] που συνεχώς μειώνουν το υπολογιστικό κόστος που απαιτείται για τον έλεγχο της ακεραιότητας των δεδομένων.

3.5.7. Εμπιστευτικότητα κλειδιών κρυπτογράφησης

Η λειτουργία όλων σχεδών των μηχανισμών ασφάλειας ενός υπολογιστικού συστήματος εν γένει, και των ευφυών μετρητών εν προκειμένω, βασίζονται σε αλγορίθμους κρυπτογράφησης και κατακερματισμού. Οι αλγόριθμοι κρυπτογράφησης με τη σειρά τους προϋποθέτουν την ύπαρξη ενός κλειδιού γνωστού μόνο στο λογισμικού του μετρητή και στα εξουσιοδοτημένα συστήματα που επικοινωνούν με τους ευφυείς μετρητές. Συνήθως, τα κλειδιά αυτά φυλάσσονται στη μη πτητική μνήμη του ευφυούς μετρητή και είναι στόχος πολλών από τις επιθέσεις που προαναφέρθηκαν.

Κρίσιμο ζήτημα για την ασφάλεια των ευφυών μετρητών και των επικοινωνιών τους με τα συστήματα του Smart Grid αποτελεί το κατά πόσο τα κλειδιά κρυπτογράφησης μπορούν να παραμείνουν κρυφά. Πολλές μέθοδοι έχουν προταθεί με πλέον υποσχόμενη τη χρήση ειδικών κυκλωμάτων που ονομάζονται PUF (Physically Unclonable Function) [27]. Κύριο χαρακτηριστικό αυτών των κυκλωμάτων είναι πως παράγουν δεδομένα βάσει ενδογενούς τυχαιότητας ώστε να μην μπορεί η έξοδός τους να προβλεφθεί. Ακόμη, η τυχαιότητα προκύπτει από κατασκευαστικά χαρακτηριστικά ώστε σε περίπτωση απόπειρας παραβίασης του κυκλώματος να αλλοιώνεται η διαδικασία παραγωγής δεδομένων με αποτέλεσμα να μην αποκτά την πληροφορία ο επιτιθέμενος [28].

Τα κυκλώματα PUF χωρίζονται σε δύο βασικές κατηγορίες, τα ασθενή PUF (Weak PUF) και τα ισχυρά PUF (Strong PUF). Η διαφορά τους έγκειται στο πλήθος τυχαίων δεδομένων που παράγουν. Τα ασθενή PUF παράγουν συγκεκριμένα δεδομένα σε κάθε εξοδό τους. Τα ισχυρά PUF δεδομένα εισόδου βάσει των οποίων παράγουν τα δεδομένα εξόδου. Τα ζεύγη εισόδου εξόδου που παράγονται από τα ισχυρά PUFs είναι πολλά σε αριθμό. Στους ευφυείς μετρητές χρήσιμα είναι τα ασθενή PUF και μια υποκατηγορία των ισχυρών PUF που ονομάζονται ελεγχόμενα PUF (Controlled PUF) [29]. Τα ελεγχόμενα PUF παρέχουν στο hardware μια διεπαφή μέσω τις οποίας δέχονται ερωτήματα.

Στην περίπτωση της χρήσης ενός ασθενούς PUF τα δεδομένα που παράγονται από το PUF χρησιμοποιούνται για την παραγωγή των κλειδιών κρυπτογράφησης. Με δεδομένο ότι το PUF παράγει τα ίδια δεδομένα κάθε φορά τα οποία όμως είναι άγνωστα και απρόβλεπτα για κάθε επιτιθέμενο τα κλειδιά που παράγονται είναι ασφαλή. Στην περίπτωση χρήσης ελεγχόμενων PUF, αν υποτεθεί ότι μόνο τα εξουσιοδοτημένα συστήματα διαθέτουν κάποια αρχικα ζεύγη εισόδου-εξόδου γνωστά κατά τη διαδικασία κατασκευής, τότε μπορούν αποστέλλοντας την είσοδο και την αναμενόμενη έξοδο να ταυτοποιηθούν. Ακόμη, μπορούν να ανανεώνουν τη λίστα ζευγών τους αφού μόλις ταυτοποιηθούν έχουν τη δυνατότητα να ερωτούν το PUF για νέα ζεύγη εισόδου-εξόδου. Ωστόσο, κάθε ζεύγος μπορεί να χρησιμοποιηθεί μόνο μια φορά για ταυτοποίηση.

Συμπερασματικά, με τη χρήση των PUF είναι δυνατή η αποφυγή της χρήσης της μη πτητικής μνήμης για την αποθήκευση των κλειδιών κρυπτογράφησης του ευφούς μετρητή γεγονός που εγκυμονούσε αρκετούς κινδύνους. Ακόμη, εξ' ορισμού τους τα PUF δεν μπορούν να προβλεφθούν από κάποιον επιτιθέμενο. Τέλος, υφίστανται PUF τα οποία σε περίπτωση φυσικής παραβίασης αλλοιώνεται το χαρακτηριστικό που προσδίδει

την τυχαιότητα, ουσιαστικά καταστρέφοντας τα κλειδιά κρυπτογράφησης πριν αυτά υποκλαπούν από τον επιτιθέμενο. Τα ανωτέρω πλεονεκτήματα τα καθιστούν ιδανική λύση για τη φύλαξη κλειδιών κρυπτογράφησης στους ευφυείς μετρητές.

3.5.8. Παρακολούθηση της ροής πληροφοριών

Η τεχνική της παρακολούθησης της ροής πληροφοριών είναι ιδιαίτερα αποτελεσματική έναντι επιθέσεων που περιλαμβάνουν την εισαγωγή κακόβουλου κώδικα και εκτέλεσή του από το μετρητή. Είναι μία τεχνική που μπορεί να αποτρέψει επιθέσεις ακόμα και όταν δεν είναι γνωστή η μεθοδολογία τους (zero-day attacks) επειδή ασφαλίζει έναντι κακόβουλων δεδομένων που ενδεχομένως εισαχθούν στον ευφυή μετρητή.

Η τεχνική αυτή βασίζεται στη σήμανση των δεδομένων που εισάγονται στο μετρητή. Ο διαχειριστής του μετρητή διαχωρίζει τα κανάλια εισόδου δεδομένων, όπως τις φυσικές θύρες επικοινωνίας και το δίκτυο, σε ασφαλή και μη ασφαλή. Η έννοια της μη ασφαλούς θύρας είναι ότι ένας κακόβουλος χρήστης μπορεί να έχει χρησιμοποιήσει αυτή τη θύρα για να εισαγάγει κακόβουλα δεδομένα στη συσκευή. Οι πληροφορίες που εισάγονται από τις θύρες εισόδου έχουν ένα bit που καταδεικνύει αν είναι από ασφαλή ή μη ασφαλή θύρα. Στη συνέχεια, αυτή η σήμανση ακολουθεί τη ροή των πληροφοριών και διατηρείται για όσο διατηρούνται οι πληροφορίες. Αν ως αποτέλεσμα ενός υπολογισμού έχουν χρησιμοποιηθεί δεδομένα μη ασφαλή, τότε και το αποτέλεσμα του υπολογισμού σημαίνεται ως μη ασφαλές.

Η τεχνική βασίζεται στα διαφορετικά δικαιώματα ανάλογα με τη σήμανση των δεδομένων στη μνήμη. Για παράδειγμα, ο επεξεργαστής δεν επιτρέπεται να τρέξει κώδικα από ο οποίος έχει σήμανση μη ασφαλούς πληροφορίας. Με τον τρόπο αυτό, αποτρέπονται σχεδόν όλες οι απόπειρες επιθέσεων τύπου buffer overflow, καθώς ο κώδικας που έχει εισαγάγει ο επιτιθέμενος ως δεδομένα στο μετρητή έχει σήμανση μη ασφαλούς πληροφορίας. Έτσι, ακόμα και αν ο επιτιθέμενος καταφέρει να οδηγήσει την εκτέλεση σε εκείνο το τμήμα της μνήμης, ο επεξεργαστής δεν θα εκτελέσει το μη ασφαλή κώδικα. Ακόμη, μπορεί να σχεδιαστεί το λειτουργικό σύστημα ώστε κρίσιμες διεργασίες να μη μπορούν χρησιμοποιήσουν μη ασφαλή δεδομένα. Για παράδειγμα, αν με κάποιο τρόπο ο επιτιθέμενος έχει αλλοιώσει τα δεδομένα της διεργασίας μέτρησης, εφόσον ο μηχανισμός ελέγχου ροής πληροφοριών λειτουργεί σωστά μπορεί να αντιληφθεί την επίθεση και να μην αποστείλει τα αλλοιωμένα στοιχεία κατανάλωσης.

Το μεγαλύτερο πλεονέκτημα της συγκεκριμένης τεχνικής είναι το ότι παρέχει υψηλά επίπεδα προστασίας από ορισμένους επικίνδυνους τύπους επιθέσεων, με πολύ μικρό κόστος σε υπολογισμούς και υλικό. Μία από τις πλέον ελαφρές υλοποιήσεις της ανωτέρω τεχνικής είναι η μέθοδος Page-level Information Flow Tracking [30]. Σύμφωνα με τη μέθοδο αυτή, η σήμανση γίνεται σε επίπεδο σελίδας στην εικονική μνήμη του λειτουργικού συστήματος με αποτέλεσμα το κόστος σε χώρο να είναι μηδενικό, ενώ η διαχείριση της σήμανσης γίνεται στατικά από το μεταγγλωτιστή. Κατά τη διάρκεια της εκτέλεσης, η διάδοση της σήμανσης (taint propagation) γίνεται από το λειτουργικό σύστημα κατά τα page faults. Ακόμη, το πολύ μικρό υπολογιστικό κόστος της την καθιστά πολύ ελκυστική για χρήση ακόμα και σε ευφυείς μετρητές χαμηλής υπολογιστικής ισχύος. Πρέπει, ωστόσο, να γίνουν μικρές προσθήκες στον πυρήνα του λειτουργικού συστήματος στο τμήμα page allocation και να γίνει η μεταγλώττιση των εφαρμογών από μεταγλωττιστές που υποστηρίζουν τη συγκεκριμένη τεχνική. Σε αντίθετη περίπτωση, μπορεί να χρησιμοποιηθεί η τεχνική Dynamic Information Flow Tracking που υλοποιείται σε επίπεδο υλικού και δεν απαιτεί υποστήριξη από το λειτουργικό σύστημα και το λογισμικό αλλά έχει αρκετά μεγαλύτερο κόστος σε υλικό και υπολογισμούς.

Κεφάλαιο 4. Εταιρικά Πληροφοριακά Δίκτυα

4.1. Εισαγωγή

Στο κεφάλαιο αυτό θα αναζητηθούν και θα αναλυθούν ζητήματα ασφαλείας που επηρεάζουν συστήματα των πληροφοριακών δικτύων του διαχειριστή του δικτύου ΗΕ και των προμηθευτών ΗΕ. Τα εταιρικά πληροφοριακά δίκτυα είναι ο συνδετικός ιστός μέσω του οποίου διακινούνται οι πληροφορίες μεταξύ των συστημάτων παραγωγής μεταφοράς, και διανομής της ηλεκτρικής ενέργειας. Από τα συστήματα ελέγχου στους σταθμούς παραγωγής και τους σταθμούς υποβιβασμού τάσης μέχρι τα συστήματα τιμολόγησης και τις βάσεις δεδομένων με τα στοιχεία των καταναλωτών, όλες οι πληροφορίες που ανταλλάσσονται μεταξύ των επιμέρους συστημάτων, μεταφέρονται μέσω των εταιρικών πληροφοριακών δικτύων του διαχειριστή του δικτύου ΗΕ και των προμηθευτών ΗΕ.

Λόγω του μεγέθους των εταιρικών πληροφοριακών δικτύων και της κρισιμότητας των πληροφοριών που διακινούνται πάνω από αυτά, αποτελούν συχνά ένα από τους πρώτους στόχους επιθέσεων εναντίον του Smart Grid. Το γεγονός ότι τα εταιρικά πληροφοριακά δίκτυα αποτελούν διαύλους επικοινωνίας μεταξύ αυτών των συστημάτων του Smart Grid, αποτελεί το μεγαλύτερο κίνητρο για κακόβουλες επιθέσεις εναντίον των εταιρικών πληροφοριακών δικτύων. Αυτό διότι αποτελεί πολύ πρόσφορο έδαφος για κακόβουλα λογισμικά worms τα οποία διαχέονται αυτόματα σε ένα εταιρικό πληροφοριακό δίκτυο.

Τα εταιρικά πληροφοριακά δίκτυα πρέπει να διασφαλίζονται αποτελεσματικά έναντι ενδεχόμενων κινδύνων, καθώς αναμένεται να αποτελέσουν στόχο σημαντικών επιθέσεων εναντίον του Smart Grid. Ο σχεδιασμός του εταιρικού πληροφοριακού δικτύου είναι εξαρχής αναγκαίο να γίνει με βασικό πυλώνα και τα ζητήματα ασφάλειας του δικτύου. Ο λόγος είναι ότι τα πληροφοριακά δίκτυα σχεδιάζονται με βασικό γνώμονα την διασύνδεση των συστημάτων που συνδέονται σε αυτά. Στην περίπτωση των εταιρικών πληροφοριακών δικτύων που ανήκουν στο Smart Grid, όμως, επειδή η ασφάλεια αποτελεί σημαντικότατη προδιαγραφή, πρέπει κατά τη σχεδίαση του δικτύου να ληφθούν υπόψη και τα ζητήματα ασφάλειας που προκύπτουν για τα συστήματα που ανήκουν σε αυτό. Ακόμη, επειδή οι κακόβουλες επιθέσεις προσαρμόζονται ταχύτατα στις αδυναμίες του δικτύου, είναι επιτακτική η συχνή επανεξέταση του σχεδιασμού της ασφάλειας δικτύου καθώς και η διεξαγωγή δοκιμών παραβίασης (penetration tests) ώστε τα συστήματα ασφαλείας να παραμένουν αποτελεσματικά.

4.2. Λειτουργίες του εταιρικού πληροφοριακού δικτύου

Στο σημείο αυτό θα αναφερθούν ορισμένες από τις λειτουργίες που πραγματοποιούν τα εταιρικά πληροφοριακά δίκτυα του διαχειριστή του δικτύου ΗΕ και των παρόχων ΗΕ ώστε να γίνουν αντιληπτές οι κατηγορίες πληροφοριών που διακινούνται μέσω αυτών. Οι κατηγορίες πληροφοριών που διακινούνται μέσω των εταιρικών πληροφοριακών δικτύων είναι ανάλογες σε αριθμό με τις δομές που αποτελούν το Smart Grid. Αυτό αυτομάτως εγγυάται ένα σύνολο πληροφοριών, ελκυστικών για υποκλοπές και άλλου είδους επιθέσεις.

4.2.1. Κέντρα τιμολόγησης

Στα κέντρα τιμολόγησης των προμηθευτών ΗΕ εντάσσονται οι λειτουργίες που αφορούν την τιμολόγηση της ΗΕ που καταναλώνεται από τους καταναλωτές ή παράγεται από ιδιώτες παραγωγούς και παρέχεται στο δίκτυο ΗΕ. Στην πρώτη περίπτωση, τα κέντρα τιμολόγησης αναλαμβάνουν τη διατήρηση δεδομένων κατανάλωσης για κάθε μετρητή ώστε να τιμολογούν την ΗΕ που καταναλώνεται. Επιπλέον, είναι υπεύθυνα για την ενημέρωση των ευφυών μετρητών ώστε να προωθούν στους καταναλωτές πιθανούς τρόπους μείωσης του κόστους ΗΕ.

Στην περίπτωση των ιδιωτών παραγωγών ΗΕ, τα κέντρα τιμολόγησης διατηρούν τα δεδομένα συναλλαγών μεταξύ των προμηθευτών ΗΕ και των παραγωγών. Αυτά τα δεδομένα αφορούν το ποσό της οφειλής, την παραχθείσα ΗΕ και ενδεχομένως τα χρονικά περιθώρια ανάμεσα στα οποία πραγματοποιήθηκε η αγορά ΗΕ από τους προμηθευτές ΗΕ. Επειδή τα δεδομένα που διακινούνται από και προς τα κέντρα τιμολόγησης είναι ιδιωτικά, είναι απαραίτητη η εξασφάλιση της ασφάλειάς τους ταυτόχρονα και κατά τη μετάδοση και κατά την αποθήκευση και διατήρησή τους στις βάσεις δεδομένων των προμηθευτών ΗΕ. Ακόμη, είναι απαραίτητη η εγγύηση της ασφάλειας των συστημάτων που διαχειρίζονται και διατηρούν τα ανωτέρω δεδομένα, καθώς αποτελούν σημαντικούς στόχους επιθέσεων με κίνητρο την οικονομική απάτη και την κλοπή ρεύματος μέσω αλλοίωσης των δεδομένων.

4.2.2. Υποστηρικτικά συστήματα της διαδικτυακής πλατφόρμας διαχείρισης λογαριασμού

Τα υποστηρικτικά συστήματα της διαδικτυακής πλατφόρμας διαχείρισης λογαριασμού αποτελούν τον ενδιάμεσο σύστημα ανάμεσα στην πλατφόρμα διαχείρισης λογαριασμού και τα συστήματα βάσεων δεδομένων που διατηρούν τα δεδομένα των καταναλωτών. Κάθε αίτημα προς τη διαδικτυακή πλατφόρμα διαχείρισης λογαριασμού ενός καταναλωτή προωθείται στα υποστηρικτικά συστήματα τα οποία ελέγχουν το αίτημα και με τη σειρά τους απευθύνουν το αίτημα προς τις κεντρικές βάσεις δεδομένων. Τα υποστηρικτικά συστήματα της διαδικτυακής πλατφόρμας διαχείρισης λογαριασμού είναι απαραίτητα για τους εξής λόγους:

- Αποκρύπτουν όλες τις λεπτομέρειες υλοποίησης των συστημάτων αποθήκευσης δεδομένων από την πλατφόρμα διαχείρισης λογαριασμού. Έτσι, τυχόν αλλαγές στον τρόπο διατήρησης των δεδομένων δεν θα απαιτεί αλλαγές στην διαδικτυακή πλατφόρμα κάθε προμηθευτή ΗΕ, αλλά μόνο στα υποστηρικτικά συστήματα.
- Αποτρέπουν τα συστήματα διαχείρισης λογαριασμού από την απευθείας σύνδεση με τις κεντρικές βάσεις δεδομένων.

Η απευθείας σύνδεση των υποστηρικτικών συστημάτων με τις κεντρικές βάσεις δεδομένων σε συνδυασμό με την ευαίσθητη φύση των δεδομένων που διαχειρίζονται τα αναγάγει σε κορυφαίους στόχους κακόβουλων επιθέσεων. Συνεπώς, τα υποστηρικτικά συστήματα πρέπει να διαθέτουν τους απαραίτητους μηχανισμούς ασφάλειας έναντι παραβιάσεων καθώς και τους μηχανισμούς που εγγυώνται την ασφάλεια των πληροφοριών που διακινούν.

4.2.3. Συστήματα ελέγχου σταθμών παραγωγής / διανομής ΗΕ

Στην κατηγορία αυτή εντάσσονται τα κέντρα ελέγχου των υποδομών παραγωγής, μεταφοράς και διανομής ΗΕ όπως οι μεγάλοι σταθμοί παραγωγής, τα συστήματα ανανεώσιμων πηγών ενέργειας και οι σταθμοί υποβιβασμού τάσης. Καίτοι οι ανωτέρω δομές έχουν διακριτούς ρόλους στο ηλεκτρικό δίκτυο, ως προς το δίκτυο επικοινωνιών και τον απομακρυσμένο έλεγχο εξετάζονται ως μία ομάδα συστημάτων. Οι πληροφορίες που μεταφέρονται μεταξύ συστημάτων αυτομάτου ελέγχου, υπό έλεγχο διατάξεων και απομακρυσμένων χρηστών που λαμβάνουν διαγνωστικές πληροφορίες, πρέπει να διακινούνται με ασφάλεια, αποτρέποντας αρχικά την υποκλοπή και αλλοίωσή τους και, στη συνέχεια, τη δυνατότητα των επίδοξων εισβολέων να αποκτήσουν πληροφορίες για τη δομή του δικτύου και τους κόμβους που το αποτελούν.

4.3. Κίνητρα επιθέσεων εναντίον του εταιρικού πληροφοριακού δικτύου

Η ηλεκτρική ενέργεια αποτελεί πρώτη ύλη για σχεδόν κάθε οικονομική δραστηριότητα ενός κράτους. Το πλήθος των δραστηριοτήτων αυτών δημιουργεί κίνητρα για κακόβουλες επιθέσεις εναντίον του Smart Grid και των εταιρικών πληροφοριακών δικτύων ειδικότερα. Τα σημαντικότερα κίνητρα τέτοιων επιθέσεων παρουσιάζονται στη συνέχεια.

4.3.1. «Χακτιβισμός» (Hacktivism)

Ο όρος «χακτιβισμός» χρησιμοποιείται τα τελευταία χρόνια κυρίως από τα ΜΜΕ για να χαρακτηρίσει ένα νέο είδος πολιτικής έκφρασης και πολιτικής διαμαρτυρίας που χρησιμοποιεί ως βήμα τους ηλεκτρονικούς υπολογιστές και τα δίκτυα υπολογιστών. Συχνά, έχει λάβει τη μορφή επιθέσεων DDoS (Distributed Denial of Service), εναντίον κυβερνητικών και εταιρικών ιστοσελίδων και βάσεων δεδομένων. Για παράδειγμα, τα τελευταία χρόνια η ομάδα Anonymous, διανέμει δωρεάν μέσω της ιστοσελίδας της λογισμικό που παρέχει τη δυνατότητα συμμετοχής μέσω του Η/Υ σε τέτοιου είδους επιθέσεις.

Ο διαχειριστής του δικτύου ΗΕ και οι προμηθευτές ΗΕ έχουν σημαντικό ρόλο στις σύγχρονες οικονομίες και κοινωνίες, κάτι το οποίο συχνά τους κάνει αποδέκτες διαμαρτυριών. Αυτό επιδεινώνεται στις σημερινές συνθήκες της οικονομικής κρίσης καθώς επικρατεί γενική απογοήτευση και οργή εναντίον των διαφόρων οντοτήτων της αγοράς ΗΕ λόγω των αυξήσεων στην τιμή της ΗΕ. Οι ανωτέρω λόγοι μπορούν να οδηγήσουν εξαγριωμένους καταναλωτές ή ομάδες χακτιβισμού, εναντίον του διαχειριστή του δικτύου ΗΕ και των προμηθευτών ΗΕ, με κίνητρο ένα είδος εκδίκησης.

4.3.2. Οικονομικά κίνητρα

Ανέκαθεν, ένα από τα σοβαρότερα και συχνότερα κίνητρα εγκληματικών ενεργειών είναι η αποκόμιση οικονομικού οφέλους. Όπως αναφέρθηκε και προηγουμένως, τα οικονομικά κίνητρα μπορούν να εκφραστούν

με ενέργειες όπως η κλοπή ΗΕ. Καθώς εισάγονται οι νέες τεχνολογίες του Smart Grid σε όλα τα επίπεδα της αρχιτεκτονικής του δικτύου ΗΕ, εμφανίζονται νέες μέθοδοι επίθεσης που μπορούν να αποφέρουν οικονομικά οφέλη.

Τέτοιες επιθέσεις έχουν ως στόχο κυρίως το κέντρο τιμολόγησης και τη βάση δεδομένων όπου αποθηκεύονται τα οικονομικά δεδομένα που αφορούν την παραγωγή και κατανάλωση ΗΕ. Οι πληροφορίες και τα προσωπικά στοιχεία που είναι αποθηκευμένα στις βάσεις δεδομένων αυτές, μπορούν να αποφέρουν σημαντικά οικονομικά οφέλη από ενδεχόμενη πώλησή τους στη μαύρη αγορά, όπως συμβαίνει με τους αριθμούς πιστωτικών καρτών και τους λογαριασμούς e-mail. Επιπλέον, με χρήση τεχνικών data mining είναι δυνατό από τα στοιχεία κατανάλωσης ΗΕ να εξαχθούν δεδομένα για το προφίλ κατανάλωσης των πελατών των προμηθευτών ΗΕ, δεδομένα τα οποία είναι μεγάλης αξίας για διαφημιστικές εταιρίες και τμήματα marketing.

Αξίζει, επίσης, να αναφερθεί ότι υπάρχουν οικονομικά κίνητρα για υποκλοπές οικονομικών δεδομένων από μεγάλες εταιρίες. Στόχο αποτελούν, συνήθως, έγγραφα σχετικά με τα οικονομικά στοιχεία των εταιριών ώστε να χρησιμοποιηθούν πριν την δημοσιοποίησή τους σε χρηματιστηριακά παιχνίδια. Επειδή, οι εταιρίες ενέργειας είναι συχνά εισηγμένες στα κατά τόπους χρηματιστήρια, το προαναφερθέν κίνητρο αποτελεί ένα ακόμη λόγο για κακόβουλες ενέργειες εναντίον των εταιριών που εμπλέκονται στην αγορά ΗΕ.

4.3.3. Εταιρική κατασκοπεία - Δολιοφθορά

Η είσοδος της τεχνολογίας του Smart Grid στα δίκτυα ΗΕ, σηματοδοτεί την έναρξη σημαντικών ανακατατάξεων στην οικονομική ιεραρχία εταιριών παραγωγής, των παρόχων, και των προμηθευτών ΗΕ στην οικονομία όπου δραστηριοποιούνται. Λόγω των ανακατατάξεων αυτών, κάποιες εταιρίες αναμένεται να υστερήσουν τεχνολογικά σε σχέση με άλλες. Μπροστά στο φάσμα οικονομικών ζημιών, εταιρίες που υστερούν του ανταγωνισμού ενδεχομένως να χρησιμοποιήσουν παράνομες τεχνικές ώστε να επανέλθουν μπροστά από τον ανταγωνισμό. Παραδείγματα τέτοιων πρακτικών είναι η εταιρική κατασκοπεία και η δολιοφθορά.

Η εταιρική κατασκοπεία εκφράζεται κυρίως μέσω επιθέσεων σε σταθμούς παραγωγής και κέντρα ελέγχου με σκοπό την υποκλοπή μετρήσεων από τους σταθμούς, ή ακόμα και των σχεδίων των σταθμών και μελλοντικών κατασκευών. Το μέσο που χρησιμοποιείται για να γίνουν τέτοιου είδους επιθέσεις, είναι τα εταιρικά πληροφοριακά δίκτυα των οντοτήτων που συμμετέχουν στην αγορά ΗΕ και το βιομηχανικό πληροφοριακό δίκτυο διαχειριστή του δικτύου ΗΕ, όπου επιχειρούν να αποκτήσουν πρόσβαση οι επίδοξοι εισβολείς. Στην περίπτωση όπου αυτό δεν επιτύχει ή δεν είναι αρκετό, ενδέχεται ο μη υγιής ανταγωνισμός να οδηγήσει σε επιθέσεις DoS εναντίον δομών μίας εταιρίας με σκοπό τη δυσφήμισή της. Μία ακραία έκφανση τέτοιων επιθέσεων μπορεί να φθάσει και στη διάπραξη δολιοφθορών εναντίον υποδομών των οντοτήτων της αγοράς ΗΕ.

4.3.4. Στρατιωτική κατασκοπεία

Η συγκεκριμένη κατηγορία κινήτρων για επιθέσεις εναντίον πληροφοριακών συστημάτων του διαχειριστή του δικτύου ΗΕ και των προμηθευτών ΗΕ, προέρχεται από την εποχή του ψυχρού πολέμου. Ωστόσο, καθώς η τεχνολογία της πληροφορικής προχωρεί με πολύ ταχείς ρυθμούς, είναι αναπόφευκτο

τέτοιες τεχνολογίες να χρησιμοποιηθούν και για στρατιωτικούς σκοπούς. Αυτό το είδος ηλεκτρονικού πολέμου έχει γίνει γνωστό τα τελευταία χρόνια με τον όρο cyber warfare (κυβερνοπόλεμος).

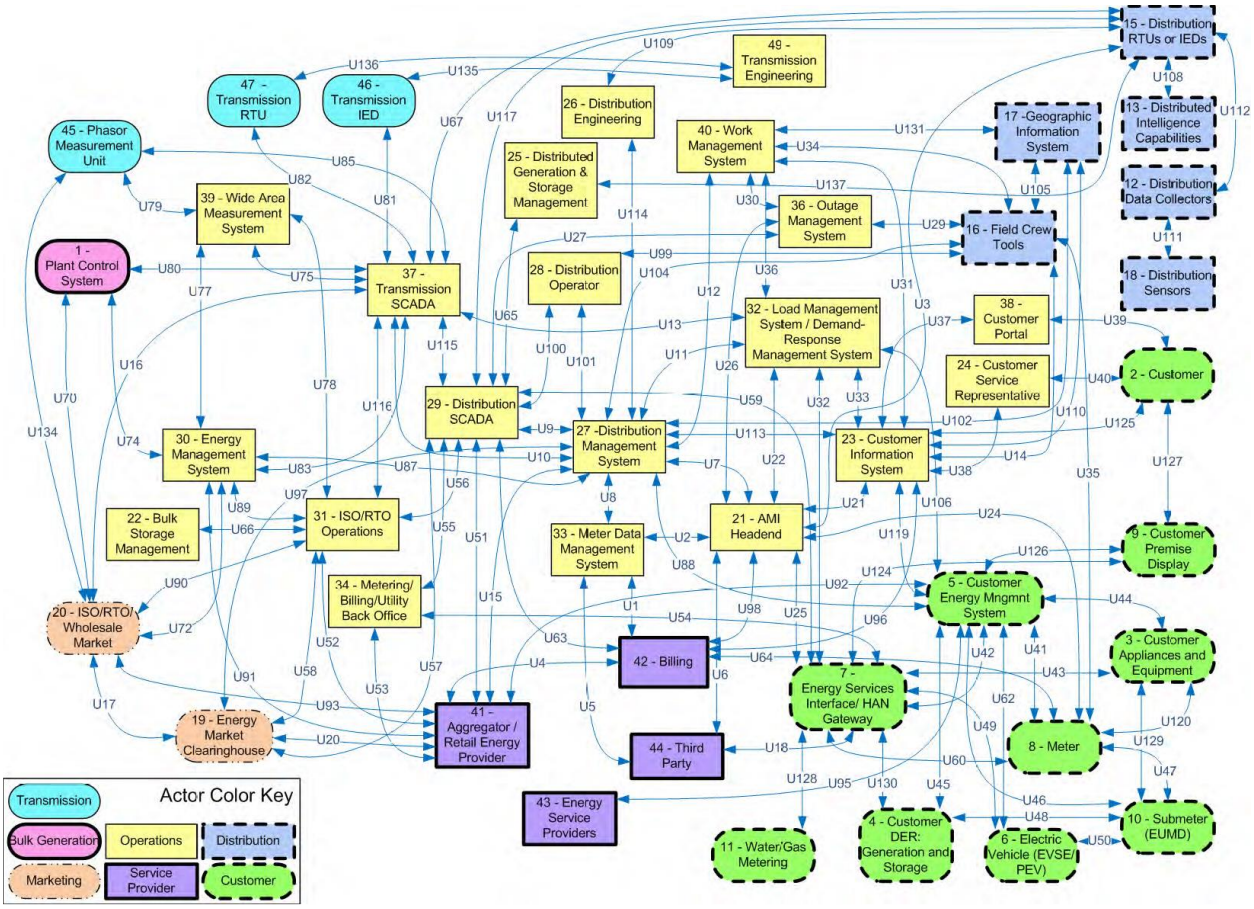
Η κατασκοπεία αποτελούσε, ανέκαθεν, σημαντικό τμήμα των στρατιωτικών επιχειρήσεων και των στρατηγικών ενός κράτους. Επειδή τα συστήματα παραγωγής και διανομής ΗΕ ενός κράτους αποτελούν κρίσιμες υποδομές, συνεπάγεται πως αποτελούν υψηλούς στόχους εχθρικών κρατών.. Στην εποχή που η πληροφορική μπαίνει στα συστήματα ΗΕ μέσω του Smart Grid, είναι αναμενόμενο να χρησιμοποιηθεί και για κακόβουλους σκοπούς, όπως, για παράδειγμα η υποκλοπή μετρήσεων από σταθμούς παραγωγής ενέργειας [31] [32].

Οι επιθέσεις από ομάδες ηλεκτρονικού πολέμου στρέφονται κυρίως εναντίον σταθμών παραγωγής και σταθμών υποβιβασμού τάσης. Επίσης, στόχο αποτελούν βάσεις δεδομένων και συστήματα εν γένει που διατηρούν σχέδια του δικτύου ΗΕ, δεδομένα για το φορτίο στους διάφορους κόμβους του δικτύου ΗΕ και τους σταθμούς, και πληροφορίες που περιγράφουν την τρέχουσα κατάσταση του δικτύου.

Σε όλες τις μέχρι σήμερα καταγραμμένες περιπτώσεις τέτοιων επιθέσεων, το εταιρικό πληροφοριακό δίκτυο και οι αδυναμίες του ήταν που οι εισβολείς εκμεταλλεύθηκαν αρχικά ώστε να εισβάλουν στις υπολογιστικές δομές σταθμών ελέγχου που είναι υπεύθυνες για τη λειτουργία των υποδομών του δικτύου ΗΕ. Από αυτό συνεπάγεται ότι μεγάλο μέρος της προσπάθειας για την ασφάλεια τέτοιων υποδομών πρέπει να αποσκοπεί στην ασφάλεια του εταιρικού πληροφοριακού δικτύου του διαχειριστή του δικτύου ΗΕ των προμηθευτών ΗΕ.

4.4. Δομή του δικτύου

Τα εταιρικά πληροφοριακά δίκτυα του διαχειριστή του δικτύου ΗΕ και των προμηθευτών ΗΕ είναι υπεύθυνα για: (i) την αποθήκευση των δεδομένων των καταναλωτών, (i) την προώθηση αυτών των δεδομένων σε συστήματα πληροφόρησης των καταναλωτών, (ii) τη μεταφορά δεδομένων μεταξύ των σταθμών παραγωγής, μεταφοράς και διανομής ΗΕ και του προσωπικού του διαχειριστή του δικτύου ΗΕ. Οι ανωτέρω απαιτήσεις από τα εταιρικά πληροφοριακά δίκτυα αυξάνουν τη σχεδιαστική πολυπλοκότητα του Smart Grid, όπως φαίνεται από τη μελέτη του ινστιτούτου NIST (National Institute of Standards and Technology) [3].



Σχήμα 4.1. Λειτουργική δομή του Smart Grid

Μία άμεση συνέπεια της πολυπλοκότητας και του μεγέθους του Smart Grid είναι οι πολλές και μεγάλες προκλήσεις ως προς την ασφάλειά του. Όσο αυξάνονται η πολυπλοκότητα και το μέγεθος των επιμέρους δομών του, αυξάνεται ο αριθμός των αδύνατων σημείων στο δίκτυο, ενώ η ανίχνευση και αντιμετώπισή τους γίνεται δυσκολότερη λόγω της αλληλεξάρτησης μεταξύ δομών του Smart Grid.

Το ζήτημα της αλληλεξάρτησης μεταξύ των δομών γίνεται εμφανές από το Σχ. 4.1. Οι ακμές μεταξύ των δομών του Smart Grid δείχνουν την εξάρτηση μεταξύ τους. Ακόμα και ένα από αυτά τα σημεία να τεθεί εκτός λειτουργίας, επηρεάζεται μεγάλος αριθμός άλλων, με συνέπεια την κατακόρυφη μείωση της διαθεσιμότητας τμημάτων του. Συνεπώς, μία ακόμη πρόκληση για το Smart Grid και τη σχεδίαση ασφάλειάς του είναι η εξασφάλιση της υψηλής διαθεσιμότητας των επιμέρους τμημάτων του.

Η ασφάλεια ενός δικτύου τόσο μεγάλης κλίμακας όσο το Smart Grid αποτελεί μεγάλη πρόκληση για τον τομέα της ασφάλειας πληροφοριών. Ο λόγος είναι το πλήθος υποδικτύων διαφορετικής φύσης που το απαρτίζουν, με συνέπεια να απαιτείται ένας συνδυασμός μηχανισμών ασφάλειας για το σύνολο του Smart Grid και μηχανισμών ασφάλειας εξειδικευμένων για κάθε τύπο υποδικτύου. Ένας σχεδιασμός ασφάλειας τέτοιας κλίμακας είναι πολύ περίπλοκος, με αποτέλεσμα να μη μπορεί συχνά να εφαρμοστεί σε ήδη υπάρχοντα δίκτυα τέτοιας κλίμακας. Συνεπώς, στην περίπτωση του Smart Grid, η ασφάλεια πρέπει είναι από τις βασικές προδιαγραφές βάσει των οποίων γίνεται ο αρχιτεκτονικός σχεδιασμός του. Ο λόγος για αυτό είναι ότι η ίδια η αρχιτεκτονική του Smart Grid μπορεί να λειτουργήσει ως αποτελεσματικός μηχανισμός άμυνας.

Το μέγεθος και η πολυπλοκότητα των εταιρικών πληροφοριακών δικτύων του διαχειριστή του δικτύου ΗΕ και των παρόχων ΗΕ αποτελεί σημαντική παράμετρο που επηρεάζει και τον τρόπο με τον οποίο οι επίδοξοι εισβολείς θα επιλέξουν να επιτεθούν σε αυτά. Ανάλογα με το στάδιο υλοποίησης μιας επίθεσης, το πολύ μεγάλο μέγεθος του δικτύου επηρεάζει σημαντικά το έργο ενός επίδοξου εισβολέα. Για παράδειγμα, η αναζήτηση πιθανής εισόδου σε ένα τέτοιο δίκτυο διευκολύνεται σημαντικά από το μέγεθός του. Αντίθετα, το μέγεθος του εταιρικού πληροφοριακού δικτύου μπορεί αν λειτουργήσει αποτρεπτικά για ένα επίδοξο εισβολέα στην περίπτωση όπου τα κακόβουλα λογισμικά που έχουν εισαχθεί στο δίκτυο πρέπει να μολύνουν μόνο συγκεκριμένα συστήματα ώστε να μην γίνουν αντιληπτά. Το μέγεθος, λοιπόν, του δικτύου αποτελεί σημαντικό παράγοντα κατά την ανάλυση της ασφάλειας των εταιρικών πληροφοριακών δικτύων του διαχειριστή του δικτύου ΗΕ και των παρόχων ΗΕ.

4.5. Μεθοδολογία επίθεσης σε εταιρικά πληροφοριακά δίκτυα

Η παραβίαση ενός πληροφοριακού συστήματος και στην συνέχεια η μόλυνση μέσω του πληροφοριακού δικτύου γειτονικών συστημάτων (κόμβοι που απέχουν 1 βήμα) είναι μια διαδικασία πολύπλοκη που περιλαμβάνει διάφορα στάδια για την υλοποίησή της. Κάθε στάδιο εξυπηρετεί διαφορετικό επί μέρους σκοπό, και για το λόγο αυτό χρησιμοποιούνται διαφορετικά εργαλεία από τους επίδοξους εισβολείς. Λόγω της λογικής συνέχειας της μεθοδολογίας η ανάλυση της ασφάλειας θα γίνει ακολουθώντας τα στάδιά της. Για κάθε στάδιο, θα αναλυθούν οι μέθοδοι που χρησιμοποιούνται από επίδοξους εισβολείς και, στη συνέχεια, μέθοδοι και εργαλεία που είτε αποτρέπουν είτε δυσκολεύουν σε μεγάλο βαθμό το έργο επίδοξων εισβολέων.

4.5.1. Ανίχνευση

Το στάδιο της ανίχνευσης αποτελεί συνήθως το πρώτο βήμα ενός επίδοξου εισβολέα, δεδομένου ότι διαθέτει μόνο γενικές γνώσεις για το εταιρικό πληροφοριακό δίκτυο και τους χρήστες του. Ως γενικές γνώσεις συνήθως θεωρούνται οι γνώσεις που μπορεί κάποιος να αποκομίσει από μία σχετικά σύντομη έρευνα στο Διαδίκτυο για την οντότητα που στοχεύει. Οι πληροφορίες που ενδιαφέρουν τους επίδοξους εισβολείς είναι IP διευθύνσεις, διευθύνσεις email του εργατικού προσωπικού, πληροφορίες τις αρμοδιότητες του προσωπικού και πληροφορίες σχετικά με τα τεχνικά χαρακτηριστικά των πληροφοριακών συστημάτων που χρησιμοποιούνται. Για ένα επίδοξο εισβολέα, η γνώση της ακριβούς έκδοσης ενός συστήματος λογισμικού που τρέχει ένας διακομιστής είναι εξαιρετικά σημαντική πληροφορία και σε καμμία περίπτωση δεν πρέπει να μπορεί να αποκτηθεί με μια απλή περιήγηση στην ιστοσελίδα της οντότητας. Τέλος, σημαντικές είναι και πληροφορίες που ενδεχομένως να είναι ξεχασμένες σε κάποια σελίδα στο Διαδίκτυο σχετικά με την αρχιτεκτονική του εταιρικού πληροφοριακού δικτύου.

Η ανίχνευση του πληροφοριακού δικτύου είναι η διαδικασία κατά την οποία ο επίδοξος εισβολέας επιχειρεί μέσω ειδικών εργαλείων να αποσπάσει όσο το δυνατό περισσότερες πληροφορίες για το δίκτυο από το ίδιο το δίκτυο. Τα εργαλεία που χρησιμοποιούνται είναι απλά στη χρήση, αυτοματοποιημένα στην πλειονότητά τους και μπορούν καταγράψουν σημαντικές πληροφορίες σχετικά με το πληροφοριακό δίκτυο

σε πολύ σύντομο χρονικό διάστημα. Κάποιες από τις λειτουργίες τους είναι η ανίχνευση υπηρεσιών που τρέχουν σε συγκεκριμένους διακομιστές, η απόκτηση πληροφοριών σχετικά με το εύρος διευθύνσεων IP των κόμβων στο δίκτυο καθώς και οι εκδόσεις των λογισμικών και των λειτουργικών συστημάτων που τρέχουν οι διακομιστές.

1. Μηχανές Αναζήτησης

Οι επίδοξοι εισβολείς, κατά το στάδιο της ανίχνευσης αναζητούν πληροφορίες στο Διαδίκτυο. Η διαδικασία της αναζήτησης και του εντοπισμού των πληροφοριών αυτών είναι δύσκολη και χρονοβόρα.. Σε αυτό βοηθούν σημαντικά οι μηχανές αναζήτησης και ιδιαίτερα οι λειτουργίες εξειδικευμένης αναζήτησης που προσφέρουν σημαντικές παραμετροποιήσεις κατά την αναζήτηση. Ένα τέτοιο παράδειγμα να είναι το ακόλουθο ερώτημα στην μηχανή αναζήτησης της Google:

```
allinurl:tsweb/default.htm
```

που επιστρέφει διακομιστές στους οποίους τρέχει το λογισμικό Windows Server με την υπηρεσία Remote Desktop Web Connection σε λειτουργία. Αν στο ερώτημα προστεθεί και το όνομα της οντότητας-στόχου, τότε μπορεί εύκολα να εξαχθεί αν κάποιο από τα προσβάσιμα μέσω Διαδικτύου συστήματα του πληροφοριακού δικτύου της οντότητας έχει ενεργοποιημένη τη συγκριμένη υπηρεσία. Η ίδια τεχνική μπορεί να χρησιμοποιηθεί με μικρές παραλλαγές, επιστρέφοντας μία πληθώρα πληροφοριών σχετικά με συστήματα της οντότητας-στόχου, που χρησιμοποιούν συγκεκριμένες εκδόσεις δημοφιλών λογισμικών. Τέλος, για να διευκολύνεται το έργο υπεύθυνων ασφαλείας και επίδοξων εισβολέων υπάρχουν έτοιμα εργαλεία και πακέτα λογισμικού που αυτοματοποιούν το ανωτέρω έργο διατηρώντας μια βάση δεδομένων με έτοιμα προς χρήση ερωτήματα τέτοιου είδους προς όλες τις μηχανές αναζήτησης. Ένα τέτοιο παράδειγμα είναι το δωρεάν λογισμικό SiteDigger της εταιρείας McAfee [33].

Άλλο ένα τέτοιο εργαλείο που αξίζει να αναφερθεί είναι η μηχανή αναζήτησης SHODAN (Sentient Hyper-Optimized Data Access Network) [34]. Είναι ιδιαιτέρως δημοφιλής σε υπεύθυνους ασφαλείας και επίδοξους εισβολείς καθώς διατηρεί μία διαρκώς ανανεωμένη βάση δεδομένων με τις IP διευθύνσεις συστημάτων προσβάσιμων μέσω Διαδικτύου και τα λογισμικά που τρέχουν σε αυτά. Επομένως, πολύ εύκολα ένας επίδοξος εισβολέας μπορεί να ψάξει για συγκεκριμένα ευάλωτα συστήματα, με περιορισμό στις IP διευθύνσεις της οντότητας, βρίσκοντας έτσι πολύ εύκολα αν υπάρχει σύστημα που μπορεί να αποτελέσει εύκολο στόχο, την IP διεύθυνσή του και τον ISP του.

2. Social Media

Πολλές πληροφορίες είναι δυνατόν να εξορυχθούν από πλατφόρμες κοινωνικής δικτύωσης. Σε προσωπικούς λογαριασμούς που διατηρούνται σε πλατφόρμες κοινωνικής δικτύωση πολύ συχνά αναγράφεται λεπτομερώς η θέση εργασίας που κατέχει κάποιος χρήστης. Ακόμη, σε πλατφόρμες κοινωνικής δικτύωσης με επαγγελματικό προσανατολισμό, οι χρήστες διατηρούν δημόσια προσβάσιμο το βιογραφικό τους σημείωμα σε συνδυασμό με τεχνικές λεπτομέρειες για όλες τις θέσεις εργασίας τους. Από τις πληροφορίες ενός τέτοιου λογαριασμού ένας επιτιθέμενος μπορεί να εξαγάγει τη διεύθυνση email βάσει το ονόματος του χρήστη. Επιπλέον, μέσω των σχέσεων μεταξύ λογαριασμών, ένας επίδοξος εισβολέας είναι σε θέση να κατασκευάσει τμήμα του οργανογράμματος της εταιρίας βασιζόμενος στις περιγραφές

αρμοδιοτήτων που κάθε χρήστης έχει δημοσιεύσει. Οι πληροφορίες αυτές είναι ιδιαίτερα σημαντικές και πολύτιμες στην περίπτωση όπου ο επίδοξος εισβολέας καταφύγει στην μέθοδο του social engineering για να επιτεθεί στην οντότητα.

3. DNS ανίχνευση και WHOIS

Στο σημείο αυτό θα αναλυθούν μέθοδοι εξαγωγής πληροφοριών για μια οντότητα από οργανωτικές δομές του Διαδικτύου. Για την εύρυθμη λειτουργία του Διαδικτύου, διάφοροι παγκόσμιοι οργανισμοί επωμίζονται συγκεκριμένους ρόλους, ένας εκ των οποίων είναι ο οργανισμός ICANN [35]. Ο οργανισμός ICANN, μεταξύ άλλων, είναι υπεύθυνος για την ιεραρχία του πρωτοκόλλου DNS και την ανάθεση των ονομάτων σε IP διευθύνσεις. Στους διακομιστές του που ονομάζονται Registries διατηρεί πληροφορίες για τους root name servers κάθε δένδρου ονομάτων της ιεραρχίας του DNS όπως τα δένδρα .com, .org κτλ. Στη συνέχεια, οι root name servers κάθε δέντρου έχουν βάσεις με τις διευθύνσεις των name servers του δεύτερου επιπέδου και διαθέτουν μηχανισμούς για την αναζήτηση των μητρώων εγγραφής για συγκεκριμένα ονόματα στους serverstου τρίτου επιπέδου.

Τα μητρώα εγγραφής σε αυτούς τους name servers περιέχουν πληροφορίες για την οντότητα που έχει στη διάθεσή της το συγκεκριμένο όνομα. Τέτοιες πληροφορίες είναι το όνομα, η φυσική διεύθυνση, μία διεύθυνση email, διευθύνσεις IP οι οποίες αντιστοιχούν στη συγκεκριμένη εγγραφή και άλλες. Από αυτές τις εγγραφές μητρώων είναι δυνατό επίδοξοι εισβολείς πολύ γρήγορα να εξάγουν πληροφορίες για τις φυσικές διευθύνσεις της εταιρείας και IP διευθύνσεις των Web και Mail διακομιστών της. Η ίδια ακριβώς διαδικασία μπορεί να ακολουθηθεί αν ο επίδοξος εισβολέας γνωρίζει μία IP διεύθυνση και θέλει να αποκτήσει όλες τις πληροφορίες που βρίσκονται στα μητρώα εγγραφής του ICANN.

4. Τρόποι αντιμετώπισης των τεχνικών ανίχνευσης

Καίτοι οι τεχνικές που χρησιμοποιούνται από επίδοξους εισβολείς σε αυτό το στάδιο δεν παρεμβαίνουν στο εταιρικό πληροφοριακό δίκτυο, υπάρχουν μέθοδοι με τις οποίες μπορεί το τμήμα ασφάλειας μιας οντότητας να δυσχεράνει το έργο όσων έχουν ως στόχο να αποκτήσουν επικίνδυνες πληροφορίες για αυτή. Παραδείγματα τέτοιων μεθόδων αποτελούν οι διάφοροι μηχανισμοί προστασίας των συστημάτων εντός του εταιρικού πληροφοριακού δικτύου και η εκπαίδευση του προσωπικού σε θέματα ασφάλειας πληροφοριών.

Ως προς το στάδιο της ανίχνευσης, το τμήμα ασφαλείας πρέπει να αποφασίσει ποιές ακριβώς πληροφορίες παρέχονται στα μητρώα διεθνών οργανισμών του Διαδικτύου ώστε να δημοσιεύονται όσο το δυνατό λιγότερες πληροφορίες που ενδεχομένως βοηθούν επίδοξους εισβολείς στο έργο τους. Επίσης, το τμήμα ασφάλειας οφείλει να οργανώνει τακτική ενημέρωση του υπαλληλικού προσωπικού της οντότητας σε ζητήματα ασφάλειας, στη συγκεκριμένη περίπτωση στη χρήση των μέσων κοινωνικής δικτύωσης. Πρέπει να τους γνωστοποιούνται οι επιπτώσεις που μπορεί να έχει η δημοσιοποίηση πληροφοριών, όπως η διεύθυνση email ή το ακριβές προφίλ εργασίας, για την οντότητα.

4.5.2. Σάρωση δικτύου

Μέχρι αυτό το στάδιο της σάρωσης δικτύου, ο επίδοξος εισβολέας έχει καταφέρει να αποκτήσει πληροφορίες σχετικά με το δίκτυο-στόχο μέσω δημοσίων πηγών χρησιμοποιώντας μη παρεμβατικές στο

δίκτυο της εταιρίας μεθόδους. Στο στάδιο αυτό προχωρεί σε παρεμβατικές πλέον μεθόδους, με σκοπό την ανακάλυψη πιθανών εισόδων στο δίκτυο. Για να το επιτύχει, είναι αναγκαίο να αναγνωριστεί ο ρόλος των συστημάτων του πληροφοριακού δικτύου και να αναγνωριστούν τα λογισμικά που εκτελούνται στα συστήματα αυτά. Για το σκοπό αυτό υπάρχει πληθώρα ελεύθερα διαθέσιμων εργαλείων στο Διαδίκτυο, η λειτουργία των οποίων θα αναλυθεί με σκοπό την ανάπτυξη μεθόδων αντιμετώπισής τους και των τεχνικών που χρησιμοποιούν.

1. Traceroute

Το εργαλείο traceroute του UNIX συμβάλλει στην κατανόηση της τοπολογίας του δικτύου-στόχου. Το εργαλείο αυτό εκμεταλλεύεται τη λειτουργικότητα του πρωτοκόλλου ICMP ώστε να λαμβάνει ένα αναγνωριστικό πακέτο από κάθε εξυπηρετητή στη διαδρομή μεταξύ του χρήστη και του προορισμού. Κατ' αυτό τον τρόπο, είναι δυνατό να χαρτογραφηθεί η διαδρομή προς διάφορα συστήματα του πληροφοριακού δικτύου της οντότητας-στόχου. Ακόμη, σε περιπτώσεις κακής ρύθμισης των firewall των εξυπηρετητών, μπορεί ο επίδοξος εισβολέας να λαμβάνει πακέτα από συστήματα στο εσωτερικό του πληροφοριακού δικτύου της οντότητας που δεν είναι απευθείας προσβάσιμα από το Διαδίκτυο. Ωστόσο, είναι δυνατή η ρύθμιση των διακομιστών ώστε να αγνοούν τα πακέτα αυτού του εργαλείο και παρόμοιων με αυτό.

2. Ping Sweep

Ping ονομάζεται το εργαλείο των λειτουργικών συστημάτων με το οποίο αποστέλλεται ένα πακέτο τύπου ICMP με σκοπό να εξακριβωθεί αν το σύστημα στην άλλη άκρη της σύνδεσης είναι online. Από αυτή τη λειτουργία έχει πάρει την ονομασία της η διαδικασία κατά την οποία σαρώνεται ένα σύνολο από IP διευθύνσεις με σκοπό να εξακριβωθεί σε ποιες από αυτές υπάρχουν συστήματα που αναμένουν συνδέσεις. Μία τέτοια μέθοδος είναι να αποσταλούν πακέτα όλων των συνήθων τύπων όπως ICMP, ARP και TCP προς όλες τις συχνά χρησιμοποιούμενες θύρες. Όταν μία διεργασία λειτουργεί σε μία από αυτές τις θύρες, απαντά στα πακέτα από αποστέλλονται, κάτι που καταδεικνύει ότι το σύστημα στη συγκεκριμένη διεύθυνση λειτουργεί. Οι θύρες που σαρώνονται πρώτες είναι οι θύρες βασικών δικτυακών πρωτοκόλλων που είναι σχεδόν σίγουρο ότι θα είναι ανοικτές. Τέτοιες θύρες είναι για παράδειγμα οι θύρες DNS και HTTP.

Για να γίνονται ταχέως και αυτοματοποιημένα όλες οι προαναφερθείσες ενέργειες, χρησιμοποιούνται εργαλεία τα οποία ελέγχουν αυτόματα σε ποιες διευθύνσεις ενός υποδικτύου υπάρχουν συστήματα, και ποιες δικτυακές θύρες τους είναι ανοικτές. Αυτά τα προγράμματα υλοποιούν μια δέσμη από ενέργειες που αποσκοπούν στο να απαντήσουν στο ερώτημα με όσο γίνεται περισσότερη βεβαιότητα. Ένα από τα κατεξοχήν εργαλεία που χρησιμοποιούνται στην περίπτωση αυτή είναι το nmap [36]. Στην περίπτωση ενός ping sweep, το nmap μπορεί να χρησιμοποιηθεί για να αποστείλει πακέτα όλων των δημοφιλών τύπων σε όλες τις θύρες ενός συστήματος. Άλλο ένα εργαλείο της ίδιας οικογένειας είναι το nping, με το οποίο ένας εισβολέας μπορεί να κατασκευάσει πακέτα με οποιεσδήποτε τιμές, για ακόμη περισσότερο παραμετροποιήσιμες σαρώσεις.

3. Αναγνώριση της λειτουργίας ενός συστήματος στο εταιρικό πληροφοριακό δίκτυο

Το επόμενο βήμα μετά την εξακρίβωση ότι σε μία διεύθυνση IP σύστημα του εταιρικού πληροφοριακού δικτύου της οντότητας είναι συνδεδεμένο ένα πληροφοριακό σύστημα, είναι να εξακριβωθούν από τον επίδοξο εισβολέα οι περισσότερες λειτουργίες που αυτό επιτελεί. Οι λειτουργίες των συστημάτων που βρίσκονται πάνω στο δίκτυο βασίζονται στις υπηρεσίες και τα προγράμματα που εκτελούνται στο εκάστοτε σύστημα.

Κάθε λογισμικό που επικοινωνεί με άλλα συστήματα μέσω δικτύου χρησιμοποιεί κάποιες από τις θύρες του λειτουργικού συστήματος. Από τις συνολικά 65535 διαθέσιμες θύρες, οι πρώτες 1024 ανήκουν σε ευρέως χρησιμοποιούμενα πρωτόκολλα, ενώ οι θύρες με υψηλό αναγνωριστικό αριθμό είναι ελεύθερες για κάθε χρήση. Για παράδειγμα, το πρωτόκολλο HTTP χρησιμοποιεί τη θύρα 80.

Για ένα επίδοξο εισβολέα, η ανακάλυψη των λειτουργιών ενός συστήματος συχνά ανάγεται στην αναγνώριση του συνόλου των δικτυακών υπηρεσιών που εκτελεί. Ο συνήθης τρόπος ανίχνευσης των υπηρεσιών είναι η αποστολή κατάλληλων αιτημάτων προς αυτές τις υπηρεσίες, σε κάθε θύρα που είναι ανοικτή στο σύστημα. Αρκετά λογισμικά πρωτοκόλλων και ασφάλειας, ωστόσο, φιλτράρουν τέτοιες αιτήσεις με βάση παραμέτρους όπως η διεύθυνση IP του αποστολέα και άλλες, ώστε να μην είναι εύκολη η αναγνώρισή τους. Έτσι, τα εργαλεία που πραγματοποιούν τέτοιες αναζητήσεις εξελίσσονται διαρκώς ώστε να υπερβαίνουν αυτά τα εμπόδια.

Η εξέταση όλων των θυρών ενός συστήματος είναι συνήθως μια χρονοβόρα διαδικασία, η οποία, επιπλέον, αφήνει σημαντικό δικτυακό αποτύπωμα καθώς δημιουργεί αρκετή κίνηση στο δίκτυο εύκολα αναγνωρίσιμη αφού εμφανίζονται πακέτα προς όλες τις θύρες. Για να αποφευχθεί αυτό από επίδοξους εισβολείς, χρησιμοποιούνται εξειδικευμένες τεχνικές μείωσης του δικτυακού αποτυπώματος, οι οποίες όμως αυξάνουν δραστικά το χρόνο που διαρκεί η αναγνώριση υπηρεσιών. Συνεπώς, ένας επίδοξος εισβολέας είναι πολύ πιθανότερο να χρησιμοποιήσει διακριτικές μεθόδους ελέγχοντας, όμως, μόνο το υποσύνολο των θυρών όπου είναι πιθανότερο να λειτουργούν ευάλωτες υπηρεσίες.

4. Αναγνώριση έκδοσης λογισμικών και λειτουργικού συστήματος

Για να αποκτήσει πρόσβαση σε κάποιο σύστημα του πληροφοριακού δικτύου του διαχειριστή του δικτύου ΗΕ ή των παρόχων ΗΕ, ένας επίδοξος εισβολέας είναι απαραίτητο να γνωρίζει το λειτουργικό σύστημα που εκτελεί, την έκδοσή του, καθώς και τις εκδόσεις των λογισμικών που αναμένουν αιτήσεις στις δικτυακές θύρες. Οι ανωτέρω πληροφορίες δεν είναι εύκολο να συγκεντρωθούν. Για το λόγο αυτό έχουν αναπτυχθεί εργαλεία τα οποία αναγνωρίζουν είτε την ακριβή έκδοση λειτουργικού και εργαλείων λογισμικού που εκτελούνται, είτε περιορίζουν το σύνολο των πιθανών εκδόσεων.

Ο τρόπος με τον οποίο συλλέγονται πληροφορίες για τις εκδόσεις του λογισμικού βασίζεται στην εξέλιξη των εργαλείων λογισμικού. Συχνά, καθώς αναπτύσσονται νέες εκδόσεις, οι αποκρίσεις σε ορισμένα αιτήματα αλλάζουν. Σε ορισμένες περιπτώσεις, όπως στους web browsers, η έκδοση αναγράφεται στις επικεφαλίδες εξερχόμενων πακέτων. Τα εργαλεία αναγνώρισης εκδόσεων λογισμικού διατηρούν βάσεις δεδομένων με τις αποκρίσεις δημοφιλών εργαλείων λογισμικού ανά έκδοση. Έτσι, τα εργαλεία αναγνώρισης εκδόσεων λογισμικού αποστέλλουν ειδικά κατασκευασμένα αιτήματα στο σύστημα-στόχο, με σκοπό να συγκρίνουν τις αποκρίσεις του συστήματος-στόχου με αυτές που διατηρεί στη βάση δεδομένων. Με τον τρόπο αυτό, τα

ανωτέρω εργαλεία αναγνωρίζουν την έκδοση λειτουργικού συστήματος και εργαλείων λογισμικού που εκτελούνται στο σύστημα-στόχο. Και στην περίπτωση αυτή, το δημοφιλέστερο εργαλείο είναι το nmap.

Εκτός των εξειδικευμένων εργαλείων που χρησιμοποιούνται σε κάθε βήμα, υπάρχουν εργαλεία λογισμικού που αναλαμβάνουν να αυτοματοποιήσουν τα ανωτέρω βήματα και να παρουσιάσουν τα αποτελέσματα μέσα από ένα γραφικό περιβάλλον. Ένα παράδειγμα είναι το Nessus [37] που παρέχει τη δυνατότητα αυτόματης σάρωσης ενός συνόλου από IP διευθύνσεις παρέχοντας όλες τις απαραίτητες πληροφορίες που αναφέρθηκαν προηγουμένως, συμπεριλαμβανομένων και πληροφοριών για την ύπαρξη δημοσιευμένων εργαλείων εκμετάλλευσης ευπαθειών στα λογισμικά που αναγνωρίσθηκαν. Άλλο ένα πακέτο παρόμοιο με το Nessus είναι η σουίτα Metasploit [38]. Η συγκεκριμένη σουίτα περιέχει εργαλεία αναγνώρισης λογισμικού και έτοιμα πρόσθετα τα οποία ανανεώνονται συνεχώς, για την αυτόματη εκμετάλλευση γνωστών ευπαθειών στα λογισμικά που αναγνωρίσθηκαν.

Και τα δύο ανωτέρω εργαλεία καθιστούν ταχεία και αυτοματοποιημένη μία αρχική αναζήτηση για ευπαθή συστήματα σε εταιρικά πληροφοριακά δίκτυα. Πρέπει να σημειωθεί ότι τα εργαλεία εκμετάλλευσης ευπαθειών που δημοσιεύονται στο Metasploit, έχουν ήδη γίνει γνωστά στην βιομηχανία λογισμικού. Ωστόσο, στην παράνομη αγορά κυκλοφορούν εργαλεία εκμετάλλευσης ευπαθειών που δεν έχουν δημοσιευτεί, όπως είναι το BlackHole exploit kit. Έτσι, για ένα επίδοξο εισβολέα με οικονομική επάρκεια γίνεται ακόμη ευκολότερο να εξαπολύσει εξελιγμένες επιθέσεις εναντίον συστημάτων του εταιρικού πληροφοριακού δικτύου μιας οντότητας της βιομηχανίας ΗΕ.

5. Τεχνικές αντιμετώπισης σάρωσης δικτύου

5.1. Μηχανισμοί Firewall

Η σάρωση των διευθύνσεων IP και η προσπάθεια αναγνώρισης συγκεκριμένων συστημάτων στα εταιρικά πληροφοριακά δίκτυα του διαχειριστή του δικτύου ΗΕ και των παρόχων ΗΕ δεν μπορεί να αντιμετωπιστεί ολοκληρωτικά. Αυτό οφείλεται στη φύση των πρωτοκόλλων που χρησιμοποιούνται. Τα πρωτόκολλα αυτά και τα λογισμικά που τα υλοποιούν βασίζουν τη λειτουργία τους σε κάποιες ελάχιστες προϋποθέσεις υπό τις οποίες λειτουργούν σωστά. Αυτές αφορούν τη συνδεσιμότητα στο πληροφοριακό δίκτυο μέσω συγκεκριμένων θυρών του λειτουργικού συστήματος καθώς και την επιτυχή μεταφορά συγκεκριμένων τύπων πακέτων. Τα ίδια πακέτα χρησιμοποιούν τα λογισμικά σάρωσης δικτύου ώστε ενδεχόμενοι μηχανισμοί άμυνας να θεωρούν ότι πρόκειται για αυθεντικά πακέτα και να επιτρέπουν τη διέλευσή τους. Ωστόσο, υπάρχουν βήματα και ενέργειες μέσω των οποίων περιορίζεται σημαντικά η αποτελεσματικότητα των εργαλείων σάρωσης δικτύου.

Ένα σημαντικό βήμα προς την ασφάλεια έναντι τέτοιων λογισμικών είναι η εγκατάσταση συστημάτων firewall. Ένα σύστημα firewall διαθέτει ένα σύνολο κανόνων τους οποίους εφαρμόζει στα πακέτα που διέρχονται μέσω αυτό. Μπορεί να απορρίπτει πακέτα από το να εισχωρήσουν στο εταιρικό πληροφοριακό δίκτυο, ανάλογα με την IP διεύθυνση αποστολέα, τον τύπο του πακέτου, και στις πλέον σύγχρονες μορφές του, ανάλογα με τα δεδομένα που μεταφέρει και τα πακέτα που έχουν προηγηθεί. Για παράδειγμα, πολλά firewall απορρίπτουν πακέτα τύπου ICMP ECHO REQUEST ώστε το εργαλείο ping να μην μπορεί να στοχεύσει συστήματα που προστατεύονται από το firewall. Επιπλέον, συχνά ορίζονται κανόνες που απορρίπτουν πακέτα που σχετίζονται με το εργαλείο traceroute ώστε αυτό να μην επιστρέφει πληροφορία για το εσωτερικό του εταιρικού πληροφοριακού δικτύου.

5.2. Συστήματα ανίχνευσης παραβίασης - Intrusion Detection Systems (IDS)

Λογισμικά όπως το ping και το traceroute προορίζονται για διαχειριστές πληροφοριακών δικτύων και, επομένως, η χρήση τους δεν συνιστά επίθεση προς ένα εταιρικό πληροφοριακό δίκτυο. Ωστόσο, πολύ συχνά, η χρήση τους αποτελεί προαναγγελία μιας επίθεσης. Επομένως, είναι σημαντικό να υπάρχουν εργαλεία τα οποία να ανιχνεύουν την δικτυακή κίνηση που παράγουν τέτοια εργαλεία ώστε να ειδοποιούν το τμήμα ασφάλειας για την πιθανότητα επικείμενης επίθεσης εναντίον του εταιρικού πληροφοριακού δικτύου.

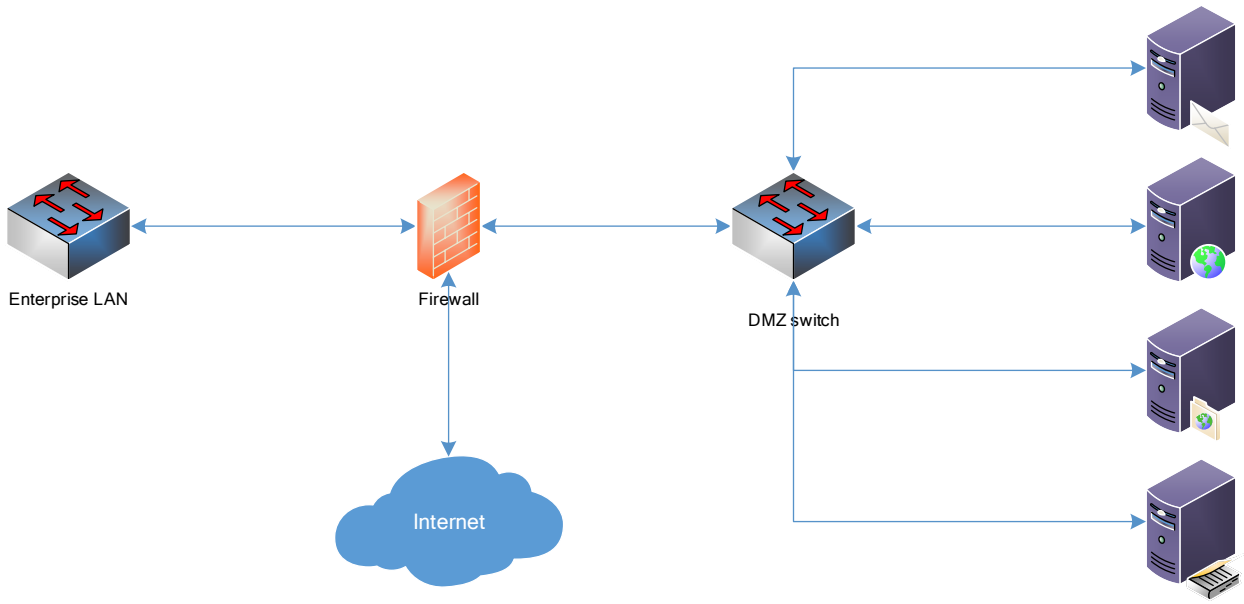
Τα συστήματα IDS έχουν την ανωτέρω δυνατότητα αφού λειτουργούν ελέγχοντας την κίνηση του δικτύου για την εμφάνιση συγκεκριμένων προτύπων που αντιστοιχούν σε λογισμικά ανίχνευσης. Η ανίχνευση προτύπων βασίζεται είτε σε βιβλιοθήκες υπαρχόντων προτύπων, διασταυρωμένων με συγκεκριμένα λογισμικά ανίχνευσης, είτε σε συστήματα μηχανικής μάθησης, τα οποία εκπαιδεύονται ώστε να ταυτοποιούν τα πρότυπα κίνησης του δικτύου. Για παράδειγμα, πακέτα τύπου ICMP υπό κανονικές συνθήκες εμφανίζονται με πολύ μικρό ρυθμό. Αν σε κάποια χρονική στιγμή αυξηθεί δραστικά ο αριθμός, τους το σύστημα IDS το αντιλαμβάνεται ως πιθανή κακόβουλη ενέργεια και ειδοποιεί το τμήμα ασφάλειας. Αντίστοιχα, αν ανιχνευθεί κίνηση παραπλήσιας συχνότητας πακέτων προς μεγάλο σύνολο θυρών, ταυτοποιείται λογισμικά ανίχνευσης θυρών και ειδοποιείται και πάλι το τμήμα ασφάλειας.

5.3. Σωστές ρυθμίσεις λειτουργικού συστήματος

Κάθε σύστημα ενός εταιρικού πληροφοριακού δικτύου χρειάζεται συγκεκριμένα πρωτόκολλα και λογισμικά ώστε να εκτελεί αποτελεσματικά τις λειτουργίες του. Κατά την εγκατάσταση του λειτουργικού συστήματος και των εργαλείων λογισμικού που απαιτούνται, πολλές από τις ρυθμίσεις τίθενται σε προεπιλεγμένες τιμές που δεν είναι οι επιθυμητές για την ασφάλεια του συστήματος. Ακόμη, το λειτουργικό σύστημα έχει εξαρχής ενεργοποιημένα πολλά εργαλεία λογισμικού που συχνά δεν είναι αναγκαία για τις συγκεκριμένες λειτουργίες που θα επιτελέσει το σύστημα. Παραμένουν, όμως πιθανές είσοδοι για το σύστημα καθώς μπορεί να παρουσιάζουν ευπάθειες που να οδηγήσουν σε παραβίαση. Επομένως, προτού εισαχθεί ένα νέο σύστημα σε ένα εταιρικό πληροφοριακό δίκτυο, είναι αναγκαίο να γίνεται σωστή ρύθμισή του ώστε να εκτελούνται μόνο τα απαραίτητα εργαλεία λογισμικού και το IDS να ρυθμίζεται με τους αυστηρότερους κανόνες που εγγυώνται την απρόσκοπτη λειτουργία του νέου συστήματος

5.4. «Αποστρατιωτικοποιημένες Ζώνες - De-Militarized Zones (DMZ)

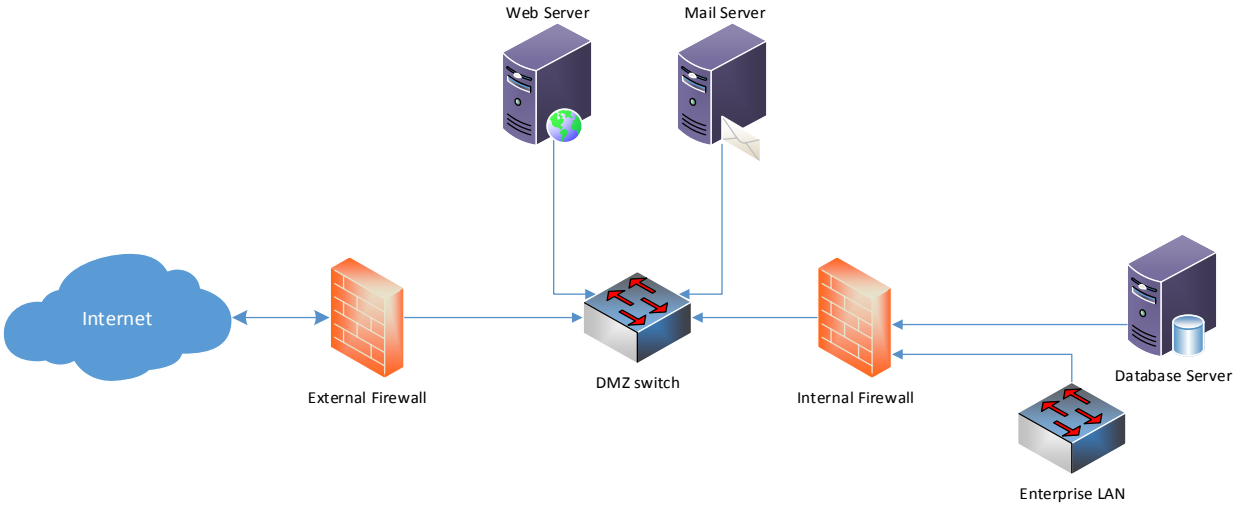
Μία περισσότερο προχωρημένη τεχνική για την αντιμετώπιση επιθέσεων προερχόμενων από το Διαδίκτυο είναι η χρήση DMZ. Μία ζώνη DMZ είναι τμήμα του πληροφοριακού δικτύου συνδεδεμένο πλησίον της εξόδου προς το Διαδίκτυο ώστε να είναι διακριτό από το εσωτερικό τμήμα του δικτύου. Στη ζώνη DMZ τοποθετούνται όλα τα συστήματα που δέχονται αιτήματα από το Διαδίκτυο, δηλαδή, συστήματα που είναι προσβάσιμα μέσω Διαδικτύου και, επομένως, εύκολοι στόχοι επιθέσεων. Παραδείγματα τέτοιων συστημάτων μπορεί να είναι διακομιστής web ή ένας διακομιστής mail.



Σχήμα 4.2. Σχηματική απεικόνιση απλής ζώνης DMZ

Στο Σχ. 4.2 δίδεται μια βασική υλοποίηση μιας ζώνης DMZ. Καθώς η κίνηση εισέρχεται από το Διαδίκτυο στο εταιρικό πληροφοριακό δίκτυο φθάνει σε ένα σύστημα το οποίο εκτελεί ταυτόχρονα χρέη DMZ switch και firewall. Στο σχήμα εμφανίζονται ως διακριτά συστήματα για να τονιστεί η λειτουργία εκάστου εξ' αυτών, ωστόσο, το firewall και το DMZ switch ανήκουν πολύ συχνά σε ενιαίο σύστημα. Αυτό το σύστημα βάσει κανόνων ασφάλειας επιτρέπει την κίνηση να εισέλθει στο δίκτυο. Στη συνέχεια, το DMZ switch προωθεί τα πακέτα στον αντίστοιχο παραλήπτη. Η ουσία της ζώνης DMZ είναι ότι τα «δημόσια» συστήματα που δέχονται κίνηση από το Διαδίκτυο, βρίσκονται σε διαφορετικό τοπικό δίκτυο από το υπόλοιπο εταιρικό πληροφοριακό δίκτυο. Κατ' αυτόν τον τρόπο, ενδεχόμενη παραβίαση παραμένει περιορισμένη στη ζώνη DMZ και δεν εξαπλώνεται στο υπόλοιπο τμήμα του δικτύου. Επιπλέον, δεν επηρεάζονται η λειτουργία των υπόλοιπων συστημάτων στο εσωτερικό του εταιρικού πληροφορικού δικτύου και η σύνδεσή τους με το Διαδίκτυο.

Σε περιπτώσεις μεγάλων εταιρικών πληροφοριακών δικτύων προτιμάται η εγκατάσταση πολυεπίπεδων ζωνών DMZ ώστε να επιτυγχάνεται μεγαλύτερη διακριτοποίηση των επιπέδων ασφάλειας των επιμέρους ζωνών. Ένας ακόμα λόγος είναι ότι τα συστήματα που λειτουργούν εντός ζωνών DMZ έχουν ανάγκη επικοινωνίας με υποστηρικτικά συστήματα όπως βάσεις δεδομένων. Τέτοια συστήματα πρέπει είναι πολύ περισσότερο προστατευμένα, και η πρόσβαση σε αυτά να ελέγχεται βάσει αυστηρών κανόνων. Αυτό επιτυγχάνεται εύκολα με την θέσπιση αποκλειστικών ζωνών DMZ για τα συστήματα αυτά με αποκλειστικό μηχανισμό firewall που εφαρμόζει αυστηρότερους κανόνες ασφάλειας.



Σχήμα 4.3. Ζώνη DMZ δύο επιπέδων

Στο Σχ. 4.3 παρουσιάζεται μία ζώνη DMZ με αρχιτεκτονική δύο επιπέδων. Όπως φαίνεται από το σχήμα, υπάρχει ένα εξωτερικό firewall ανάμεσα στο συνολικό εταιρικό πληροφοριακό δίκτυο και το Διαδίκτυο. Οι κανόνες του είναι περισσότερο γενικοί συγκριτικά με αυτούς των εσωτερικών firewalls. Στη συνέχεια, το DMZ switch αποστέλλει την κίνηση είτε στη ζώνη DMZ είτε στο εσωτερικό του εταιρικού πληροφοριακού δικτύου. Το εσωτερικό firewall διαχωρίζει τη ζώνη DMZ από το εσωτερικό δίκτυο και εφαρμόζει αυστηρότερους κανόνες ασφάλειας στην δικτυακή κίνηση που εισέρχεται στο εσωτερικό δίκτυο. Για μεγαλύτερη προστασία, μια βάση δεδομένων που υποστηρίζει τη λειτουργία των διακομιστών της ζώνης DMZ συνιστάται να βρίσκεται πίσω από το εσωτερικό firewall.

Επεκτείνοντας την ανωτέρω σχεδιαστική λογική μπορούν να κατασκευαστούν πολύπλοκες ζώνες DMZ με πολλαπλά επίπεδα, ώστε οι μηχανισμοί ασφάλειας να είναι προσαρμοσμένοι στο μέγιστο βαθμό στα συστήματα που προστατεύουν. Ακόμη, ο συνδυασμός μηχανισμών ασφάλειας με την προσθήκη συστημάτων IDS μπορεί να αυξήσει ακόμη περισσότερο την ασφάλεια των ζωνών. Ως προς την προστασία από πιθανές επιθέσεις ανίχνευσης, η προαναφερθείσα αρχιτεκτονική επιτρέπει μόνο τη βολιδοσκόπηση συστημάτων που βρίσκονται μέσα στη ζώνη DMZ, καθώς τα firewall δεν επιτρέπουν στον επιτιθέμενο πρόσβαση σε εσωτερικά συστήματα. Ως προς τα συστήματα εντός της ζώνης DMZ, το τμήμα ασφάλειας αναγνωρίζει την ικανότητα επίδοξων εισβολέων να επιχειρήσουν επιθέσεις στα συγκεκριμένα προβλήματα και προνοεί για την ασφάλειά τους.

4.5.3. Επίθεση στα συστήματα του εταιρικού πληροφοριακού δικτύου

Στο σημείο αυτό, γίνεται η υπόθεση ότι ο επίδοξος εισβολέας έχει αποκτήσει όσες πληροφορίες χρειάζεται ώστε να προχωρήσει σε επίθεση εναντίον ενός συστήματος που ανήκει στο εταιρικό πληροφοριακό δίκτυο του διαχειριστή του δικτύου ΗΕ ή των παρόχων ΗΕ. Λόγω της αρχιτεκτονικής του

εταιρικού πληροφοριακού δικτύου, όπου όλες οι διακριτές δομές παραμένουν δικτυακά διαχωρισμένες με κανάλια επικοινωνίας μεταξύ τους τα οποία ελέγχονται από συστήματα ασφαλείας, είναι σχεδόν βέβαιο ότι για να φθάσει ο εισβολέας στον πραγματικό του στόχο πρέπει να αποκτήσει πρόσβαση σε πολλά ενδιάμεσα συστήματα. Αρχικά, το πρώτο βήμα είναι συνήθως ένα σύστημα προσβάσιμο μέσω Διαδικτύου. Στη συνέχεια, κλιμακωτά, η επίθεση περιλαμβάνει συστήματα τοποθετημένα όλο και βαθύτερα στο εσωτερικό του εταιρικού πληροφοριακού δικτύου. Προς επίτευξη αυτού του στόχου, ένας επίδοξος εισβολέας μπορεί να αξιοποιήσει μια μεγάλη ποικιλία από τεχνικές που βασίζονται σε παράγοντες όπως, μεταξύ άλλων, η ικανότητα στη συγγραφή κακόβουλων προγραμμάτων, η εκμετάλλευση του ανθρώπινου παράγοντα και η εκμετάλλευση της φορητότητας των ηλεκτρονικών συσκευών. Είναι φανερό, ότι σε αυτό το στάδιο, οι μέθοδοι επίθεσης γίνονται πολλές και ποικίλες σε μορφή. Αυτή η ποικιλία των μεθόδων επίθεσης είναι η μεγαλύτερη πρόκληση για την ασφάλεια ενός εταιρικού πληροφοριακού δικτύου, και του Smart Grid κατ' επέκταση, καθώς οι μηχανικοί ασφαλείας οφείλουν να προνοήσουν για κάθε πιθανό τρόπο επίθεσης εναντίον του δικτύου.

1. Επιθέσεις χωρίς πιστοποίηση

Στην κατηγορία των επιθέσεων χωρίς πιστοποίηση (unauthenticated attacks) ανήκουν οι μέθοδοι επίθεσης στις οποίες κατά την έναρξη της επίθεσης ο εισβολέας δεν μπορεί να πιστοποιηθεί ως αυθεντικός χρήστης στο σύστημα-στόχο. Διαθέτει, δηλαδή, μόνο όσες πληροφορίες μπορεί να αποκτήσει από τις τεχνικές που αναφέρθηκαν προηγουμένως, χωρίς να διαθέτει τα κατάλληλα διαπιστευτήρια, όπως ένα username και ένα password, ενός τουλάχιστον χρήστη του συστήματος. Στο στάδιο αυτό, η πρόκληση για τον επίδοξο εισβολέα είναι η εύρεση μιας οδού προς το σύστημα-στόχο. Με δεδομένο ότι δεν διαθέτει διαπιστευτήρια για να συνδεθεί στο σύστημα ως νόμιμος χρήστης, αναζητεί τρόπους ώστε να είτε παρακαμφθούν οι δικλείδες ασφαλείας του λειτουργικού, ή κάποιου άλλου λογισμικού, είτε να εκμεταλλευτεί ανθρώπινα λάθη των πραγματικών χρηστών. Συνήθως, αμέσως μετά από αυτού του είδους τις επιθέσεις, ο εισβολέας αποκτά πρόσβαση στο σύστημα ως χρήστης με περιορισμένα δικαιώματα. Συχνά, λοιπόν, αυτού του είδους οι επιθέσεις αποτελούν την αρχή μιας σειράς ενεργειών ώστε ο εισβολέας να αποκτήσει πρόσβαση σε ένα σύστημα του εταιρικού πληροφοριακού δικτύου και από εκεί να επιχειρήσει να παραβιάσει γειτονικά συστήματα.

1.1. Εκμετάλλευση ευπαθειών

Η συνηθέστερη μέθοδος απόκτησης πρόσβασης σε ένα σύστημα-στόχο από έναν επίδοξο εισβολέα είναι η εκμετάλλευση ευπαθειών του λειτουργικού συστήματος και των εργαλείων λογισμικού που εκτελούνται στο σύστημα-στόχο. Όπως αναφέρθηκε και προηγουμένως, κάθε σύστημα εντός ενός εταιρικού πληροφοριακού δικτύου παρέχει ορισμένες υπηρεσίες. Συχνά, σε ένα ή περισσότερα από τα λογισμικά που εκτελούνται στο σύστημα ανακαλύπτονται ευπάθειες. Κάτι τέτοιο προκύπτει όταν κατά τη συγγραφή του πηγαίου κώδικα της εφαρμογής, ένα ή περισσότερα λάθη και παραλείψεις, όπως ο ελλιπής έλεγχος των δεδομένων που εισάγονται από το χρήστη ή η χρήση λάθος δομών της χρησιμοποιούμενης γλώσσας προγραμματισμού, δημιουργούν στο πρόγραμμα κενά ασφαλείας. Με χρήση κατάλληλων εργαλείων, συνήθως κάποιων scripts που εκτελούν εντολές προκειμένου να εκμεταλλευτούν την ευπάθεια, οι επίδοξοι εισβολείς επιχειρούν να αποκτήσουν πρόσβαση στο σύστημα-στόχο.

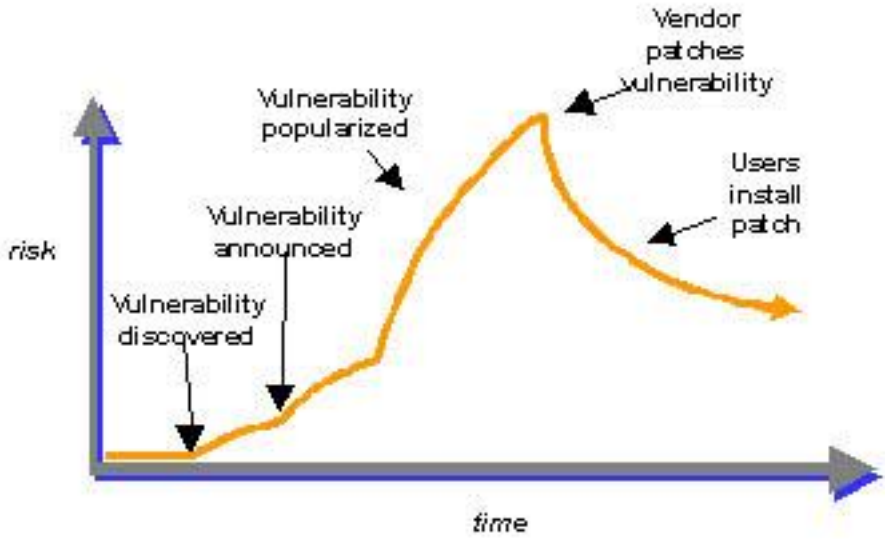
Χαρακτηριστικά παραδείγματα τέτοιων ευπαθειών είναι οι ευπάθειες τύπου buffer overflow. Οι ευπάθειες αυτού του είδους οφείλονται σε ελλιπή έλεγχο των στοιχείων εισόδου από το χρήστη και συγκεκριμένα όταν ο χρήστης εισάγει περισσότερα δεδομένα από όσα έχει προβλέψει ο προγραμματιστής και χωρίς να γίνεται έλεγχος στο μέγεθος των δεδομένων. Σύμφωνα με το μοντέλο von Neumann στο οποίο βασίζονται τα περισσότερα υπολογιστικά συστήματα, δεδομένα και εντολές αποθηκεύονται στην ίδια μνήμη και δεν διακρίνονται. Έτσι, ο επίδοξος εισβολέας εισάγει ως δεδομένα εισόδου σε ένα πεδίο, όπως μία ερώτηση για το όνομα χρήστη, τον δυαδικό κώδικα ενός εκτελέσιμου αρχείου, γραμμένου ειδικά για το συγκεκριμένο σύστημα. Ακόμη, εισάγει τον κώδικα μέσω του οποίου θα εκτραπεί η ροή εκτέλεσης του προγράμματος ώστε να εκτελέσει τα δεδομένα που έχει εισαγάγει. Κατ' αυτό τον τρόπο, τα δεδομένα που εισάγει ο επίδοξος εισβολέας είναι στην ουσία εντολές που γράφονται πάνω από τις πραγματικές εντολές της εφαρμογής. Συνεπώς, όταν το πρόγραμμα συνεχίσει μετά την είσοδο δεδομένων εκτρέπεται και εκτελεί τον κώδικα που εισήγαγε ο εισβολέας.

Το πλήθος των ευπαθειών που έχουν ανακαλυφθεί με συνέπειες παρόμοιες με μια επίθεση buffer overflow είναι μεγάλο. Ένα ακόμη παράδειγμα ευπάθειας αποτελεί ο κακόβουλος κώδικας που κρύβεται σε ιστοσελίδες και μπορεί εκμεταλλευόμενος κάποιο κενό ασφαλείας του φυλλομετρητή να εκτελέσει κώδικα εκτός του εικονικού περιβάλλοντος του φυλλομετρητή. Ακόμη, συχνά γίνεται μη ασφαλής επεξεργασία αρχείων από τις εφαρμογές που τα ανοίγουν με αποτέλεσμα και πάλι την εκτέλεση κώδικα του επίδοξου εισβολέα στο υπολογιστικό σύστημα.

Αξίζει, επιπλέον, να αναφερθεί η ύπαρξη και ανάπτυξη ενός ολόκληρου οικοσυστήματος από χρήστες που ασχολούνται αποκλειστικά με την ανακάλυψη ευπαθειών. Γύρω από αυτό το οικοσύστημα έχει επίσης αναπτυχθεί μια παράνομη αγορά για νέες ευπάθειες [39] [40]. Κενά ασφαλείας τα οποία έχουν ανακαλυφθεί αλλά δεν έχουν δημοσιευτεί, και διορθωθεί, ονομάζονται «0-day vulnerabilities». Ο όρος υποδηλώνει ότι πρόκειται για ευπάθειες των οποίων η εταιρία που κατασκευάζει το λογισμικό αγνοεί την ύπαρξη και συνεπώς δεν αποσκοπεί στην διόρθωσή τους. Το χρονικό διάστημα κατά το οποίο μια ευπάθεια μπορεί να μείνει κρυφή κυμαίνεται από ώρες, μέχρι σε ορισμένες περιπτώσεις και πάνω από ένα ή δύο χρόνια. Μία ευπάθεια συνεπώς, έχει κύκλο ζωής που περιλαμβάνει τις εξής φάσεις:

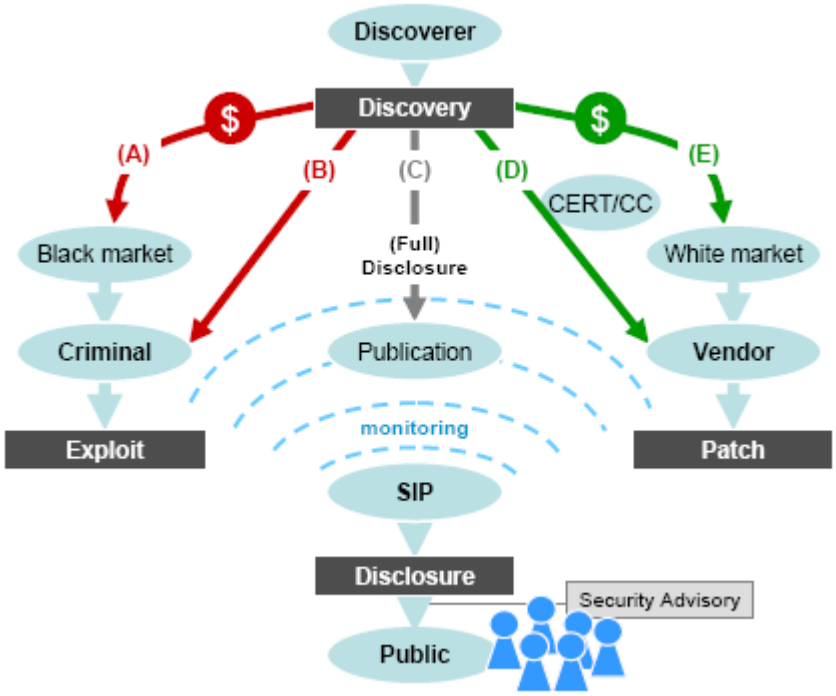
1. Ανακάλυψη
2. Εκμετάλλευση
3. Δημοσίευση
4. Διόρθωση

Ο κίνδυνος για τους χρήστες του ευάλωτου λογισμικού σε κάθε φάση φαίνεται από το παρακάτω διάγραμμα.



Σχήμα 4.4. Κίνδυνος για τους χρήστες σε κάθε φάση του κύκλου ζωής μια ευπάθειας **[41]**

Το οικοσύστημα δημιουργείται γύρω από τα οικονομικά οφέλη που σχετίζονται ευπάθειες λογισμικών. Συγκεκριμένα σημαντικά ποσά διακινούνται σε παράνομες αγορές για την αγοραπωλησία πληροφοριών για ευπάθειες 0-day και εργαλείων που αυτοματοποιούν την εκμετάλλευσή τους. Σχηματικά, οι κινήσεις αυτές φαίνονται στο Σχ. 4.5 περιλαμβάνοντας και την παράνομη αγορά που έχει δημιουργηθεί γύρω από 0-day ευπάθειες.



Σχήμα 4.5. Οικοσύστημα γύρω από τις 0-day ευπάθειες **[42]**

Στο ανωτέρω σχήμα διακρίνονται οι εναλλακτικές διαδρομές που μπορεί να ακολουθηθούν μετά την ανακάλυψη μιας ευπάθειας. Οι διαδρομές A και B του σχήματος καταδεικνύουν τα στάδια μετά την

ανακάλυψη μιας ευπάθειας με στόχο την εγκληματική εκμετάλλευση αυτής. Είτε ο χρήστης που την ανακάλυψε την μεταπωλεί στη παράνομη αγορά, οπότε και αποκτά άμεσο οικονομικό όφελος (διαδρομή A) είτε την χρησιμοποιεί απευθείας για εγκληματικούς σκοπούς (διαδρομή B) οπότε και αναμένει να αποκτήσει έμμεσα οικονομικά οφέλη. Η διαδρομή C είναι η διαδρομή που ακολουθείται όταν μια ευπάθεια έχει ανακαλυφθεί στους κύκλους της επιστημονικής κοινότητας σε κάποιο πανεπιστήμιο ή κάποιο ερευνητικό κέντρο. Η διαδρομή αυτή περιλαμβάνει τη δημοσίευση της ευπάθειας και των συνεπειών της σε συνέδρια και επιστημονικά περιοδικά, και στη συνέχεια την πλήρη δημοσιοποίησή της στο κοινό. Πρέπει να σημειωθεί, ωστόσο, ότι η εταιρία παραγωγής του ευπαθούς λογισμικού έχει ενημερωθεί εξαρχής, ώστε να ενημερώσει το λογισμικό πριν τη δημοσίευση της ευπάθειας από τους επιστήμονες. Τέλος, οι διαδρομές D και E περιγράφουν τη διαδρομή που ακολουθείται εφόσον ο χρήστης που ανακάλυψε την ευπάθεια αποφασίσει να ενημερώσει την εταιρία παραγωγής του λογισμικού. Συχνά, μεγάλες εταιρίες προσφέρουν αμοιβές για ευπάθειες σε λογισμικά που παράγουν και διοργανώνουν διαγωνισμούς εύρεσης ευπαθειών με σημαντικά έπαθλα. Κατ' αυτό τον τρόπο προσφέρονται κίνητρα ώστε χρήστες που ανακαλύπτουν μια ευπάθεια να επιλέξουν να ενημερώσουν τις εταιρίες παραγωγής του ευπαθούς λογισμικού.

Όπως είναι φανερό, οι ευπάθειες στα προγράμματα αποτελούν φαινόμενο που θα συνεχίσει να εμφανίζεται, με μεγαλύτερη συχνότητα και δυναμική. Το ότι σε κάθε περίπτωση υπάρχει ένα χρονικό διάστημα κατά το οποίο μία ευπάθεια παραμένει κρυφή χωρίς να έχει διορθωθεί και χωρίς να έχει γίνει γνωστή η ύπαρξή της, προκαλεί μεγάλα προβλήματα ασφάλειας των συστημάτων. Η απειλή από τέτοιες ευπάθειες είναι μεγάλη στο Smart Grid αλλά και τα εταιρικά πληροφοριακά δίκτυα των εμπλεκόμενων σε αυτό οντοτήτων, αφού πολλά από αυτά τα συστήματα είναι κρίσιμα για την εύρυθμη λειτουργία του Smart Grid. Συνεπώς, οι υπεύθυνοι ασφάλειας για όλα τα υποδίκτυα και υποσυστήματα του Smart Grid είναι αναγκαίο να γνωρίζουν σε βάθος τις δημοσιευμένες ευπάθειες για κάθε λογισμικό που χρησιμοποιείται καθώς και τις τεχνικές αποτροπής των συνεπειών τους.

1.2. Bring Your Own Device (BYOD)

Όπως έχει αναφερθεί προηγουμένως, στο συγκεκριμένο στάδιο της επίθεσης στόχος ενός επίδοξου εισβολέα είναι η παραβίαση και απόκτηση πρόσβασης σε ένα σύστημα το οποίο είναι συνδεδεμένο στο εσωτερικό εταιρικό πληροφοριακό δίκτυο της εταιρίας. Κάτι τέτοιο είναι αναγκαίο ώστε παραβιάζοντας γειτονικά προς το δίκτυο υπολογιστικά συστήματα να προχωρά βαθύτερα στο εσωτερικό του δικτύου με σκοπό να αποκτήσει πρόσβαση σε προστατευμένα κεντρικά συστήματα. Μέχρι πριν λίγα χρόνια, ο μόνος τρόπος για να το επιτύχει ήταν μέσω της εκμετάλλευσης είτε ευπαθειών σε λογισμικά που εκτελούνται τοπικά στα συστήματα-στόχους είτε ευπαθειών σε λογισμικά δικτυακών πρωτοκόλλων και web εφαρμογών. Τα τελευταία χρόνια, όμως, παρατηρείται ραγδαία αύξηση του αριθμού των έξυπνων κινητών συσκευών και των υπολογιστικών δυνατοτήτων τους. Συνεπώς, μεγάλο ποσοστό χρηστών συνηθίζει, πλέον, να πραγματοποιεί εργασίες χρησιμοποιώντας έξυπνες κινητές συσκευές, που έχουν καταστεί απαραίτητες και στο χώρο εργασίας. Εδώ ακριβώς εμφανίζεται ένα από τα πλέον σύγχρονα και δυσεπίλυτα ζητήματα ασφαλείας που έχει προκύψει τα τελευταία χρόνια.

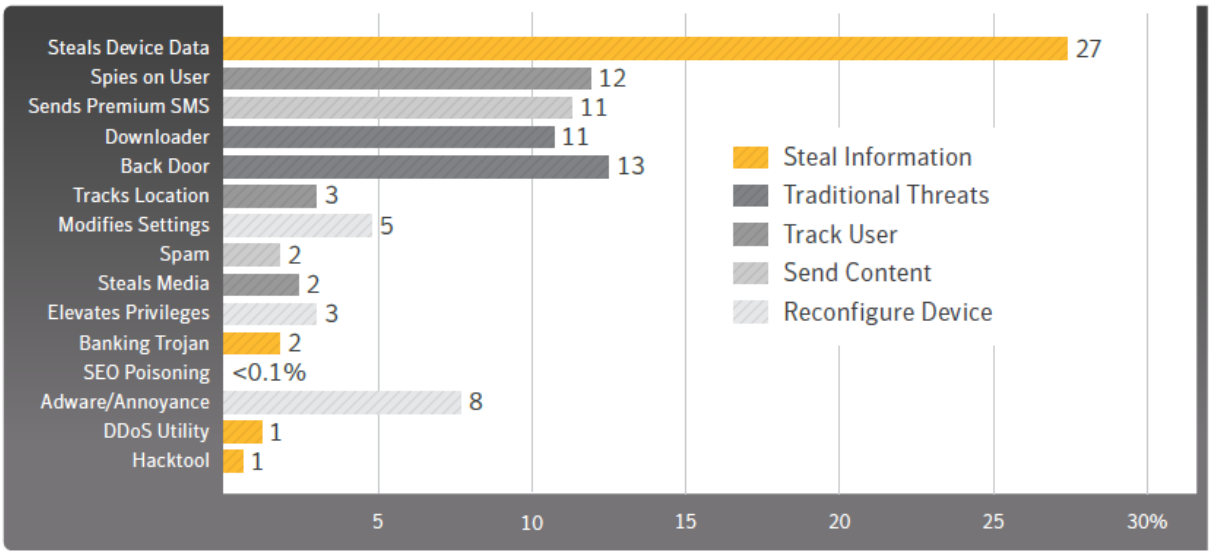
Το ζήτημα ασφαλείας προκύπτει από το ότι η κινητή συσκευή δεν είναι συνεχώς συνδεδεμένη στο εσωτερικό-ασφαλές πληροφοριακού δίκτυο μιας οντότητας της αγοράς ΗΕ. Αντίθετα, κατά τη διάρκεια κάποιων ημερών ή εβδομάδων η κινητή συσκευή συνδέεται στο Διαδίκτυο μέσω πληθώρας δικτύων Wi-Fi, που είναι στην πλειονότητά τους μη ασφαλή. Έτσι είναι ενδεχόμενο η κινητή συσκευή να έχει εκτεθεί σε κακόβουλο λογισμικό από το Διαδίκτυο ή να έχει πέσει θύμα παραβίασης κατά τη σύνδεσή της σε κάποιο μη

ασφαλές δίκτυο. Με δεδομένο το χειρότερο σενάριο, σύμφωνα με το οποίο ένας εισβολέας έχει πρόσβαση στην κινητή συσκευή και στις πληροφορίες που αυτή διαθέτει [43], όταν η συσκευή αυτή εισέλθει στο χώρο εργασίας και συνδεθεί στο εταιρικό πληροφοριακό δίκτυο, ο επίδοξος εισβολέας μπορεί, χρησιμοποιώντας την κινητή συσκευή ως ενδιάμεσο βήμα, να παραβιάσει συστήματα στο εσωτερικό δίκτυο της εταιρίας.

Ακόμη, ο επίδοξος εισβολέας μπορεί παραβιάζοντας μια έξυπνη κινητή συσκευή να υποκλέψει κωδικούς πρόσβασης του χρήστη. Αυτοί μπορούν υπό προϋποθέσεις να χρησιμοποιηθούν από τον επίδοξο εισβολέα για πρόσβαση στο εσωτερικό πληροφοριακό δίκτυο. Συχνά, οι διαχειριστές δικτύων χρησιμοποιούν την υπηρεσία VPN ώστε να παρέχουν στο υπαλληλικό προσωπικό απομακρυσμένη πρόσβαση στο εσωτερικό πληροφοριακό δίκτυο μέσω ασφαλούς καναλιού επικοινωνίας. Η ταυτοποίηση των χρηστών γίνεται συνήθως μέσω κωδικών πρόσβασης. Συνεπώς, εφόσον ένας επίδοξος εισβολέας υποκλέψει αυτά τα στοιχεία από κάποια κινητή συσκευή θα μπορεί να συνδεθεί μέσω VPN να συνδεθεί στο εσωτερικό πληροφοριακό δίκτυο.

Επιπλέον, οι κινητές συσκευές έχουν τη δυνατότητα να συνδέονται μέσω USB και να μεταφέρουν αρχεία από και προς έναν Η/Υ. Στην περίπτωση όπου έχει εγκατασταθεί κατάλληλη κακόβουλη εφαρμογή, η τελευταία μπορεί αντιλαμβανόμενη τη σύνδεση με τον Η/Υ να μεταφέρει χωρίς να γίνει αντιληπτό, αρχεία που περιέχουν κακόβουλο λογισμικό από την κινητή συσκευή στον Η/Υ . Κατ' αυτό τον τρόπο, το κακόβουλο λογισμικό μεταφέρεται από κάποια κινητή συσκευή σε ένα από τα συστήματα που είναι συνδεδεμένα συνεχώς στο εσωτερικό πληροφοριακό δίκτυο.

Η ποικιλία των πιθανών κακόβουλων ενεργειών που μπορεί να πηγάζουν από μία κινητή συσκευή μπορεί να φανεί από τα είδη κακόβουλου λογισμικού για πλατφόρμες κινητών συσκευών που αναφέρονται.



Σχήμα 4.6. Είδη κακόβουλου λογισμικού σε κινητές πλατφόρμες **[44]**

Όπως φαίνεται από το Σχ. 4.6, οι κινητές πλατφόρμες εισέρχονται στο στόχαστρο επίδοξων εισβολέων και ήδη εμφανίζεται μεγάλη ποικιλία στα είδη κακόβουλου λογισμικού που μπορεί να εκτελεστεί σε αυτές. Ως προς την ασφάλεια των συστημάτων του διαχειριστή του δικτύου ΗΕ και των παρόχων ΗΕ, από Σχ. 4.6 ενδιαφέρον παρουσιάζουν τα στοιχεία ότι το 52% των κακόβουλων λογισμικών είτε υποκλέπτει προσωπικά δεδομένα, όπως, π.χ. κωδικούς πρόσβασης, είτε δημιουργεί διόδους στο σύστημα ώστε κάποιος εισβολέας να αποκτήσει απομακρυσμένο έλεγχο είτε κατασκοπεύει το χρήστη της κινητής συσκευής και το περιβάλλον

διαβάζοντας μηνύματα και τραβώντας φωτογραφίες [43], χωρίς καμιά από τις ενέργειες αυτές να γίνεται αντιληπτή.

Με δεδομένη την αλματώδη αύξηση που παρατηρείται στα κακόβουλα λογισμικά για κινητές συσκευές, το BYOD αναδεικνύεται σε ένα εκ των κορυφαίων ζητημάτων για την ασφάλεια των συστημάτων εντός των εταιρικών πληροφοριακών δικτύων του διαχειριστή του δικτύου ΗΕ και των παρόχων ΗΕ. Η απειλή της άμεσης εισόδου στο εσωτερικό πληροφοριακό δίκτυο και της εύκολης εισχώρησης σε αυτό μέχρι το επίπεδο προστατευμένων κεντρικών συστημάτων αποτελεί το λόγο για τον οποίο το ζήτημα του BYOD πρέπει να αντιμετωπίζεται με τους πλέον αυστηρούς κανόνες και τα πλέον σύγχρονα συστήματα ασφάλειας ώστε να περιοριστούν οι ενδεχόμενοι κίνδυνοι για την ασφάλεια των εταιρικών πληροφοριακών δικτύων των εμπλεκόμενων στην αγορά ΗΕ.

1.3. Είσοδος στο δίκτυο μέσω δικτύων συνεργαζόμενων εταιριών

Για να παρέχει υπηρεσίες προς τους καταναλωτές και να υποστηρίξει την αυξημένη συνδεσιμότητα στα στοιχεία κατανάλωσης των πελατών του, ένας προμηθευτής ΗΕ πρέπει να συνεργάζεται με άλλες εταιρίες, που χρειάζονται κάποιο επίπεδο πρόσβασης σε συστήματα του εταιρικού πληροφοριακού δικτύου του προμηθευτή ΗΕ, όπως οι βάσεις δεδομένων κατανάλωσης. Αντίστοιχα, ο προμηθευτής ΗΕ χρειάζεται πρόσβαση σε δεδομένα που φυλάσσονται σε συστήματα του πληροφοριακού δικτύου του διαχειριστή του δικτύου ΗΕ. Για να επιτευχθεί αυτή η ανταλλαγή δεδομένων πραγματοποιούνται συνδέσεις μεταξύ διακομιστών των εκατέρωθεν δικτύων. Ωστόσο, δεν υπάρχει απόλυτη βεβαιότητα για την ασφάλεια του δικτύου της απέναντι πλευράς. Στην περίπτωση όπου δεν έχουν εγκατασταθεί οι κατάλληλες δικλείδες ασφαλείας για τέτοιες συνδέσεις, είναι δυνατό μέσω παραβίασης του πληροφοριακού δικτύου κάποιας συνεργαζόμενης εταιρίας, να υπάρξει παραβίαση του εσωτερικού πληροφοριακού δικτύου ενός προμηθευτή ΗΕ ή του διαχειριστή του δικτύου ΗΕ [45]. Κάθε δίοδος εισόδου στα εταιρικά πληροφοριακά δίκτυα των προμηθευτών ΗΕ και του διαχειριστή του δικτύου ΗΕ, είτε από το Διαδίκτυο είτε από απευθείας σύνδεση με δίκτυα συνεργαζόμενων εταιριών, πρέπει να θεωρείται ότι παρέχει μη ασφαλή δεδομένα κατά την επικοινωνία με το δίκτυο ενός προμηθευτή.

1.4. Εισαγωγή κακόβουλου λογισμικού μέσω USB

Ένας ακόμη πολύ συχνός τρόπος εισαγωγής και εκτέλεσης κακόβουλου κώδικα σε ένα υπολογιστικό σύστημα είναι μέσω φορητών μνημών Flash. Οι μνήμες Flash χρησιμοποιούνται από τους χρήστες για τη μεταφορά αρχείων. Ένας επίδοξος εισβολέας εισάγει τα κακόβουλα αρχεία στη μνήμη Flash και, στη συνέχεια, την τοποθετεί σε κάποιο σημείο όπου κάποιος υπάλληλος της οντότητας-στόχου θα το ανακαλύψει. Στη συνέχεια, ο επίδοξος εισβολέας βασίζεται στην περιέργεια του υπαλλήλου, ο οποίος θεωρώντας ότι ανήκει σε κάποιον εργαζόμενο στην οντότητα-στόχο, θα το συνδέσει στον Η/Υ του ώστε να δει τα αρχεία που περιέχει.

Στο σημείο αυτό, αν ο Η/Υ όπου συνδέεται η μνήμη Flash διαθέτει κάποια παλαιότερη έκδοση λογισμικού, όπως τα Windows XP [46], ο επίδοξος εισβολέας μπορεί να ρυθμίσει τη μνήμη Flash ώστε μόλις συνδεθεί να εκτελέσει κάποιο από τα αρχεία που είναι αποθηκευμένα στη μνήμη χωρίς να ενημερωθεί ο χρήστης. Σε νεότερες εκδόσεις, η λειτουργία αυτή έχει αφαιρεθεί. Στην περίπτωση αυτή, ο επίδοξος εισβολέας επιχειρεί να εξαπατήσει τον υπάλληλο, μετονομάζοντας αρχεία που περιέχουν κακόβουλο κώδικα και αποδίδοντάς τους ονομασίες έμπιστων λογισμικών, ώστε ο υπάλληλος να τα εκτελέσει πιστεύοντας ότι είναι το λογισμικό που αναγράφεται στο όνομα.

Η ανωτέρω τεχνική παραβίασης ενός εταιρικού πληροφοριακού δικτύου μιας οντότητας της αγοράς ΗΕ, έχει χρησιμοποιηθεί ως αρχικό στάδιο εισόδου σε αρκετές επιθέσεις ηλεκτρονικού πολέμου, με πλέον αξιοσημείωτο παράδειγμα την επίθεση δολιοφθοράς εναντίον των πυρηνικών σταθμών του Ιράν, γνωστή με την ονομασία Stuxnet.

1.5. Social Engineering

Το social engineering αποτελεί μία από τις παλαιότερες και ευρέως χρησιμοποιούμενες μεθόδους απόκτησης μη εξουσιοδοτημένης πρόσβασης σε ένα σύστημα. Βασίζεται σε πολύ μεγάλο βαθμό στον ανθρώπινο παράγοντα, καθώς στοχεύει αποκλειστικά κάποιο χρήστη του συστήματος-στόχου. Σε αντίθεση με τις προηγούμενες μεθόδους, είναι μια τεχνική η οποία δεν προϋποθέτει ευπάθειες στο σύστημα-στόχο. Το μόνο προαπαιτούμενο είναι η ελλιπής ενημέρωση ή η απροσεξία του χρήστη του συστήματος.

Το social engineering βασίζεται στην προτροπή από πλευράς ενός επίδοξου εισβολέα προς τον χρήστη του συστήματος-στόχου είτε να μεταβεί σε μια ιστοσελίδα είτε να εγκαταστήσει κάποιο κακόβουλο λογισμικό. Ο συνηθισμένος τρόπος με τον οποίο πραγματοποιείται κάτι τέτοιο είναι μέσω e-mail. Στα κακόβουλα αυτά e-mail, είτε αναγράφεται κάποιο link είτε υπάρχουν συνημμένα αρχεία τα οποία περιέχουν το κακόβουλο λογισμικό. Επισημαίνεται ότι εφόσον το κακόβουλο λογισμικό εγκατασταθεί με έγκριση κάποιου χρήστη, του συστήματος-στόχου έχει δικαιώματα αντίστοιχα του χρήστη στο σύστημα-στόχο.

Το social engineering, όμως, έχει εξελιχθεί κατά πολύ από το απλό παράδειγμα που παρατέθηκε προηγουμένως. Εκμεταλλευόμενος τις ιστοσελίδες κοινωνικής δικτύωσης, ένας επίδοξος εισβολέας μπορεί να συλλέξει πολλές πληροφορίες σχετικά με το χρήστη και τους συναδέλφους του. Σε συνδυασμό με τη γνώση των διευθύνσεων e-mail των συναδέλφων αυτών, μπορεί να αποστείλει e-mail τα οποία να φαίνεται πως έχουν σταλεί από διευθυντικά στελέχη της εταιρίας ή υπεύθυνους ασφαλείας. Ένα χαρακτηριστικό παράδειγμα είναι ένα mail από μια διεύθυνση σχεδόν ίδια με αυτή του υπευθύνου ασφαλείας, όπου παρακαλεί τον υπάλληλο να του αποστείλει το username και το password του για το σύστημα για να ελέγξει κάποιες ρυθμίσεις. Λόγω και της φύσης των συναδελφικών σχέσεων και της ιεραρχίας σε μια εταιρία, είτε λόγω φόβου είτε λόγω συνήθειας, ένας υπάλληλος απαντά σε ένα τέτοιο mail. Αντίστοιχο παράδειγμα είναι αυτό στο οποίο ο χρήστης μεταφέρεται σε μία ιστοσελίδα δήθεν σημαντική για το project στο οποίο εργάζεται, μία ιστοσελίδα όμως η οποία περιέχει κακόβουλο κώδικα ο οποίος παραβιάζει το σύστημά του.

Επιθέσεις τέτοιου είδους είναι σχεδόν καθημερινό φαινόμενο σε μεγάλες εταιρίες. Όπως φαίνεται, ο αριθμός των επιθέσεων ανά ημέρα είναι αρκετά υψηλός, ώστε οι επιθέσεις social engineering να αποτελούν ένα σημαντικό ποσοστό των επιθέσεων που δέχεται μια εταιρία.

Σχήμα 4.7. Αριθμός επιθέσεων μέσω στοχευμένων e-email ανά ημέρα για το έτος 2012 **[44]**

Σύμφωνα με την ίδια αναφορά το 10% αυτών των επιθέσεων στοχεύει εταιρίες του ενεργειακού κλάδου. Καθώς, λοιπόν, θα εισάγονται οι νέες τεχνολογίες του Smart Grid και θα αυξάνονται τα ενδεχόμενα οφέλη για τους επίδοξους εισβολείς, είναι αναμενόμενο το ποσοστό αυτό να αυξηθεί. Είναι επιτακτική ανάγκη αυτού του είδους οι επιθέσεις να λαμβάνονται πολύ σοβαρά υπόψη και να μην υποτιμώνται από τους υπευθύνους ασφαλείας, διότι είναι επιθέσεις με πολύ εύκολη υλοποίηση, μηδενικό κόστος για τον επιτιθέμενο και σημαντικές συνέπειες για την οντότητα-στόχο.

2. Απόκτηση δικαιωμάτων διαχειριστή

Το βήμα αυτό είναι το τελευταίο της μακράς σειράς επιθέσεων και παραβιάσεων που αναμένεται να πραγματοποιήσει ένας επίδοξος εισβολέας προκειμένου να επιτεθεί σε ένα υπολογιστικό σύστημα. Στόχος του συγκεκριμένου βήματος, είναι η αναβάθμιση των δικαιωμάτων πρόσβασης που έχει στο σύστημα ένας επίδοξος εισβολέας, από αυτά ενός απλού χρήστη σε εκείνα του διαχειριστή. Ο λόγος είναι ότι ο διαχειριστής έχει πλήρη δικαιώματα και έλεγχο των συνδεδεμένων συσκευών, των αρχείων και όλου του λογισμικού που είναι εγκατεστημένο στο εν λόγω σύστημα-στόχο. Επομένως, αν ο επίδοξος εισβολέας καταφέρει να εκτελέσει κακόβουλο λογισμικό με πλήρη δικαιώματα, αυτό έχει πρόσβαση σε κάθε τμήμα του συστήματος μεγιστοποιώντας την αποτελεσματικότητά του και τις συνέπειες για το σύστημα-στόχο. Ένας ακόμη λόγος που επιδιώκονται τα πλήρη δικαιώματα σε ένα σύστημα είναι να γίνει αποτελεσματικά η απόκρυψη από το σύστημα των ιχνών παραβίασης και η διατήρηση της δυνατότητας παραβίασης μετά από μία επανεκκίνηση.

Οι μέθοδοι μέσω των οποίων μπορεί να επιτευχθεί ο ανωτέρω στόχος είναι ίδιες με εκείνες που χρησιμοποιήθηκαν σε προηγούμενα στάδια. Μία μέθοδος είναι η εκ νέου εκμετάλλευση ευπαθειών είτε του λειτουργικού συστήματος είτε των λογισμικών που τρέχουν με πλήρη δικαιώματα. Γενικά, η εύρεση ευπαθειών τέτοιου είδους στα λειτουργικά συστήματα είναι πιο δύσκολη καθώς λόγω της καθολικής χρήσης

τους οποιαδήποτε ευπάθεια έχει μεγάλες πιθανότητες να ανακαλυφθεί και να διορθωθεί, ωστόσο έχουν παρατηρηθεί εξαιρέσεις. Αντίθετα, πολύ συχνότερα, ένα κακόβουλο λογισμικό επιτυγχάνει να αποκτήσει πλήρη δικαιώματα εκμεταλλευόμενο ένα κενό ασφαλείας σε ένα άλλο λογισμικό που τρέχει νόμιμα υπό πλήρη δικαιώματα. Μία επιτυχημένη παραβίαση του λογισμικού αυτού μπορεί να εγκαταστήσει στον κώδικα της νόμιμης εφαρμογής ένα σύνδεσμο προς το κακόβουλο λογισμικό ώστε να το καλεί όταν εκτελείται. Κατ' αυτό τον τρόπο, το κακόβουλο λογισμικό οικειοποιείται τα δικαιώματα του νόμιμου λογισμικού, που σε αυτή την περίπτωση είναι δικαιώματα διαχειριστή, επιτυγχάνοντας έτσι το σκοπό του.

Μία δεύτερη μέθοδος είναι η υποκλοπή των κωδικών πρόσβασης ενός χρήστη με πλήρη δικαιώματα όπως είναι ο διαχειριστής του συστήματος. Η πλέον συνηθισμένη περίπτωση είναι η δοκιμή των πιθανότερων κωδικών πρόσβασης. Αν η δοκιμή αυτή αποτύχει, ο επίδοξος εισβολέας επιχειρεί να υποκλέψει τα αρχεία του συστήματος που περιέχουν τις τιμές κατακερματισμού του κωδικού πρόσβασης κάθε χρήστη. Σε παλαιότερες, μη ασφαλείς, εκδόσεις λειτουργικών συστημάτων της οικογένειας UNIX, οι τιμές κατακερματισμού ήταν συγκεντρωμένες σε ένα αρχείο το οποίο ήταν προσβάσιμο από όλους τους χρήστες. Έτσι, ένας επίδοξος εισβολέας, μπορούσε να το μεταφέρει στο τοπικό του σύστημα και με τη βοήθεια λογισμικών για παραβίαση κωδικών πρόσβασης να επιχειρήσει να ανακαλύψει τον κωδικό. Σε νεότερες εκδόσεις, το αρχείο με τις τιμές κατακερματισμού των κωδικών πρόσβασης, είναι προσβάσιμο μόνο από χρήστες με πλήρη δικαιώματα, αυξάνοντας κατ' αυτό τον τρόπο σημαντικά την ασφάλεια των κωδικών πρόσβασης.

Στην περίπτωση όμως, όπου το σύστημα που έχει παραβιαστεί χρησιμοποιείται μόνο ως ένα βήμα εντός του εταιρικού πληροφοριακού δικτύου, με στόχο το κακόβουλο λογισμικό να διαδοθεί βαθύτερα, είναι πιθανότερο ο επίδοξος εισβολέας να μη χρειάζεται πλήρη δικαιώματα. Είναι πιθανό, λοιπόν, αυτό το στάδιο να παραλειφθεί σε συστήματα μικρής σημασίας για τον τελικό στόχο κάποιου επίδοξου εισβολέα. Εντούτοις, οι επιθέσεις για αναβάθμιση δικαιωμάτων αποτελούν αναπόσπαστο τμήμα της αλληλουχίας επιθέσεων εναντίον κεντρικών συστημάτων ενός εταιρικού πληροφοριακού δικτύου.

4.5.4. Διαγραφή - απόκρυψη του κακόβουλου λογισμικού

Μετά από μια επιτυχημένη παραβίαση ενός συστήματος από κακόβουλο λογισμικό, αυτό αναλαμβάνει να εκτελέσει την κύρια λειτουργία του. Στην περίπτωση ενός κεντρικού συστήματος μιας οντότητας της αγοράς ΗΕ, η λειτουργία αυτή ενδέχεται να είναι η υποκλοπή δεδομένων των πελατών της. Μέχρι στιγμής, προκειμένου να τα επιτύχει αυτά, ένα κακόβουλο λογισμικό πρέπει να διαθέτει εργαλεία ώστε να εκμεταλλεύεται ευπάθειες του συστήματος στο οποίο εκτελείται και να μπορεί μέσω του δικτύου να παραβιάσει γειτονικά συστήματα, με στόχο να αποκτήσει πρόσβαση σε συστήματα τοποθετημένα βαθύτερα στο εταιρικό πληροφοριακό δίκτυο.

Στα συστήματα όμως που έχουν ήδη παραβιαστεί, το κακόβουλο λογισμικό περνά στο τελευταίο στάδιο της μεθοδολογίας επίθεσης που ακολουθείται, το οποίο είναι είτε η διαγραφή του, είτε η απόκρυψή του. Όταν το λογισμικό αντιληφθεί ότι η αποστολή του σε ένα σύστημα έχει ολοκληρωθεί, αυτοκαταστρέφεται διαγράφοντας κάθε ίχνος της ύπαρξής του στο συγκεκριμένο σύστημα από τα αρχεία καταγραφής, ώστε να μην γίνει αντιληπτή στο μέλλον η παραβίαση. Στην περίπτωση όπου πρέπει η παραβίαση να διατηρηθεί, το λογισμικό παραμένει σε λανθάνουσα μορφή στο σύστημα, αναμένοντας εντολές ή τη διαμόρφωση συγκεκριμένων συνθηκών στις οποίες έχει προγραμματιστεί η επανενεργοποίησή του. Ακόμα και στο σημείο όπου το δίκτυο και τα συστήματα που είναι συνδεδεμένα σε αυτό έχουν ήδη παραβιαστεί, είναι μεγάλης σημασίας να υπάρχουν εξειδικευμένα συστήματα παρακολούθησης ώστε να συγκεντρωθούν στοιχεία και ίχνη από την παραβίαση. Αυτό αφού ακόμη και μετά από μία επιτυχημένη παραβίαση, είναι πολύ σημαντικό

για τους υπεύθυνους ασφαλείας να έχουν συλλέξει στοιχεία ικανά να ρίξουν φως στις επιμέρους λειτουργίες ενός κακόβουλου λογισμικού με σκοπό την αποφυγή παρόμοιων παραβιάσεων στο μέλλον. Επιπλέον, αν οι υπεύθυνοι ασφάλειας διαθέτουν στοιχεία για τη δράση του κακόβουλου λογισμικού, είναι σε θέση να υπολογίσουν τις συνέπειες της δράσης του. Για το λόγο αυτό, είναι αναγκαία η αποτροπή του λογισμικού από το να καταφέρει να εξαφανίσει πλήρως τα ίχνη του.

4.5.5. Επιθέσεις DoS (Denial of Service)

Μέχρι στιγμής έχουν αναλυθεί μέθοδοι επίθεσης εναντίον συστημάτων ενός εταιρικού πληροφοριακού δικτύου μιας οντότητας της αγοράς ΗΕ με σκοπό την παραβίασή τους και την εισαγωγή κακόβουλου λογισμικού είτε για έλεγχο των συστημάτων είτε για την απόκτηση πρόσβασης σε περισσότερο προστατευμένα συστήματα εντός του εταιρικού πληροφοριακού δικτύου. Πολύ συχνά, ωστόσο, στόχος μιας επίθεσης είναι να τεθεί ένα σύστημα ή μια υπηρεσία, που παρέχεται από το διαχειριστή του δικτύου ΗΕ ή ένα προμηθευτή ΗΕ, προσωρινά εκτός λειτουργίας. Προς αυτή την κατεύθυνση κινούνται οι επιθέσεις τύπου DoS.

Οι επιθέσεις DoS υπήρχαν ως ιδέα από τις αρχές της δεκαετίας του 1990. Ωστόσο, τα τελευταία χρόνια, έχει παρατηρηθεί αύξηση στον αριθμό των επιθέσεων τέτοιου είδους, καθώς και στην κλίμακα των επιθέσεων αυτών. Η ισχύς μια επίθεσης DoS μετράται με το ρυθμό δεδομένων και αιτήσεων με τον οποίο κατακλύζεται το σύστημα-στόχος. Τέτοιες αιτήσεις μπορούν να είναι:

- Ψεύτικα πακέτα με τυχαίες τιμές
- Ημιτελείς αιτήσεις TCP, όπου αφήνουν το διακομιστή με χιλιάδες ημιτελείς συνδέσεις. Οι αιτήσεις ανανεώνονται με ρυθμό μεγαλύτερο από αυτόν με τον οποίο ο διακομιστής τις απορρίπτει, ώστε να μην μπορεί να ανταποκριθεί σε νέες πραγματικές αιτήσεις.
- Αιτήματα HTTP για πόρους και ιστοσελίδες που διαθέτει ο διακομιστής με πολύ μικρή ταχύτητα. [47]

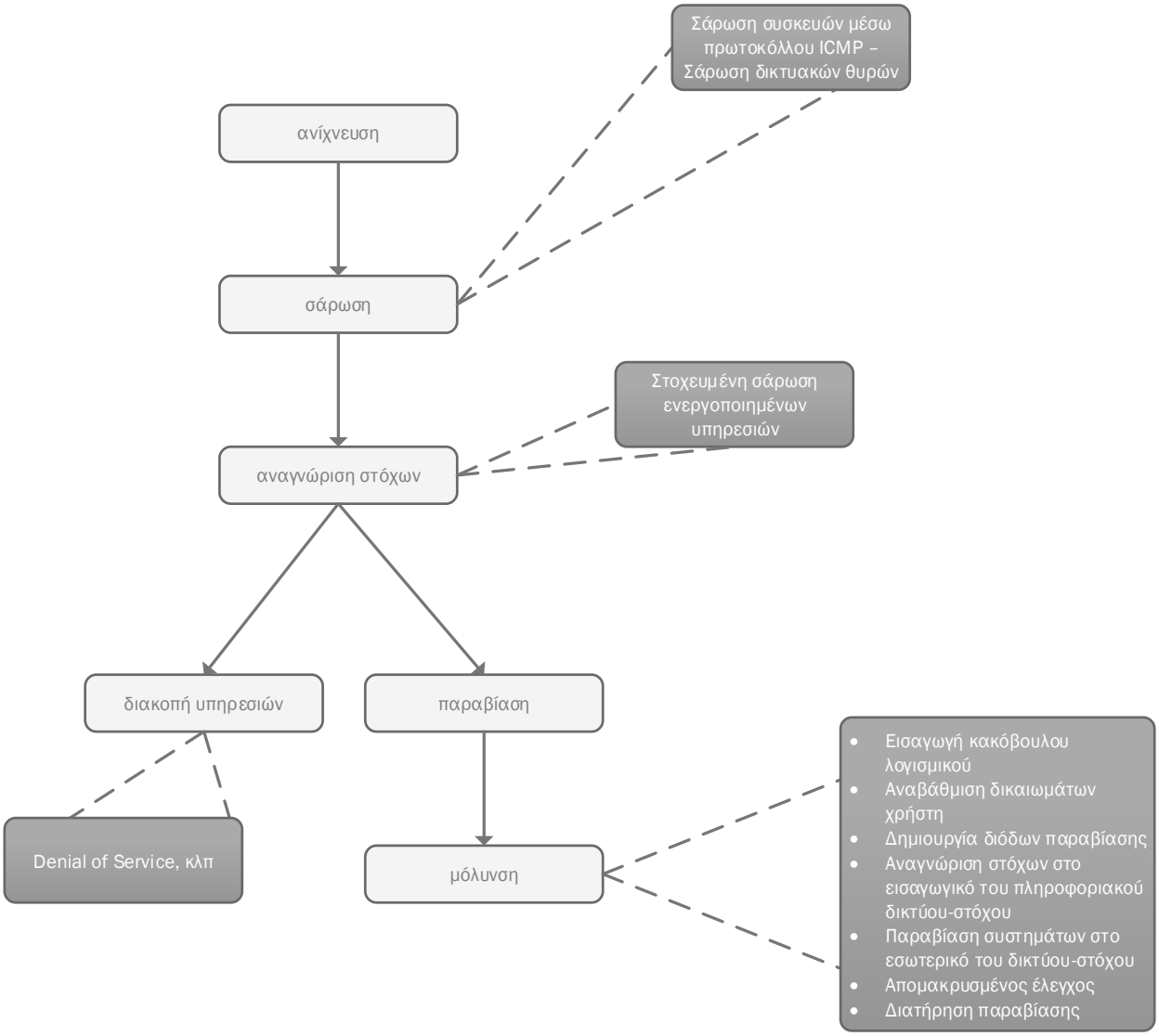
Ο ρυθμός με το οποίο αποστέλλονται οι αιτήσεις των ανωτέρω τύπων είναι τέτοιος ώστε μετά από λίγο ο διακομιστής να μην είναι σε θέση να ανταποκριθεί σε νέες αιτήσεις, καθώς οι πόροι του, είτε υπολογιστικοί (CPU/RAM) είτε δικτυακοί (bandwidth) φθάνουν σε σημείο κορεσμού και δεν μπορούν να δεχθούν τις πραγματικές αιτήσεις. Πλέον, οι περισσότερες επιθέσεις DoS εμπίπτουν στην υποκατηγορία DDoS (Distributed Denial of Service), όπου τα συστήματα που κατακλύζουν με αιτήματα ένα στόχο είναι εκατοντάδες. Τα συστήματα αυτά ανήκουν συνήθως σε δίκτυα παραβιασμένων συστημάτων που ονομάζονται botnets, και στα οποία κάποιος διαχειριστής αποστέλλει εντολές. Με τη βοήθεια λογισμικών όπως το High Orbit Ion Cannon [48], τέτοιες επιθέσεις μπορούν να πραγματοποιηθούν με χαρακτηριστική ευκολία και με πλήρως αυτοματοποιημένο τρόπο.

Στόχοι τέτοιων επιθέσεων είναι τα συστήματα ενός εταιρικού πληροφοριακού δικτύου που είναι προσβάσιμα μέσω Διαδικτύου και τα οποία συχνά για λόγους λειτουργικότητας δεν βρίσκονται πίσω από αυστηρά firewall. Τυπικούς στόχους αποτελούν οι web και mail servers του δικτύου καθώς και εξυπηρετητές που εκθέτουν ορισμένες από τις πληροφορίες στο καταναλωτικό κοινό όπως τα στοιχεία κατανάλωσης και τιμολόγησης. Σε όλες αυτές τις περιπτώσεις και για όλη την διάρκεια μιας επίθεσης, οι ανωτέρω υπηρεσίες δεν είναι στη διάθεση του καταναλωτικού κοινού. Οι επιθέσεις DoS είναι μία από τις σημαντικότερες επιθέσεις εναντίον του Smart Grid, καθώς είναι μια μέθοδος που υλοποιείται ταυτοχρόνως από πολλά

επιμέρους συστήματα που πρέπει να είναι συγχρόνως διαθέσιμα ώστε να προσφέρονται όλες οι υπηρεσίες του.

4.5.6. Σύνοψη μεθοδολογίας επίθεσης

Στα εδάφια που προηγήθηκαν έγινε η ανάλυση της μεθοδολογίας που ακολουθείται από κάποιους επίδοξους εισβολείς που έχουν ως στόχο την παραβίαση του εταιρικού πληροφοριακού δικτύου μιας οντότητας της αγοράς ΗΕ και συστημάτων που είναι συνδεδεμένα σε αυτό. Στη συνέχεια, γίνεται η ανάλυση των μεθόδων με τις οποίες μπορεί να προστατευτεί ένα εταιρικό πληροφοριακό από κακόβουλες επιθέσεις. Στο σημείο αυτό, πραγματοποιείται μια μικρή σύνοψη των βημάτων που ακολουθούνται από επίδοξους εισβολείς, ώστε να είναι ευκολότερη η κατανόηση των επόμενων εδαφίων.



Σχήμα 4.8 Σχηματική απεικόνιση των σταδίων μιας ολοκληρωμένης επίθεσης εναντίον ενός εταιρικού πληροφοριακού δικτύου **[49]**

Στο Σχ. 4.8 απεικονίζονται τα στάδια μιας ολοκληρωμένης επίθεσης εναντίον ενός εταιρικού πληροφοριακού δικτύου και η ακολουθία με την οποία αυτά πραγματοποιούνται. Το πρώτο στάδιο της αλληλουχίας μεθόδων επίθεσης είναι αυτό της ανίχνευσης της οντότητας-στόχου. Στο στάδιο αυτό ο επίδοξος εισβολέας επιχειρεί να συλλέξει όσο το δυνατό περισσότερες πληροφορίες για την οντότητα-στόχο, το εταιρικό πληροφοριακό της δίκτυο και τα συστήματα που βρίσκονται σε αυτό, από το Διαδίκτυο και άλλες δημόσια προσβάσιμες πηγές. Στη συνέχεια, προχωρεί στη σάρωση του δικτύου, όπου ο επίδοξος εισβολέας έρχεται για πρώτη φορά σε επαφή με το δίκτυο, καθώς χρησιμοποιεί κατάλληλα εργαλεία για να σαρώσει τις δικτυακές θύρες συστημάτων του εταιρικού πληροφοριακού δικτύου και να εξακριβώσει τα στοιχεία των διάφορων εργαλείων και λογισμικών που εκτελούνται σε κάθε σύστημα. Έπειτα, γίνεται η αναγνώριση και επιλογή των αρχικών στόχων μεταξύ των συστημάτων στην περίμετρο του δικτύου . Γίνεται περαιτέρω έρευνα των υπηρεσιών που εκτελούνται από κάθε σύστημα, μέχρι να κριθεί σκόπιμη η συνέχεια στο επόμενο στάδιο, αυτό της επίθεσης. Στο στάδιο της επίθεσης υπάρχουν δύο επιλογές που μπορεί να ακολουθήσει ένας επίδοξος εισβολέας. Η πρώτη είναι να επιχειρήσει την παραβίαση του συστήματος με τελικό στόχο τη μόλυνση του συστήματος και τον πλήρη έλεγχό του. Η δεύτερη επιλογή είναι να επιχειρήσει τη διακοπή της διαθεσιμότητας του συστήματος-στόχου. Αυτό πραγματοποιείται μέσω μιας επίθεσης DoS για την οποία δεν είναι απαραίτητη η παραβίαση του συστήματος. Τέλος, ο επίδοξος εισβολέας επιχειρεί είτε την απόκρυψη και διατήρηση της παραβίασης, είτε τη διείσδυση του κακόβουλου λογισμικού προς συστήματα προς το εσωτερικό του εταιρικού πληροφοριακού δικτύου.

4.6. Τρόποι αντιμετώπισης των απειλών στο εταιρικό πληροφοριακό δίκτυο

Όπως ήδη έχει γίνει φανερό, οι απειλές για το εταιρικό πληροφοριακό δίκτυο μιας οντότητας της αγοράς ΗΕ είναι πολλαπλές και παρουσιάζουν μεγάλη ποικιλομορφία. Κάθε στάδιο μιας επίθεσης έχει διαφορετικό στόχο και διαφορετικά εργαλεία τα οποία χρησιμοποιεί ένας επίδοξος εισβολέας για να τον επιτύχει. Η επίτευξη της ασφάλειας ενός εταιρικού πληροφοριακού δικτύου είναι δύσκολη και απαιτεί εργαλεία και συστήματα ασφάλειας τελευταίας τεχνολογίας και μεγάλης πολυπλοκότητας. Η μεγάλη πρόκληση της ασφάλειας του δικτύου έγκειται στο ότι για την επίτευξή της είναι απαραίτητο να έχουν διασφαλιστεί όλες οι πιθανές δίοδοι επίθεσης. Αντίθετα, για την παραβίασή της απαιτείται μόνο μία μη ασφαλισμένη δίοδος επίθεσης. Αν συνυπολογιστεί και το μέγεθος ενός εταιρικού πληροφοριακού δικτύου στην εποχή του Smart Grid, γίνεται φανερό ότι χρειάζεται κεντρικός σχεδιασμός και διαχείριση του δικτύου, ώστε να εξασφαλιστεί στο μέγιστο βαθμό η ασφάλεια των υποδομών του.

Το Smart Grid περιλαμβάνει πληθώρα διαφορετικών ειδών συστημάτων, με διαφορετική αρχιτεκτονική, λειτουργικό σύστημα υπηρεσίες που εκτελούνται σε αυτά. Καίτοι η μεγάλη πλειοψηφία αυτών δεν είναι συνδεδεμένη στο εταιρικό πληροφοριακό δίκτυο μιας οντότητας της αγοράς ΗΕ, τα εταιρικά πληροφοριακά δίκτυα των οντοτήτων αυτών συχνά αποτελούν συνδετικό κρίκο μεταξύ τέτοιων συστημάτων. Για παράδειγμα, τα δεδομένα από τους αυτόματους μετρητές μεταφέρονται στο κέντρο τιμολόγησης ενός προμηθευτή ΗΕ και, μετά από επεξεργασία, δίνεται σήμα για προσαρμογή της παραγωγής ηλεκτρικής ενέργειας στα δεδομένα της ζήτησης. Ακόμη, δεδομένα κατανάλωσης μεταφέρονται προς συστήματα καταγραφής του διαχειριστή του δικτύου ΗΕ και προς τα κεντρικά συστήματα επεξεργασίας των σταθμών παραγωγής ΗΕ. Από τις ανωτέρω πληροφορίες, πολλές περνούν σε κάποιο στάδιο της διάδοσής τους από ένα ή περισσότερα πληροφοριακά

δίκτυα των οντοτήτων της αγοράς ΗΕ. Για να διασφαλιστεί, επομένως, η ασφάλεια του Smart Grid, πρέπει να διασφαλιστούν και όλα τα επιμέρους δίκτυα με τα οποία συνεργάζεται όπως είναι τα εταιρικά πληροφοριακά δίκτυα.

4.6.1. Ασφάλεια της περιμέτρου του δικτύου

Η συντριπτική πλειοψηφία των επιθέσεων εναντίον εταιρικών πληροφοριακών δικτύων πηγάζει από το εξωτερικό του δικτύου και συχνότερα από το Διαδίκτυο. Για να διασφαλιστεί το δίκτυο από τέτοιες επιθέσεις, απαιτούνται εργαλεία που δημιουργούν μια περίμετρο στο δίκτυο, την οποία έχουν στόχο να διασφαλίσουν. Ενδεικτικά, τέτοια εργαλεία είναι τα firewalls, IDS/IPS (Intrusion Detection/Prevention Systems), Access Control Lists, VPNs και άλλα.

Η περίμετρος ενός δικτύου περιλαμβάνει όλα τα συστήματα που επικοινωνούν με εξωτερικά δίκτυα ή το Διαδίκτυο. Εφόσον διασφαλιστούν τα συστήματα της περιμέτρου του εταιρικού πληροφοριακού δικτύου και οι εξωτερικές συνδέσεις που πραγματοποιούν, επιτυγχάνεται η ασφάλεια του δικτύου σε αρκετά μεγάλο βαθμό. Αυτό το στόχο έχουν οι μέθοδοι που αναλύονται στη συνέχεια.

1. Ασφάλεια συστημάτων προσβάσιμων από το Διαδίκτυο

Ορισμένα συστήματα ενός εταιρικού πληροφοριακού δικτύου παρέχουν υπηρεσίες σε χρήστες από το Διαδίκτυο, όπως οι web εξυπηρετητές. Τα συστήματα αυτά είναι αναγκαίο να είναι διαχωρισμένα από το υπόλοιπο δίκτυο, μέσω ζωνών DMZ, ώστε, ακόμα και σε περίπτωση παραβίασής τους, το υπόλοιπο δίκτυο να παραμένει ασφαλές. Επιπλέον, ανάλογα με τις υπηρεσίες που παρέχουν τα συστήματα αυτά, πρέπει να εντάσσονται σε διαφορετικές ζώνες DMZ ανά παρεχόμενη υπηρεσία.

Τα συστήματα που είναι προσβάσιμα μέσω Διαδικτύου αποτελούν τους πιθανότερους στόχους για επιθέσεις DoS. Καίτοι πολύ μεγάλης σημασίας, η ασφάλεια έναντι τέτοιων επιθέσεων είναι πολύ δύσκολη καθώς δεν είναι δυνατή η ολοκληρωτική αποφυγή τους. Προς την κατεύθυνση της ασφάλειας από επιθέσεις DoS, εγκαθίστανται συστήματα firewall και IPS στην περίμετρο του δικτύου, με σκοπό των έλεγχο των συνδέσεων. Τα συστήματα αυτά πρέπει υλοποιούν σύγχρονες τεχνικές, όπως Deep Packet Inspection και Application Session Inspection, για μεγαλύτερα ποσοστά ανίχνευσης και αποτροπής επιθέσεων. Συγκεκριμένα, η μέθοδος Application Session Inspection, η οποία είναι και η πλέον εξελιγμένη, πραγματοποιεί έλεγχο στο εσωτερικό των πακέτων αναγνωρίζοντας τις λειτουργίες των πρωτοκόλλων που συναντά και αναγνωρίζοντας τις υψηλού επιπέδου λειτουργίες που επιτελεί κάθε σύνδεση. Επιπλέον, τα συστήματα αυτά ελέγχουν την εισερχόμενη κίνηση για εμφάνιση προτύπων που έχουν αναγνωριστεί ως ίχνη επιθέσεων DoS και αποτρέπουν τα αντίστοιχα πακέτα από το να φθάσουν το στόχο τους, ενημερώνοντας παράλληλα τους υπευθύνους ασφάλειας όταν η απειλή κριθεί σημαντική. Για παράδειγμα, αν παρατηρηθεί εκθετική αύξηση των εισερχόμενων πακέτων που είτε είναι «σκουπίδια» είτε έχουν συγκεκριμένη μορφή που δεν συνάδει με την κανονική κίνηση του δικτύου, τα συστήματα IPS μπορούν να αναγνωρίσουν μια επίθεση και να την αναχαιτίσουν.

2. Απομακρυσμένη σύνδεση

Τα τελευταία χρόνια η πληροφορική και τα προϊόντα της έχουν αναπτύξει έντονα το χαρακτηριστικό της κινητικότητας αξιοποιώντας συσκευές όπως notebooks, tablets, smartphones και υπηρεσίες cloud που παρέχουν τη δυνατότητα στο χρήστη να μπορεί να εργάζεται απομακρυσμένα χωρίς κανένα πρόβλημα. Αυτό επιτυγχάνεται με την απομακρυσμένη σύνδεση χρηστών με συστήματα στο εσωτερικό εταιρικών πληροφοριακών δικτύων. Μία τέτοια δυνατότητα από την πλευρά του διαχειριστή του δικτύου προς του χρήστες του, αν και αναγκαία, δημιουργεί πολλαπλές διόδους επίθεσης. Επομένως, είναι απαραίτητο να διασφαλίζονται αυτές οι συνδέσεις ώστε να μην είναι εύκολο για επίδοξους εισβολείς να παραβιάσουν την ασφάλεια του δικτύου.

Για το σκοπό αυτό χρησιμοποιείται το πρωτόκολλο VPN για απομακρυσμένη είσοδο στο εταιρικό πληροφοριακό δίκτυο και πρωτόκολλα remote desktop όπως τα VNC και RDP, που παρέχουν από άκρο σε άκρο κρυπτογράφηση της σύνδεσης και διασφάλιση της ακεραιότητας των δεδομένων. Το τρωτό σημείο των προαναφερθέντων πρωτοκόλλων είναι η ταυτοποίηση των χρηστών. Η ταυτοποίηση χρηστών βασίζεται στο απλό μοντέλο χρήσης username/password και σπανιότερα σε αυτό των ψηφιακών πιστοποιητικών. Όμως, για τη σύνδεση σε ένα δίκτυο όπου είναι συνδεδεμένα πολλά συστήματα κρίσιμα για τις υποδομές του Smart Grid, δεν είναι επαρκής κανένας από τους δύο αυτούς τρόπους. Ως προς το μοντέλο κωδικών πρόσβασης, το ότι πολλοί χρήστες είτε επιλέγουν εύκολους κωδικούς είτε κάποιο δύσκολο που όμως χρησιμοποιούν παντού στο Διαδίκτυο, καθιστά τον τρόπο αυτόν ταυτοποίησης μακροπρόθεσμα μη ασφαλή. Ακόμα και αν επιβληθεί από το τμήμα ασφάλειας πολιτική αλλαγής κωδικών ανά τακτά χρονικά διαστήματα, οι χρήστες επιλέγουν πολύ εύκολους κωδικούς ή τον ίδιο με προβλέψιμες μικροαλλαγές. Ως προς το μοντέλο των ψηφιακών πιστοποιητικών, αυτά παρέχουν μεγαλύτερη ασφάλεια σε σχέση με τους κωδικούς πρόσβασης έναντι μεθόδων ανίχνευσης κλειδιών πρόσβασης, ωστόσο, δημιουργούν κενά ασφαλείας από τη στιγμή που μία από τις κινητές συσκευές του χρήστη κλαπεί και μέχρι να ακυρωθεί η πρόσβαση στο συγκεκριμένο πιστοποιητικό.

Η προτεινόμενη λύση είναι η ταυτοποίηση των χρηστών σε δύο ή περισσότερα στάδια (multi-factor authorization). Η συγκεκριμένη μέθοδος ταυτοποίησης απαιτεί δεύτερο προσωρινό κωδικό κατά την ταυτοποίηση. Αυτός ο κωδικός παράγεται από μια συνάρτηση με παράμετρο, συνήθως, το παράθυρο χρόνου μέσα στο οποίο γίνεται η αίτηση για ταυτοποίηση. Ο προσωρινός κωδικός είναι έγκυρος μόνο στο διάστημα του χρονικού παραθύρου που έχει οριστεί και συνήθως είναι 30s. Η συνάρτηση που παράγει αυτούς τους κωδικούς είναι γνωστή μόνο στη συσκευή του εκάστοτε χρήστη και σε ένα εξυπηρετητή πιστοποίησης, και δημιουργείται με βάση κάποιο τυχαίο αριθμό seed. Έτσι, κατά την ταυτοποίηση, ο χρήστης παράγει και αποστέλλει, μαζί με τα κανονικά του στοιχεία πρόσβασης, και τον προσωρινό κωδικό. Ο εξυπηρετητής, μέσω των στοιχείων πρόσβασης του χρήστη προσδιορίζει τη συνάρτηση παραγωγής προσωρινών κωδικών που χρησιμοποιείται για τον συγκεκριμένο χρήστη. Στη συνέχεια, ο εξυπηρετητής υπολογίζει μέσω της συνάρτηση τον προσωρινό κωδικό επανυπολογίζει για το χρονικό παράθυρο της σύνδεσης. Αν οι δύο κωδικοί συμπίπτουν τότε ο χρήστης είναι έγκυρος και ταυτοποιείται επιτυχώς. Πρακτικά, τέτοιοι κωδικοί παράγονται είτε από εφαρμογές έξυπνων κινητών συσκευών, είτε από εξειδικευμένες για το σκοπό αυτό συσκευές. Έτσι, ένας επίδοξος εισβολέας ακόμη και αν υποκλέψει τα στοιχεία πρόσβασης ενός χρήστη, δεν μπορεί να συνδεθεί καθώς δεν έχει τρόπο να ανιχνεύσει τον προσωρινό κωδικό.

Ένα ακόμη αποτελεσματικότερο μέτρο ασφάλειας, εφόσον κριθεί απαραίτητη η χρησιμοποίησή του, είναι να φιλτράρονται οι συνδέσεις βάσει των διευθύνσεων IP των χρηστών. Κάτι τέτοιο είναι εφικτό με την εγκατάσταση συστημάτων ACL (Access Control List), τα οποία ελέγχουν τις επιχειρούμενες συνδέσεις και απορρίπτουν όσες δεν προέρχονται από γνωστά συστήματα. Έτσι, ένας επίδοξος εισβολέας δεν μπορεί να

εγκαταστήσει σύνδεση με τον εξυπηρετητή VPN ώστε να επιχειρήσει να τον παραβιάσει ή να συνδεθεί με στοιχεία που έχουν υποκλαπεί. Τέλος, οι εξυπηρετητές VPN πρέπει να είναι τοποθετημένοι σε δική τους ζώνη DMZ, όντας συστήματα προσβάσιμα από το Διαδίκτυο, ώστε, ακόμα και αν παραβιαστούν να μη διατρέχουν κίνδυνο τα υπόλοιπα συστήματα του εταιρικού πληροφοριακού δικτύου.

4.6.2. Έλεγχος της κίνησης του δικτύου

Μέχρι εδώ, αναλύθηκαν μέθοδοι ασφάλειας εναντίον απειλών που πηγάζουν εκτός του εταιρικού πληροφοριακού δικτύου. Ωστόσο, υπάρχουν σημαντικές απειλές που πηγάζουν από το εσωτερικό του δικτύου. Αυτές οι απειλές μπορούν να δημιουργηθούν από σύνδεση άγνωστων συσκευών USB και κινητών συσκευών που εμπίπτουν στην κατηγορία BYOD.

Τα συστήματα ασφάλειας εναντίον απειλών όπως το BYOD (Bring Your Own Device) βασίζονται σε τεχνικές παρακολούθησης της δικτυακής κίνησης, της αναγνώρισης προτύπων και της μηχανικής μάθησης. Ως προς τις τεχνικές παρακολούθησης της δικτυακής κίνησης, όπως και τα εξελιγμένα firewalls, έχουν τη δυνατότητα να αναγνωρίζουν τα πρωτόκολλα της δικτυακής κίνησης και τις υψηλού επιπέδου λειτουργίες που αυτά επιτελούν με κάθε σύνδεση. Στη συνέχεια, επί των δεδομένων δικτυακής κίνησης εφαρμόζουν τεχνικές αναγνώρισης προτύπων και μηχανικής μάθησης, με στόχο να αναγνωρίσουν το πρότυπο της κίνησης και να αποφασίσουν αν αυτό το πρότυπο έχει παραχθεί από τη φυσιολογική λειτουργία των συστημάτων εντός του δικτύου. Όταν παρατηρηθεί κίνηση στο δίκτυο που δεν εμπίπτει σε γνωστά πρότυπα και θεωρηθεί μη φυσιολογική, ενημερώνονται οι υπεύθυνοι ασφαλείας και ενεργοποιούνται αυτόματοι μηχανισμοί αποτροπής επιθέσεων. Πρέπει, ωστόσο, να σημειωθεί ότι τα συγκεκριμένα συστήματα έχουν υψηλό υπολογιστικό κόστος και είναι αποτελεσματικότερα όταν προστατεύουν συστήματα με σχετικά σταθερή λειτουργία. Έτσι, η χρήση τους στο εταιρικό πληροφοριακό δίκτυο προτείνεται μόνο για προστασία κρίσιμων υποδομών του Smart Grid.

Τα σύγχρονα συστήματα παρακολούθησης κίνησης μπορούν να εφοδιαστούν με πρόσθετες δυνατότητες. Μία από αυτές είναι ο ορισμός ρόλων για τους χρήστες των κρίσιμων υποδομών του εταιρικού πληροφοριακού δικτύου. Κατ' αυτό τον τρόπο συσχετίζονται οι ρόλοι που επιτελεί κάθε εργαζόμενος με επιτρεπτά πρότυπα κίνησης που παράγει. Έτσι, όταν παρατηρηθεί απόκλιση της δικτυακής κίνησης που παράγεται από αυτή που παράγεται υπό φυσιολογικές συνθήκες, θεωρείται πιθανή η παραβίαση του συστήματος και ενημερώνεται ο διαχειριστής του δικτύου. Ακόμη, είναι δυνατή η αποθήκευση της κίνησης που παρατηρήθηκε ώστε να είναι δυνατή η αναπαραγωγή της μετά από μία επιτυχημένη επίθεση και να γίνει ανάλυσή της.

Καίτοι τα εξελιγμένα συστήματα παρακολούθηση της κίνησης του εταιρικού πληροφοριακού δικτύου είναι πολύ αποτελεσματικά, εμφανίζουν ορισμένα μειονεκτήματα που αποτρέπουν τη χρήση τους σε όλο το εταιρικό πληροφοριακό δίκτυο. Αρχικά, έχουν αυξημένο οικονομικό κόστος σε σχέση με απλούστερες λύσεις ασφάλειας. Επιπλέον, η λειτουργία τους απαιτεί υψηλή υπολογιστική ισχύ. Τέλος, δεν ενδείκνυται η χρήση τους για παρακολούθηση συστημάτων απλών χρηστών καθώς η αυστηρότητα των ελέγχων και των αυτόματων ενεργειών που εκτελούν αυτά τα συστήματα, μπορεί να μειώσει σημαντικά την παραγωγικότητα των χρηστών, προστατεύοντας παράλληλα συστήματα που δεν θεωρούνται κρίσιμα για τη λειτουργία του Smart Grid. Ωστόσο, επειδή το Smart Grid είναι από τις πλέον κρίσιμες υποδομές ενός κράτους, το επίπεδο ασφάλειας πρέπει να είναι το μέγιστο δυνατό. Για το λόγο αυτό η εγκατάσταση συστημάτων παρακολούθησης κίνησης τελευταίας τεχνολογίας σε κάθε κρίσιμο σύστημα εντός του εταιρικού πληροφοριακού δικτύου είναι απαραίτητη.

4.6.3. Κατάτμηση του Δικτύου

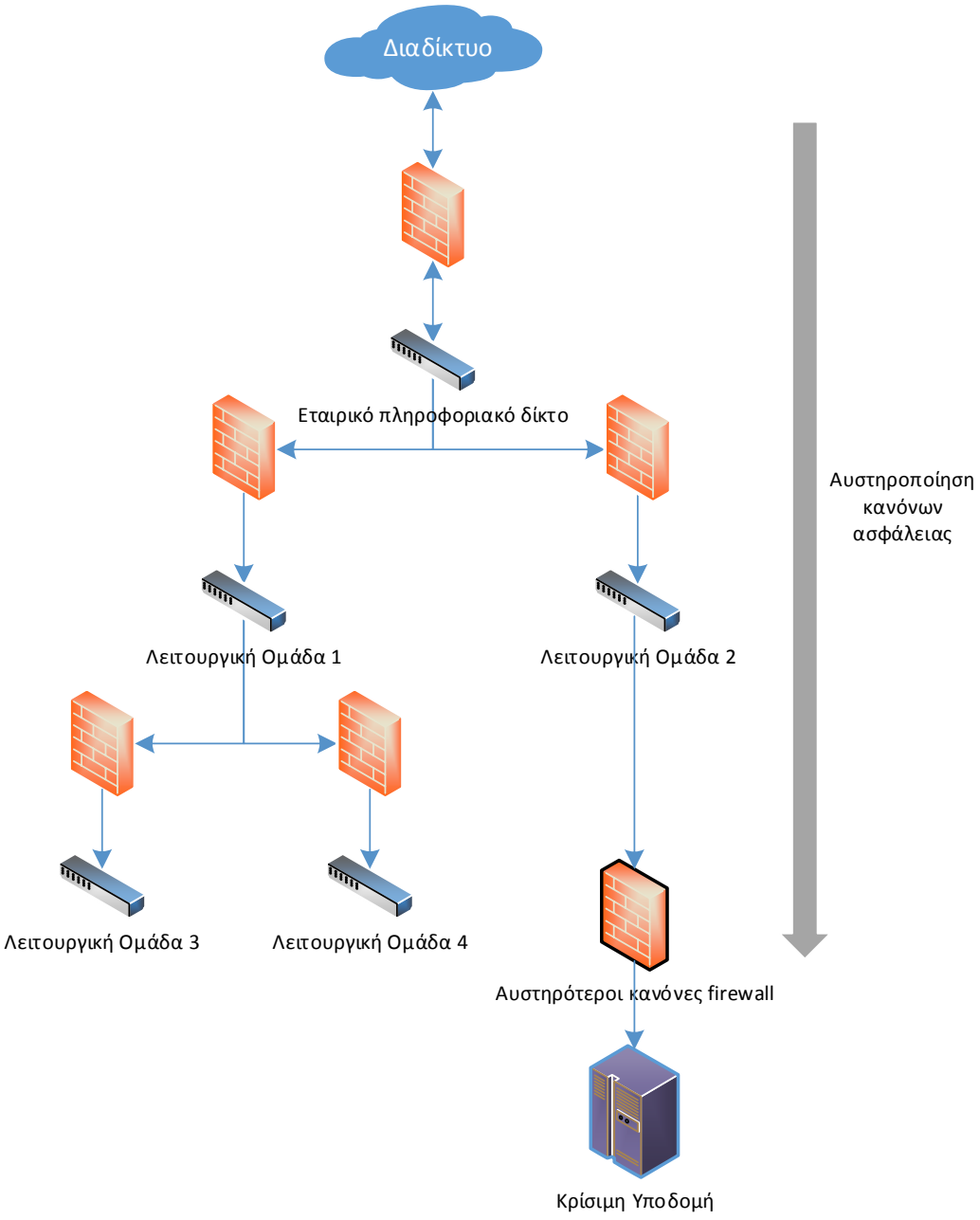
Η μεγαλύτερη πρόκληση για την ασφάλεια ενός εταιρικού πληροφοριακού δικτύου είναι το μέγεθός του. Το μεγάλο μέγεθος του δικτύου, σε συνδυασμό με την πληθώρα τύπων συστημάτων που είναι συνδεδεμένα σε αυτό, καθιστούν πρακτικά αδύνατη την εγκατάσταση αποτελεσματικών μηχανισμών ασφάλειας δικτύου για το σύνολό του. Αυτό συμβαίνει διότι οι πιθανές δίοδοι επίθεσης στο δίκτυο είναι πολλές και οι μέθοδοι ασφάλειας για κάποιες δημιουργούν προβλήματα στις υπηρεσίες άλλων συστημάτων του δικτύου. Για την αντιμετώπιση της ανωτέρω πρόκλησης, υιοθετείται μια στρατηγική του τύπου «διαίρει και βασίλευε». Η στρατηγική αυτή υλοποιείται διαχωρίζοντας τις διάφορες λειτουργικές ομάδες συστημάτων που ανήκουν στο εταιρικό πληροφοριακό δίκτυο. Για παράδειγμα, ένας εξυπηρετητής HTTP μαζί με τις βάσεις δεδομένων που υποστηρίζου την λειτουργία του ανήκουν σε μια λειτουργική ομάδα του δικτύου που αφορά τις ιστοσελίδες και υπηρεσίες μέσω Διαδικτύου. Σε αντιπαραβολή, εντελώς διαφορετικές λειτουργικές ομάδες είναι τα συστήματα καταγραφής δεδομένων του κέντρου ελέγχου ενός σταθμού παραγωγής ή τα συστήματα του κέντρου τιμολόγησης. Έτσι, με βάση τη λειτουργία των διαφόρων ομάδων συστημάτων πραγματοποιείται η κατάτμηση του δικτύου σε υποδίκτυα. Κατά τη σχεδίαση της αρχιτεκτονικής αυτής λαμβάνονται υπόψη οι προδιαγραφές επικοινωνίας μεταξύ των διαφόρων διακριτών λειτουργικών ομάδων. Για παράδειγμα, πρέπει να διασφαλιστεί ότι η ομάδα υπηρεσιών Διαδικτύου μπορεί να επικοινωνεί με το κέντρο τιμολόγησης ώστε να λαμβάνει δεδομένα λογαριασμών των καταναλωτών.

Μετά τη σχεδίαση και υλοποίηση της ανωτέρω αρχιτεκτονικής, είναι αναγκαία η εγκατάσταση συστημάτων firewall και IDS στις περιμέτρους κάθε ομάδας. Βάσει της λειτουργίας κάθε ομάδας, διαμορφώνεται ένας χάρτης με τους κόμβους με τους οποίους κάθε ομάδα χρειάζεται να επικοινωνεί ώστε να επιτελέσει τη λειτουργία της. Στη συνέχεια, γίνεται ρύθμιση των κανόνων των συστημάτων firewall και IDS ώστε να υλοποιούν μια λογική λευκού καταλόγου κόμβων, δηλαδή, να απορρίπτουν όλη την κίνηση εκτός από αυτή που γίνεται από και προς κόμβους απαραίτητους για τη λειτουργία της ομάδας. Μόνο στην περίπτωση όπου δεν είναι εκ των προτέρων γνωστοί οι κόμβοι με τους οποίους πρέπει να επικοινωνήσει μια ομάδα, πρέπει να υιοθετείται η λογική μαύρου καταλόγου κόμβων. Προτιμάται η στρατηγική λευκού καταλόγου για τους κανόνες των IDS και firewall, διότι είναι πολύ δυσκολότερο να παρακαμφθεί από κάποιο επίδοξο εισβολέα, μειώνοντας έτσι την επιφάνεια επίθεσης κάθε ομάδας.

Η στρατηγική της κατάτμησης του δικτύου σε λειτουργικές ομάδες γίνεται ακόμη αποτελεσματικότερη όταν υλοποιείται σε πολλαπλά επίπεδά. Για παράδειγμα, πολλές ομάδες συστημάτων να εκτελούν επιμέρους λειτουργίας μιας συνολικότερης υπηρεσίας. Αντίστοιχα, οι συγκεκριμένες υπό-ομάδες συστημάτων δημιουργούν μια μεγαλύτερη ομάδα συστημάτων που αφορά τη συγκεκριμένη υπηρεσία. Στην περίπτωση αυτή, πρέπει να υλοποιηθούν μηχανισμοί δικτυακής ασφάλειας και στην περίμετρο της συνολικής ομάδας και στις περιμέτρους των επιμέρους υποομάδων. Ακόμη, πρέπει οι κανόνες κάθε υπό-ομάδας να είναι αυστηρότεροι ανάλογα με την κρισιμότητα των αντίστοιχων συστημάτων και επιλεγμένοι κατάλληλα ώστε να καλύπτουν κάθε πιθανή δίοδο επίθεσης.

Τα πλεονεκτήματα μιας τέτοιας αρχιτεκτονικής ασφάλειας είναι ποικίλα. Ένας πολυεπίπεδος σχεδιασμός κατάτμησης του εταιρικού πληροφοριακού δικτύου επιτρέπει στους υπευθύνους ασφαλείας να σχεδιάζουν και να υλοποιούν τεχνικές ασφάλειας προσαρμοσμένες στα συστήματα κάθε λειτουργικής ομάδας ώστε να επιτυγχάνεται στο μέγιστο βαθμό η ασφάλειά τους. Απορρίπτονται περιττές συνδέσεις και παύουν να υφίστανται άμεσες συνδέσεις μεταξύ συστημάτων όπου δεν είναι αναγκαίες. Ο προηγούμενος κανόνας εμπίπτει και στις συνδέσεις συστημάτων με το Διαδίκτυο. Έτσι, σύνδεση με το Διαδίκτυο υφίσταται μόνο για

λειτουργικές ομάδες που το απαιτούν, με συνέπεια να μειώνεται δραστικά το πλήθος πιθανών διόδων επίθεσης εναντίον του εταιρικού πληροφοριακού δικτύου. Ακόμα παρέχεται η δυνατότητα για πιο λεπτομερή και ευέλικτη υλοποίηση κανόνων στα firewall και τα IDS. Τέλος, η συγκεκριμένη αρχιτεκτονική χαρακτηρίζεται ως αρθρωτή, καθώς μπορεί να προστεθεί μία νέα λειτουργική ομάδα και να γίνουν οι απαραίτητες ρυθμίσεις ασφάλειας με μικρές αλλαγές στις ρυθμίσεις μόνο των υπερ-ομάδων της.



Σχήμα 4.9. Αρχιτεκτονική λειτουργικών ομάδων και κλίμακα αυστηρότητας κανόνων firewall

Στο Σχ. 4.9, απεικονίζεται σχηματικά η κατάτμηση ενός δικτύου σε λειτουργικές ομάδες και η αυστηροποίηση των κανόνων των μηχανισμών ασφάλειας καθώς αυξάνει η σημαντικότητα των λειτουργικών ομάδων και η απόστασή τους από την περίμετρο του δικτύου και την έξοδο προς το Διαδίκτυο.

4.6.4. Εγκατάσταση ενημερώσεων λογισμικού

Με το πέρασμα το χρόνου, όλα τα εργαλεία λογισμικού βελτιώνονται και αποκτούν νέες δυνατότητες και χαρακτηριστικά. Επιπλέον, συχνά εμφανίζονται προβλήματα σε εκδόσεις λογισμικού τα οποία διορθώνονται στις επόμενες. Η διανομή νέων εκδόσεων λογισμικού γίνεται μέσω ενημερώσεων από το Διαδίκτυο. Η διαδικασία ενημερώσεων λογισμικού για συνήθεις χρήστες είναι κάτι συνηθισμένο, εύκολο και αυτοματοποιημένο. Ωστόσο, στα συστήματα παραγωγής, δηλαδή εκείνα που είναι επιφορτισμένα με τη παροχή υπηρεσιών, συμβαίνει ακριβώς το αντίθετο. Είναι μια διαδικασία επικίνδυνη, χρονοβόρα, η οποία ορισμένες φορές απαιτεί να τεθεί το σύστημα εκτός λειτουργίας για κάποιο χρονικό διάστημα. Ταυτόχρονα, όμως, η ενημέρωση λογισμικού είναι αναγκαία καθώς διορθώνονται λάθη και κενά ασφαλείας προηγούμενων εκδόσεων.

Συνεπώς, η διαδικασία ενημέρωσης λογισμικού αποτελεί μία αμοιβαία αντιστάθμιση (trade-off) για τους διαχειριστές συστημάτων. Από τη μία πλευρά υπάρχει με τη νέα έκδοση λογισμικού ο κίνδυνος να διακοπεί η συμβατότητα με άλλα εργαλεία λογισμικού που εκτελούνται στο σύστημα, με αποτέλεσμα το σύστημα να μη μπορεί να επιτελέσει επιτυχώς τη λειτουργία του. Από την άλλη πλευρά, η μη ενημέρωση λογισμικού οδηγεί στη διαιώνιση κενών ασφαλείας τα οποία έχουν λυθεί σε μεταγενέστερες εκδόσεις καθιστώντας το σύστημα ευάλωτο γνωστές επιθέσεις. Μέχρι σήμερα, σε μεγάλες εταιρίες υιοθετείται, συνήθως, η πρώτη περίπτωση. Σε ένα σύστημα παραγωγής εγκαθίστανται οι εκδόσεις εργαλείων λογισμικού για τις οποίες το σύστημα λειτουργεί δίχως προβλήματα και δεν αλλάζουν για μεγάλο χρονικό διάστημα.

1. Patch Management System

Στα εταιρικά πληροφοριακά δίκτυα οντοτήτων της αγοράς ΗΕ, τα λογισμικά που χρησιμοποιούνται πρέπει να διαθέτουν τις τελευταίες εκδόσεις λογισμικών που αντιμετωπίζουν κενά ασφάλειας ώστε να επιτυγχάνεται η ασφάλεια του δικτύου και των συστημάτων του στο μέγιστο βαθμό. Αυτή η ανάγκη απαιτεί ένα κεντρικό μηχανισμό διαχείρισης των ενημερώσεων λογισμικού. Ένα τέτοιο σύστημα ονομάζεται Patch Management System και, μέσω ενός καταλόγου όλων των λογισμικών που χρησιμοποιούνται από συστήματα του εταιρικού πληροφοριακού δικτύου, αναλαμβάνει να συνδέεται τακτικά στο Διαδίκτυο και να λαμβάνει τις ενημερωμένες εκδόσεις των λογισμικών. Ακόμη, μέσω τιμών κατακερματισμού (hash sums) των δεδομένων των αρχείων των νέων εκδόσεων, το Patch Management System επαληθεύει τη γνησιότητα των αρχείων που λαμβάνει. Στη συνέχεια, κάθε σύστημα ενημερώνεται μέσω του Patch Management System ώστε να μην απαιτείται η σύνδεσή του στο Διαδίκτυο.

Καίτοι το Patch Management System προσφέρει ασφαλή αυτοματοποίηση των ενημερώσεων λογισμικού των συστημάτων του εταιρικού πληροφοριακού δικτύου, εμφανίζει ένα σημαντικό μειονέκτημα. Αποτελεί μοναδικό σημείο αποτυχίας (single point of failure) του δικτύου, καθώς αν παραβιαστεί, ο επιτιθέμενος μπορεί εύκολα και ταχέως να παραβιάσει πολλά από τα συστήματα του εταιρικού πληροφοριακού δικτύου. Για το λόγο αυτό, το Patch Management System πρέπει να εγκατασταθεί μέσα σε

μία ζώνη DMZ με πολύ αυστηρούς κανόνες και να προστατεύεται από όλους τους μηχανισμούς ασφάλειας που προαναφέρθηκαν. Επίσης, σε συστήματα κρίσιμα για το Smart Grid, κρίνεται σκόπιμο η ενημέρωση λογισμικού να γίνεται χειροκίνητα, και εκτός σύνδεσης, μέσω μνημών Flash ώστε, ακόμα και σε πιθανή παραβίαση του Patch Management System, τα πλέον κρίσιμα συστήματα για το Smart Grid να παραμένουν ασφαλή.

2. Εργαστήριο ελέγχου ενημερώσεων λογισμικού

Όπως προαναφέρθηκε, δεν είναι λίγες οι περιπτώσεις όπου μία ενημέρωση λογισμικού σε ένα σύστημα προκαλεί απώλεια συμβατότητας με άλλα εργαλεία λογισμικού δημιουργώντας προβλήματα στη λειτουργία του συστήματος. Ακόμη, έχουν εμφανιστεί κακόβουλα λογισμικά που ενώ εμφανίζονται ως αυθεντικές ενημερώσεις λογισμικού χρησιμοποιούνται για να παραβιάσουν το σύστημα [50]. Για την αποφυγή των ανωτέρω καταστάσεων, είναι απαραίτητος ένας μηχανισμός ελέγχου των ενημερώσεων πριν αυτές εγκατασταθούν σε κρίσιμα συστήματα του εταιρικού πληροφοριακού δικτύου.

Αυτό μπορεί να γίνει υλοποιώντας ένα εργαστήριο εικονικών μηχανών που προσομοιώνουν τα κύρια συστήματα του εταιρικού πληροφοριακού δικτύου. Οι εικονικές μηχανές του εργαστηρίου αυτού πρέπει να είναι ακριβείς κλώνοι των συστημάτων που χρησιμοποιούνται ώστε τα αποτελέσματα των ελέγχων να είναι αξιόπιστα. Αρχικά, οι ενημερώσεις λογισμικού γίνονται στα εικονικά συστήματα ελέγχου των οποίων η λειτουργία παρακολουθείται για κάποιο δοκιμαστικό χρονικό διάστημα ώστε να εξαχθούν αξιόπιστα συμπεράσματα. Εφόσον τα εικονικά συστήματα λειτουργούν επιτυχώς μετά από μία αναβάθμιση, τότε αυτή μπορεί να εφαρμοστεί και στα πραγματικά συστήματα. Το δοκιμαστικό χρονικό διάστημα είναι σημαντική παράμετρος αυτής της διαδικασίας και πρέπει να αυξάνεται ανάλογα με την κρισιμότητα της υποδομής που ελέγχεται ή να μειώνεται ανάλογα με το πόσο επείγουσα είναι η συγκεκριμένη αναβάθμιση.

Η μέγιστη ασφάλεια για το εταιρικό πληροφοριακό δίκτυο συνδυάζοντας ένα Patch Management System με ένα εργαστήριο ελέγχου ενημερώσεων. Έτσι, αποφεύγονται παραβιάσεις από κακόβουλα λογισμικά που μεταμφιέζονται σε ενημερώσεις λογισμικού και αστοχίες από αυθεντικές ενημερώσεις. Ακόμη, σημαντικά συστήματα του εταιρικού πληροφοριακού δικτύου δεν χρειάζεται να συνδεθούν στο Διαδίκτυο προκειμένου να γίνουν οι ενημερώσεις, διατηρώντας έτσι την οργάνωση του δικτύου στις ομάδες που αναλύθηκαν προηγουμένως. Έτσι, τα συστήματα που ενημερώνονται διασφαλίζονται στο μέγιστο βαθμό από τους κινδύνους που συνοδεύουν μια ενημέρωση λογισμικού, αποφεύγοντας ταυτόχρονα αυτούς που προκύπτουν από τη μη ενημέρωσή τους.

4.6.5. Ενημέρωση υπαλλήλων για ζητήματα ασφάλειας

Οι αλλαγές που φέρνει το Smart Grid στα εταιρικά πληροφοριακά δίκτυα των οντοτήτων της αγοράς ΗΕ αναμένεται να επηρεάσουν και το υπαλληλικό προσωπικό των οντοτήτων αυτών. Λόγω της κρισιμότητας των νέων δομών του Smart Grid που βρίσκονται εντός του εταιρικού πληροφοριακού δικτύου, η συχνότητα των επιθέσεων αναμένεται να αυξηθεί σημαντικά. Για να αντιμετωπιστούν οι επιθέσεις αυτές είναι απαραίτητο το προσωπικό της οντότητας να έχει εκπαιδευτεί σε ασφαλείς πρακτικές χρήσης των συστημάτων εντός του εταιρικού πληροφοριακού δικτύου.

Το πρώτο ζήτημα ασφάλειας για το οποίο απαιτείται λεπτομερής ενημέρωση είναι το social engineering. Το συγκεκριμένο είδος επιθέσεων αποτελεί προτεραιότητα καθώς στοχεύει το υπαλληλικό προσωπικό της

οντότητας. Αρχικά, το προσωπικό, διασταυρώνοντας τα στοιχεία του αποστολέα, πρέπει να αναγνωρίζει ηλεκτρονικά μηνύματα που έχουν ως στόχο την εξαπάτησή του. Ακόμη, σύνδεσμοι μέσα από μηνύματα ηλεκτρονικού ταχυδρομείου πρέπει να ελέγχονται λεπτομερώς πριν ακολουθηθούν, καθώς σε περίπτωση κακόβουλης ιστοσελίδας είναι πολύ πιθανή η παραβίαση του φυλλομετρητή και του συστήματος. Ως προς τις άγνωστες μνήμες Flash, πρέπει να δεσμευθούν μικρός αριθμός συστημάτων τα οποία να βρίσκονται εκτός σύνδεσης ώστε να μπορεί ένας υπάλληλος να δοκιμάσει σε αυτά μια άγνωστη συσκευή Flash δίχως το κίνδυνο μόλυνσης του εταιρικού πληροφοριακού δικτύου. Όμως, το προσωπικό πρέπει να γνωρίζει ότι σε καμία περίπτωση μία άγνωστη συσκευή Flash δεν πρέπει να συνδεθεί σε σύστημα που είναι συνδεδεμένο στο εταιρικό πληροφοριακό δίκτυο.

Το δεύτερο ζήτημα ασφάλειας για το οποίο απαιτείται ενημέρωση του προσωπικού των οντοτήτων της αγοράς ΗΕ ως προς τους κινδύνους που αυτό προκαλεί είναι το BYOD (Bring Your Own Device). Κάθε εργαζόμενος που έχει πρόσβαση στο εταιρικό πληροφοριακό δίκτυο οφείλει να έχει μια σωστή αντίληψη των απειλών που μπορεί να εμφανιστούν στα συστήματα του δικτύου μέσω των προσωπικών συσκευών του προσωπικού. Καίτοι ένα πρώτο βήμα για την αποτελεσματική αντιμετώπιση τέτοιων απειλών γίνεται με τη δημιουργία υποδικτύου αφιερωμένου σε προσωπικές συσκευές, η ενημέρωση και σωστή αντίληψη του προσωπικού επί των ζητημάτων ασφάλειας του BYOD είναι απαραίτητη.

Αρχικά, είναι απαραίτητη η ενημέρωση του προσωπικού ως προς τις σωστές πρακτικές χρήσης προσωπικών συσκευών εντός του εταιρικού πληροφοριακού δικτύου. Τέτοιες πρακτικές αφορούν την αποφυγή σύνδεσης σε δημόσια δίκτυα και την αποφυγή επίσκεψης σε μη γνωστές ιστοσελίδες. Προς αυτή την κατεύθυνση, υπάρχουν εργαλεία που ενημερώνουν το χρήστη για την ποιότητα της ιστοσελίδας που πρόκειται να επισκεφτεί και τον ειδοποιούν σε περίπτωση κινδύνου. Ακόμη, είναι αναγκαίο να οριστούν συγκεκριμένες περιπτώσεις για τις οποίες επιτρέπεται στο προσωπικό να χρησιμοποιεί προσωπικές συσκευές, ώστε να ελαχιστοποιηθεί ο αριθμός τους στις απολύτως απαραίτητες. Τέλος, οι πρακτικές χρήσης και ασφάλειας πρέπει να προσαρμόζονται συχνά στα είδη συσκευών που ενδεχομένως διαθέτει το προσωπικό, καθώς και σε νέες τεχνολογίες που εμφανίζονται και μπορούν να έχουν επιπτώσεις στο σχεδιασμό ασφάλειας του εταιρικού πληροφοριακού δικτύου.

Καίτοι οι ανωτέρω ενέργειες ενημέρωση μειώνουν σε μεγάλο βαθμό την έκθεση του δικτύου σε επιθέσεις BYOD, δεν προσφέρουν πραγματική προστασία. Για το λόγο αυτό, είναι απαραίτητη η θέσπιση συγκεκριμένων αυστηρών κανόνων στα συστήματα ασφάλειας, όπως τα firewall, συγκεκριμένα για προσωπικές συσκευές, ώστε ο έλεγχος της δικτυακής συμπεριφοράς τους να είναι αυστηρός. Έτσι, πιθανές επιθέσεις μέσω προσωπικών συσκευών μπορούν να γίνουν αντιληπτές ταχέως και να μην επιτραπεί στον επιτιθέμενο να προωθηθεί στο εταιρικό πληροφοριακό δίκτυο με ευκολία.

4.7. Συμπεράσματα

Το εταιρικό πληροφοριακό δίκτυο μιας οντότητας της αγοράς ΗΕ αποκτά αναβαθμισμένο ρόλο σε ένα περιβάλλον όπου χρησιμοποιούνται τεχνολογίες Smart Grid. Αποτελεί μεγάλο και θεμελιώδες τμήμα του συστήματος του Smart Grid, καθώς μεταφέρει: (i) πληροφορίες από τους αυτόματους μετρητές των καταναλωτών και των τοπικών ανεξάρτητων παραγωγών, (ii) τα δεδομένα προμηθευτών ΗΕ και συνεργαζόμενων τρίτων εταιριών, (iii) τα δεδομένα ελέγχου από σταθμούς παραγωγής, μεταφοράς και διανομής ΗΕ. Σε πολλές περιπτώσεις, οι πληροφορίες που διακινούνται από όλα τα τμήματα του Smart Grid

έχουν ως προορισμό συστήματα εντός των εταιρικών πληροφοριακών δικτύων των οντοτήτων της αγοράς ΗΕ. Σε άλλες περιπτώσεις, ακόμα και συστήματα που ανήκουν στο βιομηχανικό πληροφοριακό δίκτυο, για λόγους εποπτείας αποστέλλουν ορισμένες διαγνωστικές πληροφορίες μέσω των εταιρικών πληροφοριακών δικτύων σε διευθυντικά στελέχη της εκάστοτε οντότητας. Τέλος, πολλά από τα κρίσιμα συστήματα του Smart Grid όπως τα κέντρα τιμολόγησης, οι διακομιστές web υπηρεσιών ή οι συνδέσεις με τρίτες εταιρίες που έχουν αναλάβει να παρέχουν τέτοιες υπηρεσίες για λογαριασμό προμηθευτών ΗΕ, βρίσκονται εντός των εταιρικών πληροφοριακών δικτύων των οντοτήτων της αγοράς ΗΕ.

Είναι φανερό, λοιπόν, ότι η αναβάθμιση του ρόλου του εταιρικού πληροφοριακού δικτύου στην εποχή του Smart Grid συνδέεται με αναβαθμισμένες ευθύνες σχετικά με την ποιότητα της παρεχόμενης υπηρεσίας, είτε αυτή είναι η αδιάκοπη παροχή ηλεκτρικού ρεύματος είτε η ακριβής τιμολόγηση και η έγκαιρη και έγκυρη ενημέρωση των καταναλωτών. Κάθε οντότητα της αγοράς ΗΕ οφείλει να εγγυάται την ασφάλεια των δομών του εταιρικού πληροφοριακού δικτύου της ώστε να εξασφαλίζεται η ορθή λειτουργία του συνόλου του Smart Grid, παρέχοντας επαρκείς εγγυήσεις για τη διαθεσιμότητα των συστημάτων της. Προς το σκοπό αυτό, η ασφάλεια του εταιρικού πληροφοριακού δικτύου αποτελεί δύσκολη υπόθεση καθώς το τμήμα ασφάλειας της οντότητας πρέπει να διαχειρίζεται απειλές και κινδύνους που αφορούν συστήματα με πολύ διαφορετικά χαρακτηριστικά τα οποία, ωστόσο, είναι αναγκαίο να είναι συνδεδεμένα μεταξύ τους. Ο στόχος αυτός μπορεί να επιτευχθεί μόνο με κεντρικό σχεδιασμό της αρχιτεκτονικής του δικτύου, με την ασφάλεια να αποτελεί ακρογωνιαίο λίθο σε αυτό το οικοδόμημα.

Εφαρμόζοντας κεντρική πολιτική ασφάλειας σε όλες τις δομές ενός εταιρικού πληροφοριακού δικτύου και τις τεχνικές που αναλύθηκαν προηγουμένως, το εταιρικό πληροφοριακό δίκτυο είναι σε θέση να αντιμετωπίσει τις νέες απειλές που θα εμφανιστούν με την είσοδο των τεχνολογιών του Smart Grid στα δίκτυα ΗΕ. Αυτή η πολιτική οφείλει να λαμβάνει υπόψη και όλα τα συστήματα που βασίζονται στο εταιρικό πληροφοριακό δίκτυο, αν και δεν βρίσκονται εντός αυτού, θέτοντας ως στόχο την εγγύηση ασφάλειας των κρίσιμων υποδομών των βιομηχανικών πληροφοριακών δικτύων για όσες περιπτώσεις υπάρχει σύνδεση αυτών των υποδομών ή τμημάτων τους με το επιχειρησιακό δίκτυο. Κατ΄αυτό τον τρόπο, θα διασφαλιστούν οι προδιαγραφές διαθεσιμότητας των κρίσιμων υποδομών ώστε να παρέχονται αξιόπιστα οι υπηρεσίες του Smart Grid.

Στους πίνακες που ακολουθούν συνοψίζονται οι μέθοδοι επίθεσης που παρουσιάστηκαν στο κεφάλαιο αυτό, τα κίνητρα που συνήθως οδηγούν σε αυτές, και οι αντίστοιχοι μηχανισμοί άμυνας. Στον Πίνακα 4.1, παρατίθενται οι στόχοι επιθέσεων εντός των εταιρικών πληροφοριακών δικτύων και συνδέονται με τα κίνητρα που οδηγούν σε αυτές τις επιθέσεις. Σε όλες τις περιπτώσεις υπάρχει το κίνητρο της υποκλοπής δεδομένων, ενώ σε πολλές περιπτώσεις ο επίδοξος εισβολέας μπορεί να προκαλέσει διακοπή της παρεχόμενης υπηρεσίας. Επιπλέον, αρκετά συστήματα, όπως οι βάσεις δεδομένων και τα κέντρα τιμολόγησης, αποτελούν στόχο με κίνητρο την οικονομική απάτη. Σημειώνεται, επίσης, ότι όλα τα συστήματα εντός των εταιρικών πληροφοριακών δικτύων αποτελούν στόχους καθώς μπορούν να χρησιμοποιηθούν ως βήμα για την προώθηση των παραβιάσεων σε γειτονικά στο δίκτυο συστήματα.

ΣΥΣΤΗΜΑΤΑ - ΣΤΟΧΟΙ	ΚΙΝΗΤΡΑ ΕΠΙΘΕΣΕΩΝ
Web servers προμηθευτών ΗΕ	• Υποκλοπή δεδομένων. • Προώθηση παραβίασης στο εσωτερικό του δικτύου. • Δολιοφθορά – Διακοπή παρεχόμενης υπηρεσίας.
Κέντρα τιμολόγησης	• Υποκλοπή δεδομένων. • Οικονομική απάτη. • Διακοπή παρεχόμενης υπηρεσίας.
Βάσεις δεδομένων υπηρεσιών διαχείρισης λογαριασμού	• Υποκλοπή δεδομένων. • Οικονομική απάτη. • Διακοπή παρεχόμενης υπηρεσίας.
Συστήματα συγκέντρωσης δεδομένων αυτομάτου ελέγχου των σταθμών παραγωγής/διανομής ΗΕ	• Υποκλοπή δεδομένων. • Δολιοφθορά. • Προώθηση παραβίασης στο βιομηχανικό πληροφοριακό δίκτυο.
Υπόλοιπα συστήματα εταιρικών πληροφοριακών δικτύων	• Υποκλοπή δεδομένων. • Προώθηση παραβίασης στο εσωτερικό του εταιρικού πληροφοριακού δικτύου.

Πίνακας 4.1. Αντιστοίχηση στόχων στα εταιρικά πληροφοριακά δίκτυα με τα κίνητρα που οδηγούν σε επιθέσεις εναντίον τους.

Στον Πίνακα 4.2 παρουσιάζονται όλες οι κατηγορίες επιθέσεων που αναλύθηκαν στο κεφάλαιο αυτό και οι επιπτώσεις που συνεπάγεται μια επιτυχημένη υλοποίησή τους για το σύστημα-στόχο και το εταιρικό πληροφοριακό δίκτυο γενικά.

ΜΕΘΟΔΟΙ ΕΠΙΘΕΣΗΣ	ΕΠΙΠΤΩΣΕΙΣ
Εκμετάλλευση ευπαθειών λογισμικού	• Απομακρυσμένος έλεγχος του συστήματος-στόχου. • Υποκλοπή / Αλλοίωση δεδομένων. • Πρόσβαση σε γειτονικά συστήματα.
Bring Your Own Device (BYOD)	• Υποκλοπή προσωπικών δεδομένων. • Δίοδος εισόδου στο εταιρικό πληροφοριακό δίκτυο. • Πρόσβαση σε γειτονικά συστήματα.
Social Engineering (Κοινωνική Μηχανική)	• Απομακρυσμένος έλεγχος συστήματος-στόχου. • Υποκλοπή προσωπικών δεδομένων. • Πρόσβαση σε γειτονικά συστήματα.
DoS (Denial of Service)	• Διακοπή παρεχόμενης υπηρεσίας. • Απώλεια δεδομένων.

Πίνακας 4.2. Κατάλογος κατηγοριών επιθέσεων εναντίον συστημάτων των εταιρικών πληροφοριακών δικτύων και των επιπτώσεών τους.

Τέλος, στον Πίνακα 4.3 συνοψίζονται όλοι οι μηχανισμοί άμυνας που αναλύθηκαν στο κεφάλαιο αυτό, το είδος επιθέσεων που αποτρέπουν και το κόστος εγκατάστασής τους.

ΜΗΧΑΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ	ΕΙΔΟΣ ΕΠΙΘΕΣΕΩΝ ΠΟΥ ΑΠΟΤΡΕΠΕΤΑΙ	ΚΟΣΤΟΣ ΕΓΚΑΤΑΣΤΑΣΗΣ
Firewall, IDS/IPS στην περίμετρο του δικτύου	• Σάρωση συστημάτων. • Απομακρυσμένη παραβίαση. • DoS.	• Μέτριο οικονομικό κόστος αγοράς. • Μικρό κόστος σε πολυπλοκότητα ρύθμισης-εγκατάστασης.
Κατάτμηση του δικτύου	• Σάρωση συστημάτων. • Εξάπλωση παραβίασης στο εσωτερικό του εταιρικού πληροφοριακού δικτύου. • BYOD.	• Μικρό οικονομικό κόστος για firewall και IDS/IPS στα υποδίκτυα. • Υψηλό κόστος σε πολυπλοκότητα της αρχιτεκτονικής του δικτύου.
Ζώνες DMZ (De-Militarized Zones – Αποστρατιωτικοποιημένες ζώνες)	• Σάρωση συστημάτων. • Εξάπλωση παραβίασης στο εσωτερικό του πληροφοριακού δικτύου.	• Μέτριο οικονομικό κόστος για firewall και IDS/IPS στα όρια των ζωνών. • Υψηλό κόστος σε πολυπλοκότητα της αρχιτεκτονικής του δικτύου και του ορισμού κανόνων για την κίνηση στα firewall.
Λογισμικά Firewall, IDS/IPS, anti-malware εντός των συστημάτων	• Εκμετάλλευση ευπαθειών στο σύστημα.	• Μικρό οικονομικό κόστος που μπορεί να μηδενιστεί με τη χρήση εργαλείων ανοικτού κώδικα.
Εργαστήριο εικονικών μηχανών	• Παραβίαση μέσω δίσκων USB. • Παραβίαση μέσω κακόβουλου λογισμικού που υποδύεται μια αναβάθμιση λογισμικού.	• Μικρό οικονομικό κόστος αγοράς φυσικών συστημάτων ή ενοικίασης εικονικών μηχανών ως υπηρεσία. • Μικρό οικονομικό κόστος λογισμικού εικονικών μηχανών που μπορεί να μηδενιστεί με χρήση εργαλείων ανοικτού κώδικα.
Σύστημα ελέγχου αναβαθμίσεων λογισμικού	• Εκμετάλλευση ευπαθειών παλαιών εκδόσεων λογισμικού.	• Μικρό οικονομικό κόστος για το φυσικό σύστημα.

	• Παραβίαση μέσω λογισμικού που υποδύεται μια αναβάθμιση λογισμικού.	• Υψηλό κόστος σε πολυπλοκότητα για τη θέσπιση κανόνων πρόσβασης.

Πίνακας 4.3. Κατάλογος μηχανισμών άμυνας, των επιθέσεων που αποτρέπουν και του κόστους εγκατάστασής τους.

Κεφάλαιο 5. Βιομηχανικό πληροφοριακό δίκτυο – Industrial Network

5.1. Εισαγωγή

Το βιομηχανικό πληροφοριακό δίκτυο ΗΕ αποτελεί το δίκτυο επικοινωνίας μέσω του οποίου είναι συνδεδεμένες όλες οι διατάξεις που σχετίζονται τη λειτουργία των συστημάτων παραγωγής μεταφοράς και διανομής ΗΕ. Διαχωρίζεται ως οντότητα από τα υπόλοιπα δίκτυα του Smart Grid λόγω του ειδικού σκοπού που επιτελεί, των διαφορετικών προδιαγραφών σχεδιασμού του, των εξειδικευμένων πρωτοκόλλων επικοινωνίας που χρησιμοποιεί και του τύπου των διατάξεων που συνδέονται μέσω αυτού.

Μέσω του βιομηχανικού πληροφοριακού δικτύου ΗΕ συνδέονται υποδομές όπως τα συστήματα SCADA, τα συστήματα PLC (Programmable Logic Controller – Προγραμματιζόμενοι λογικοί ελεγκτές) που υλοποιούν τον αυτόματο έλεγχο, γεννήτριες και μετασχηματιστές, καθώς και μετρητές που είναι εγκατεστημένοι στο δίκτυο ΗΕ. Το βιομηχανικό πληροφοριακό δίκτυο ΗΕ προσφέρει τη δυνατότητα επικοινωνίας με όλες αυτές τις διατάξεις με ελάχιστη καθυστέρηση, ώστε διευκολύνεται η παρακολούθηση μεγάλου αριθμού αυτών και ο έλεγχος της λειτουργίας τους.

Το βιομηχανικό πληροφοριακό δίκτυο ΗΕ διασυνδέει όλες, σχεδόν, τις κρίσιμες υποδομές του Ευφυούς Δικτύου, που είναι απαραίτητες για την αξιόπιστη λειτουργία του. Οι πληροφορίες που διακινούνται πάνω μέσω του βιομηχανικού πληροφοριακού δικτύου ΗΕ αφορούν, ως επί το πλείστο, πληροφορίες κατάστασης των κρίσιμων υποδομών καθώς και εντολές αυτομάτου ελέγχου προς αυτές. Ένα σφάλμα ή μια παραβίαση στις επικοινωνίες αυτές είναι δυνατό να έχει καταστροφικές συνέπειες για τις κρίσιμες υποδομές του Ευφυούς Δικτύου. Επομένως, η ασφάλεια του βιομηχανικού πληροφοριακού δικτύου ΗΕ και των πληροφοριών που ανταλλάσσονται πάνω από αυτό αποτελεί ζήτημα ύψιστης σημασίας.

5.2. Δομή και ιεραρχία του βιομηχανικού πληροφοριακού δικτύου ΗΕ

Η δομή ενός βιομηχανικού πληροφοριακού δικτύου ΗΕ διαφέρει σε αρκετά σημεία από αυτή ενός παραδοσιακού δικτύου υπολογιστών αφού το βιομηχανικό πληροφοριακό δίκτυο ΗΕ δεν είναι ένα δίκτυο επικοινωνιών γενικής χρήσης αλλά ένα δίκτυο ειδικού σκοπού. Οι κόμβοι που διασυνδέονται μέσω του βιομηχανικού πληροφοριακού δικτύου ΗΕ επιτελούν ειδικές και πολύ συγκεκριμένες λειτουργίες με αντίστοιχες προδιαγραφές. Αντίστοιχα, και το βιομηχανικό πληροφοριακό δίκτυο ΗΕ σχεδιάζεται ώστε να διευκολύνει στο μέγιστο δυνατό βαθμό τη λειτουργία των κόμβων που διασυνδέει. Τα χαρακτηριστικά στα οποία διαφέρουν τα βιομηχανικά πληροφοριακά δίκτυα από τα υπόλοιπα δίκτυα επικοινωνιών του Smart Grid είναι η ιεραρχία των κόμβων και η ανάγκη διαδικτύωσής τους.

5.2.1. Ιεραρχία κόμβων – Μοντέλο Master/Slave

Σε ένα βιομηχανικό πληροφοριακό δίκτυο ΗΕ τα καθήκοντα που επιτελούν οι κόμβοι είναι διακριτά. Τα σημαντικότερα είναι αυτά του κέντρου ελέγχου και αυτά των διατάξεων υπό τον έλεγχο κάθε κέντρου ελέγχου. Η ιεραρχία κέντρου ελέγχου και διατάξεων υπό τον έλεγχό του ακολουθείται και στις επικοινωνίες μεταξύ των κόμβων του βιομηχανικού πληροφοριακού δικτύου ΗΕ, όπου τα πρωτόκολλα επικοινωνίας υιοθετούν ως επί το πλείστο την ιεραρχία master/slave. Master στο βιομηχανικό πληροφοριακό δίκτυο ΗΕ θεωρείται το κέντρο ελέγχου, για παράδειγμα ένας εποπτικός σταθμός SCADA, ενώ slaves θεωρούνται οι διατάξεις οι οποίες ελέγχονται από το συγκεκριμένο κέντρο ελέγχου.

Η ιεραρχία αυτή έχει άμεση επίδραση στον τρόπο που πραγματοποιούνται οι επικοινωνίες μεταξύ των κόμβων. Οι διαφορές αφορούν στα δικαιώματα που έχει κάθε κόμβος για να εγκαθιστά συνδέσεις με άλλες διατάξεις του βιομηχανικού πληροφοριακού δικτύου. Τα δικαιώματα αυτά ορίζονται στο βιομηχανικό πρωτόκολλο. Καίτοι κάθε πρωτόκολλο υιοθετεί διαφορετικές παραλλαγές στα δικαιώματα που ορίζει, η βασική πολιτική δικαιωμάτων παραμένει σταθερή για όλα τα πρωτόκολλα. Ο κόμβος master μεταδίδει ερωτήματα για αποστολή δεδομένων ή εντολές στους κόμβους slaves. Με τη σειρά τους, οι κόμβοι αυτοί έχουν το δικαίωμα μόνο να απαντούν σε ερωτήματα και εντολές που δέχονται από τον κόμβο master. Η μόνη περίπτωση κατά την οποία ένας κόμβος slave μπορεί να εγκαταστήσει μια σύνδεση με τον κόμβο master είναι όταν εμφανιστεί κάποιο σφάλμα ή κάποια κρίσιμη τιμή σε κάποια παράμετρο, δηλαδή περίπτωση για την οποία κρίνεται σκόπιμη η ενημέρωση του master. Τέλος, η επικοινωνία ανάμεσα σε κόμβους slave δεν επιτρέπεται.

5.2.2. Απουσία διαδικτύωσης

Στα παραδοσιακά δίκτυα υπολογιστών, ο σχεδιαστής του δικτύου δεν μπορεί να γνωρίζει εκ των προτέρων με ποιές συσκευές επικοινωνεί κάθε υπολογιστής. Για το λόγο αυτό, παρέχεται η δυνατότητα διαδικτύωσης, δηλαδή επικοινωνίας με κόμβους που δεν ανήκουν στο ίδιο δίκτυο. Καίτοι πολλά βιομηχανικά πρωτόκολλα την υποστηρίζουν μέσω στης στοίβας πρωτοκόλλων TCP/IP, στην περίπτωση του βιομηχανικού πληροφοριακού δικτύου ΗΕ η δυνατότητα διαδικτύωσης δεν είναι απαραίτητη, όπως γίνεται φανερό από την ιεραρχία των κόμβων. Κάθε κόμβος slave επικοινωνεί μόνο με τον κόμβο master που τον ελέγχει. Αφού δεν επικοινωνούν μεταξύ τους κόμβοι slave, δεν προκύπτει περίπτωση όπου κάποιος κόμβος slave πρέπει να επικοινωνήσει με άλλο κόμβο slave, ακόμα περισσότερο όταν ο δεύτερος βρίσκεται σε άλλο δίκτυο. Επομένως, όλες οι επικοινωνίες ανάμεσα σε κόμβους master και slave παραμένουν στο εσωτερικό του τοπικού δικτύου κάθε κόμβου master.

Η απουσία ανάγκης για διαδικτύωση όσον αφορά τις επικοινωνίες του βιομηχανικού πληροφοριακού δικτύου ΗΕ απλοποιεί πολύ τη σχεδίαση των αντίστοιχων πρωτοκόλλων και των διατάξεων που τα υλοποιούν. Ενδεικτικά, δεν υφίσταται η ανάγκη για δρομολόγηση των πακέτων. Η απουσία δρομολόγησης μειώνει κατά πολύ τις υπολογιστικές απαιτήσεις από τις διατάξεις του δικτύου, γεγονός που μειώνει δραστικά την καθυστέρηση μεταφοράς των πακέτων. Αυτό το χαρακτηριστικό καθιστά τα πρωτόκολλα που εφαρμόζονται στο βιομηχανικό πληροφοριακό δίκτυο ΗΕ κατάλληλα για επικοινωνία πραγματικού χρόνου.

5.3. Κίνητρα επιθέσεων εναντίον του βιομηχανικού πληροφοριακού δικτύου

Το βιομηχανικό δίκτυο ΗΕ είναι το τμήμα του Smart Grid στο οποίο πραγματοποιούνται οι βασικές εργασίες που αφορούν την παραγωγή, μεταφορά και διανομή της ΗΕ. Τα δεδομένα που παράγονται από τις διατάξεις και μεταδίδονται μέσω του βιομηχανικού πληροφοριακού δικτύου ΗΕ είναι ζωτικής σημασίας για τη λειτουργία των κρίσιμων υποδομών παραγωγής και διανομής ΗΕ. Συχνά, αυτά τα δεδομένα φανερώνουν πολλά για την αρχιτεκτονική του δικτύου και την κατάσταση λειτουργίας των διατάξεων που είναι συνδεδεμένες στο βιομηχανικό πληροφοριακό δίκτυο ΗΕ.

Λόγω της πληθώρας ευαίσθητων πληροφοριών που διακινούνται μέσω του βιομηχανικού πληροφοριακού δικτύου ΗΕ και τις κρισιμότητας πολλών εκ των συνδεδεμένων διατάξεων, το βιομηχανικό πληροφοριακό δίκτυο ΗΕ αποτελεί συχνά στόχο επιθέσεων. Επειδή ο εξοπλισμός που απαιτείται για επιθέσεις εναντίον υποδομών του βιομηχανικού πληροφοριακού δικτύου ΗΕ είναι περισσότερο εξειδικευμένος και ακριβός, οι επιθέσεις αυτές προέρχονται συνήθως από άρτια εξοπλισμένες και οργανωμένες ομάδες, όπως μυστικά τμήματα ανταγωνιζόμενων εταιριών, ομάδες μυστικών υπηρεσιών κρατών και ομάδες ηλεκτρονικού πολέμου του στρατού. Στη συνέχεια, αναλύονται τα κίνητρα επίθεσης για κάθε είδους κακόβουλη ομάδα.

5.3.1. Βιομηχανική κατασκοπεία

Η βιομηχανική κατασκοπεία υπάρχει από τις απαρχές της βιομηχανίας σε όλους σχεδόν τους τομείς της. Ένας από τους βασικότερους τομείς, όπως αυτός της ΗΕ, δεν θα μπορούσε να αποτελεί εξαίρεση. Η εξάπλωση του Smart Grid αναμένεται να φέρει μεγάλες ανακατατάξεις στον ανταγωνισμό των εμπλεκομένων στην αγορά ΗΕ. Αναπόφευκτα, κάποιοι θα ακολουθήσουν αρνητική οικονομική πορεία, οπότε είναι αναμενόμενο ορισμένοι από αυτούς να καταφύγουν σε μη νόμιμες μεθόδους βιομηχανικής κατασκοπείας.

Στο πλαίσιο της βιομηχανικής κατασκοπείας το βιομηχανικό πληροφοριακό δίκτυο ΗΕ είναι πιθανό να αποτελέσει στόχο κακόβουλων επιθέσεων. Αυτό οφείλεται στην αξία που έχουν τα δεδομένα που διακινούνται μέσω αυτού για ανταγωνίστριες εταιρίες. Για παράδειγμα, πληροφορίες σχετικά με τον ακριβή τύπο των διατάξεων που χρησιμοποιούνται, τις παραμέτρους λειτουργίας και τις διαδικασίες αυτομάτου ελέγχου μπορούν να χρησιμοποιηθούν από ανταγωνίστριες εταιρίες προς όφελός τους. Επιπλέον, αναγνωρίζοντας τους κόμβους τους κόμβους του δικτύου μπορεί να ανιχνευθεί η αρχιτεκτονική τμήματος του βιομηχανικού πληροφοριακού δικτύου ΗΕ. Όλες οι προαναφερθείσες πληροφορίες αποτελούν πειρασμό για εταιρίες που δεν διαθέτουν επαρκή τεχνογνωσία στους τομείς παραγωγής, μεταφοράς και διανομής ΗΕ.

5.3.2. Στρατιωτική κατασκοπεία

Το δίκτυο ΗΕ αποτελεί τον ενεργειακό κορμό ενός κράτους επί του οποίου στηρίζονται σχεδόν όλες οι βασικές υποδομές του. Επομένως, αποτελεί ενδεχόμενο στόχο στρατιωτικών ενεργειών. Το Smart Grid προκειμένου να επιτελέσει πολλές από τις λειτουργίες του είναι απαραίτητο να διατηρεί κάθε χρονική στιγμή δεδομένα τις κατάστασης των κόμβων του. Αυτά τα δεδομένα έχουν μεγάλη αξία για τις υπηρεσίες πληροφοριών αντίπαλων κρατών και ομάδων. Το γεγονός αυτό αυξάνει σημαντικά την πιθανότητα επιθέσεων εναντίον του βιομηχανικού πληροφοριακού δικτύου ΗΕ.

Αν δεδομένα κατάστασης των κόμβων του Smart Grid λαμβάνονται συστηματικά και σε μεγάλη κλίμακα, μπορούν να προσφέρουν γνώση της κατάστασης και της λειτουργίας του δικτύου. Από τη συλλογή των πληροφοριών αυτών, μπορεί να προκύψει γνώση για τα εξής:

1. Κόμβοι των οποίων η λειτουργία βρίσκεται κοντά στο όριο των προδιαγραφών λειτουργίας.
2. Ακριβής ώρα αιχμής του φόρτου για κάθε κόμβο του δικτύου.
3. Σταθμοί παραγωγής με τη μεγαλύτερη παραγόμενη ισχύ.
4. Αντιστοίχιση υποδομών με τους σταθμούς παραγωγής που τις τροφοδοτούν.

Τα ανωτέρω είναι ορισμένες μόνο από τις πληροφορίες που μπορούν εύκολα να εξαχθούν από τα δεδομένα κατάστασης των κόμβων του Smart Grid. Η γνώση τους κρίνεται πολύ χρήσιμη για το σχεδιασμό στρατιωτικών επιχειρήσεων και για το λόγο αυτό το βιομηχανικό πληροφοριακό δίκτυο ΗΕ αποτελεί συχνά στόχο κατασκοπείας.

5.3.3. Δολιοφθορά

Το δίκτυο ΗΕ αποτελεί ένα από τους συχνότερους στόχους επιθέσεων, αφού πλήττονται ταυτοχρόνως πολλές από τις υποδομές που βασίζονται σε αυτό.

Οι νέες δυνατότητες απομακρυσμένης διαχείρισης και επικοινωνίας που προσφέρει το Smart Grid παρέχουν την ευκαιρία για διακριτικά πλήγματα ηλεκτρονικού πολέμου εναντίον του. Έτσι, το δίκτυο ΗΕ γίνεται ευάλωτο σε ηλεκτρονικές παραβιάσεις των συστημάτων ελέγχου. Κατ' αυτό τον τρόπο, μπορεί να υπάρξει δολιοφθορά στα συστήματα του Smart Grid απομακρυσμένα και, συχνά, χωρίς να γίνονται αμέσως αντιληπτά τα αποτελέσματά της.

5.4. Μέθοδοι επίθεσης εναντίον του βιομηχανικού πληροφοριακού δικτύου

Τα κίνητρα που αναφέρθηκαν προηγουμένως αποτελούν το λόγο για τον οποίο το βιομηχανικό πληροφοριακό δίκτυο ΗΕ, και, κατ' επέκταση, το Smart Grid, αποτελούν στόχο κακόβουλων ενεργειών και επιθέσεων. Αντίστοιχα προς το κίνητρο της επίθεσης και το επιδιωκόμενο αποτέλεσμα, χρησιμοποιούνται διαφορετικές μέθοδοι επίθεσης. Στη συνέχεια, γίνεται η ανάλυση των μεθόδων αυτών, των κινήτρων για τα οποία αυτές πραγματοποιούνται, καθώς και το επιδιωκόμενο αποτέλεσμά τους.

5.4.1. Επιθέσεις προερχόμενες από το εταιρικό πληροφοριακό δίκτυο του διαχειριστή του δικτύου ΗΕ

Όπως έχει αναφερθεί προηγουμένως, ένα μεγάλο τμήμα του Smart Grid είναι το εταιρικό πληροφοριακό δίκτυο του διαχειριστή του δικτύου ΗΕ. Αποτελεί το συνδετικό ιστό ανάμεσα σε διαφορετικά τμήματα του Smart Grid, ένα από τα οποία είναι και το βιομηχανικό πληροφοριακό δίκτυο ΗΕ. Αν και οι περισσότερες διατάξεις του βιομηχανικού πληροφοριακού δικτύου ΗΕ βρίσκονται σε σταθμούς παραγωγής και σε κόμβους του δικτύου μεταφοράς και διανομής, υπάρχουν και διατάξεις που βρίσκονται στα όρια βιομηχανικού και

εταιρικού πληροφοριακού δικτύου. Αυτά τα συστήματα είναι συνήθως, τα συστήματα διατήρησης ιστορικού καταγραφών και τα συστήματα HMI (Human-Machine Interface).

Τα συστήματα διατήρησης ιστορικού ανήκουν στο βιομηχανικό πληροφοριακό δίκτυο ΗΕ καθώς πρέπει να έχουν πρόσβαση στα συστήματα καταγραφής, που συνδέονται με το βιομηχανικό πληροφοριακό δίκτυο ΗΕ. Το σύστημα καταγραφής από το οποίο αντλεί συνήθως τις μετρήσεις το σύστημα διατήρησης ιστορικού είναι το σύστημα SCADA. Από την άλλη πλευρά, ωστόσο, τα συστήματα καταγραφής περιέχουν πληροφορίες που είναι χρήσιμες για επιχειρησιακά στελέχη του διαχειριστή του δικτύου ΗΕ και των προμηθευτών ΗΕ και συνεπώς πρέπει να είναι προσβάσιμα, οπότε είναι συνδεδεμένα και στο εταιρικό πληροφοριακό δίκτυο. Συχνά, και τα συστήματα HMI πρέπει να παρέχουν δυνατότητες απομακρυσμένης σύνδεσης. Προς υποστήριξη αυτής της υπηρεσίας, είναι απαραίτητη η πρόσβαση στο σύστημα με το οποίο γίνεται η σύνδεση μέσω του εταιρικού πληροφοριακού δικτύου. Η προσβασιμότητα σε αυτά τα συστήματα από το εταιρικό πληροφοριακό δίκτυο δίνει τη δυνατότητα σε κακόβουλους εισβολείς να απειλήσουν τα συστήματα του βιομηχανικού πληροφοριακού δικτύου ΗΕ. Μία επίθεση, όμως που, εκκινεί από τα προαναφερθέντα συστήματα έχει αρκετά βήματα μέχρι την ολοκλήρωσή της τα οποία αναλύονται ξεχωριστά στη συνέχεια.

1. Παραβίαση συστημάτων διατήρησης ιστορικού και HMI

Το πρώτο βήμα κατά την πραγματοποίηση μιας επίθεσης έναντι των συστημάτων διατήρησης ιστορικού και των συστημάτων HMI είναι η απόκτηση πρόσβασης σε μια διάταξη που ανήκει στο βιομηχανικό πληροφοριακό δίκτυο ΗΕ. Επειδή η άμεση δικτυακή πρόσβαση στο βιομηχανικό πληροφοριακό δίκτυο ΗΕ δεν είναι εφικτή, πρέπει αρχικά να παραβιαστούν συστήματα προσβάσιμα μέσω του εταιρικού πληροφοριακού δικτύου. Στο σημείο αυτό θα θεωρηθεί ότι ο επιτιθέμενος έχει αποκτήσει πρόσβαση στο εταιρικό πληροφοριακό δίκτυο του διαχειριστή του δικτύου ΗΕ, με τρόπους που αναλύθηκαν στο προηγούμενο κεφάλαιο.

Αρχικά, επιχειρείται παραβίαση είτε του συστήματος διατήρησης ιστορικού είτε του συστήματος HMI. Ο σκοπός του επιτιθέμενου στο στάδιο αυτό είναι η παραβίαση του λογισμικού που επικοινωνεί με τα συστήματα SCADA. Συχνά, στην περίπτωση του HMI, τα λογισμικά για το HMI και την επικοινωνία με τα συστήματα SCADA εκτελούνται στο ίδιο υπολογιστικό σύστημα. Έτσι, αν ο επιτιθέμενος αποκτήσει πρόσβαση στο σύστημα HMI, μπορεί αμέσως να επιχειρήσει την παραβίαση και του λογισμικού SCADA. Στην περίπτωση, αντίθετα, όπου HMI και SCADA λειτουργούν σε διαφορετικά υπολογιστικά συστήματα ο επιτιθέμενος πρέπει αρχικά να παραβιάσει το σύστημα HMI και, ακολούθως, να αποκτήσει πρόσβαση και να παραβιάσει το σύστημα SCADA.

Για την παραβίαση είτε του συστήματος HMI είτε του συστήματος διατήρησης ιστορικού χρησιμοποιούνται τεχνικές που αναλύθηκαν στο προηγούμενο κεφάλαιο, καθώς πρόκειται για υπολογιστικά συστήματα με κοινά λειτουργικά συστήματα. Συνήθως, η παραβίαση γίνεται μέσω εκμετάλλευσης ευπαθειών είτε στο ίδιο το λειτουργικό είτε σε λογισμικά που τρέχουν στο σύστημα-στόχο. Το κακόβουλο λογισμικό εκμεταλλεύεται ευπάθειες ώστε να αποκτήσει πρόσβαση ως χρήστης στο σύστημα-στόχο. Στη συνέχεια, εφόσον είναι αναγκαίο, επιχειρεί να αναβαθμίσει τα δικαιώματά του στο συγκεκριμένο σύστημα και να καλύψει τα ηλεκτρονικά ίχνη της παραβίασης.

2. Παραβίαση λογισμικού SCADA

Το επόμενο στάδιο αυτής της μεθόδου επίθεσης είναι η παραβίαση του λογισμικού που ελέγχει το σύστημα SCADA. Στο στάδιο αυτό, θεωρείται ότι το κακόβουλο λογισμικό έχει παραβιάσει το υπολογιστικό σύστημα στο οποίο τρέχει το λογισμικό SCADA. Το λογισμικό SCADA είναι ο κόμβος master ενός τμήματος του βιομηχανικού πληροφοριακού δικτύου ΗΕ και επικοινωνεί με όσους κόμβους slave βρίσκονται υπό τον έλεγχό του. Στόχος, λοιπόν, κατά το στάδιο αυτό είναι η παραβίαση από το κακόβουλο λογισμικό του λογισμικού SCADA, ώστε να αποκτήσει πρόσβαση στους υπό έλεγχο κόμβους slave.

Και στην περίπτωση αυτή η παραβίαση του λογισμικού γίνεται μέσω της εκμετάλλευσης ευπαθειών που υπάρχουν σε αυτό. Επειδή τα λογισμικά αυτά είναι ιδιόκτητα, ο μέσος κύκλος ζωής μιας ευπάθειας είναι μεγαλύτερος. Αυτό εντείνεται στην περίπτωση βιομηχανικών εφαρμογών όπου οι ευπάθειες δεν γίνονται αντιληπτές υπό κανονικές συνθήκες λειτουργίας. Επαφίεται, επομένως, στις εταιρίες παραγωγής του λογισμικού να κάνουν τους απαραίτητους ελέγχους ασφαλείας προτού κυκλοφορήσει το λογισμικό στην αγορά. Ωστόσο, για λόγους εξοικονόμησης πόρων, οι εταιρίες αυτές συχνά υποβάλλουν το λογισμικό μόνο σε στοιχειώδεις ελέγχους ασφάλειας. Συνεπώς, ένας κακόβουλος χρήστης που διαθέτει τους οικονομικούς πόρους να αποκτήσει την εφαρμογή και χρόνο για να αναζητήσει κενά ασφαλείας σε αυτή, έχει μεγάλες πιθανότητες να επιτύχει.

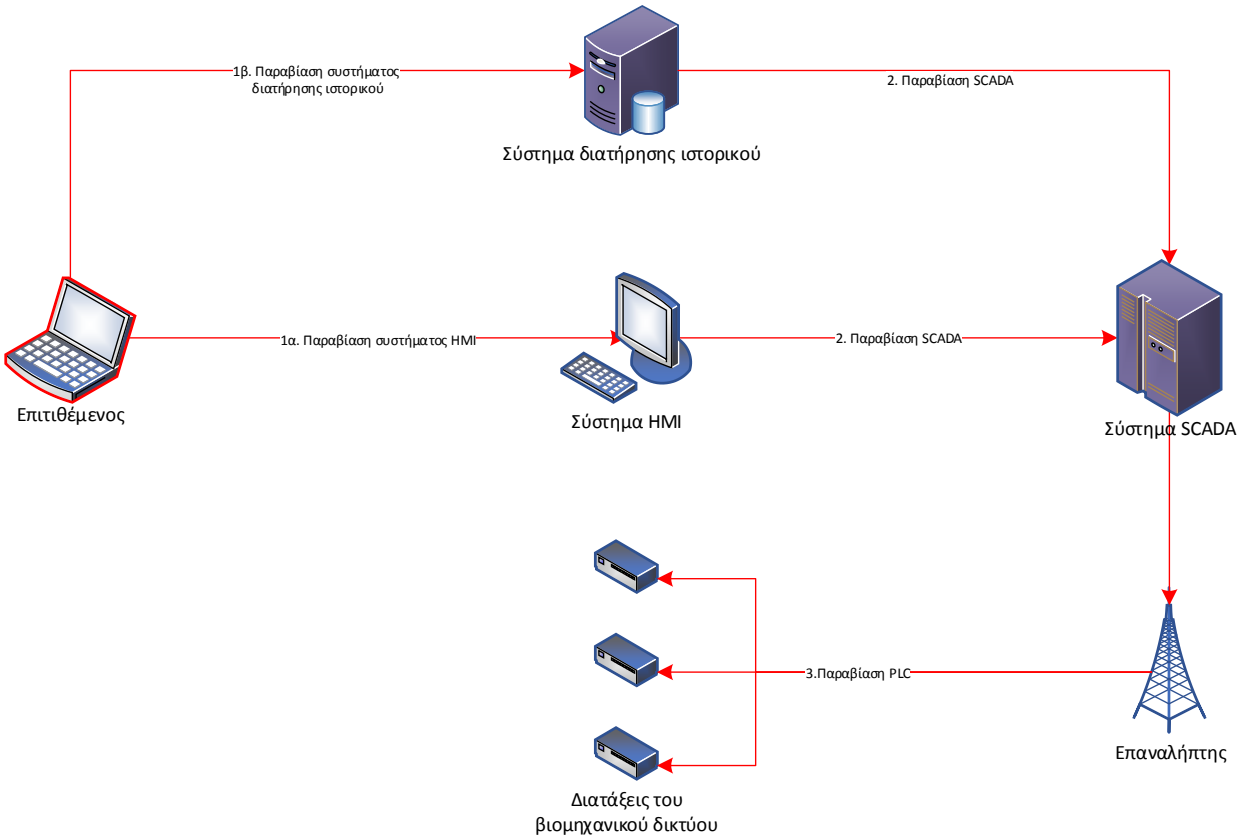
Κατάλληλα κατασκευασμένα κακόβουλα λογισμικά, εκμεταλλευόμενα ευπάθειες στα λογισμικά SCADA, είναι σε θέση να αποκτήσουν το έλεγχο του συστήματος. Έτσι, αποκτούν τη δυνατότητα να επικοινωνούν με τις διατάξεις που είναι υπό τον έλεγχο του συγκεκριμένου συστήματος SCADA, και κατά συνέπεια αποκτούν τα ίδια δικαιώματα στο δίκτυο που έχει και το πραγματικό λογισμικό ελέγχου SCADA. Στο σημείο αυτό, οι ενέργειες του κακόβουλου λογισμικού εξαρτώνται από το κίνητρο της επίθεσης. Αν η επίθεση γίνεται για λόγους κατασκοπείας, ένα κακόβουλο λογισμικό προβαίνει σε ενέργειες απόκρυψης και «μονιμοποίησης» του ώστε να διατηρηθεί η παραβίαση του συστήματος σε περίπτωση επανεκκίνησης. Καταγράφει την κατάσταση λειτουργίας των υπό έλεγχο διατάξεων και δημιουργεί δίαυλο επικοινωνίας με κάποιο διακομιστή του εισβολέα στον οποίο μεταφέρει τις υποκλαπείσες πληροφορίες. Και στην περίπτωση όπου η επίθεση γίνεται για λόγους δολιοφθοράς, το λογισμικό αποκρύπτει τα ίχνη του ώστε να καταστήσει μόνιμη την παραβίαση του συστήματος. Ωστόσο, στην περίπτωση αυτή δεν γίνεται σύνδεση με κάποιον διακομιστή του εισβολέα προκειμένου η έλλειψη κίνησης δεδομένων στο δίκτυο εκ μέρους του κακόβουλου λογισμικού να δυσχεράνει την ανακάλυψή του. Τέλος, για να γίνει η δολιοφθορά απαιτείται ένα ακόμα στάδιο, αυτό της παραβίασης της τελικής συσκευής-στόχου.

3. Παραβίαση του Προγραμματιζόμενου Λογικού Ελεγκτή (Programmable Logic Controller - PLC) της υπό έλεγχο διάταξης

Τα υπό τον έλεγχο του SCADA συστήματα διαθέτουν διατάξεις PLC στις οποίες προγραμματίζονται οι διαδικασίες αυτομάτου ελέγχου που υλοποιούνται. Αυτές είναι προγραμματιζόμενες μέσω του βιομηχανικού πληροφοριακού δικτύου ΗΕ από το σύστημα SCADA. Εφόσον το τελευταίο έχει παραβιαστεί, ένα κακόβουλο λογισμικό είναι πλέον σε θέση να αλλοιώσει τις διαδικασίες ελέγχου των υπό έλεγχο διατάξεων.

Στην περίπτωση της δολιοφθοράς, το τελευταίο στάδιο αυτής της μεθόδου επίθεσης είναι η αλλοίωση του κώδικα στο PLC της τελικής διάταξης-στόχου. Το κακόβουλο λογισμικό πρέπει να είναι σε θέση να διαβάσει τον κώδικα με τις διαδικασίες ελέγχου και να είναι προγραμματισμένο ώστε να εισάγει τις

κακόβουλες εντολές στη σωστή θέση. Συνήθως, το πρώτο βήμα είναι η αλλοίωση των βασικών διαδικασιών αυτομάτου ελέγχου ώστε να διακόπτεται η σωστή λειτουργία της διάταξης του βιομηχανικού δικτύου ΗΕ. Ωστόσο, αυτό γίνεται αμέσως αντιληπτό από τις διαδικασίες καταγραφής του συστήματος. Επομένως, ταυτόχρονα, αλλοιώνονται και οι διαδικασίες μέτρησης και καταγραφής της διάταξης-στόχου, ώστε να εμφανίζονται φυσιολογικές τιμές στο HMI. Κατ' αυτό τον τρόπο, η δολιοφθορά δεν γίνεται αντιληπτή από τα συστήματα SCADA.



Σχήμα 5.1. Σχηματική απεικόνιση επίθεσης προερχόμενης από το εταιρικό πληροφοριακό δίκτυο του διαχειριστή του δικτύου ΗΕ

Στο Σχ. 5.1 απεικονίζεται σχηματικά η μέθοδος επίθεσης που περιεγράφηκε προηγουμένως. Αρχικά φαίνεται η παραβίαση είτε του HMI είτε του συστήματος διατήρησης ιστορικού από τον επιτιθέμενο για τον οποίο έχει υποτεθεί ότι διαθέτει πρόσβαση στο εταιρικό πληροφοριακό δίκτυο του διαχειριστή του δικτύου ΗΕ. Στη συνέχεια, γίνεται παραβίαση του συστήματος SCADA, που απεικονίζεται ως ξεχωριστό σύστημα αν και είναι σύνηθες να λειτουργεί στο ίδιο υπολογιστικό σύστημα με το HMI. Τελευταίο βήμα είναι η παραβίαση των PLC των υπό έλεγχο διατάξεων του βιομηχανικού πληροφοριακού δικτύου ΗΕ οι οποίες μπορεί να βρίσκονται σε μεγάλη απόσταση, όπως υποδηλώνεται από την ύπαρξη του επαναλήπτη.

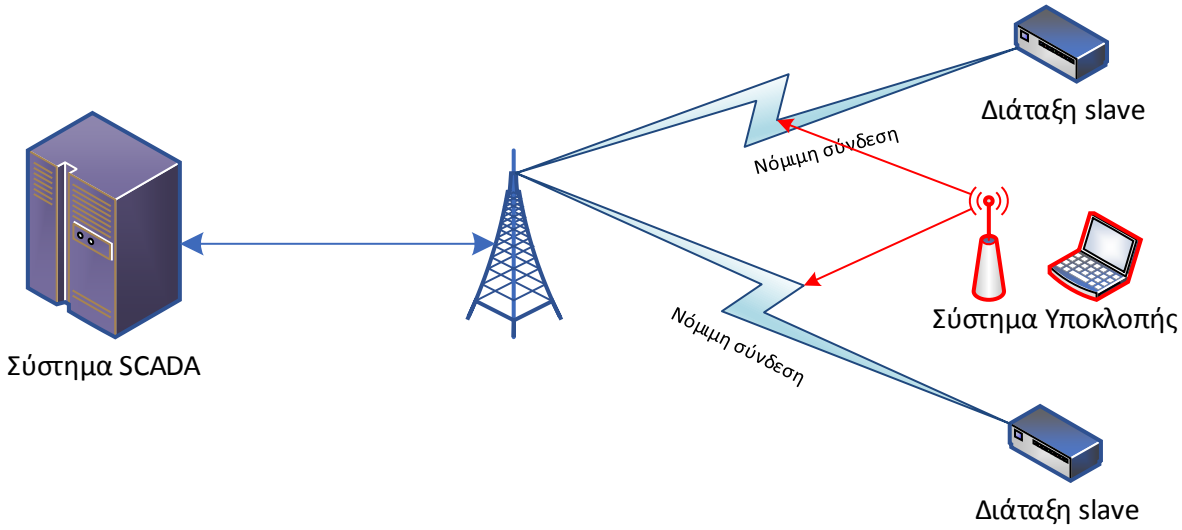
5.4.2. Εισαγωγή άγνωστης διάταξης

Σε αντίθεση με την προηγούμενη κατηγορία επιθέσεων όπου οι επιθέσεις προέρχονταν από το εταιρικό πληροφοριακό δίκτυο του διαχειριστή του δικτύου ΗΕ, στη συγκεκριμένη κατηγορία επιθέσεων, οι επιθέσεις εκκινούν από το βιομηχανικό πληροφοριακό δίκτυο ΗΕ και βασίζονται στην εκμετάλλευση σχεδιαστικών ατελειών και παραλείψεων σε πολλά βιομηχανικά πρωτόκολλα. Συγκεκριμένα, οι κακόβουλοι εισβολείς εκμεταλλεύονται το ότι δεν κρυπτογραφούνται τα μηνύματα που διακινούνται και το ότι δεν υπάρχει ταυτοποίηση των κόμβων. Οι επιθέσεις αυτής της κατηγορίας πραγματοποιούνται με την εισαγωγή από τον εισβολέα μιας κακόβουλης διάταξης στο βιομηχανικό πληροφοριακό δίκτυο. Πρέπει, ωστόσο, να σημειωθεί ότι η δυνατότητα πραγματοποίησης τέτοιων επιθέσεων εξαρτάται από το φυσικό μέσο, μέσω του οποίου γίνεται η επικοινωνία μεταξύ του συστήματος SCADA και των υπό έλεγχο διατάξεων. Η επιθέσεις εισαγωγής άγνωστης διάταξης εμφανίζονται σε αρκετές παραλλαγές. Ορισμένες από αυτές είναι παθητικές, όπου ο εισβολέας μόνο υποκλέπτει την κίνηση, άλλες είναι ενεργητικές, όπου ο εισβολέας δημιουργεί κακόβουλη κίνηση στο δίκτυο. Στη συνέχεια, αναλύονται χαρακτηριστικά δείγματα τέτοιων επιθέσεων.

1. Παθητική υποκλοπή πληροφοριών

Η συγκεκριμένη επίθεση γίνεται με την εκ μέρους του επίδοξου εισβολέα εισαγωγή ενός κόμβου στο βιομηχανικό πληροφοριακό δίκτυο ΗΕ, σε τέτοια θέση ώστε να μπορεί να υποκλέπτει τα δεδομένα που ανταλλάσσονται μεταξύ του κόμβου master και ορισμένων, τουλάχιστον, κόμβων slave. Επειδή τα δεδομένα δεν είναι κρυπτογραφημένα, ο επιτιθέμενος μπορεί αμέσως να εξαγάγει τις πληροφορίες από κάθε πακέτο που ανταλλάσσεται. Η συλλογή των δεδομένων πραγματοποιείται στο φυσικό στρώμα. Δηλαδή, η άγνωστη διάταξη δεν διευθυνσιοδοτείται στο βιομηχανικό πληροφοριακό δίκτυο ΗΕ, αλλά επιχειρεί να υποκλέψει πληροφορίες από το φυσικό μέσο επικοινωνίας. Η επιτυχία της ανωτέρω διαδικασίας εξαρτάται, επομένως, από το είδος του φυσικού μέσου μετάδοσης.

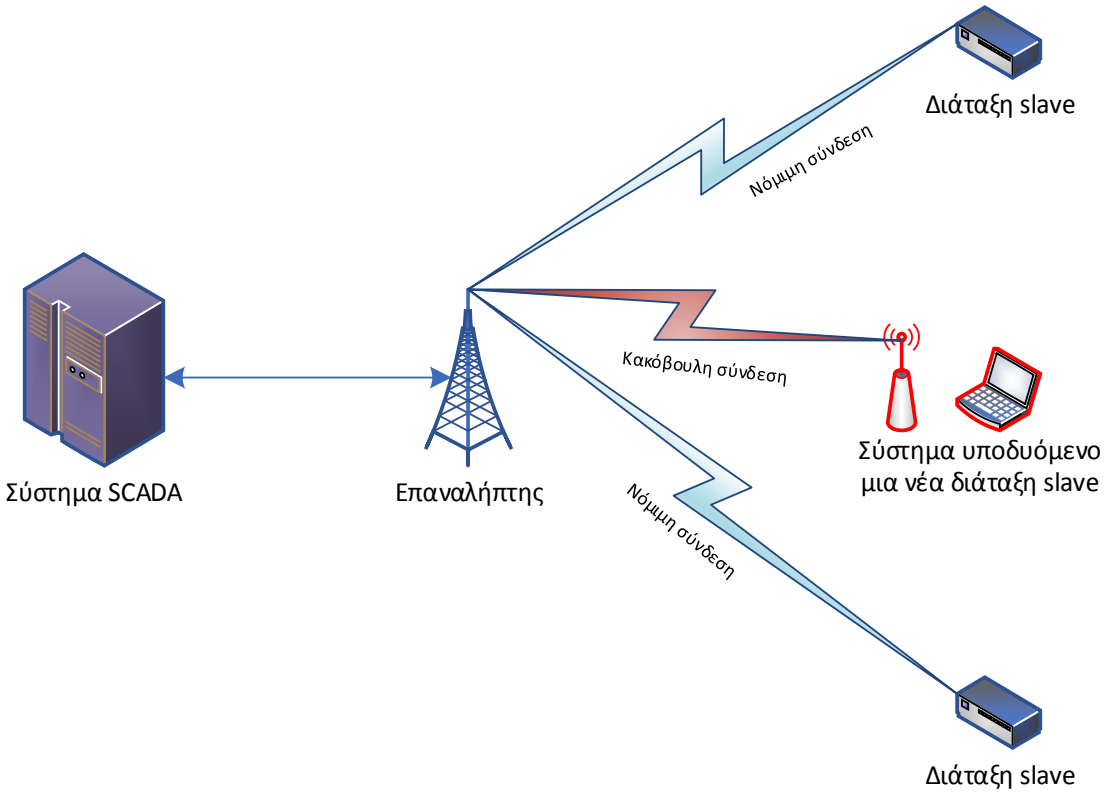
Μία επίθεση τέτοιου τύπου είναι εφικτή σε ασύρματα δίκτυα όπου οι πληροφορίες είναι διαθέσιμες σε όσους βρίσκονται εντός της εμβέλειας των επαναληπτών SCADA, εφόσον οι επικοινωνίες δεν είναι κρυπτογραφημένες. Η έλλειψη κρυπτογράφησης σε βιομηχανικά πληροφοριακά δίκτυα ΗΕ είναι σύνηθες φαινόμενο, αφενός λόγω της πρόσθετης καθυστέρησης που εισάγει, και αφετέρου, διότι μέχρι σήμερα δεν θεωρήθηκε αναγκαίο. Αντίθετα, μια τέτοια επίθεση είναι σημαντικά δυσκολότερη έως αδύνατη όταν χρησιμοποιείται η τεχνολογία Power Line Communications ή ενσύρματων μέσων για τη σύνδεση των κόμβων του βιομηχανικού πληροφοριακού δικτύου ΗΕ, καθώς δεν μπορεί να συνδεθεί ένας κακόβουλος κόμβος στο δίκτυο δίχως την ύπαρξη κατάλληλων υποδοχών από την πλευρά του δικτύου. Στο Σχ. 5.2 απεικονίζεται η επίθεση αυτού του τύπου, όπου εφόσον ο κόμβος είναι στην εμβέλεια του επαναλήπτη, μπορεί να υποκλέπτει τα δεδομένα των νόμιμων συνδέσεων των διατάξεων του βιομηχανικού πληροφοριακού δικτύου ΗΕ με το σύστημα SCADA.



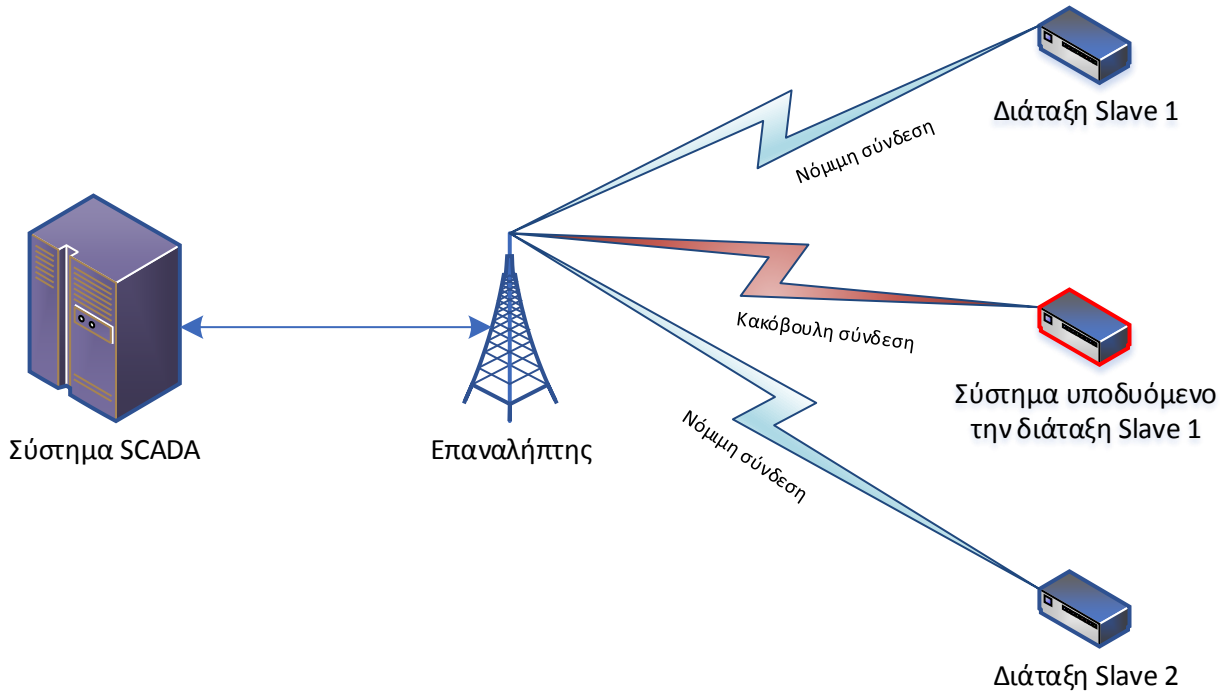
Σχήμα 5.2. Σχηματική απεικόνιση της μεθόδου υποκλοπής δεδομένων

2. Κόμβος υποκρινόμενος μια διάταξη slave

Η συγκεκριμένη μέθοδος αποτελεί μία ενεργητική παραλλαγή της προηγούμενης μεθόδου. Η διάταξη του επιτιθέμενου εισάγεται στο βιομηχανικό πληροφοριακό δίκτυο ΗΕ και υποδύεται μια διάταξη slave. Η διάταξη του επιτιθέμενου μπορεί είτε να εμφανίζεται ως ένας νέος κόμβος, όπως στο Σχ. 5.3, είτε να μιμείται ένα από τους υπάρχοντες κόμβους του δικτύου, όπως στο Σχ. 5.4. Συνήθως, προτιμάται η δεύτερη εκδοχή, αφού είναι δυσκολότερο να ανακαλυφθεί. Με την ανωτέρω επίθεση, η κακόβουλη διάταξη μπορεί να επιστρέφει αλλοιωμένα στοιχεία για να προκαλέσει συγκεκριμένη αρνητική αντίδραση από το σύστημα ελέγχου SCADA. Κάτι τέτοιο μπορεί να έχει πολύ αρνητικές συνέπειες για τη λειτουργία του δικτύου ΗΕ, καθώς είναι δυνατό να τίθενται διατάξεις εκτός λειτουργίας ή να εντέλλονται να λειτουργούν με ακραίες τιμές παραμέτρων που οδηγούν στην καταστροφή τους.



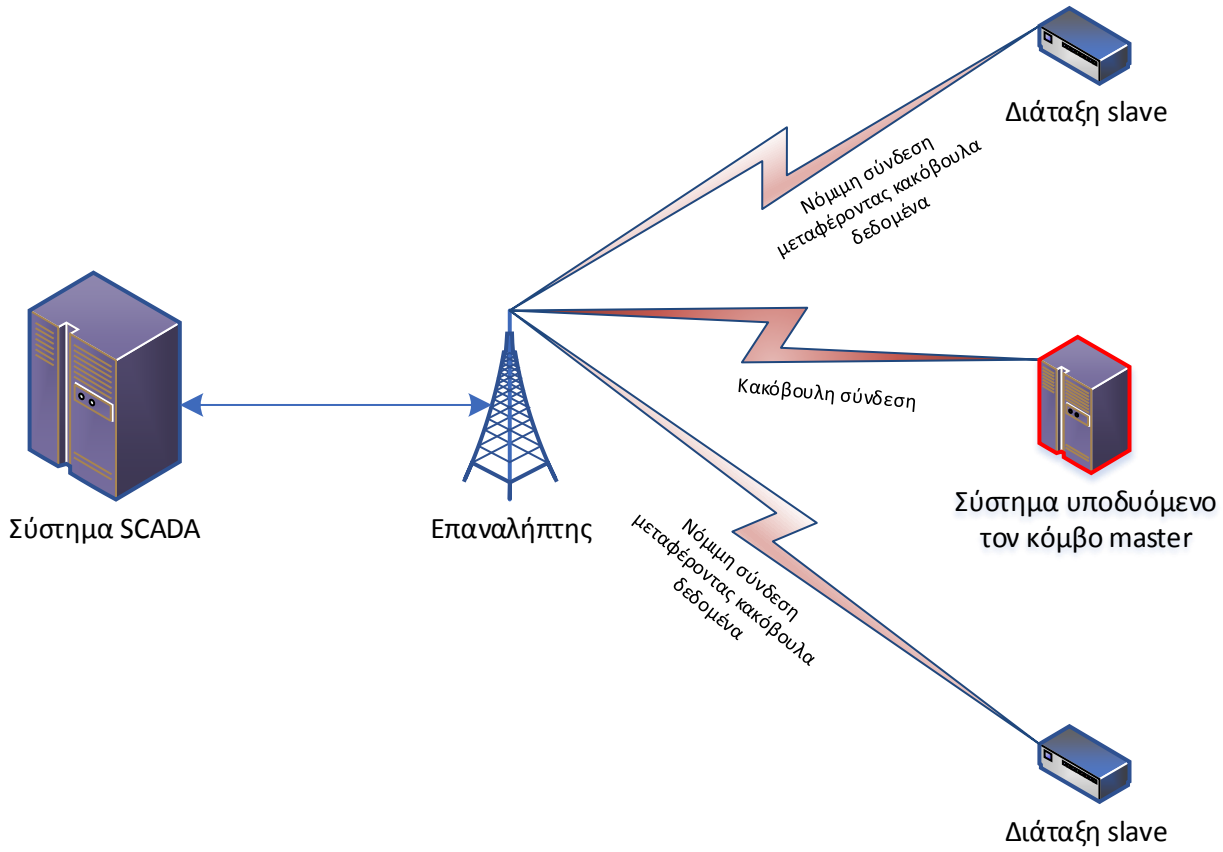
Σχήμα 5.3. Σχηματική απεικόνιση επίθεσης μέσω εισαγωγής συστήματος που υποδύεται μια νέα διάταξη slave.



Σχήμα 5.4. Σχηματική απεικόνιση επίθεσης μέσω εισαγωγής συστήματος που υποδύεται υπάρχουσα διάταξη slave.

3. Κόμβος υποκρινόμενος τον κόμβο master

Η κακόβουλη διάταξη του επιτιθέμενου που εισάγεται στο βιομηχανικό πληροφοριακό δίκτυο ΗΕ μπορεί να μιμηθεί και τον ίδιο τον κόμβο master. Κατ' αυτό τον τρόπο, μπορεί να μεταφέρει εντολές στις διατάξεις slave, τροποποιώντας την λειτουργία τους. Ωστόσο, η διάταξη του επιτιθέμενου πρέπει να αποστέλλει ορθά τα κακόβουλα δεδομένα με τους ορθούς κωδικούς συναρτήσεων του βιομηχανικού πρωτοκόλλου που χρησιμοποιείται. Κάτι τέτοιο, όμως, είναι εφικτό αν, πριν από την ενεργητική επίθεση, έχει πραγματοποιήσει παθητική υποκλοπή των ανταλλασσόμενων πληροφοριών. Έτσι, μπορεί να ανιχνεύσει τις συναρτήσεις και τους κωδικούς τους καθώς και τις συνήθεις τιμές των παραμέτρων. Πιθανές επιδιώξεις και αυτού του τύπου επίθεσης είναι η διακοπή της λειτουργίας διατάξεων, η λειτουργία τους εκτός των προδιαγραφών ασφαλείας, ακόμα και η διακοπή λειτουργίας όλων των διατάξεων στο βιομηχανικό πληροφοριακό δίκτυο ΗΕ. Η σχηματική απεικόνιση της επίθεσης φαίνεται στο Σχ. 5.5.



Σχήμα 5.5. Σχηματική απεικόνιση επίθεσης μέσω διάταξης που μιμείται τον κόμβο master.

4. Ενεργητική επίθεση Denial of Service (DoS)

Η συγκεκριμένη επίθεση μπορεί πραγματοποιηθεί μέσω μιας ενεργητικής διάταξης στο βιομηχανικό πληροφοριακό δίκτυο ΗΕ, δηλαδή μιας διάταξης που εισάγει δεδομένα στο βιομηχανικό πληροφοριακό δίκτυο ΗΕ, όπως και στις δύο προηγούμενες περιπτώσεις. Η ιδιαίτερη αναφορά της γίνεται λόγω της σοβαρότητας των συνεπειών της. Τα περισσότερα βιομηχανικά πρωτόκολλα που χρησιμοποιούνται σήμερα δεν έχουν σχεδιαστεί με κριτήριο και την ασφάλεια, χαρακτηριστικό που επιτρέπει την εκμετάλλευση δομών

του πρωτοκόλλου ώστε να τίθεται εκτός λειτουργίας το βιομηχανικό πληροφοριακό δίκτυο ΗΕ. Ενδεικτικά, για το πρωτόκολλο DNP3 που χρησιμοποιείται ευρέως στη βιομηχανία ΗΕ, υπάρχουν αρκετοί τρόποι ώστε μέσω του πρωτοκόλλου να γίνει επίθεση DoS εναντίον του δικτύου. Ορισμένοι από αυτούς είναι οι εξής:

1. Εισαγωγή μηνυμάτων broadcast τα οποία προκαλούν το φαινόμενο της πλημμύρας μηνυμάτων (flooding) στο βιομηχανικό πληροφοριακό δίκτυο ΗΕ.
2. Αλλοίωση των πακέτων χρονικού συγχρονισμού, με αποτέλεσμα διατάξεις να αποσυγχρονίζονται και τα πακέτα τους να καθίστανται άκυρα.
3. Αλλοίωση ή απώλεια μηνυμάτων επιβεβαίωσης που θα οδηγούν σε καταστάσεις συνεχούς αναμετάδοσης δεδομένων, κάτι που διακόπτει τη λειτουργία του δικτύου.

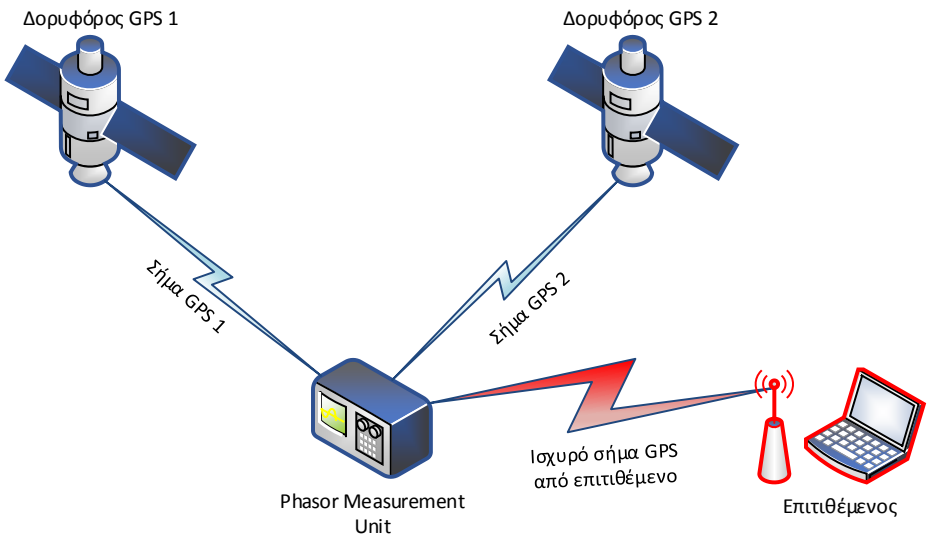
Οι ανωτέρω μέθοδοι δεν εκμεταλλεύονται κάποια ευπάθεια του πρωτοκόλλου DNP3 για να προκαλέσουν απώλεια διαθεσιμότητας αλλά, αντίθετα, εκμεταλλεύονται υπάρχουσες λειτουργίες του πρωτοκόλλου σε συνδυασμό με έλλειψη ελέγχου των τιμών των πακέτων. Ωστόσο, μπορεί να προκληθεί απώλεια διαθεσιμότητας από εκμετάλλευση ευπαθειών του πρωτοκόλλου DNP3 [51]. Σε πολλές από αυτές τις επιθέσεις, η απώλεια διαθεσιμότητας επιτυγχάνεται με την αποστολή ειδικά διαμορφωμένων πακέτων στη διάταξη master, με στόχο να τεθεί ο εποπτικός σταθμός σε ατέρμονα βρόχο ώστε να μη λειτουργεί μέχρι να γίνει χειροκίνητη επανεκκίνηση. Έτσι, τίθεται ολοκληρωτικά εκτός λειτουργίας ο εποπτικός σταθμός SCADA.

Όλες οι ανωτέρω μέθοδοι μπορούν να υλοποιηθούν με μεγάλη ευκολία, έχοντας ταυτόχρονα καταστροφικές συνέπειες για τη λειτουργία του βιομηχανικού πληροφοριακού δικτύου ΗΕ για το χρονικό διάστημα κατά το οποίο πραγματοποιούνται. Συνεπώς, αν ένα τμήμα του βιομηχανικού πληροφοριακού δικτύου ΗΕ τεθεί εκτός λειτουργίας, οι υπηρεσίες και η λειτουργικότητα του Smart Grid εμφανίζουν σημαντικό πρόβλημα. Επομένως, πρέπει να λαμβάνεται ειδική μέριμνα για αυτού του είδους τις επιθέσεις.

5.4.3. GPS Spoofing

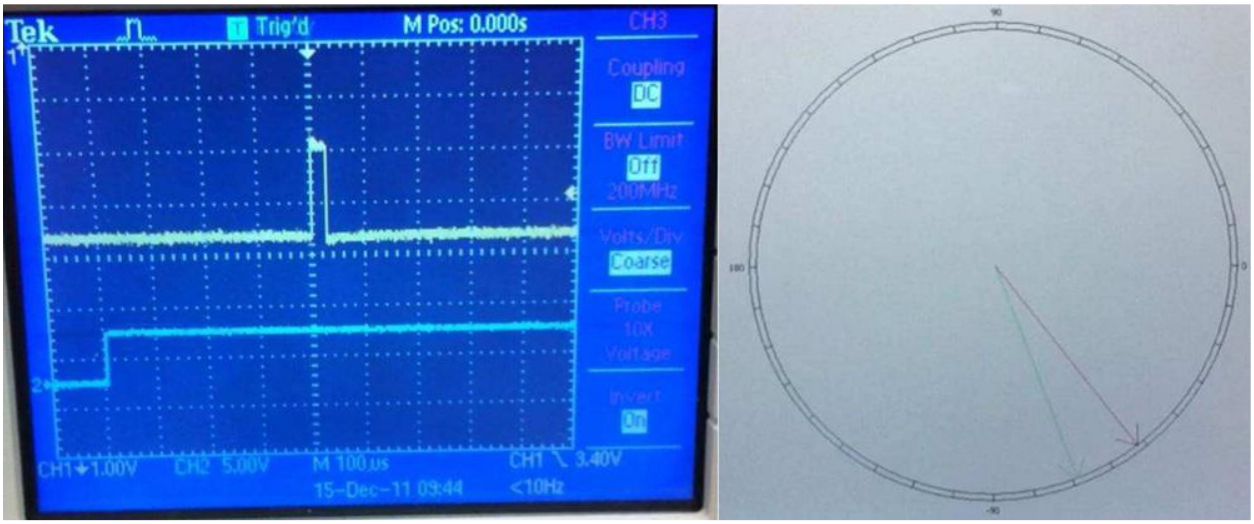
Η επίθεση GPS spoofing έχει ως στόχο ειδικές διατάξεις, οι οποίες, επειδή απαιτούν ακριβή χρονικό συγχρονισμό, χρησιμοποιούν το σύστημα GPS. Τυπικό παράδειγμα στο Smart Grid αποτελούν οι μονάδες Phasor Measurement Units. Το σκεπτικό τέτοιων επιθέσεων είναι η αντικατάσταση του πραγματικού σήματος χρονικού συγχρονισμού του GPS με ένα σήμα προερχόμενο από τον επιτιθέμενο. Κατ' αυτό τον τρόπο, αλλοιώνεται ο χρονικός συγχρονισμός της διάταξης, αφού η διάταξη λαμβάνει χρονικό συγχρονισμό επιλεγμένο από τον επιτιθέμενο [52], οδηγώντας το σύστημα ελέγχου να ενεργοποιήσει μεθόδους για την αποτροπή των ακραίων τιμών που παρατηρούνται, ενεργοποίηση η οποία, στην προκειμένη περίπτωση, έχει αρνητικά αποτελέσματα.

Η επίθεση GPS spoofing αναλύεται σε δύο στάδια. Το πρώτο στάδιο αφορά τον εξαναγκασμό του συστήματος στόχου να επιλέξει το σταθμό του επιτιθέμενου ως πηγή συγχρονισμού, σε αντικατάσταση των πραγματικών δορυφόρων GPS. Αρχικά, ο επιτιθέμενος εκπέμπει ακριβώς τα ίδια μηνύματα συγχρονισμού με τους πραγματικούς δορυφόρους. Αυτό είναι εφικτό, αφού στις εμπορικές εφαρμογές του συστήματος GPS, τα μηνύματα που αποστέλλουν οι δορυφόροι είναι προσδιορίσιμα. Στη συνέχεια, ο επιτιθέμενος αυξάνει σταδιακά την ισχύ εκπομπής μέχρι να υπερκαλύψει το σήμα των πραγματικών δορυφόρων, οπότε ο δέκτης του στόχου κλειδώνει στο δικό του σήμα. Για το στάδιο αυτό είναι απαραίτητη η γειτνίαση του επιτιθέμενου με το στόχο, ώστε, αρχικά, ο πομπός του επιτιθέμενου να μπορεί να λαμβάνει αρχικά τα πραγματικά σήματα GPS που λαμβάνει και ο στόχος, ώστε να προβλέψει τα επόμενα, και στη συνέχεια, να είναι σε θέση υπερκαλύψει το σήμα των δορυφόρων GPS. Το πρώτο στάδιο φαίνεται στο Σχ. 5.6.



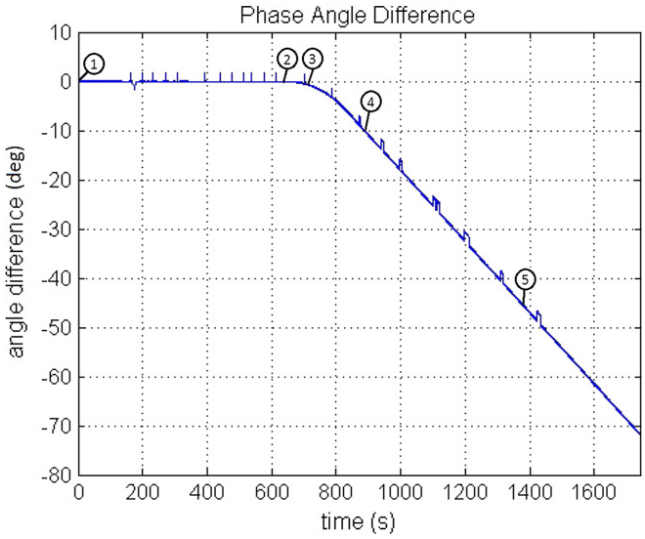
Σχήμα 5.6. Σχηματική απεικόνιση του πρώτου σταδίου μιας επίθεσης GPS Spoofing

Το δεύτερο στάδιο εκκινεί από τη στιγμή όπου ο δέκτης της διάταξης-στόχου έχει κλειδώσει στο σήμα του επιτιθέμενου. Στο χρονικό σημείο αυτό, η διάταξη του επιτιθέμενου μετατοπίζει σε κάθε δευτερόλεπτο κατά μερικά ns τη χρονική στιγμή που αναφέρει στη διάταξη. Έτσι, ο στόχος, ολισθαίνει κατά ορισμένα ns κάθε δευτερόλεπτο. Κατ' αυτό τον τρόπο δεν ενεργοποιείται κάποιος συναγερμός στο σύστημα, οπότε μετά από κάποια λεπτά, η διάταξη εμφανίζει σημαντική απόκλιση χρόνου, με συνέπεια να λαμβάνονται στο κέντρο ελέγχου τιμές με σημαντικές αποκλίσεις φάσης. Με τη σειρά του το κέντρο ελέγχου ενεργοποιεί τις αντίστοιχες διαδικασίες ελέγχου ώστε να επαναφέρει τη φάση στην ορθή τιμή. Αυτό όμως, έχει καταστροφικές συνέπειες για τη λειτουργία της διάταξης, αφού η διαδικασία ελέγχου βασίζεται σε αλλοιωμένα δεδομένα εισόδου. Στο Σχ. 5.7 που ακολουθεί [52], φαίνεται η μετατόπιση χρονικού συγχρονισμού ανάμεσα στο πραγματικό σήμα GPS και αυτό του επιτιθέμενου, καθώς και η διαφορά του μετρούμενου phasor με το πραγματικό, 870s μετά την έναρξη της επίθεσης.



Σχήμα 5.7. Αριστερά φαίνεται η προήγηση του παλμού συγχρονισμού του επιτιθέμενου (μπλε) σε σχέση με το πραγματικό σήμα (κίτρινο), ενώ δεξιά φαίνεται η απόκλιση του μετρούμενου phasor από την πραγματική τιμή.

Στη γραφική παράσταση του Σχ. 5.8 [52], φαίνεται και η διαφορά φάσης που εισάγεται στις μετρήσεις ως αποτέλεσμα της συγκεκριμένης επίθεσης.



Σχήμα 5.8. Γραφική παράσταση της διαφοράς φάσης ανάμεσα στο μετρούμενο φασιθέτη και τον πραγματικό συναρτήσει της χρονικής διάρκειας της επίθεσης.

Καίτοι σχετικά απλή στην υλοποίησή της εφόσον ο επιτιθέμενος έχει τον κατάλληλο εξοπλισμό και βρίσκεται κοντά στη διάταξη στόχο, η συγκεκριμένη επίθεση μπορεί να εξαναγκάσει τα συστήματα αυτομάτου ελέγχου του δικτύου ΗΕ να λάβουν λανθασμένα μέτρα αποκατάστασης με αρνητικές συνέπειες για τη λειτουργία της διάταξης-στόχου.

5.4.4. Εισαγωγή κακόβουλου hardware

Η πλειονότητα, αν όχι το σύνολο, των εμπλεκόμενων στην αγορά ΗΕ δεν έχουν τη δυνατότητα να κατασκευάσουν οι ίδιοι τα συστήματα που χρησιμοποιούν στα διάφορα τμήματα του δικτύου. Συνεπώς, προμηθεύονται τμήματα του εξοπλισμού από τρίτες κατασκευάστριες εταιρίες, που συνήθως προέρχονται από διαφορετικές χώρες. Ωστόσο, επειδή το Smart Grid ως δίκτυο ΗΕ έχει σημαίνοντα ρόλο στα γεωστρατηγικά σχέδια διάφορων χωρών, υπάρχει σημαντικό κίνητρο για την εισαγωγή κακόβουλου hardware στις διατάξεις που θα χρησιμοποιηθούν σε ευφυή δίκτυα ΗΕ άλλων χωρών.

Η ύπαρξη κακόβουλου hardware είναι σχεδόν αδύνατον να εντοπιστεί από το διαχειριστή του δικτύου ΗΕ. Τα συστήματα έρχονται κλειδωμένα σε φυσικό και λογικό επίπεδο, ώστε να μη μπορεί εκ των υστέρων να γίνει παρέμβαση στο hardware. Ωστόσο, δεν υπάρχει απόδειξη για μη εισαγωγή κακόβουλου τμήματος hardware κατά τη διαδικασία κατασκευής και συναρμολόγησης ενός συστήματος από την κατασκευάστρια εταιρία. Κακόβουλο hardware μπορεί να εισαχθεί σε κάθε σύστημα ή διάταξη που χρησιμοποιείται στο Smart Grid. Μπορεί να εισαχθεί σε ελεγκτές SCADA, ή σε διατάξεις του βιομηχανικού δικτύου ΗΕ όπως τα PMUs, μετατροπείς τάσης, γεννήτριες κλπ.

Μία συνέπεια της συγκεκριμένης επίθεσης είναι η καταγραφή σημαντικών πληροφοριών ανάλογα με τη λειτουργία που επιτελεί το συγκεκριμένο σύστημα. Ακόμη, εφόσον υπάρχει κακόβουλη πρόθεση, τα συγκεκριμένα τμήματα hardware είναι σε θέση να εισάγουν στα συστήματα κενά ασφαλείας, τα οποία, στη συνέχεια μπορεί να εκμεταλλευθεί είτε η κατασκευάστρια εταιρία, είτε στρατιωτικές οντότητες της χώρας κατασκευής, με στόχο να παραβιάσουν τη διάταξη και να ανακτήσουν τις αποθηκευμένες πληροφορίες.

Το στοιχείο που εισάγει μεγάλο επίπεδο δυσκολίας στην προαναφερθείσα διαδικασία είναι η εύρεση και χρήση ενός καναλιού εξόδου για τα δεδομένα που έχουν υποκλαπεί. Η υποκλοπή δεδομένων είναι εύκολη καθώς το κακόβουλο hardware είναι σχεδιασμένο να έχει πρόσβαση στη μνήμη. Πρέπει, όμως, η εξαγωγή των δεδομένων να γίνεται με τέτοιο τρόπο που να μην είναι διακριτή στην έξοδο των καναλιών εξόδου που χρησιμοποιούνται κατά την κανονική λειτουργία της διάταξης-θύμα. Ενδεικτικά, ως πιθανά φυσικά μέσα εξαγωγής των δεδομένων που έχουν υποκλαπεί μπορούν να είναι η ισχύς που καταναλώνει το ολοκληρωμένο κύκλωμα [53], η θερμοκρασία του [54], ή και πραγματικές έξοδοι όπως η έξοδος RS232 [54].

Η ισχύς μπορεί να χρησιμοποιηθεί ως κανάλι εξόδου δεδομένων, μέσω ειδικών ολοκληρωμένων κυκλωμάτων τα οποία μεταβάλλουν την ισχύ που καταναλώνουν βάσει των δεδομένων που δέχονται στις εισόδους τους. Οι κακόβουλες οντότητες που κατασκευάζουν το κακόβουλο hardware προκειμένου να μην είναι ανιχνεύσιμη η πληροφορία που εξάγεται από το κανάλι ισχύος κατά τον έλεγχο της συσκευής, χρησιμοποιούν πολύ μικρά bitrates σε συνδυασμό με τεχνικές εξάπλωσης φάσματος (spread-spectrum) ώστε να μην είναι εύκολα αναγνωρίσιμο το σήμα από τον θόρυβο, και να περνά τις δοκιμασίες ελέγχου στο τέλος της διαδικασίας κατασκευής. Αντίστοιχα με την ισχύ, είναι δυνατόν μέσω αλλαγής της συχνότητας των διακοπτών του κακόβουλου ολοκληρωμένου κυκλώματος να μεταβάλλεται η θερμοκρασία της διάταξης-θύμα αποκαλύπτοντας έτσι τα δεδομένα που έχουν υποκλαπεί από το κακόβουλο hardware.

Όμως η χρήση κακόβουλου hardware σε διατάξεις του βιομηχανικού πληροφοριακού δικτύου για λόγους κατασκοπείας υποκρύπτει μία δυσκολία. Στην περίπτωση όπου το βιομηχανικό πληροφοριακό δίκτυο είναι επαρκώς περιορισμένο (self-contained), δηλαδή το πλήθος των διόδων μέσω των οποίων ένας κακόβουλος εισβολέας μπορεί να εισέλθει σε αυτό είναι μικρό, είναι δύσκολη η εξαγωγή των δεδομένων που έχουν υποκλαπεί καθώς δεν είναι εύκολη η πρόσβαση στη διάταξη-θύμα και τα δεδομένα του κακόβουλου υλικού. Αντ’ αυτού, το κακόβουλο hardware μπορεί να σχεδιαστεί με σκοπό την δολιοφθορά της διάταξης-θύμα και την απώλεια διαθεσιμότητας τμήματος του βιομηχανικού πληροφοριακού δικτύου. Σε αυτή την περίπτωση, δεν απαιτείται η πρόσβαση από τον επιτιθέμενο στη διάταξη-θύμα. Αντιθέτως, κατά τη σχεδίαση του κακόβουλου hardware ορίζονται οι συνθήκες υπό τις οποίες θα ενεργοποιηθεί η κακόβουλη λειτουργία του.

Έτσι, μπορεί να εισαχθεί κακόβουλο hardware το οποίο να βρίσκεται σε λανθάνουσα κατάσταση, χωρίς να επηρεάζει τη λειτουργία της διάταξης, μέχρι να κριθεί σκόπιμη η ενεργοποίησή του. Κατά την ενεργοποίησή του μπορεί για παράδειγμα να αλλοιώσει το σήμα ρολογιού του ολοκληρωμένου κυκλώματος οδηγώντας τη διάταξη σε δυσλειτουργία [55]. Συνεπώς, ακόμη και η ανίχνευση της ύπαρξης του κακόβουλου hardware είναι σχεδόν αδύνατη. Ακόμη, όμως, και όταν ενεργοποιηθεί, η αντιμετώπιση της απειλής και η ελαχιστοποίηση των συνεπειών είναι πολύπλοκη διαδικασία. Αυτό συμβαίνει διότι, αντίθετα με το software, το hardware δεν παρέχει τον ίδιο βαθμό ευελιξίας. Σε πολλές περιπτώσεις δεν είναι δυνατή η άμεση αφαίρεση της διάταξης από το βιομηχανικό πληροφοριακό δίκτυο. Ακόμη, η παραβιασμένη διάταξη δεν μπορεί να αντικατασταθεί άμεσα από μία με διορθωμένο hardware καθώς το ακριβές μοντέλο hardware που εγκαθίσταται καθορίζεται κατά τη διαδικασία κατασκευής. Τα ανωτέρω χαρακτηριστικά καθιστούν το συγκεκριμένο είδος επίθεσης ένα από τα πλέον απειλητικά για το Smart Grid.

5.5. Αντιμετώπιση επιθέσεων στο βιομηχανικό πληροφοριακό δίκτυο

Στο παρόν εδάφιο αναλύονται και προτείνονται μέθοδοι για την ασφάλεια των διατάξεων του βιομηχανικού πληροφοριακού δικτύου από επιθέσεις όπως αυτές που προαναφέρθηκαν. Οι μέθοδοι αυτές αφορούν τους εποπτικούς σταθμούς SCADA, τις διατάξεις PLC και τα συστήματα PMU.

Η υιοθέτηση τεχνολογιών του Smart Grid αναμένεται να εισαγάγει μεγάλες αλλαγές στο σχεδιασμό ασφάλειας του βιομηχανικού πληροφοριακού δικτύου. Μέχρι σήμερα, η απουσία επικοινωνίας των διατάξεων με εξωτερικά δίκτυα παρείχε επαρκή ασφάλεια ώστε να μην απαιτούνται ειδικοί μηχανισμοί ασφάλειας με αποτέλεσμα οι διατάξεις και τα πρωτόκολλα επικοινωνίας να σχεδιάζονται με γνώμονα την αξιοπιστία και την απόδοση. Στο Smart Grid, όμως, συστήματα του βιομηχανικού πληροφοριακού δικτύου θα είναι προσβάσιμα από εξωτερικά δίκτυα, όπως το εταιρικό πληροφοριακό δίκτυο του διαχειριστή του δικτύου ΗΕ. Συνεπώς, το βιομηχανικό πληροφοριακό δίκτυο εκτίθεται σε πληθώρα, πλέον, νέων απειλών.

Το πλήθος νέων απειλών, σε συνδυασμό με την απουσία μηχανισμών ασφάλειας στα σημερινά συστήματα, καθιστά απαραίτητο ένα ολοκληρωμένο σχεδιασμό ασφάλειας για όλες τις διατάξεις του βιομηχανικού δικτύου ΗΕ, λαμβάνοντας ταυτόχρονα υπόψη τις προδιαγραφές λειτουργίας κάθε διάταξης. Ο ανωτέρω στόχος δεν είναι εύκολος καθώς υπάρχει αμοιβαία αντιστάθμιση (trade-off) ανάμεσα στην ποιότητα ασφάλειας και την επιβάρυνση στη λειτουργία της εκάστοτε διάταξης. Σε αυτή την αμοιβαία αντιστάθμιση, οι μέθοδοι ασφάλειας που ακολουθούν αποσκοπούν στην εξασφάλιση του μέγιστου βαθμού ασφάλειας κάθε διάταξης για τον οποίο εξασφαλίζονται στο ακέραιο οι προδιαγραφές λειτουργίας της.

5.5.1. Μέθοδοι ασφάλειας εποπτικών σταθμών SCADA έναντι απειλών εκτός του βιομηχανικού πληροφοριακού δικτύου

Λόγω του διαχειριστικού ρόλου τους στο βιομηχανικό πληροφοριακό δίκτυο, οι εποπτικοί σταθμοί SCADA αποτελούν κορυφαίο στόχο επίθεσης εντός του βιομηχανικού πληροφοριακού δικτύου. Επιπλέον, η ασφάλεια των εποπτικών σταθμών SCADA παρουσιάζει προκλήσεις για τους μηχανικούς ασφάλειας συγκριτικά με άλλες διατάξεις του βιομηχανικού πληροφοριακού δικτύου. Η βασικότερη πρόκληση απορρέει από το γεγονός ότι τα λογισμικά ελέγχου SCADA εκτελούνται σε εμπορικά λειτουργικά συστήματα. Ευπάθειες εμπορικών λειτουργικών συστημάτων ανακαλύπτονται με μεγάλη συχνότητα. Αυτό συνεπάγεται πληθώρα ευπαθειών που μπορούν να αξιοποιηθούν προς την παραβίαση ενός συστήματος με εμπορικό λειτουργικό σύστημα. Ακόμη, τα συστήματα SCADA και HMI είναι πολύ συχνά συνδεδεμένα με το εταιρικό πληροφοριακό δίκτυο του διαχειριστή του δικτύου ΗΕ, ώστε να παρέχονται σε εσωτερικά συστήματα πληροφορίες σχετικές με τη λειτουργία των βιομηχανικών διατάξεων. Η σύνδεση αυτή αυξάνει την επιφάνεια επίθεσης εναντίον συστημάτων SCADA και HMI καθώς μια επίθεση μπορεί να πηγάζει και από το εταιρικό πληροφοριακό δίκτυο του διαχειριστή του δικτύου ΗΕ. Συμπερασματικά, η κρισιμότητα των συστημάτων SCADA, σε συνδυασμό με τις πρόσθετες προκλήσεις για την ασφάλεια, επιβάλλει την υλοποίηση αυστηρών μηχανισμών ασφάλειας.

1. Εγκατάσταση μηχανισμών firewall και Intrusion Detection System (IDS) / Intrusion Prevention System (IPS)

Οι μηχανισμοί firewall και IDS/IPS είναι οι βασικοί μηχανισμοί ασφάλειας των δικτυακών συνδέσεων ενός συστήματος. Στην περίπτωση των εποπτικών σταθμών SCADA, οι μηχανισμοί firewall και IDS/IPS έχουν ως στόχο την ενίσχυση της ασφάλειας του από επιθέσεις προερχόμενες από το εταιρικό πληροφοριακό δίκτυο του διαχειριστή του δικτύου ΗΕ.

Ο μηχανισμός firewall φιλτράρει τη δικτυακή κίνηση του συστήματος SCADA από και προς άλλα συστήματα. Βάσει των κανόνων λειτουργίας ενός σταθμού SCADA, διαμορφώνεται ένας χάρτης με τα συστήματα με τα οποία είναι αναγκαίο να επικοινωνεί και τα πρωτόκολλα μέσω των οποίων θα γίνεται η ανωτέρω επικοινωνία. Στη συνέχεια, ο χάρτης αυτός μεταφράζεται σε ένα σύνολο κανόνων στο μηχανισμό firewall ώστε να απορρίπτεται κάθε κίνηση που δεν εμπίπτει στο πλαίσιο κανονικής λειτουργίας που έχει τεθεί. Για παράδειγμα, όταν ένας κακόβουλος χρήστης επιχειρήσει να επικοινωνήσει με το σταθμό SCADA, το firewall παρατηρεί ότι η κίνηση, βάσει των κανόνων που υλοποιεί, δεν προέρχεται από εξουσιοδοτημένη πηγή και την απορρίπτει. Στους κανόνες περιλαμβάνονται και συνθήκες που πρέπει να πληρούνται σχετικά με το πρωτόκολλο επικοινωνίας και τις δικτυακές θύρες μέσω των οποίων γίνεται η επικοινωνία. Στην περίπτωση, όμως, που η δικτυακή κίνηση προέλθει από παραβιασμένα συστήματα που έχουν το δικαίωμα να επικοινωνούν με το σταθμό SCADA, το firewall θα επιτρέψει την συγκεκριμένη επικοινωνία. Αυτό το κενό ασφάλειας έρχονται να καλύψουν οι μηχανισμοί IDS/IPS.

Οι μηχανισμοί IDS ελέγχουν την κίνηση και χρησιμοποιούν ευριστικές μεθόδους αναγνώρισης ιχνών επίθεσης εναντίον σταθμών SCADA. Κάθε επίθεση εναντίον του σταθμού SCADA αφήνει το αποτύπωμά της στις μετρήσεις της κίνησης του δικτύου από το οποίο προήλθε, είτε αυτό είναι αύξηση του όγκου πληροφοριών είτε εμφάνιση πακέτων ασυνήθιστων πρωτοκόλλων. Εφόσον ο μηχανισμός IDS αναγνωρίσει κάποιο πρότυπο στην κίνηση που αντιστοιχεί σε επίθεση εναντίον του συστήματος SCADA, ενεργοποιείται ο μηχανισμός IPS. Ο μηχανισμός IPS θέτει αυτόματα σε λειτουργία εξειδικευμένες μεθόδους αποτροπής της επίθεσης που έχει αναγνωριστεί από το IDS. Έτσι, οι πρώτοι μηχανισμοί αποτροπής ενδεχόμενης παραβίασης τίθενται σε εφαρμογή αυτόματα από το IPS. Όταν οι μηχανισμοί αυτοί δεν αποδειχθούν επαρκείς ή η επίθεση κριθεί σημαντική, το IPS αναλαμβάνει την ενημέρωση του υπεύθυνου ασφάλειας.

Η περίπτωση των σταθμών SCADA και των διατάξεων του βιομηχανικού πληροφοριακού δικτύου διαθέτει ένα χαρακτηριστικό που αυξάνει σημαντικά την αποτελεσματικότητα των μηχανισμών firewall και IDS/IPS. Η δικτυακή κίνηση που δημιουργούν οι σταθμοί SCADA όταν βρίσκονται σε κανονική λειτουργία έχει μικρή διακύμανση. Δηλαδή, το προφίλ της δικτυακής κίνησης που δημιουργεί ένας σταθμός SCADA στο δίκτυο παραμένει σταθερό όταν αυτός βρίσκεται σε συνθήκες κανονικής λειτουργίας. Απόρροια αυτού είναι ότι μέθοδοι αναγνώρισης ανωμαλιών που χρησιμοποιούνται από τους ανωτέρω μηχανισμούς ασφάλειας εμφανίζουν υψηλά ποσοστά επιτυχίας στην αναγνώριση απειλών και πολύ μικρά ποσοστά άκυρων συναγερμών (false alarms).

2. Έλεγχος εκτέλεσης εφαρμογών (Application Control)

Το προφίλ δικτυακής κίνησης ενός εποπτικού σταθμού SCADA υπό συνθήκες κανονικές λειτουργίες παρουσιάζει μικρή διακύμανση. Ομοίως, μικρή διακύμανση παρουσιάζει και το προφίλ εκτέλεσης εφαρμογών κατά τη λειτουργία του εποπτικού σταθμού. Δηλαδή, για να λειτουργήσει ένας εποπτικός

σταθμός SCADA χρησιμοποιεί ορισμένες εφαρμογές που εκτελούνται συνήθως καθ' όλη τη διάρκεια της λειτουργίας του. Είναι πολύ σπάνιο να εκτελεστεί κάποια διαφορετική εφαρμογή στο σύστημα κατά την κανονική του λειτουργία. Ενδεικτικά, οι εφαρμογές που συνήθως χρησιμοποιούνται είναι το λογισμικό ελέγχου της εταιρίας κατασκευής των συστημάτων SCADA και των PLC που βρίσκονται υπό τον έλεγχό τους, τα λογισμικά εφαρμογής πρωτοκόλλων και ορισμένες εφαρμογές του λειτουργικού συστήματος.

Αντίστοιχα με την περίπτωση του firewall όπου επιτρεπόταν η δικτυακή κίνηση μόνο από συγκεκριμένους κόμβους του δικτύου προς τον εκάστοτε σταθμό SCADA, στην περίπτωση του ελέγχου εκτέλεσης εφαρμογών, καταρτίζεται από τους υπεύθυνους ασφάλειας ένας κατάλογος με τις εφαρμογές που είναι αναγκαίες για τη σωστή λειτουργία του εποπτικού σταθμού SCADA. Στη συνέχεια, καταρτίζονται κανόνες για κάθε εφαρμογή ως προς το αν η εκτέλεσή της πρέπει να επιτρέπεται, να απορρίπτεται ή να ερωτάται ο χρήστης του συστήματος HMI πριν κάθε εκτέλεση. Ακόμη, κάθε ενέργεια του εργαλείου ελέγχου εκτέλεσης εφαρμογών καταγράφεται σε αρχεία καταγραφής για την περίπτωση όπου χρειαστεί να γίνει περαιτέρω μελέτη σχετικά με τη λειτουργία του.

Τα σύγχρονα εργαλεία ελέγχου εκτέλεσης εφαρμογών διαθέτουν ορισμένες πρόσθετες δυνατότητες συγκριτικά με τις ανωτέρω που αναβαθμίζουν την ποιότητα ασφάλειας που προσφέρουν. Ενδεικτικά, δίδεται η δυνατότητα στον υπεύθυνο ασφάλειας να ορίσει κανόνες για συγκεκριμένες λειτουργίες κάποιας εφαρμογής. Δηλαδή, μπορεί να επιτρέπεται μια λειτουργία Α, και να απορρίπτεται μια λειτουργία Β, από την ίδια εφαρμογή. Ακόμη, ο υπεύθυνος ασφάλειας έχει τη δυνατότητα να ορίσει χειροκίνητα δικές του λειτουργίες και να ορίσει για αυτές κανόνες στο σύστημα ελέγχου εκτέλεσης εφαρμογών. Έτσι, γίνεται περισσότερο λεπτομερής, ευέλικτος και αποτελεσματικός ο έλεγχος και η επιβολή των κανόνων εκτέλεσης για κάθε εφαρμογή.

Το εργαλείο ελέγχου εκτέλεσης εφαρμογών συμβάλλει στην άμυνα του συστήματος σε περίπτωση αρχικής παραβίασης του συστήματος. Μόλις ένας επίδοξος εισβολέας είναι σε θέση να επικοινωνήσει με τον εποπτικό σταθμό SCADA μέσω του δικτύου και παρακάμψει τους μηχανισμούς firewall και IDS/IPS, θα επιχειρήσει να εκμεταλλευτεί κάποια ευπάθειά του για να τον παραβιάσει. Αυτό γίνεται μέσω εκτέλεσης κακόβουλου κώδικα του επίδοξου εισβολέα στο σύστημα SCADA. Στις περιπτώσεις όπου αυτός ο κώδικας εκτελείται μέσω του συνδεδεμένου χρήστη, με εφαρμογή σωστών κανόνων στο εργαλείο ελέγχου εκτέλεσης εφαρμογών είναι δυνατόν να αποτραπεί η εκτέλεσή του εφόσον δεν συνάδει με την κανονική λειτουργία του εποπτικού σταθμού SCADA.

Όμως, ακόμη και σε περίπτωση αρχικής παραβίασης, ενόσω ο εισβολέας δεν διαθέτει δικαιώματα διαχειριστή είναι πιθανό ο κακόβουλος κώδικας που θα επιχειρήσει να εκτελέσει στο σταθμό SCADA για να προκαλέσει δολιοφθορά στις διατάξεις που ελέγχει, να αποτραπεί από το εργαλείο ελέγχου εκτέλεσης εφαρμογών. Κατ' αυτό τον τρόπο, ακόμη και αν γίνει μια αρχική παραβίαση του εποπτικού σταθμού SCADA, ο μηχανισμός ελέγχου εκτέλεσης εφαρμογών μπορεί να προσφέρει ασφάλεια στο σύστημα, ώστε ο επίδοξος εισβολέας να μην είναι σε θέση να προξενήσει ζημιά στο σύστημα μέχρι να ενημερωθεί ο υπεύθυνος ασφάλειας του βιομηχανικού πληροφοριακού δικτύου.

5.5.2. Μέθοδοι ασφάλειας έναντι μη εξουσιοδοτημένης εισόδου στο βιομηχανικό πληροφοριακό δίκτυο

Πολλές από τις επιθέσεις εναντίον διατάξεων του βιομηχανικού πληροφοριακού δικτύου που αναφέρθηκαν στο προηγούμενο εδάφιο προϋποθέτουν την είσοδο του επίδοξου εισβολέα στο βιομηχανικό πληροφοριακό δίκτυο. Από εκεί ο επίδοξος εισβολέας μπορεί (i) να υποκλέψει δεδομένα του δικτύου (ii) να μιμηθεί κάποια διάταξη του δικτύου και να παράγει πλαστά δεδομένα (iii) να επιχειρήσει μια επίθεση DoS προσβάλλοντας τη διαθεσιμότητα του δικτύου. Οι μέθοδοι άμυνας εναντίον τέτοιων επιθέσεων χωρίζονται σε δύο κατηγορίες. Η πρώτη κατηγορία περιλαμβάνει όλες τις μεθόδους που έχουν σκοπό να εμποδίσουν κάποιο επίδοξο εισβολέα να αποκτήσει πρόσβαση στο βιομηχανικό πληροφοριακό δίκτυο. Η δεύτερη κατηγορία περιλαμβάνει τις μεθόδους που αποσκοπούν στην ασφάλεια των διατάξεων και των δεδομένων που μεταδίδουν επιθέσεις που πηγάζουν από το εσωτερικό του βιομηχανικού πληροφοριακού δικτύου. Ένας ολοκληρωμένος σχεδιασμός ασφάλειας πρέπει να περιλαμβάνει μηχανισμούς ασφάλειας και των δύο κατηγοριών ώστε να υπάρχει η απαραίτητη αλληλοκάλυψη μεταξύ των μηχανισμών.

1. Χρήση Power Line Communications (PLC)

Καίτοι δεν είναι μηχανισμός ασφάλειας, η επιλογή φυσικού μέσου επικοινωνίας των διατάξεων και του πρωτοκόλλου επικοινωνίας επί αυτού μπορούν να βελτιώσουν σημαντικά την ασφάλεια του βιομηχανικού πληροφοριακού δικτύου. Αντίστοιχα με το φυσικό μέσο το οποίο χρησιμοποιείται για τις επικοινωνίες των διατάξεων εντός του βιομηχανικού πληροφοριακού δικτύου γίνεται εύκολο ή δύσκολο για τον επίδοξο εισβολέα να εισέλθει στο δίκτυο. Η ιδιότητα του φυσικού μέσου η οποία επηρεάζει εμμέσως την ασφάλεια είναι το πόσο περιορισμένο (self-contained) είναι. Για παράδειγμα, αν η επικοινωνία είναι ασύρματη είναι δύσκολος ο περιορισμός της εμβέλειας μόνο στις περιοχές που περιλαμβάνουν διατάξεις. Έτσι, ένας επίδοξος εισβολέας που βρίσκεται σε κοντινή απόσταση είναι σε θέση να διαβάσει τα δεδομένα του ασύρματου δικτύου. Αντιθέτως, στην περίπτωση όπου χρησιμοποιείται ενσύρματο μέσο, ο επίδοξος εισβολέας πρέπει να έρθει σε φυσική επαφή με αυτό ώστε να μπορέσει υπό προϋποθέσεις να αποκτήσει πρόσβαση σε κάποια από τα δεδομένα του δικτύου. Με κριτήριο την ασφάλεια, επομένως, ένα ενσύρματο μέσο επικοινωνίας μεταξύ των διατάξεων είναι προτιμότερο.

Από τους ενσύρματους τρόπους επικοινωνίας αυτός που ταιριάζει στην περίπτωση του βιομηχανικού πληροφοριακού δικτύου είναι τα Power Line Communications. Ο βασικός λόγος είναι ότι το βιομηχανικό πληροφοριακό δίκτυο περιορίζεται μόνο στο δίκτυο ΗΕ. Έτσι, γίνεται πολύ δύσκολο για κάποιο επίδοξο εισβολέα να αποκτήσει φυσική πρόσβαση στις γραμμές του δικτύου μέσω των οποίων γίνεται η μεταφορά δεδομένων. Ακόμη, όμως, και αν αποκτήσει φυσική επαφή η σύνδεση δεν είναι εύκολη καθώς απαιτούνται ειδικοί υποδοχείς για τη σύνδεση στη γραμμή μεταφοράς δεδομένων. Είναι φανερό, λοιπόν, πως με την επιλογή μιας τεχνολογίας PLC για τις επικοινωνίες του βιομηχανικού πληροφοριακού δικτύου αυξάνεται σημαντικά η ασφάλεια της περιμέτρου του βιομηχανικού πληροφοριακού δικτύου χωρίς να χρησιμοποιηθεί κάποιος μηχανισμός ασφάλειας. Ωστόσο, και στην περίπτωση αυτή, είναι αναγκαία η χρήση των μηχανισμών ασφάλειας και τεχνικών σχεδίασης που ακολουθούν ώστε η ασφάλεια του δικτύου να είναι ολοκληρωμένη.

2. Κατάτμηση του βιομηχανικού πληροφοριακού δικτύου

Στην περίπτωση των εταιρικών πληροφοριακών δικτύων που εξετάστηκαν στο προηγούμενο κεφάλαιο, κρίθηκε αναγκαίος ο χωρισμός των συστημάτων σε λειτουργικές ομάδες και υποδίκτυα. Ο λόγος ήταν η μείωση της επιφάνειας επίθεσης εναντίον κάθε συστήματος και ο περιορισμός της εξάπλωσης μιας πιθανής παραβίασης.

Η ίδια ακριβώς λογική μπορεί να εφαρμοστεί και στην περίπτωση του βιομηχανικού πληροφοριακού δικτύου. Ειδικότερα, στην περίπτωση του βιομηχανικού πληροφοριακού δικτύου αναμένεται να είναι ακόμη αποδοτικότερη καθώς οι λειτουργίες του είναι διακριτές και τα όρια ανάμεσα στις λειτουργικές ομάδες περισσότερο ευδιάκριτα. Κάθε λειτουργική ομάδα στο βιομηχανικό πληροφοριακό δίκτυο περιλαμβάνει τον εποπτικό σταθμό SCADA και τις συσκευές PLC που αυτός ελέγχει. Εντός κάθε λειτουργικής ομάδας, κάθε διάταξη PLC πρέπει να είναι κατάλληλα ρυθμισμένη ώστε να επιτρέπεται η επικοινωνία μόνο από και προς τον εποπτικό σταθμό SCADA.

Στο επίπεδο των εποπτικών σταθμών SCADA, ο έλεγχος που πραγματοποιείται απαιτεί, πολύ συχνά, δεδομένα από τη λειτουργία διατάξεων που βρίσκονται υπό τον έλεγχο άλλων εποπτικών σταθμών. Για το λόγο αυτό, είναι απαραίτητη η επικοινωνία μεταξύ εποπτικών σταθμών SCADA. Τέτοιες εξαρτήσεις μεταξύ των δεδομένων που χειρίζονται οι σταθμοί SCADA είναι γνωστές από τη φάση του σχεδιασμού της τοπολογίας του βιομηχανικού πληροφοριακού δικτύου. Έτσι, δημιουργούνται ευρύτερες λειτουργικές ομάδες που μπορούν να περιλαμβάνουν τις λειτουργικές ομάδες διαφορετικών εποπτικών σταθμών. Στις περιπτώσεις αυτές, πρέπει να επιτρέπεται η επικοινωνία μόνο μεταξύ των εποπτικών σταθμών και όχι των υπόλοιπων διατάξεων. Για παράδειγμα, μία διάταξη PLC μιας ομάδας δεν επιτρέπεται να επικοινωνήσει με τον εποπτικό σταθμό μιας άλλης.

Τα προαναφερθέντα υλοποιούνται με τη χρήση μηχανισμών άμυνας εξειδικευμένων για βιομηχανικά πληροφοριακά δίκτυα. Αρχικά, στις συνδέσεις μεταξύ εποπτικών σταθμών SCADA τοποθετούνται μηχανισμοί firewall. Κάθε σύνδεση με αφετηρία ή προορισμό μία διάταξη PLC εκτός των ορίων της λειτουργικής ομάδας του εποπτικού σταθμού SCADA πρέπει να αποκόπτεται καθώς μόνο οι συσκευές εντός της λειτουργικής του ομάδας ανήκουν στην δικαιοδοσία του.

Προηγουμένως, παρουσιάστηκαν μέθοδοι παραβίασης εποπτικών σταθμών SCADA μέσω του εταιρικού πληροφοριακού δικτύου του διαχειριστή του δικτύου ΗΕ. Στην περίπτωση όπου μια τέτοια επίθεση είναι επιτυχείς, αυτή μπορεί να εξαπλωθεί σε γειτονικούς εποπτικούς σταθμούς με χρήση των μεταξύ τους συνδέσεων. Για την αποτροπή τέτοιας γενικευμένης παραβίασης του βιομηχανικού πληροφοριακού δικτύου, είναι αναγκαία η εγκατάσταση μηχανισμών IDS/IPS εξειδικευμένων και για βιομηχανικά δικτυακά πρωτόκολλα. Με τον τρόπο αυτό, όταν ένας παραβιασμένος εποπτικός σταθμός αποστέλλει κακόβουλα δεδομένα προς γειτονικούς σταθμούς, το IDS θα αναγνωρίσει τα δεδομένα ως τμήμα μιας επίθεσης και θα απορρίψει τα πακέτα.

Στην περίπτωση παραβίασης ενός εποπτικού σταθμού, εκτός από τους γειτονικούς εποπτικούς σταθμούς, σε κίνδυνο βρίσκονται και όλες οι διατάξεις PLC της λειτουργικής του ομάδας. Σε μια τέτοια περίπτωση, είναι αναγκαία η χρήση ενός IDS βιομηχανικού πρωτοκόλλου για να ελέγχει τα δεδομένα που διακινούνται από όλες τις διατάξεις της λειτουργικής ομάδας και να ειδοποιεί σε περίπτωση πιθανής παραβίασης. Επιπλέον, είναι απαραίτητη η εγκατάσταση ενός IPS που θα ελέγχει τον εποπτικό σταθμό, ώστε σε περίπτωση παραβίασης να εφαρμοστούν αυτόματα κάποιες ορισμένες ελάχιστες ενέργειες άμυνας.

Επειδή, όμως, τα δεδομένα ελέγχου του εποπτικού σταθμού SCADA είναι απαραίτητα για τη σωστή λειτουργία των διατάξεων PLC εντός της λειτουργικής του ομάδας, δεν επιτρέπονται στο IPS περισσότερο

δραστικές ενέργειες όπως η άμεση αποκοπή του από το δίκτυο. Αντ' αυτού, είναι απαραίτητη η ύπαρξη κάποιων εφεδρικών εποπτικών σταθμών που να είναι σε θέση να εκτελέσουν τις βασικές λειτουργίες πολλών λειτουργικών ομάδων. Ακόμη, είναι αναγκαία η ύπαρξη τμήματος ασφάλειας του βιομηχανικού πληροφοριακού δικτύου που τίθεται σε επιφυλακή σε τέτοιες περιπτώσεις, ώστε να είναι εφικτές άμεσες ενέργειες άμυνας. Έτσι, εφόσον κριθεί αναγκαίο από τον υπεύθυνο ασφάλειας, μπορεί να αποκοπεί από το δίκτυο ο παραβιασμένος εποπτικός σταθμός και το ρόλο του να αναλάβει ο εφεδρικός μέχρι το πέρας του κινδύνου.

Όλες οι ανωτέρω μέθοδοι άμυνας αποτελούν τμήμα του γενικού σχεδιασμού άμυνας που ακολουθεί την κατάτμηση του βιομηχανικού πληροφοριακού δικτύου σε υποδίκτυα. Ο λόγος που προκρίνεται ένας τέτοιος σχεδιασμός του δικτύου είναι ακριβώς για να είναι δυνατή η υιοθέτηση των προαναφερθεισών μεθόδων άμυνας και η μεγιστοποίηση της απόδοσής τους. Συμπερασματικά, το βιομηχανικό πληροφοριακό δίκτυο χωρίζεται σε λειτουργικές υπό-ομάδες, εκάστη εκ των οποίων είναι επιφορτισμένη με συγκεκριμένη λειτουργία στο βιομηχανικό πληροφοριακό δίκτυο. Μηχανισμοί άμυνας λειτουργούν εντός κάθε λειτουργικής ομάδας ώστε να ανιχνεύουν πιθανώς παραβιασμένες διατάξεις, καθώς και στα όρια των λειτουργικών ομάδων ώστε να αποτρέπουν την εξάπλωση μιας πιθανής παραβίασης σε γειτονικές λειτουργικές ομάδες. Ακόμη μηχανισμοί άμυνας τοποθετούνται για τον έλεγχο της κίνησης και την αποφυγή πιθανής παραβίασης των εποπτικών σταθμών SCADA από γειτονικούς σταθμούς σε περίπτωση όπου κάποιος εξ αυτών πέσει θύμα επίθεσης. Με τον τρόπο αυτό, γίνεται σημαντικά δυσκολότερη η παραβίαση μιας διάταξης εντός του βιομηχανικού πληροφοριακού δικτύου, ενώ, ακόμα και στην περίπτωση όπου υπάρξει παραβίαση, η εξάπλωσή της σε γειτονικές διατάξεις περιορίζεται σε μεγάλο βαθμό.

3. *Χρήση βιομηχανικών πρωτοκόλλων με ενσωματωμένους μηχανισμούς ασφάλειας*

Τα βιομηχανικά πρωτόκολλα που έχουν σχεδιαστεί, μέχρι σήμερα, δεν είχαν προδιαγραφές ασφάλειας από κακόβουλες ενέργειες. Για το λόγο αυτό, και για να επιτυγχάνουν καλύτερες επιδόσεις σε κύριες προδιαγραφές τους όπως η ελαχιστοποίηση της καθυστέρησης, τα βιομηχανικά πρωτόκολλα δεν υιοθετούν μηχανισμούς ασφάλειας. Αυτό μεταφράζεται πρακτικά σε δεδομένα που μεταφέρονται στο δίκτυο χωρίς κρυπτογράφηση, και χωρίς επιβεβαίωση της ακεραιότητας των δεδομένων και σε διατάξεις που επικοινωνούν χωρίς να έχει πιστοποιηθεί η ταυτότητά τους.

Στο Smart Grid, αντίθετα, η ασφάλεια αποτελεί μία από τις σημαντικότερες προδιαγραφές. Συνεπώς, είναι απαραίτητη η χρήση βιομηχανικών πρωτοκόλλων που διαθέτουν μηχανισμούς ασφάλειας. Ως εκ τούτου, οι εταιρίες που σχεδιάζουν βιομηχανικά πρωτόκολλα έχουν σχεδιάσει εκδόσεις που διαθέτουν μηχανισμούς ασφάλειας. Συγκεκριμένα, ως προς το πρωτόκολλο DNP3, το οποίο χρησιμοποιείται σε μεγάλο βαθμό στα βιομηχανικά πληροφοριακά δίκτυα του τομέα της ηλεκτρικής ενέργειας, διατίθεται έκδοση που εγγυάται την πιστοποίηση της ταυτότητας των διατάξεων [56]. Ακόμη, περιλαμβάνει μηχανισμούς εγγύησης της ακεραιότητας των δεδομένων. Συνεπώς, με τη χρήση της ασφαλούς έκδοσης του πρωτοκόλλου DNP3, οι διατάξεις του δικτύου και τα δεδομένα τους προστατεύονται από ενεργητικές επιθέσεις, όπως η επανάληψη πακέτων, η κακόβουλη τροποποίηση πακέτων και η μίμηση διατάξεων.

Ωστόσο, για λόγους μείωσης της καθυστέρησης μεταφοράς των πακέτων και επεξεργασίας τους από τις διατάξεις, η συγκεκριμένη έκδοση του πρωτοκόλλου DNP3 δεν παρέχει μηχανισμούς έναντι παθητικών κακόβουλων ενεργειών, όπως είναι για παράδειγμα η υποκλοπή δεδομένων. Προκειμένου να μην αυξηθεί σε

μεγάλο βαθμό το υπολογιστικό κόστος της χρήσης του πρωτοκόλλου από τις διάφορες διατάξεις, αυτό δεν χρησιμοποιεί κρυπτογράφηση στα δεδομένα που διακινούνται. Έτσι, αν ένας επίδοξος εισβολέας έχει πρόσβαση στο βιομηχανικό πληροφοριακό δίκτυο, είναι σε θέση να υποκλέπτει τα δεδομένα που διακινούνται από τις διατάξεις PLC από και προς τους εποπτικούς σταθμούς SCADA.

Όταν τα δεδομένα που διακινούνται είναι εμπιστευτικά ή για οποιονδήποτε άλλο λόγο κρίνεται αναγκαία η προστασία από υποκλοπή τους, πρέπει να εγκαθίστανται εξωτερικές συσκευές που να αναλαμβάνουν την κρυπτογράφηση των δεδομένων κατά την μεταφορά τους στο βιομηχανικό πληροφοριακό δίκτυο. Όμως, μια απόφαση αυτού του είδους πρέπει να ληφθεί μετά από ενδελεχή ανάλυση των επιπτώσεων που θα έχουν οι συσκευές αυτές στις επιδόσεις του δικτύου και κατά πόσο θα επηρεάσουν τη λειτουργία των βιομηχανικών διατάξεων. Ακόμη, απαιτείται ανάλυση κινδύνου ώστε να εξακριβωθεί αν ο κίνδυνος χρήσης επικοινωνιών χωρίς κρυπτογράφηση συγκριτικά με τις πιθανές επιπτώσεις χρήσης συσκευών κρυπτογράφησης στις προδιαγραφές λειτουργίας των διατάξεων του δικτύου και το κόστος εγκατάστασής τους δικαιολογεί μία επένδυση σε τέτοιες συσκευές.

Συμπερασματικά, η μέγιστη ασφάλεια απέναντι σε επιθέσεις υποκλοπής πληροφοριών και παραβίασης διατάξεων του βιομηχανικού πληροφοριακού δικτύου επιτυγχάνεται με συνδυασμό των προαναφερθεισών μεθόδων. Συγκεκριμένα, απαιτείται ορθός σχεδιασμός της αρχιτεκτονικής του δικτύου με κατάτμησή του σε διακριτές λειτουργικές ομάδες. Στη συνέχεια, οι ομάδες αυτές πρέπει να προστατεύονται από μηχανισμούς IDS/IPS εγκατεστημένους ταυτόχρονα στο εσωτερικό τους και στις συνδέσεις των εποπτικών σταθμών κάθε ομάδας με εποπτικούς σταθμούς άλλων ομάδων. Ακόμη, στο Smart Grid, είναι απαραίτητη η υιοθέτηση ενός βιομηχανικού πρωτοκόλλου με αυστηρές προδιαγραφές ασφάλειας, ενώ, επίσης συνιστάται η χρήση ενός φυσικού μέσου μετάδοσης των πληροφοριών, όπως η τεχνολογία Power Line Communications, που να περιορίζει σημαντικά την πρόσβαση στο βιομηχανικό πληροφοριακό δίκτυο.

5.5.3. Ασφάλεια έναντι επιθέσεων απώλειας διαθεσιμότητας (Denial of Service)

Στο εδάφιο 5.4.Β, έγινε αναφορά σε μεθόδους με τις οποίες μπορεί να προκληθεί απώλεια διαθεσιμότητας σε διατάξεις του βιομηχανικού πληροφοριακού δικτύου. Η πρώτη μέθοδος κάνει χρήση ορισμένων λειτουργιών που παρέχονται από το βιομηχανικό πρωτόκολλο DNP3 ώστε να προκαλέσει απώλεια διαθεσιμότητας. Η δεύτερη μέθοδος ήταν η εκμετάλλευση ευπαθειών του πρωτοκόλλου DNP3 κατά την επεξεργασία ορισμένων πακέτων, ώστε με ειδικά διαμορφωμένα πακέτα να τίθεται εκτός λειτουργίας ο εποπτικός σταθμός SCADA.

Και οι δύο μέθοδοι επίθεσης αντιμετωπίζονται με τη χρήση μηχανισμών IDS για βιομηχανικά πρωτοκόλλα. Σε ό,τι αφορά την πρώτη περίπτωση, το IDS πρέπει να παρακολουθεί την κίνηση εντός μιας λειτουργικής ομάδας και να αναγνωρίζει την αλληλουχία των αποδεκτών πακέτων του DNP3 που προκαλούν την απώλεια διαθεσιμότητας. Όταν, εμφανιστεί μια τέτοια αλληλουχία, πρέπει να απορρίπτεται και να ενημερώνεται ο υπεύθυνος ασφάλειας του βιομηχανικού πληροφοριακού δικτύου.

Η ίδια αντιμετώπιση αρμόζει και στα πακέτα που περιέχουν ειδικό περιεχόμενο που προκαλεί ατέρμονο βρόχο στον εποπτικό σταθμό. Ωστόσο, στη συγκεκριμένη περίπτωση ο έλεγχος πρέπει να γίνεται και στις συνδέσεις με άλλους σταθμούς SCADA αλλά και στις συνδέσεις με το εταιρικό πληροφοριακό δίκτυο του διαχειριστή του δικτύου ΗΕ. Στις συνδέσεις μεταξύ εποπτικών σταθμών SCADA απαιτούνται εξειδικευμένες

μέθοδοι ανίχνευσης κακόβουλων πακέτων και ενεργειών ώστε να αναγνωρίζονται από το IDS κακόβουλες ενέργειες που υποκρύπτονται εντός της φυσιολογικής δικτυακής κίνησης. Επειδή τα πακέτα αυτά εμφανίζονται σπάνια υπό κανονικές συνθήκες λειτουργίας, η ανίχνευσή τους είναι εύκολη. Αντίθετα, στις συνδέσεις του εποπτικού σταθμού με το εταιρικό πληροφοριακό δίκτυο απαιτείται μόνο ένα φίλτρο που απορρίπτει όλα τα πακέτα βιομηχανικών δικτυακών πρωτοκόλλων και ταυτόχρονα να ενημερώνει σχετικά τον υπεύθυνο ασφάλειας. Ο λόγος για αυτό είναι ότι δεν υπάρχει περίπτωση πακέτα του βιομηχανικού πληροφοριακού δικτύου να αποσταλούν προς το εταιρικό πληροφοριακό δίκτυο, όπως, επίσης, δεν υπάρχει περίπτωση τέτοια δεδομένα να πηγάζουν από το εταιρικό πληροφοριακό δίκτυο. Αν συμβεί κάτι τέτοιο θα πρόκειται είτε για κακόβουλη ενέργεια είτε για πολύ σοβαρό σφάλμα, οπότε και στις δύο περιπτώσεις είναι απαραίτητη η ενημέρωση του υπεύθυνου ασφάλειας του βιομηχανικού πληροφοριακού δικτύου.

5.5.4. Μέθοδοι ασφάλειας εναντίον επιθέσεων στο μηχανισμό χρονικού συγχρονισμού

Ένας από τους μεγαλύτερους κινδύνους για το Smart Grid πηγάζει από το μηχανισμό χρονικού συγχρονισμού των Phasor Measurement Units (PMU) μέσω GPS. Ο κίνδυνος οφείλεται στο ότι τα δεδομένα της επικοινωνίας μεταξύ δέκτη και δορυφόρου στο πρωτόκολλο GPS μεταφέρονται χωρίς πιστοποίηση των συσκευών. Σε προηγούμενο εδάφιο αναλύθηκε ο τρόπος επίθεσης μέσω του οποίου ο δέκτης του PMU λαμβάνει λανθασμένες τιμές χρονικού συγχρονισμού και ως συνέπεια εμφανίζει λανθασμένες τιμές φάσης και συχνότητας.

Μία εύκολη λύση για την προαναφερθείσα απειλή είναι η χρήση των λειτουργιών πιστοποίησης συσκευών που προσφέρονται από το πρωτόκολλο του GPS. Ωστόσο, αυτές οι λειτουργίες είναι δεσμευμένες μόνο για στρατιωτικές εφαρμογές. Συνεπώς, πρέπει να αναζητηθούν άλλες λύσεις για την προστασία από επιθέσεις όπως η ανωτέρω.

Μία πιθανή λύση είναι ο υπολογισμός ορισμένων στατιστικών μεγεθών του σήματος που λαμβάνεται από τους δορυφόρους, ώστε να εξακριβωθεί αν το σήμα όντως λαμβάνεται από αυτούς και όχι από κακόβουλους πομπούς που τους μιμούνται. Ενδεικτικό παράδειγμα είναι η μέση τιμή της έντασης του σήματος του δορυφόρου το οποίο υπό κανονικές συνθήκες είναι πολύ ασθενές λόγω της απόστασης των δορυφόρων. Αν χρησιμοποιείται πομπός που μιμείται το δορυφόρο, λόγω της εγγύτητας η τιμή του σήματος ενδέχεται να είναι κατά τάξεις μεγέθους υψηλότερη, αποτελώντας ένδειξη επίθεσης [57]. Επιπλέον, μπορεί να χρησιμοποιηθεί η στιγμιαία τιμή του σήματος από κάθε δορυφόρο ώστε αν παρατηρηθούν σημαντικές και αδικαιολόγητες μεταβολές να σηματοδοτείται ως κακόβουλη επίθεση.

Ωστόσο, η ανωτέρω μέθοδος εμφανίζει τρία σημαντικά μειονεκτήματα. Πρώτον, βασίζεται σε κακή υλοποίηση των συσκευών μίμησης του σήματος GPS αφού μελλοντικά οι συσκευές μίμησης αναμένεται να βελτιωθούν τόσο ώστε το σήμα να μην ξεχωρίζει από το αυθεντικό σήμα των δορυφόρων. Δεύτερον, η υλοποίηση της ανωτέρω μεθόδου απαιτεί την εγκατάσταση του μηχανισμού ανίχνευσης κακόβουλων επιθέσεων στις διατάξεις PMU κατά την κατασκευή τους. Έτσι, οι ήδη εγκατεστημένες διατάξεις στα δίκτυα ΗΕ δε μπορούν να προστατευθούν. Τρίτον, η ανωτέρω μέθοδος δεν προσφέρει καμία προστασία από επιθέσεις DoS, όπου ο επιτιθέμενος χρησιμοποιεί μια συσκευή παρεμπόδισης του σήματος ώστε να εισάγει θόρυβο στη ζώνη συχνοτήτων του GPS με συνέπεια το PMU να μην μπορεί να συγχρονιστεί.

Ένας ασφαλής τρόπος χρονικού συγχρονισμού των PMUs μπορεί να βασιστεί στο πρωτόκολλο PTP (IEEE 1855) που υποστηρίζει ακριβή χρονικό συγχρονισμό σε ενσύρματα δίκτυα. Με τη χρήση ενός τέτοιου πρωτοκόλλου η ασφάλεια έναντι επιθέσεων κατά του συγχρονισμού των PMUs βασίζεται στους μηχανισμούς ασφάλειας έναντι παρόμοιων επιθέσεων που αναλύθηκαν προηγουμένως. Αν ο συγχρονισμός πραγματοποιείται ενσύρματα, ο επιτιθέμενος δεν έχει πρόσβαση ώστε να αλλοιώσει τα πακέτα συγχρονισμού. Αν προσπαθήσει να εισβάλει στο δίκτυο, οι μηχανισμοί που αναλύθηκαν προηγουμένως θα τον αποτρέψουν. Ομοίως, ο επιτιθέμενος δεν είναι σε θέση να πλήξει τη διαθεσιμότητα της υπηρεσίας χρονικού συγχρονισμού εφόσον δεν βρίσκεται εντός του βιομηχανικού πληροφοριακού δικτύου.

Το μόνο ζήτημα που περιόριζε τη χρήση του συγκεκριμένου πρωτοκόλλου ήταν η χρονική ακρίβεια που προσφέρει. Το πρωτόκολλο GPS μπορεί να προσφέρει ακρίβεια μικρότερη του 1μs. Η πρώτη υλοποίηση του PTP δεν ήταν σε θέση να παρέχει τέτοια ακρίβεια και συνεπώς δεν μπορούσε να χρησιμοποιηθεί σε PMUs. Ωστόσο, η δεύτερη έκδοση του πρωτοκόλλου (IEEE 1588-2008) παρέχει χρονική ακρίβεια που υποστηρίζει τη λειτουργία των PMUs [58]. Για να υποστηριχτεί μια τόσο υψηλή ακρίβεια είναι απαραίτητη η εγκατάσταση δικτυακού υλικού με προδιαγραφές για πολύ μικρή καθυστέρηση. Επιπλέον, ο διαχειριστής του δικτύου ΗΕ πρέπει να έχει άμεση δικτυακή πρόσβαση σε έναν από τους εξυπηρετητές που αποτελούν πηγή των χρονικών δεδομένων. Συνήθως, τέτοιοι εξυπηρετητές διατίθενται από κυβερνητικούς ή στρατιωτικούς φορείς.

Συμπερασματικά, το πρωτόκολλο PTP μπορεί να διατηρήσει την υψηλή ακρίβεια του πρωτοκόλλου GPS, εξαλείφοντας, παράλληλα, τους πρόσθετους κινδύνους που αυτό εισάγει για το Smart Grid. Συνεπώς, κατά το σχεδιασμό νέων Ευφυών Δικτύων, ο χρονικός συγχρονισμός των διατάξεων PMU πρέπει να βασίζεται στο πρωτόκολλο PTP. Στις περιπτώσεις όπου υπάρχουν ήδη εγκατεστημένα PMUs που χρησιμοποιούν το πρωτόκολλο GPS, είναι αναγκαίος ο έλεγχος των τιμών χρονικού συγχρονισμού και η σύγκρισή τους με αυτές που προέρχονται από το PTP ώστε όταν παρατηρηθούν αποκλίσεις να ανιχνεύεται κακόβουλη επίθεση και να λαμβάνονται κατάλληλα μέτρα.

5.5.5. Μέθοδοι αντιμετώπισης κακόβουλου hardware

Για λόγους που έχουν ήδη αναφερθεί, η συγκεκριμένη μέθοδος επίθεσης αποτελεί μία από τις σημαντικότερες απειλές εναντίον του Ευφυούς Δικτύου. Στους λόγους που προαναφέρθηκαν έρχεται να προστεθεί και η εγγενής δυσκολία στην ανίχνευση κακόβουλου hardware. Αυτό εντείνεται από το ότι πολλά από τα ολοκληρωμένα κυκλώματα που χρησιμοποιούνται σε διατάξεις του βιομηχανικού πληροφοριακού δικτύου αποτελούν πνευματική ιδιοκτησία άλλων εταιριών, με αποτέλεσμα να αντιμετωπίζονται ως μαύρα κουτιά. Αν και έχουν προταθεί μέθοδοι ανίχνευσης κακόβουλου hardware, εντούτοις καμία από αυτές δεν εμφανίζει επαρκή ποσοστά επιτυχούς ανίχνευσης.

Προκειμένου να απλοποιηθεί η ανάλυση που ακολουθεί απαιτείται ο διαχωρισμός των φάσεων κατασκευής και χρήσης ενός ολοκληρωμένου κυκλώματος. Το πρώτο στάδιο είναι η περιγραφή των λειτουργιών που πρέπει αυτό να πραγματοποιεί. Στη συνέχεια, ακολουθεί ο σχεδιασμός του ολοκληρωμένου κυκλώματος όπου επιλέγονται η τοπολογία και των είδος των εξαρτημάτων που θα υλοποιήσουν τις επιμέρους λειτουργίες του ολοκληρωμένου κυκλώματος. Ακολουθεί η κατασκευή του ολοκληρωμένου κυκλώματος και ο έλεγχος της ορθής λειτουργίας του. Τέλος, ακολουθεί η λειτουργία του υπό πραγματικές συνθήκες.

Το κακόβουλο υλικό μπορεί να εισαχθεί είτε κατά τη φάση του σχεδιασμού του ολοκληρωμένου κυκλώματος είτε κατά τη φάση κατασκευής του. Οι δύο φάσεις αυτές είναι πολύ διαφορετικές μεταξύ τους, με αποτέλεσμα οι μέθοδοι ανίχνευσης για κάθε φάση να διαφέρουν σημαντικά. Ενδεικτικά, στη φάση

σχεδιασμού το ολοκληρωμένο κύκλωμα βρίσκεται σε μορφή ψηφιακών αρχείων σχεδίασης. Σε αυτή την περίπτωση, το κακόβουλο hardware βρίσκεται κρυμμένο μέσα στην πληθώρα εξαρτημάτων που βρίσκονται εντός του συνολικού ψηφιακού σχεδίου. Στην περίπτωση της φάσης κατασκευής, το κακόβουλο hardware έχει ήδη τυπωθεί στο ολοκληρωμένο κύκλωμα. Επιπλέον, είναι πιθανό, η εισαγωγή να πραγματοποιηθεί στο στάδιο της κατασκευής, δηλαδή να μην υπάρχει στα ψηφιακά σχέδια του ολοκληρωμένου κυκλώματος αλλά να εισαχθεί κατά την κατασκευή του.

Αντίστοιχα με τη φάση στην οποία εισάγεται το κακόβουλο hardware, διαφοροποιούνται και οι μέθοδοι ανίχνευσής του. Στην περίπτωση όπου αυτό εισαχθεί κατά τη φάση του σχεδιασμού στα ψηφιακά αρχεία σχεδίασης, έχει προταθεί μία μέθοδος προσομοίωσης με σκοπό την εύρεση τμημάτων που ενδέχεται να ανήκουν σε κακόβουλο υλικό. Η συγκεκριμένη μέθοδος πραγματοποιεί μια διαδικασία τεσσάρων βημάτων, μέσω της οποίας σταδιακά απορρίπτει λογικές πύλες και σήματα του ολοκληρωμένου κυκλώματος από το ενδεχόμενο να ανήκουν σε κακόβουλο hardware. Συνεπώς, στο τέλος της διαδικασίας καταδεικνύονται οι λογικές πύλες που με μεγάλη πιθανότητα ανήκουν σε κάποιο κακόβουλο hardware [59].

Κατά τη φάση εκτύπωσης του ολοκληρωμένου κυκλώματος πραγματοποιούνται έλεγχοι προκειμένου να διασφαλιστεί η ποιότητά του. Στο πλαίσιο των ελέγχων αυτών πραγματοποιούνται και έλεγχοι για την ύπαρξη κακόβουλου hardware. Μία μέθοδος που έχει προταθεί βασίζεται στην ανάλυση της λογικής του ολοκληρωμένου κυκλώματος. Υποθέτει ότι η συνθήκη ενεργοποίησης του κακόβουλου hardware ικανοποιείται σπάνια, αλλιώς το κακόβουλο λογισμικό θα ήταν πολύ συχνά ενεργοποιημένο και, επομένως, ευκολότερο να ανιχνευθεί. Βάσει αυτού, η μέθοδος βασίζεται στην επανειλημμένη ενεργοποίηση κόμβων που ενεργοποιούνται πολύ σπάνια κατά την κανονική λειτουργία του ολοκληρωμένου κυκλώματος, προκειμένου να ανακαλύψει ενδεχόμενο κακόβουλο hardware [60]. Άλλες μέθοδοι ανίχνευσης βασίζονται στην παρατήρηση της ισχύος και του ρεύματος εισόδου του ολοκληρωμένου κυκλώματος και τμημάτων του [61] [62]. Άλλες κάνουν χρήση της τάσης εισόδου του ολοκληρωμένου κυκλώματος [63] ή της διαφοράς στην καθυστέρηση του σήματος που προκύπτει από το πρόσθετο κύκλωμα του κακόβουλου λογισμικού [64].

Προκειμένου να μεγιστοποιηθεί η ασφάλεια εναντίον κακόβουλου hardware, είναι αναγκαία η εφαρμογή συνδυασμού των μεθόδων που αναλύθηκαν προηγουμένως από τους κατασκευαστές των διατάξεων του βιομηχανικού πληροφοριακού δικτύου. Αυτό είναι απαραίτητο διότι δεν υπάρχει κάποια μέθοδος που να εξασφαλίζει αρκετά μεγάλα ποσοστά ανίχνευσης ώστε να μπορεί η ασφάλεια διατάξεων να βασιστεί εξ ολοκλήρου σε αυτή. Επιπλέον, είναι πολύ σημαντικό να γίνει λεπτομερής μελέτη των πρώτων βημάτων που πρέπει να ακολουθηθούν εφόσον γίνει επίθεση DoS από κακόβουλο hardware. Η μελέτη αυτή είναι σημαντική διότι (i) οι ενέργειες μετά από μια τέτοια επίθεση δεν είναι σταθερές αλλά εξαρτώνται από την παραβιασμένη διάταξη, και (ii), επειδή η επίθεση προέρχεται από hardware δεν είναι άμεση και σαφής η αντιμετώπισή της.

5.6. Συμπεράσματα

Το βιομηχανικό δίκτυο είναι ο πυρήνας του Smart Grid, καθώς περιλαμβάνει όλες οι διατάξεις που είναι υπεύθυνες για την παραγωγή, μεταφορά και διανομή ΗΕ. Επειδή μεγάλο μέρος των υπηρεσιών που προσφέρει το Smart Grid βασίζονται στις προαναφερθείσες διατάξεις, αυτές αποτελούν το κύριο στόχο των πλέον στοχευμένων και επικίνδυνων επιθέσεων εναντίον του Smart Grid. Τέτοιες επιθέσεις γίνονται σχεδόν πάντα με σκοπό είτε τη δολιοφθορά διατάξεων του βιομηχανικού δικτύου είτε την υποκλοπή δεδομένων λειτουργίας τους. Αντίστοιχα, τα κίνητρα των επιθέσεων εναντίον του βιομηχανικού δικτύου του Smart Grid

είναι πρωτίστως στρατιωτικά. Ο λόγος είναι η υψηλή πολυπλοκότητα και το μεγάλο οικονομικό κόστος των της πλειονότητας των επιθέσεων αυτών.

Οι επιθέσεις εναντίον των διατάξεων του βιομηχανικού δικτύου ΗΕ πραγματοποιούνται μέσω του βιομηχανικού πληροφοριακού δικτύου ΗΕ. Το βιομηχανικό πληροφοριακό δίκτυο ΗΕ είναι το επικοινωνιακό δίκτυο μέσω του οποίου διασυνδέονται οι διατάξεις του βιομηχανικού δικτύου ΗΕ και ανταλλάσσουν πληροφορίες με τους ελεγκτικούς σταθμούς SCADA. Πολλές επιθέσεις εκμεταλλεύονται την έλλειψη μηχανισμών ασφάλειας πληροφοριών στα βιομηχανικά πρωτόκολλα επικοινωνίας. Ο λόγος είναι ότι μέχρι σήμερα η ασφάλεια πληροφοριών δεν συμπεριλαμβανόταν στις προδιαγραφές των βιομηχανικών πρωτοκόλλων. Στο Smart Grid, ωστόσο, η ασφάλεια πληροφοριών είναι απαραίτητη ώστε να μπορούν να αποτραπούν πολλές από τις επιθέσεις που σήμερα είναι εφικτές. Η επιτυχία τέτοιων επιθέσεων εναντίον διατάξεων του βιομηχανικού πληροφοριακού δικτύου είναι δυνατό να μετριαστεί περαιτέρω με τη χρήση πρωτοκόλλων φυσικού στρώματος ώστε να διατηρείται περιορισμένο (self-contained) το δίκτυο, όπως η τεχνολογία PLC, και με σωστή αρχιτεκτονική του δικτύου με τον διαχωρισμό των διατάξεων σε λειτουργικές ομάδες.

Σημαντικό στόχο επιθέσεων εναντίον των διατάξεων PMU του βιομηχανικού δικτύου αποτελεί ο μηχανισμός συγχρονισμού. Η χρήση από αυτές τις διατάξεις της τεχνολογίας GPS τις καθιστά ευάλωτες και σε επιθέσεις αλλοίωσης δεδομένων και σε επιθέσεις διακοπής διαθεσιμότητας (DoS). Στην περίπτωση αυτή, προτείνεται η αντικατάσταση του ευάλωτου πρωτοκόλλου GPS από το πρωτόκολλο χρονικού συγχρονισμού PTP, όπου ο συγχρονισμός γίνεται μέσω του ήδη υπάρχοντος επικοινωνιακού δικτύου και, συνεπώς, προστατεύεται από τους μηχανισμούς ασφάλειας που εκείνο διαθέτει.

Μία ακόμη μέθοδος επίθεσης είναι η εισαγωγή κακόβουλου hardware στις διατάξεις του βιομηχανικού δικτύου ΗΕ κατά τη διαδικασία κατασκευής τους. Μοναδική μέθοδος άμυνας εναντίον τέτοιων επιθέσεων είναι η θέσπιση αυστηρότατων ελέγχων κατά τη διαδικασία κατασκευής των διατάξεων. Από την πλευρά του διαχειριστή του δικτύου ΗΕ, οι μόνες ενέργειες που μπορούν να αποτρέψουν τέτοιες επιθέσεις είναι εκείνες που δυσχεραίνουν την εξαγωγή των δεδομένων που έχουν υποκλαπεί από το κακόβουλο hardware.

ΜΕΘΟΔΟΙ ΕΠΙΘΕΣΗΣ	**ΜΗΧΑΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ**
Παραβίαση συστήματος HMI/SCADA από το εταιρικό πληροφοριακό δίκτυο	• Χρήση συστημάτων IDS/IPS στις συνδέσεις ανάμεσα στο εταιρικό και το βιομηχανικό πληροφοριακό δίκτυο. • Εγκατάσταση εργαλείων ελέγχου εκτέλεσης λογισμικού στα συστήματα HMI/SCADA.
Εισαγωγή άγνωστης διάταξης στο βιομηχανικό πληροφοριακό δίκτυο	• Χρήση βιομηχανικών πρωτοκόλλων επικοινωνίας με ενσωματωμένους μηχανισμούς ασφάλειας πληροφοριών. • Χρήση τεχνολογίας Power Line Communications. • Κατάτμηση του βιομηχανικού πληροφοριακού δικτύου.

	• Εγκατάσταση μηχανισμών IDS/IPS στην περίμετρο και το εσωτερικό των λειτουργικών ομάδων.
GPS Spoofing	• Χρήση του πρωτοκόλλου PTP για το χρονικό συγχρονισμό των PMU.
Εισαγωγή κακόβουλου hardware	• Επιβολή υψηλών προδιαγραφών κατά τη διαδικασία κατασκευής των διατάξεων του βιομηχανικού δικτύου. • Χρήση σύγχρονων μεθόδων ανίχνευσης κακόβουλου hardware κατά τη διαδικασία ελέγχου ορθής λειτουργίας.

Πίνακας 5.1. Σύνοψη των μεθόδων επιθέσεων εναντίον διατάξεων του βιομηχανικού δικτύου ΗΕ και των μηχανισμών αντιμετώπισής τους.

Στον Πίν. 5.1 συνοψίζονται όλες οι επιθέσεις εναντίον διατάξεων του βιομηχανικού δικτύου ΗΕ. Η κρισιμότητα των διατάξεων αυτών για το Smart Grid επιβάλλει την πλήρη υιοθέτηση των μεθόδων αντιμετώπισης που αναλύθηκαν στο κεφάλαιο αυτό. Η ασφαλής λειτουργία και η ευρωστία των διατάξεων του βιομηχανικού δικτύου ΗΕ είναι ακρογωνιαίος λίθος για την εξασφάλιση υψηλής διαθεσιμότητας για το Smart Grid. Συνεπώς, είναι σημαντική ευθύνη του τμήματος ασφάλειας του διαχειριστή του δικτύου ΗΕ να εγκαταστήσει τους προαναφερθέντες μηχανισμούς άμυνας.

Παράρτημα 1. Βασικοί Όροι Ασφάλειας Πληροφοριών

Ως ασφάλεια πληροφοριών ορίζεται η διατήρηση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών [65]. Ως εμπιστευτικότητα ορίζεται η προστασία της πληροφορίας ώστε να μην είναι δυνατό να αποκτηθεί από κάποια οντότητα που δεν έχει την απαραίτητη εξουσιοδότηση. Ως ακεραιότητα ορίζεται η προστασία της πληροφορίας από μη εξουσιοδοτημένες αλλοιώσεις. Ως διαθεσιμότητα ορίζεται η δυνατότητα να είναι πάντα διαθέσιμη η πληροφορία. Συμερασματικά, μια πληροφορία θεωρείται ασφαλής όταν είναι ταυτόχρονα εμπιστευτική, ακέραια και διαθέσιμη.

Η εμπιστευτικότητα εξασφαλίζεται μέσω κρυπτογράφησης της πληροφορίας. Το μήνυμα της πληροφορίας μετασχηματίζεται σε ένα μη αναγνωρίσιμο μήνυμα μέσω ενός αλγορίθμου που δέχεται ως είσοδο το κλειδί κρυπτογράφησης. Προκειμένου να ανακτηθεί το πρωτότυπο μήνυμα από το κρυπτογραφημένο, το τελευταίο πρέπει να εισαχθεί μαζί με ένα κλειδί αποκρυπτογράφησης. Σε αυτό το γενικευμένο παράδειγμα, ο παραλήπτης του μηνύματος εξουσιοδοτείται μέσω της απόκτησης του κλειδιού αποκρυπτογράφησης.

Οι αλγόριθμοι κρυπτογράφησης χωρίζονται σε δύο βασικές πληροφορίες. Η πρώτη κατηγορία είναι οι συμμετρικοί αλγόριθμοι κρυπτογράφησης, όπου το κλειδί κρυπτογράφησης είναι ταυτόχρονα και το κλειδί αποκρυπτογράφησης. Ο καθιερωμένος συμμετρικός αλγόριθμος που χρησιμοποιείται σήμερα είναι ο AES. Η δεύτερη κατηγορία είναι οι μη συμμετρικοί αλγόριθμοι κρυπτογράφησης, όπου τα κλειδιά κρυπτογράφησης και αποκρυπτογράφησης είναι διαφορετικά. Σημαντική ομάδα μη συμμετρικών αλγόριθμων είναι οι αλγόριθμοι δημόσιου κλειδιού. Σε αυτούς, κάθε οντότητα διαθέτει δύο κλειδιά ένα δημόσιο και ένα ιδιωτικό. Προκειμένου η οντότητα Α να στείλει ένα μήνυμα στην οντότητα Β, το κρυπτογραφεί με το δημόσιο κλειδί της οντότητας Β το οποίο είναι διαθέσιμο. Το κρυπτογραφημένο μήνυμα μπορεί να αποκωδικοποιηθεί μόνο μέσω του ιδιωτικού κλειδιού της οντότητας Β που το διαθέτει αυτή. Έτσι, μόνο η οντότητα Β μπορεί να διαβάσει το μήνυμα της εμπιστευτικής πληροφορίας. Ο γνωστότερος αλγόριθμος δημοσίου κλειδιού είναι ο αλγόριθμος RSA. Επειδή, όμως, οι αλγόριθμοι δημοσίου κλειδιού είναι ιδιαίτερα απαιτητικοί σε υπολογιστική ισχύ, σε μια σύνδεση χρησιμοποιούνται μόνο στην αρχή ώστε να συμφωνήσουν τα δύο μέρη σε ένα κοινό κλειδί κρυπτογράφησης, το οποίο χρησιμοποιούν με συμμετρικούς αλγόριθμους κρυπτογράφησης, ώστε στη συνέχεια να κρυπτογραφηθεί η πληροφορία.

Η ακεραιότητα μιας πληροφορίας εξασφαλίζεται μέσω της χρήσης κωδικών πιστοποίησης μηνύματος (message authentication code – MAC). Οι αλγόριθμοι κατασκευής MAC ονομάζονται κρυπτογραφικές συναρτήσεις κατακερματισμού. Οι συναρτήσεις αυτές αντιστοιχούν τιμές από ένα σύνολο Α σε λιγότερς σε πλήθος τιμές ενός συνόλου Β. Ωστόσο, η κατανομή τιμών στο σύνολο Β πρέπει να είναι ομοιόμορφη και να μη μπορούν αν βρεθούν σε λογικά σύντομο χρονικό διάστημα δύο τιμές του συνόλου Α που να αντιστοιχούνται στην ίδια τιμή του συνόλου Β. Στην περίπτωση της μεταφοράς μηνυμάτων, οι αλγόριθμοι αυτοί παράγουν ένα κωδικό σταθερού μήκους από ένα μήνυμα αυθαίρετου μήκους. Οι πλέον δημοφιλείς αλγόριθμοι κατακερματισμού είναι της οικογένειας SHA (Secure Hash Algorithm). Οι αλγόριθμοι κατακερματισμού δέχονται ως είσοδο το μήνυμα και ένα κλειδί προκειμένου να παραγάγουν τον κωδικό του μηνύματος. Ο αποστολέας σε κάθε μήνυμα προσθέτει τον κωδικό MAC του μηνύματος για ορισμένο κλειδί. Ο παραλήπτης, γνωρίζοντας το κλειδί, επανυπολογίζει το κωδικό MAC. Εφόσον κάποια κακόβουλη οντότητα επιθυμεί να αλλοιώσει ένα μήνυμα, πρέπει να ανανεώσει και τον κωδικό MAC, άλλως θα ανιχνευτεί η αλλοίωση. Κάτι τέτοιο όμως είναι αδύνατο καθώς η κακόβουλη οντότητα δεν γνωρίζει τον κωδικό ώστε να

χρησιμοποιήσει τον αλγόριθμο και επίσης δεν μπορεί να μαντέψει άλλο μήνυμα που να παράγει τον ίδιο κωδικό MAC λόγω των χαρακτηριστικών των συναρτήσεων κατακερματισμού. Ο παραλήπτης επανυπολογίζει τον κωδικό MAC και τον συγκρίνει με αυτόν που ήδη υπάρχει στο μήνυμα. Εφόσον συμπίπτουν το μήνυμα είναι αυθεντικό. Σε αντίθετη περίπτωση, ανιχνεύεται αλλοίωση και απορρίπτεται.

Ως διαθεσιμότητα ορίζεται η πιθανότητα ένα σύστημα να λειτουργεί ορθά μια συγκεκριμένη χρονική στιγμή. Αποτελεί προδιαγραφή των πληροφοριακών συστήματων και επικοινωνιακών μέσων που είναι υπεύθυνα για τη μετάδοση της πληροφορίας. Υψηλές τιμές διαθεσιμότητας απαιτούν εξειδικευμένο εξοπλισμό με μεγάλη ευρωστία και μηχανισμούς αποτροπής κακόβουλων ενεργείων που αποσκοπούν στη διακοπή της παροχής των πληροφοριών.

Βιβλιογραφία

[1] IEEE, «IEEE Standard 802.11ad-2012,» 2012.

[2] A. V. A. V. P. C. MP Anastasopoulos, «A secure network management protocol for SmartGrid BPL networks: Design, implementation and experimental results,» *Computer Communications,* τόμ. 31, αρ. 18, pp. 4333-4342, 2008.

[3] NIST, «NISTIR 7628 Guidelines for Smart Grid Cyber Security: Vol.1, Smart Grid Cyber Security Strategy, Architecture and High-Level Requirements,» 2010.

[4] P. Jelly-Detwiler, «Electricity Theft: A Bigger Issue Than You Think,» Forbes, 23 4 2013. [Ηλεκτρονικό]. Available: http://www.forbes.com/sites/peterdetwiler/2013/04/23/electricity-theft-a-bigger-issue-than-you-think/. [Πρόσβαση 20 1 2014].

[5] Kaspersky, «Kaspersky Security Bulletin 2013. Overall statistics for 2013,» Kaspersky, 10 December 2013. [Ηλεκτρονικό]. Available: http://www.securelist.com/en/analysis/204792318/Kaspersky_Security_Bulletin_2013_Overall_statistics_for_2013#02. [Πρόσβαση 20 January 2014].

[6] IEC, «IEC 62056-62,» 2002. [Ηλεκτρονικό]. Available: http://212.175.131.171/IEC/iec62056-62%7Bed1.0%7Den.pdf.

[7] D. P. P. M. Stephen McLaughlin, «Energy Theft in the Advanced Metering Infrastructure,» Systems and Internet Infrastructure Security Laboratory (SIIS), 2009.

[8] D. P. S. M. A. D. P. M. S. McLaughlin, «Multi-vendor Penetration Testing in the Advanced Metering Infrastructure,» Department of Computer Science and Engineering , Pennsylvania State University, 2010.

[9] J. A. J. e. al., «Lest We Remember: Cold Boot Attacks on Encryption Keys,» σε *Proc. 2008 USENIX Security Symposium*, San Jose, 2008.

[10] P. Kocher, «Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems,» σε *CRYPTO '96*, New York, 1996.

[11] J. J. B. J. P. Kocher, «Differential Power Analysis,» σε *19th Annual International Cryptology Conference (CRYPTO)*, New York, 1999.

[12] B. A. J. R. P. R. D. Agrawal, «The EM Side–Channel(s):Attacks and Assessment,» σε *Cryptographic Hardware and Embedded Systems, CHES 2002*, Redwood Shores, California, 2002.

[13] A. S. E. T. D. Genkin, «RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis,» 2013.

[14] C. W. S. Skorobogatov, «In the blink of an eye: There goes your AES key,» IACR Cryptology ePrint Archive, 2012.

[15] R. A. S. Skorobogatov, «Optical Fault Induction Attacks,» σε *Cryptographic Hardware and Embedded Systems Workshop (CHES 2002)*, 2002.

[16] S. Skorobogatov, «Local Heating Attacks on Flash Memory Devices,» σε *2nd IEEE International Workshop on Hardware-Oriented Security and Trust (HOST-2009)*, San Frascisco, 2009.

[17] S. Skorobogatov, «Flash memory 'bumping' attacks,» σε *Cryptographic Hardware and Embedded Systems Workshop (CHES 2010)*, 2010.

[18] K. R. a. R. K. -. N. Poly, «Attacks and Defences for JTAG,» January/February 2010. [Ηλεκτρονικό]. Available: http://isis.poly.edu/~securejtag/design_and_test_final.pdf.

[19] R. D. A. C. Xi Chen, «Operating System Controlled Processor–Memory Bus Encryption,» March 2008. [Ηλεκτρονικό]. Available: http://robertdick.org/publications/chen08mar-a.pdf.

[20] G. L. L. R. T. A. Bucci M, «Three-phase dual-rail pre-charge logic,» σε *Cryptographic Hardware Embeded System*, 2006.

[21] M. K. Menendez E, «A high-performance, low-overhead, power-analysis-resistant, single-rail logic style,» σε *Hardware-Oriented Security and Trust*, Anaheim, CA, 2008.

[22] D. S. v. D. M. G. B. E. S. G. Clarke DE, «Incremental Multiset Hash Functions and Their Application to Memory Integrity Checking,» σε *ASIACRYPT*, 2003.

[23] G. O. G. S. Bellare M, «Incremental Cryptography: The Case of Hashing and Signing,» σε *Advances in Cryptology*, 1994.

[24] D. S. E. S. G. G. B. S. A. v. D. M. Clarke DE, «Towards constant bandwidth overhead integrity checking of untrusted data,» 2005.

[25] H. G. S. B. Hu Y, «A fast real-time memory authentication protocol,» σε *3rd ACM workshop on Scalable trusted computing*, New York, 2008.

[26] S. B. Hu Y, «An improved memory integrity protection scheme,» *Trust and Trustworthy Computing,* pp. 273-281, 2010.

[27] B. W. F. K. Holcomb D, «Initial SRAM state as a fingerprint and source of true random numbers for RFID tags,» σε *Conference on RFID Security*, 2007.

[28] S. G.-J. S. B. v. G. J. V. N. W. R. Tuyls P, «Read-proof hardware from protective coatings,» σε *Cryptographic Hardware and Embedded Systems*, 2006.

[29] C. D. v. D. M. D. S. Gassend B, «Controlled physical random functions,» σε *Annual Computer Security Applications*, 2002.

[30] F. Y. S. Z. Martinez Santos JC, «PIFT: Efficient dynamic information flow tracking using secure page allocation,» σε *Workshop on Embedded System Security*, 2009.

[31] D. S. C. T. U. Silas Cutler, «The Mirage Campaign,» 18 September 2012. [Ηλεκτρονικό]. Available: http://www.secureworks.com/cyber-threat-intelligence/threats/the-mirage-campaign/.

[32] Symantec, «Dragonfly: Western Energy Companies Under Sabotage Threat,» 30 June 2014. [Ηλεκτρονικό]. Available: http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat.

[33] McAfee, «SiteDigger,» [Ηλεκτρονικό]. Available: http://www.mcafee.com/us/downloads/free-tools/sitedigger.aspx.

[34] SHODAN. [Ηλεκτρονικό]. Available: http://www.shodanhq.com/.

[35] I. C. f. A. N. a. Numbers. [Ηλεκτρονικό]. Available: www.icann.org.

[36] nmap. [Ηλεκτρονικό]. Available: nmap.org.

[37] T. N. S. -. Nessus. [Ηλεκτρονικό]. Available: www.tenable.com/products/nessus.

[38] Metasploit. [Ηλεκτρονικό]. Available: http://www.metasploit.com/.

[39] M. J. Schwartz, «Another Java Zero-Day Vulnerability Hits Black Market,» [Ηλεκτρονικό]. Available: http://www.informationweek.com/security/attacks/another-java-zero-day-vulnerability-hits/240146416. [Πρόσβαση 3 September 2013].

[40] A. Greenberg, «Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits,» [Ηλεκτρονικό]. Available: http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/. [Πρόσβαση 3 September 2013].

[41] B. Schneier, «Crypto-Gram,» [Ηλεκτρονικό]. Available: http://www.schneier.com/crypto-gram-0009.html.

[42] D. S. B. P. B. T. Stefan Frei, «Modelling the Security Ecosystem,» [Ηλεκτρονικό]. Available: http://www.techzoom.net/publications/security-ecosystem/.

[43] R. Lemos, «Mobile Trojans Can Give Attackers An Inside Look,» 8 October 2012. [Ηλεκτρονικό]. Available: http://www.darkreading.com/insider-threat/mobile-trojans-can-give-attackers-an-ins/240008705. [Πρόσβαση 3 September 2013].

[44] Symantec, «Internet Security Threat Report,» 2013.

[45] K. Poulsen, «Slammer worm crashed Ohio nuke plant network,» 19 August 2003. [Ηλεκτρονικό]. Available: http://www.securityfocus.com/news/6767. [Πρόσβαση 4 September 2013].

[46] D. Kushner, «The Real Story of Stuxnet,» IEEE Spectrum, 26 February 2013. [Ηλεκτρονικό]. Available: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

[47] OWASP, «HTTP Post,» 2010 November 2010. [Ηλεκτρονικό]. Available: https://www.owasp.org/images/4/43/Layer_7_DDOS.pdf.

[48] J. Breeden, «Hackers' new super weapon adds firepower to DDOS,» 24 October 2012. [Ηλεκτρονικό]. Available: http://gcn.com/articles/2012/10/24/hackers-new-super-weapon-adds-firepower-to-ddos.aspx.

[49] E. D. Knapp, «Industrial Network Security,» Syngress, 2011, p. 113.

[50] K. Zetter, «Flame Hijacks Microsoft Update to Spread Malware Disguised As Legit Code,» 4 June 2012. [Ηλεκτρονικό]. Available: http://www.wired.com/threatlevel/2012/06/flame-microsoft-certificate/.

[51] C. S. A. Crain, «Project Robus,» [Ηλεκτρονικό]. Available: http://www.automatak.com/robus/.

[52] D. P. S. A. A. F. Todd E. Humphreys, «Evaluation of the vulnerability of phasor measurement units to GPS Spoofing attacks,» *International Journal of Critical Infrastructure Protection,* τόμ. 5, αρ. 3-4, pp. 146-153, December 2012.

[53] W. B. C. P. L. Lin, «MOLES: Malicious off-chip leakage enabled by side-channels,» IEEE/ACM International Conference on Computer-Aided Design, 2009.

[54] M. C. B. L. M. S. B. T. J. Z. A. Baumgarten, «Embedded Systems Challenge,» 2008. [Ηλεκτρονικό]. Available: http://isis.poly.edu/~vikram/iowa_state.pdf.

[55] C. M. C. A. D. Stefan, «Trojan Attacks for compromising cryptographic security in FPGA encryption systems,» 2008. [Ηλεκτρονικό]. Available: http://isis.poly.edu/~vikram/cooper.pdf.

[56] DNP, «DNP3 Secure Authentication Version 5,» November 2011. [Ηλεκτρονικό]. Available: https://www.dnp.org/Lists/Announcements/Attachments/7/Secure%20Authentication%20v5%202011-11-08.pdf.

[57] R. G. J. J. S. Warner, «GPS Spoofing Countermeasures,» Vulnerability Assessment Team - Los Alamos National Laboratory, 2003.

[58] G. S. J. Amelot, «Testing Phasor Measurement Units using IEEE 1588 Precision Time Protocol,» National Institute of Standards and Technology, 2012.

[59] M. S. H. M. Banga, «Trusted RTL: Trojan Detection Methodology in Pre-Silicon Designs,» Bradley Department of Electrical and Computer Engineering, Virginia Tech, 2010.

[60] F. W. P. S. C. P. S. B. R. S. Chakraborty, «MERO: A Statistical Approach for Hardware Trojan Detection,» Department of Electrical and Computer Engineering and Computer Science Case Western Reserve University, 2009.

[61] J. P. M. T. R. Rad, «Sensitivity Analysis to Hardware Trojans using Power Supply Transient Signals,» 2008.

[62] M. S. H. M. Banga, «A Region Based Approach for the Identification of Hardware Trojans,» 2008.

[63] M. S. H. M. Banga, «VITAMIN: Voltage Inversion Technique to Ascertain Malicious Insertions in ICs,» 2009.

[64] Y. M. Y. Jin, «Hardware Trojan Detection Using Path Delay Fingerprint,» 2008.

[65] ISO/IEC, «ISO/IEC 27000:2009. Information technology - Security techniques - Information security management systems - Overview and vocabulary,» 2009.