ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΑΣΦΑΛΕΙΑ ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΑ ΕΞΥΠΝΑ ΗΛΕΚΤΡΙΚΑ ΔΙΚΤΥΑ

Διπλωματική εργασία

Τσιάλτας Θεόφιλος

Επιβλέπων καθηγητής: Μπαργιώτας Δημήτριος

Βόλος 2020

ΠΑΝΕΠΙΣΤΗΜΙΟΘΕΣΣΑΛΙΑΣ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΑΣΦΑΛΕΙΑ ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΑ ΕΞΥΠΝΑ ΗΛΕΚΤΡΙΚΑ ΔΙΚΤΥΑ

Διπλωματική Εργασία

Τσιάλτας Θεόφιλος

Επιβλέπων: Μπαργιώτας Δημήτριος

Βόλος 2020

UNIVERSITY OF THESSALY

SCHOOL OF ENGINEERING

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

SECURITY AND PROTECTION OF PERSONAL DATA IN THE SMART GRIDS

Diploma Thesis

Tsialtas Theofilos

Supervisor: Bargiotas Dimitrios

Volos 2020

ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ ΠΕΡΙ ΑΚΑΔΗΜΑΪΚΗΣ ΔΕΟΝΤΟΛΟΓΙΑΣ ΚΑΙ ΠΝΕΥΜΑΤΙΚΩΝ ΔΙΚΑΙΩΜΑΤΩΝ

«Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ρητά ότι η παρούσα διπλωματική εργασία, καθώς και τα ηλεκτρονικά αρχεία και πηγαίοι κώδικες που αναπτύχθηκαν ή τροποποιήθηκαν στα πλαίσια αυτής της εργασίας, αποτελεί αποκλειστικά προϊόν προσωπικής μου εργασίας, δεν προσβάλλει κάθε μορφής δικαιώματα διανοητικής ιδιοκτησίας, προσωπικότητας και προσωπικών δεδομένων τρίτων, δεν περιέχει έργα/εισφορές τρίτων για τα οποία απαιτείται άδεια των δημιουργών/δικαιούχων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον και πληρούν τους κανόνες της επιστημονικής παράθεσης. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο, αρχεία ή/και πηγές άλλων συγγραφέων, αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής».

Ο/Η Δηλών/ούσα

(Υπογραφή)
Ονοματεπώνυμο Φοιτητή/ήτριας
Ημερομηνία

ΠΕΡΙΛΗΨΗ

Ο όρος "Έξυπνα Δίκτυα" αναφέρεται στην εξέλιξη των σημερινών δικτύων ηλεκτρικής ενέργειας. Τα έξυπνα δίκτυα θα επιτρέπουν την αποδοτικότερη χρήση της υπάρχουσας εγκατεστημένης ισχύος και της υποδομής μεταφοράς και διανομής ενέργειας, με χαμηλότερη ένταση εκπομπών αερίων του θερμοκηπίου. Θα διευκολύνουν επίσης την επέκταση των ανανεώσιμων πηγών ενέργειας, με χρήση φωτοβολταϊκών και ανεμογεννητριών. Στόχος είναι η μείωση κατανάλωσης ενέργειας και εκπομπών CO2. Εισάγοντας τις νέες τεχνολογίες επικοινωνιών και πληροφορικής σε καίρια σημεία του δικτύου, επιτυγχάνεται η ενσωμάτωση ανανεώσιμων πηγών ενέργειας καθώς και η ενεργητικότητα των καταναλωτών στο σενάριο λειτουργίας του έξυπνου δικτύου. Το γενικό επιθυμητό αποτέλεσμα είναι η βέλτιστη αξιοποίηση ηλεκτρικής ενέργειας τόσο στην πλευρά της παραγωγής όσο και στην πλευρά της κατανάλωσης. Ωστόσο, η ενσωμάτωση των νέων τεχνολογιών, ειδικά αυτών που σχετίζονται με το Διαδίκτυο, ίσως εισάγουν νέες απειλές για την ασφάλεια του έξυπνου δικτύου. Υπάρχει κίνδυνος εκμετάλλευσης των ευάλωτων σημείων του δικτύου επικοινωνιών, υποκλοπής απόρρητων ή προσωπικών πληροφοριών, απαγόρευσης της διαθεσιμότητας απαραίτητων υπηρεσιών όπως πρόκληση μιας εκτεταμένης διακοπής ρεύματος, με συνέπεια ένα δυσμενές οικονομικό κόστος. Για αυτό το λόγο, η αντιμετώπιση των ζητημάτων ασφάλειας στο έξυπνο δίκτυο παίζει πρωταρχικό ρόλο. Η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των διακινούμενων πληροφοριών είναι ανάγκη να προστατευθούν, έτσι ώστε να αυξηθεί η αξιοπιστία του συστήματος. Παραδείγματος χάρη μια αποτελεσματική λύση είναι η κρυπτογράφηση των δεδομένων μέτρησης.

Λέξεις Κλειδιά: έξυπνα δίκτυα, δίκτυο, ενέργεια, νέες τεχνολογίες, διαδίκτυο, ασφάλεια.

ABSTRACT

The term "smart grids" refers to the evolution of current electricity grids. Smart grids will allow more efficient use of existing installed power and energy transmission and distribution infrastructure with lower greenhouse gas emissions. They will also facilitate the expansion of renewable energy sources using solar cells and wind turbines. The goal is to reduce energy consumption and CO2 emissions. By introducing new communications and IT technologies at key points in the network, integration of renewable energy sources and consumer energy into the smart grid scenario is achieved. The overall desired result is the optimal use of electricity on both the production side and the consumption side. However, the integration of new technologies, especially those related to the Internet, may introduce new threats to the security of the smart grid. There is a risk of exploiting vulnerabilities in the communications network, classified or personal information, prohibiting the availability of necessary services such as causing an excessive power outage, resulting in an unfavorable financial cost. For this reason, addressing security issues in the smart grid plays a leading role. The confidentiality, integrity and availability of the exchanged information need to be protected in order to increase the credibility of the system. For example, an effective solution is encryption of measurement data.

Keywords: smart grid, network, energy, new technology, internet, security.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

1.1 Το ιστορικό της ηλεκτρικής ενέργειας στην Ελλάδα

Ο ηλεκτρισμός στην Ελλάδα έρχεται το 1889. Η πρώτη μονάδα παραγωγής ηλεκτρικής ενέργειας, κατασκευάστηκε στην Αθήνα, στην οδό Αριστείδου, από την Γενική Εταιρία Εργοληψιών, σύμφωνα με την ΔΕΗ Α.Ε. Με αρχή φωτισμού τα Ανάκτορα, ξεκινάει η επέκταση του ηλεκτροφωτισμού στο σημερινό ιστορικό κέντρο της πόλης. Η Θεσσαλονίκη, η οποία είναι ακόμα κτήμα της Οθωμανικής Αυτοκρατορίας, ηλεκτροδοτείται τον ίδιο χρόνο. Τον φωτισμό και την τροχοδρόμηση της πόλης με την κατασκευή ενός εργοστασίου παραγωγής ηλεκτρικής ενέργειας αναλαμβάνει η Βελγική Εταιρεία από τις τουρκικές αρχές. Μετά το πέρας μίας δεκαετίας, εμφανίζονται στην Ελλάδα οι πολυεθνικές εταιρείες ηλεκτρισμού. Η Ελληνική Ηλεκτρική Εταιρεία, η οποία ιδρύθηκε από την αμερικανική Thomson-Houstonμε την συμμετοχή της Εθνικής Τράπεζας, ανέλαβε την ηλεκτροδότηση μεγάλων ελληνικών πόλεων. 250 πόλεις άνω των 5000 κατοίκων θα έχουν ηλεκτροδοτηθεί μέχρι το 1929. Όσον αφορά τις απομακρυσμένες και μικρές περιοχές, επειδή δεν συνέφερε τις μεγάλες εταιρίες να δημιουργήσουν και εκεί μονάδες παραγωγής ηλεκτρικής ενέργειας, η ηλεκτροδότηση έγινε από μικρά εργοστάσια τα οποία κατασκευάστηκαν από ιδιώτες ή κοινοτικές αρχές. Μέχρι το πέρας της επόμενης εικοσαετίας υπήρχαν στην Ελλάδα περίπου 400 εταιρίες παραγωγής ηλεκτρικής ενέργειας. Το πετρέλαιο και ο γαιάνθρακας τα οποία εισάγονταν και τα δύο από το εξωτερικό, αποτελούσαν την πρωτογενή ύλη καυσίμων. Τα εισαγόμενα καύσιμα όμως και ο διαμοιρασμός της ενέργειας σε αρκετές μικρές μονάδες, οδήγησε την τιμή της ενέργειας πολύ υψηλά, πόσο μάλλον συγκριτικά με την υπάρχουσα τιμή σε άλλες ευρωπαϊκές χώρες.

Αυτό είχε ως αποτέλεσμα, η απόκτηση της ηλεκτρικής ενέργειας να μην είναι εύκολη, ή ακόμα και όταν παρεχόταν, ήταν για συγκεκριμένο ωράριο και με ύπαρξη πολλών ξαφνικών διακοπών. Η παραγωγή, η μεταφορά και η διανομή της ηλεκτρικής ενέργειας, έγιναν αρμοδιότητες ενός δημόσιου φορέα όταν τον Αύγουστο του 1950 δημιουργήθηκε η ΔΕΗ. Πρώτοι στόχοι της ΔΕΗ ήταν η αξιοποίηση εγχώριων πηγών ενέργειας και η δημιουργία ενός εθνικού συστήματος διασύνδεσης των δικτύων μεταφοράς ηλεκτρικής ενέργειας. Η ΔΕΗ δημιούργησε λιγνιτικές μονάδες ηλεκτροπαραγωγής, οι οποίες χρησιμοποιούσαν ως καύσιμη ύλη τα πλούσια και εγχώρια λιγνιτικά κοιτάσματα που είχαν

ήδη εντοπισθεί. Ταυτόχρονα βέβαια, στα μεγάλα ποτάμια της χώρας, δημιουργήθηκαν υδροηλεκτρικοί σταθμοί με στόχο να αξιοποιήσουν την δύναμη των υδάτων. Στις αρχές του 2001, η ΔΕΗ ξεκίνησε να λειτουργεί ως ανώνυμη εταιρεία, ενώ μέχρι το τέλος του ίδιου χρόνου κατάφερε να εισαχθεί στα Χρηματιστήρια Αξιών Αθηνών και Λονδίνου. Πλέον η ΔΕΗ Α.Ε αποτελεί τον παραγωγό και τον κύριο προμηθευτή ηλεκτρικής ενέργειας. Με βάση τα στοιχεία του 2013, η ΔΕΗ κατέχει στην ηπειρωτική Ελλάδα τα τρία τέταρτα της ισχύος των θερμοηλεκτρικών σταθμών ηλεκτροπαραγωγής εμπεριέχοντας στο ενεργειακό της μείγμα υδροηλεκτρικούς, λιγνιτικούς και πετρελαϊκούς σταθμούς, όπως επίσης και σταθμούς φυσικού αερίου και μονάδων ανανεώσιμων πηγών ενέργειας. Το γεγονός ότι περίπου η μισή ποσότητα της ηλεκτρικής ενέργειας που παραγόταν ήταν από λιγνίτη, έκανε την ΔΕΗ τον δεύτερο μεγαλύτερο παραγωγό στην Ευρωπαϊκή Ένωση της ηλεκτρικής ενέργειας από λιγνίτη. Πάλι με βάση στοιχεία του 2013, το 98% της ηλεκτρικής ενέργειας, προμηθεύεται από την ΔΕΗ. Με βάση στοιχεία του 2009, παραμένει στην ιδιοκτησία της το δίκτυο διανομής μήκους 217.000 χλμ., ενώ από την άλλη η κυριότητα του εθνικού συστήματος μεταφοράς ηλεκτρικής ενέργειας μήκους 11.650 χλμ. μεταβιβάζεται στον ΑΔΜΗΕ Α.Ε.(Ανεξάρτητος Διαχειριστής Μεταφοράς Ηλεκτρικής Ενέργειας Α.Ε.). Δύο θυγατρικές εταιρείες της ΔΕΗ Α.Ε. δημιουργήθηκαν όταν έγινε ο χωρισμός των κλάδων Μεταφοράς και Διανομής. Ο ΑΔΜΗΕ Α.Ε. που αναφέρθηκε προηγουμένως και ο ΔΕΔΔΗΕ Α.Ε. (Διαχειριστής Ελληνικού Δικτύου Διανομής Ηλεκτρικής Ενέργειας Α.Ε.).

Ο πρώτος αναλαμβάνει τις αρμοδιότητες της διαχείρισης, λειτουργίας, ανάπτυξης και συντήρησης του Ελληνικού Συστήματος Μεταφοράς Ηλεκτρικής Ενέργειας και των διασυνδέσεών του, ενώ ο δεύτερος αναλαμβάνει τις αρμοδιότητες για τη διαχείριση, ανάπτυξη, λειτουργία και συντήρηση του Ελληνικού Δικτύου Διανομής Ηλεκτρικής Ενέργειας. Η διαχείριση των Ανανεώσιμων Πηγών Ενέργειας αναλαμβάνεται από την ΔΕΗ Ανανεώσιμες Α.Ε. η οποία αποτελούσε μια 100% θυγατρική εταιρεία της ΔΕΗ Α.Ε. με απώτερο σκοπό την αξιοποίηση και ανάπτυξη του συγκεκριμένου κλάδου. [1],[2]

1.2 Το ηλεκτρικό δίκτυο σήμερα

Στο παραδοσιακό ηλεκτρικό δίκτυο, η επικοινωνία είναι μονόπλευρη – μόνο από τους καταναλωτές προς τις επιχειρήσεις παραγωγής ηλεκτρικής ενέργειας – και προσπαθεί να προσαρμοστεί στις αλλαγές της ζήτησης μέσω της ρύθμισης της παραγωγής προς τα πάνω ή προς τα κάτω. Όταν οι ηλεκτροπαραγωγικές επιχειρήσεις δεν μπορούν να ανταποκριθούν στις ανάγκες, τότε μπορεί να προκύψουν προβλήματα στο σύστημα όπως διακοπές στην ηλεκτροδότηση.

Το σημερινό ηλεκτρικό δίκτυο αποτελείται από τρεις κύριους τομείς. Από τις μονάδες από τις οποίες παράγεται, από το σύστημα μέσω του οποίου διανέμεται και τέλος από τους τελικούς παραλήπτες προς χρήση (-κατοικίες, επιχειρήσεις, βιομηχανίες και άλλα). Η ιδιαιτερότητα του ηλεκτρικού δικτύου έχει σχέση με το γεγονός ότι η προσφορά και η ζήτηση του πρέπει να έχουν στενή ισορροπία καθώς δεν έχει βρεθεί κάποιος τρόπος αποθήκευσης μεγάλης ποσότητας ενέργειας σε περίπτωση περίσσιας ή έλλειψης . Είναι σημαντική η μετατροπή του τρέχοντος ηλεκτρικού δικτύου σε έξυπνο ηλεκτρικό δίκτυο έτσι ώστε να υπάρχει αξιόπιστη, υψηλής ποιότητας ηλεκτρική ενέργεια στις ψηφιακές κοινωνίες με έναν φιλικό προς το περιβάλλον και βιώσιμο τρόπο. Αυτός ο στόχος θα επιτευχθεί μέσω της εφαρμογής ενός συνδυασμού υπαρχουσών και νέων τεχνολογιών για την ενεργειακή αποδοτικότητα, την ενσωμάτωση των ανανεώσιμων πηγών ενέργειας, την ανταπόκριση στη ζήτηση και άλλων μέσων.

Λόγω του γεγονότος ότι τα δίκτυα ενέργειας στις βιομηχανικές χώρες είναι μεγάλης ¨ηλικίας¨, δέχονται πολλές προκλήσεις που δεν υπολογίστηκαν ποτέ, όπως επίσης δέχονται πίεση από πολλά λειτουργικά σενάρια. Οι κύριες προκλήσεις συνοψίζονται παρακάτω:

- Η απελευθέρωση της αγοράς ενέργειας οδήγησε σε πρωτοφανές εμπόριο ενέργειας στα κατά τόπους ηλεκτρικά δίκτυα, παρουσιάζοντας σενάρια και αβεβαιότητες ροής ενέργειας που το σύστημα δεν σχεδιάστηκε να διαχειρίζεται.
- Η αυξανόμενη διείσδυση της ανανεώσιμης ενέργειας στο σύστημα αυξάνει περαιτέρω την αβεβαιότητα στην τροφοδοσία των φορτίων και προσθέτει συγχρόνως πίεση στην υπάρχουσα υποδομή λόγω της διασποράς των γεωγραφικών θέσεων όπου η ενέργεια παράγεται.
- Η ψηφιακή κοινωνία μας εξαρτάται και απαιτεί παροχή ηλεκτρικού ρεύματος υψηλής ποιότητας και υψηλής διαθεσιμότητας.

- Η απειλή τρομοκρατικών επιθέσεων είτε στις εγκαταστάσεις είτε στα ηλεκτρονικά συστήματα του ηλεκτρικού δικτύου εισάγει περαιτέρω αβεβαιότητα.
- Υπάρχει μια οξεία ανάγκη να επιτευχθεί η βιώσιμη αύξηση ενέργειας και να ελαχιστοποιηθεί η περιβαλλοντική επίδραση μέσω π.χ. της μεταπήδησης στις πράσινες και ανανεώσιμες πηγές ενέργειας. Μπορούμε μόνο να επιτύχουμε αυτόν τον στόχο με την αύξηση της ενεργειακής αποδοτικότητας, μειώνοντας τη μέγιστη ζήτηση, και μεγιστοποιώντας τη χρήση της ανανεώσιμης ενέργειας.

Η τεχνολογία των έξυπνων δικτύων αποτελεί την απάντηση στην αυξανόμενη συναίνεση στην βιομηχανία καθώς και ενδιάμεσα πολλών κυβερνήσεων. Αυτό το γεγονός επιβεβαιώνεται από τα ειδικά μέτρα ύψους δισεκατομμυρίων-δολαρίων που προέρχονται από την Αμερικάνικη Κυβέρνηση και αποσκοπούν την έρευνα και την ανάπτυξη, επίδειξη, καθώς επίσης και την επέκταση των τεχνολογιών έξυπνων δικτύων και των σχετικών προτύπων. Με επίσης τεράστια ποσά χρηματοδότησης με απώτερο σκοπό την επίδειξη και επέκταση την τεχνολογική έρευνα των έξυπνων δικτύων έχουν συμβάλλει η Ευρωπαϊκή Ένωση και η Κίνα. Το βασικό επιθυμητό αποτέλεσμα που θα αποφέρει η μετατροπή του κλασσικού δικτύου σε έξυπνο δίκτυο, είναι η παροχή υψηλής και αξιόπιστης ποιότητας ηλεκτρικής ενέργειας, με συνάμα ένα βιώσιμο και φιλικό τρόπο προς το περιβάλλον, στις ψηφιακές κοινωνίες. Αυτό μπορεί να γίνει πραγματοποιήσιμο, συνδυάζοντας τις ήδη υπάρχουσες τεχνολογίες με τις νέες, για την ενεργειακή αποδοτικότητα, την ενσωμάτωση των ανανεώσιμων πηγών ενέργειας, την ανταπόκριση στη ζήτηση, την παρακολούθηση και έλεγχο εκτενών ζωνών, την αυτό-θεραπεία, HVDC, το εύκαμπτο σύστημα μεταφοράς εναλλασσόμενου ρεύματος (FACTS), κ.λπ. Η ευφυΐα του έξυπνου δικτύου έγκειται στο στρώμα αυτόματης λήψης αποφάσεων, σε όλα τα προγράμματα υπολογιστών που τρέχουν στους ηλεκτρονόμους, στα έξυπνα ηλεκτρικά μηχανήματα (IEDs), στα συστήματα αυτοματοποίησης υποσταθμών, στα κέντρα ελέγχου, και στα επιχειρηματικά κέντρα. Η αναφορά στο έξυπνο ηλεκτρικό δίκτυο περιλαμβάνει θέματα όλων των διασυνδεδεμένων συστημάτων ηλεκτρικής ενέργειας, από τη συγκεντρωμένη μαζική παραγωγή στη διανεμημένη παραγωγή (DG), από τα υψηλής τάσεως συστήματα μεταφοράς στα χαμηλής τάσης συστήματα διανομής, από τα κέντρα ελέγχου των αρχών διαχείρισης ενέργειας, στο μικροδίκτυο χαμηλής τάσης του τελικού καταναλωτή – οικιακής χρήσης, από τις μαζικές αγορές ενέργειας στους τοπικούς παρόχους ηλεκτρικής ενέργειας, και από τους παραδοσιακούς ενεργειακούς πόρους στη διανεμημένη και ανανεώσιμη παραγωγή και αποθήκευση. [3]

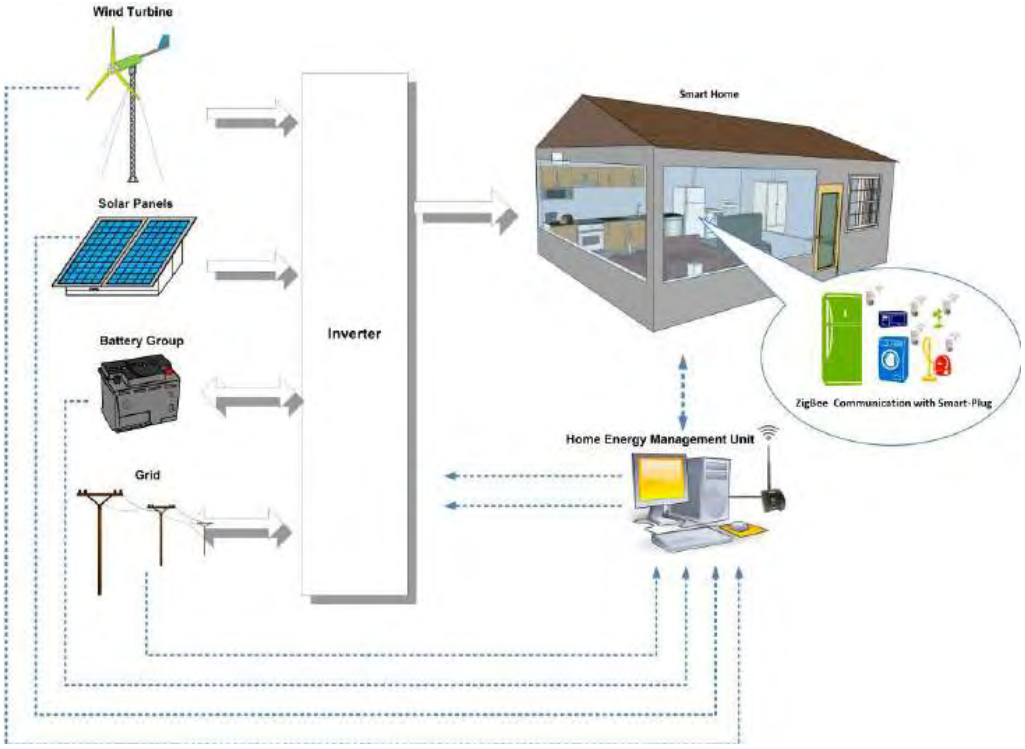
1.3 Έξυπνα δίκτυα

Ο όρος "Έξυπνα Δίκτυα" αναφέρεται στην εξέλιξη των σημερινών δικτύων ηλεκτρικής ενέργειας. Με στόχο την δημιουργία ενός πιο αποτελεσματικού δικτύου ηλεκτρικής ισχύος, τα έξυπνα δίκτυα αποτελούν έναν κόμβο της πληροφορικής, των επικοινωνιών και των συστημάτων ισχύος. Η υπόσχεση που δίνουν στον κόσμο τα έξυπνα δίκτυα είναι μια αποτελεσματική και ευφυή προσέγγιση διαχείρισης της προμήθειας και κατανάλωσης ηλεκτρικής ενέργειας. Είναι ικανότητα του έξυπνου δικτύου να παίρνει έξυπνες αποφάσεις για να διατηρήσει την ισορροπία στο ηλεκτρικό δίκτυο. Η διαχείριση ενέργειας σε πραγματικό χρόνο δίνει το πλεονέκτημα στους καταναλωτές και προμηθευτές ενέργειας να επωφεληθούν από την πρακτικότητα, την ευκολία, τη φιλικότητα προς το περιβάλλον, την αξιοπιστία, την ασφάλεια και την εξοικονόμηση ενέργειας. Σε καθημερινή βάση μεγάλη ποσότητα ενέργειας καταναλώνεται στις κατοικίες. Με την ενσωμάτωση του έξυπνου δικτύου (Σχήμα 1) επιτυγχάνονται πολλά πλεονεκτήματα όπως :

- απομακρυσμένος έλεγχος έξυπνων οικιακών συσκευών μέσω έξυπνων μετρητών
- αύξηση ενεργειακής απόδοσης και ποιότητας ισχύος
- εξοικονόμηση κόστους από τη μείωση του φορτίου αιχμής
- αυτόνομη ανάρρωση δικτύου *
- τιμολόγηση πραγματικού χρόνου
- ένταξη εναλλακτικών κατανεμημένων πηγών παραγωγής, όπως ανεμογεννήτριες και φωτοβολταϊκά συστήματα
- ένταξη plug-in υβριδικών ηλεκτρικών οχημάτων για αποθήκευση ενέργειας

* Αυτόνομη ανάρρωση σημαίνει ότι το δίκτυο μπορεί να ανακατευθύνει και να αναπροσαρμόσει τη ροή του ηλεκτρικού ρεύματος στην περίπτωση που ένα μονοπάτι μετάδοσης διακοπεί. Αυτό επιτυγχάνεται με συνεχή αυτοεκτίμηση της κατάστασης του συνολικού δικτύου. Σαν αποτέλεσμα μπορεί να μειωθεί η συχνότητα και η διάρκεια διακοπών ρεύματος.

Με γνώμονα αυτά τα πλεονεκτήματα και θεωρώντας αυτονόητο ότι χρειάζεται μεγάλη ποσότητα ενέργειας ανά τον κόσμο (Σχήμα 2), είναι σημαντική λοιπόν η μετατροπή του σημερινού δικτύου σε έξυπνο (Σχήμα 3).



Σχήμα 1. Έξυπνο δίκτυο κατοικίας

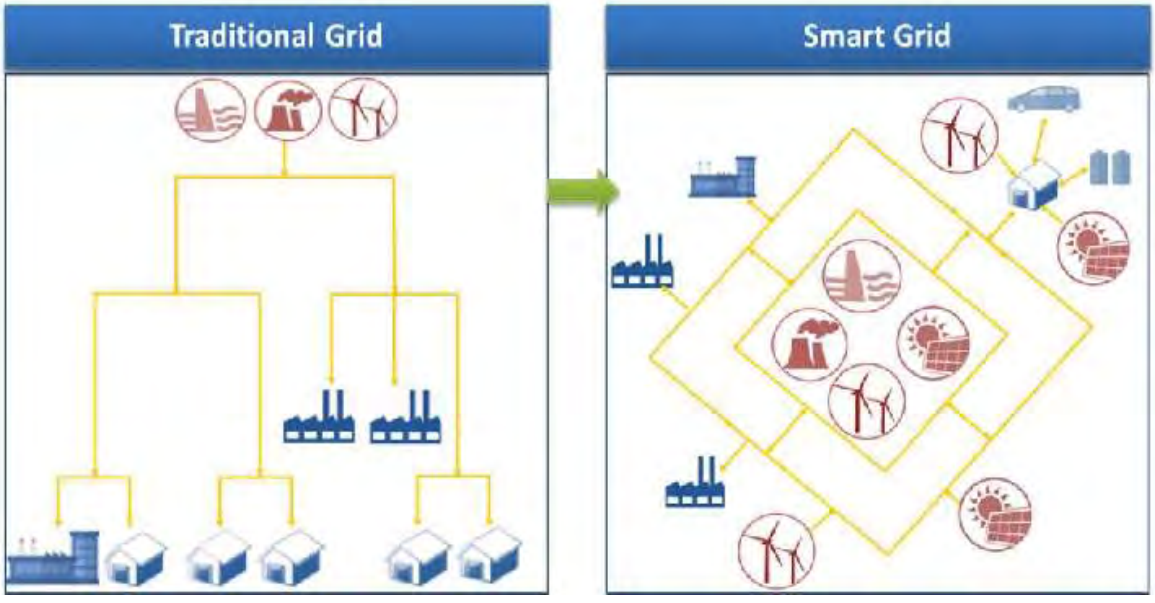
Ένα ευφυές δίκτυο δίνει δυνατότητες :

- Ευφυής συνύπαρξης της κεντρικής και διεσπαρμένης παραγωγής με αποτέλεσμα την μείωση της χρήσης άνθρακα και αποδοτικού χειρισμού της ζήτησης.
- Εμπορία ενέργειας και βελτιστοποίηση κόστους μέσω χρονομεταβλητών τιμολογίων και διαφόρων κινήτρων εξαρτώμενων από το μεταβαλλόμενο φορτίο.
- Ενεργός συμμετοχή του πελάτη με βάση την επικοινωνία σε δύο κατευθύνσεις και μεγάλη ροή πληροφορίας.

Ένα ευφυές δίκτυο προσφέρει :

- Αυξημένη αξιοπιστία.
- Αποκεντρωμένη παραγωγή (οικιακοί καταναλωτές που μπορούν να γίνουν και παραγωγοί).
- Ελαστικότητα στη ζήτηση ενέργειας με τη χρήση ΑΠΕ.
- Εξοικονόμηση Ενέργειας – Μείωση Απωλειών.
- Προστασία Περιβάλλοντος. [4]

Σχήμα 2. Ενέργεια και ο κόσμος



Σχήμα 3. Από παραδοσιακό δίκτυο σε έξυπνο δίκτυο

Σημαντικός παράγοντας υψηλής ενεργειακής κατανάλωσης και περιβαλλοντικής μόλυνσης είναι η καθημερινή χρήση οχημάτων. Τα plug-in ηλεκτρικά υβριδικά οχήματα (Σχήμα 4), παρόλο που δεν χρησιμοποιούνται ευρέως ακόμα, περιορίζουν σε μεγάλο βαθμό τις εκπομπές αερίων και κόστους μεταφοράς σε σχέση με τα υπόλοιπα οχήματα.

Σχήμα 4. Υβριδικό plug-in όχημα

1.4 Έξυπνα δίκτυα και η εισαγωγή τους στον κόσμο

Η ανάπτυξη των ευφυών δικτύων είναι καθολική για όλο τον κόσμο. Στο Κολοράντο στην πόλη Μπούλντερ πραγματοποιείται πιλοτικό πρόγραμμα για τη δημιουργία μιας έξυπνης πόλης, η οποία έχει ως σκοπό να αποτελείται από έξυπνα σπίτια κατά κόρον. Φυσικά υπάρχουν και άλλες πόλεις στον κόσμο που δραστηριοποιούνται με το έξυπνο δίκτυο.

Το πρώτο και μεγαλύτερο παράδειγμα είναι στην Ιταλία και ολοκληρώθηκε το 2005. Το έργο αυτό στο οποίο για πρώτη φορά χρησιμοποιήθηκαν σε εμπορική κλίμακα οι τεχνολογίες των έξυπνων δικτύων εξοικονομεί ετησίως 500 εκατομμύρια € και το κόστος του ήταν 2,1 δισεκατομμύρια €.

Στις ΗΠΑ, στην πόλη Όστιν του Τέξας, γίνονται προσπάθειες για τη δημιουργία έξυπνου δικτύου από το 2003, όπου το ένα τρίτο των χειροκίνητων μετρητών του δικτύου αντικαταστήθηκε με έξυπνους μετρητές οι οποίοι επικοινωνούν μέσω ενός ασύρματου δικτύου. Το ηλεκτρικό δίκτυο της πόλης διαχειρίζεται 200000 συσκευές σε πραγματικό χρόνο (αισθητήρες, έξυπνους μετρητές και θερμοστάτες) και ευελπιστεί οι συσκευές να φθάσουν τις 500000.

Η μάχη κατά της κλιματικής αλλαγής σε συνδυασμό με την έρευνα για ενεργειακή αποδοτικότητα, αργά αλλά σταθερά, σπρώχνει το θέμα των έξυπνων δικτύων στην ημερήσια διάταξη πολλών εταιρειών. Στην πραγματικότητα, οι ευρωπαϊκές και αμερικάνικες τα θεωρούν καίρια για την επίτευξη περιβαλλοντικών τους στόχων και σημαντικά για την επίτευξη ασφαλείας στα δίκτυα ηλεκτρικής ενέργειας. Οι έρευνες επικεντρώνονται στην έξυπνη μεταφορά ισχύος και στην ενσωμάτωση έξυπνων λειτουργιών στα προϊόντα των εταιρειών παροχής και στην υποδομή των καταναλωτών. Οι σημερινές αντικρουόμενες απαιτήσεις για πιο αξιόπιστη, μεγαλύτερου όγκου παραγωγή ενέργειας από τις πιο καθαρές και Ανανεώσιμες Πηγές υπογραμμίζει την ανάγκη για βαθμιαία μετατροπή των παλιών υποδομών σε ένα πιο έξυπνο, πιο αποτελεσματικό, και περιβαλλοντικά φιλικό δίκτυο, που μπορεί να δεχτεί κάθε ποιότητα ισχύος, από κάθε είδος πηγής (κεντρική και διεσπαρμένη παραγωγή), και να παρέχει αξιόπιστη ενέργεια, κατά παραγγελία, σε κάθε είδος καταναλωτή. Με άλλα λόγια, αυτό

που χρειαζόμαστε είναι ένα έξυπνο δίκτυο, δηλαδή ένα αυτό-ελεγχόμενο σύστημα, που βασίζεται σε βιομηχανικά πρότυπα και διασχίζει τα διεθνή σύνορα, συμμετέχοντας στη χονδρική αγορά ενέργειας και παρέχοντας ένα σταθερό, ασφαλές, αποδοτικό και περιβαλλοντικά βιώσιμο δίκτυο. Ενώ είναι αλήθεια πως τα έξυπνα δίκτυα είναι ακόμα ένα μελλοντικό όραμα, τα πρότυπα και οι τεχνολογίες που θα απαιτηθούν αναπτύσσονται εδώ και μερικά χρόνια και ορισμένα είναι ήδη σε χρήση. Υπήρξε μεγάλη συζήτηση στα μέσα μαζικής ενημέρωσης σχετικά με τα έξυπνα δίκτυα. Τον Οκτώβριο του 2009, ο Πρόεδρος Μπαράκ Ομπάμα των ΗΠΑ υποσχέθηκε 340 εκατομμύρια δολάρια για τη χρηματοδότηση "ενός ευρύτατου φάσματος τεχνολογιών που θα προωθήσουν την μετάβαση σε ένα πιο έξυπνο, πιο ισχυρό, πιο αποτελεσματικό και αξιόπιστο ηλεκτρικό σύστημα". Στην Ευρώπη, η Ευρωπαϊκή Επιτροπή έχει χρηματοδοτήσει έρευνες με σκοπό να αναπτύξουν τις τεχνολογίες που «διαδραματίζουν καίριο ρόλο στη μετατροπή των συμβατικών δικτύων μεταφοράς και διανομής ηλεκτρικής ενέργειας σε ένα ενιαίο και διαδραστικό σύστημα υπηρεσιών, με χρήση των κοινών ευρωπαϊκών μεθόδων και συστημάτων σχεδιασμού και λειτουργίας».

Συμπεράσματα:

- Τα έξυπνα δίκτυα αναγκαία για αειφόρο ηλεκτρικό σύστημα.
- Μεγάλη διείσδυση διεσπαρμένης παραγωγής μεσοπρόθεσμα και μακροπρόθεσμα.
- Η παραγωγή μεταφέρεται σε μεγάλο αριθμό παραγωγών αλλά σε μικρότερη κλίμακα.
- Ο έλεγχος του συστήματος μετακινείται και σε μικρότερη κλίμακα.
- Περισσότερη χρήση λογισμικού και έξυπνων ελέγχων με λιγότερο εξοπλισμό.
- Χρειάζεται περισσότερη έρευνα και επιδεικτικά έργα.
- Άρση των εμποδίων ώστε να διευκολυνθεί η διείσδυση των νέων τεχνολογιών.
- Δραστήριος Διαχειριστής Δικτύου με σύγχρονο Κώδικα Δικτύου, με νέες και καινοτόμες ιδέες και τεχνολογίες για τα μελλοντικά δίκτυα.

Κεφάλαιο 2
Κίνδυνοι στο έξυπνο ηλεκτρικό δίκτυο

2.1 Εισαγωγή

Το ηλεκτρικό δίκτυο όπως έχει αναφερθεί ήδη είναι βαθιά συνδεδεμένο με το διαδίκτυο. Αυτό είναι ένα γεγονός που επιφυλάσσει πολλούς κινδύνους στο ηλεκτρικό δίκτυο και ασφάλεια και προστασία των προσωπικών δεδομένων. Οι έξυπνοι μετρητές έχοντας ως στόχο την αλλαγή του ήδη υπάρχοντος ηλεκτρικού δικτύου και έχοντας βέβαια πολλά προβλήματα ασφάλειας, τα δεδομένα χρήστη ή το προφίλ του κατοίκου μπορούν να αποσπαστούν κακόβουλα με κακοπροαίρετη χρήση του ηλεκτρικού ρεύματος. Μέχρι στιγμής έχουν βρεθεί αρκετά βασικά ψεγάδια ασφάλειας στα συστήματα υπολογιστών που ελέγχουν γεννήτριες, διακόπτες και υποσταθμούς.

Σε ένα ηλεκτρικό δίκτυο έγκειται η εξής απορία. Σε ποιόν ανήκουν τα δεδομένα του πελάτη; Ποιος έχει πρόσβαση σε αυτά; Ποιος εγγυάται την ασφάλεια και την ιδιωτικότητα των προσωπικών δεδομένων; Είναι επιτρεπτή η πώληση ή η μεταφορά των δεδομένων, και αν ναι κάτω υπό ποιες συνθήκες και προς όφελος ποιου; Για παράδειγμα μια εταιρία παροχής ηλεκτρικού ρεύματος μπορεί να χρησιμοποιήσει τα αντίστοιχα δεδομένα για να προσαρμόσει το στρατηγικό της επιχειρηματικό πλάνο και να δημιουργήσει αντίστοιχες προσφορές.

2.2 Κίνδυνοι

Πέραν του γεγονότος ότι υπάρχουν ήδη κίνδυνοι που απειλούν ήδη τα συστήματα υπολογιστών και επικοινωνιών όπως malware, spyware και computer viruses, η εισαγωγή των νέων τεχνολογιών στο ηλεκτρικό δίκτυο όπως οι έξυπνοι μετρητές και τα επιπλέον υποδίκτυα προσθέτουν καινούριους κινδύνους. Τρύπες ασφάλειας μπορούν να επιτρέψουν στους hackers να εισβάλουν στο ηλεκτρικό δίκτυο μέσω των έξυπνων μετρητών για παράδειγμα. Μέσω αυτών των τρυπών ασφάλειας που υπάρχουν στους έξυπνους μετρητές (είτε ακόμα και από προεγκατεστημένη κακόβουλη δίοδο) μπορούν να γίνουν αλλαγές όπως στην αποστολή χαμηλότερου ποσού κατανάλωσης στον πάροχο ή ακόμα και αποστολή του λογαριασμού σε διαφορετική ταυτότητα ατόμου. Τα τείχη προστασίας όσο καλά δομημένα και να είναι δεν παρέχουν την εγγύηση της πλήρους προστασίας. Οι έξυπνοι μετρητές έχουν μια συνεχή διατήρηση επικοινωνίας και με άλλους μετρητές μέσα

στο ίδιο δίκτυο όπως επίσης και με έξυπνες οικιακές συσκευές και συστήματα διαχείρισης ενέργειας. Αυτές οι διασυνδέσεις αυξάνουν την έκθεση του έξυπνου δικτύου σε απομακρυσμένες απειλές όπως την υποκλοπή των προσωπικών δεδομένων και πληροφοριών. Διάφορες από τις νέες τεχνολογίες αυτές που μπορούν να εισαχθούν, διαθέτουν κάποιο σύστημα το οποίο επιτρέπει σε μηχανικούς από απομακρυσμένη πρόσβαση να εκτελέσουν διαδικασίες διάγνωσης και διαμόρφωσης. Αυτό βέβαια δίνει και την δυνατότητα απομακρυσμένου ελέγχου και από άτομα που δεν θα έπρεπε να είχαν πρόσβαση προσφέροντας τους τις εξής ικανότητες : κακόβουλη τροποποίηση δεδομένων και παραπλάνηση του διαχειριστή του συστήματος ελέγχου, πιθανή πρόκληση κάποιας ζημιάς στον εξοπλισμό ενός τομέα μετά από εφαρμογή μη ακριβών δεδομένων, και πιθανή απώλεια υπηρεσίας σε περίπτωση που ο εισβολέας απενεργοποιήσει τη συσκευή. Γενικότερα υπάρχει ο κίνδυνος μιας άμεσης πρόσβασης με μια οποιαδήποτε συσκευή με αποτέλεσμα τον κίνδυνο της ασφάλειας και προστασίας των προσωπικών δεδομένων. [3],[5]

Είδη κινδύνων συνοπτικά:

- Spyware
- Malware
- Computer viruses
- Νέες τεχνολογίες με ελλιπή δόμηση προστασίας για κακόβουλες εισόδους
- Hacking μέσω απομακρυσμένου ελέγχου

Αρνητικά αποτελέσματα αυτών των κινδύνων συνοπτικά:

- Έλλειψη ασφάλειας των προσωπικών δεδομένων
  - Υποκλοπή προσωπικών δεδομένων
  - Μετατροπή προσωπικών δεδομένων
- Ζημιά στον εξοπλισμό ενός τομέα
- Αλλαγή δεδομένων και παραπλάνηση του παρόχου (αλλαγή ποσού κατανάλωσης, αλλαγή ταυτότητας καταναλωτή)
- Απώλεια υπηρεσίας [5], [6]

Παρακάτω παρατίθεται μια επιπρόσθετη λίστα με μια σειρά από εξαιρετικά ορατά παραδείγματα επιθέσεων που θα μπορούσαν να δημιουργηθούν ενάντια στα έξυπνα δίκτυα:

- Καθυστέρηση, αποκλεισμός ή αλλοίωση της διαδικασίας παραγωγής ηλεκτρικής εγκατάστασης, με αποτέλεσμα την αλλαγή της ποσότητας ενέργειας που παράγεται.
- Καθυστέρηση, παρεμπόδιση ή τροποποίηση πληροφοριών που σχετίζονται με μια διαδικασία, σχετικά με την απόκτηση μετρήσεων παραγωγής που χρησιμοποιούνται στην εμπορία ενέργειας ή σε άλλες επιχειρηματικές δραστηριότητες, αποτρέποντας την μαζική παραγωγή ενέργειας.
- Ψευδείς πληροφορίες για την ζήτηση ή προσφορά ρεύματος που αποτέλεσμα τις λανθασμένες απαιτήσεις, που μπορεί να προκαλέσουν είτε διακοπή ρεύματος είτε υψηλές οικονομικές απώλειες.
- Σκόπιμη χειραγώγηση της αγοράς ενέργειας μέσω της αλλαγής των πληροφοριών σχετικά με την ζήτηση/προσφορά ενέργειας.
- Μία φυσική είτε και κυβερνητική επίθεση σε ένα μικρό ή μεγάλο ευάλωτο σημείο του έξυπνου δικτύου.
- Προπαγάνδα που δημιουργεί αρνητικό κλίμα, όπως για παράδειγμα η ιδέα ότι η ακτινοβολία των έξυπνων δικτύων δημιουργεί περισσότερα προβλήματα υγείας, χωρίς να υπάρχει κάποια αντίστοιχη απόδειξη.
- Έγκλημα που απευθύνεται σε μεγαλύτερη κλίμακα πληθυσμού ή και χωρών, απενεργοποιώντας ένα μεγάλο ποσοστό έξυπνων ηλεκτρικών συσκευών.
- Χακάρισμα των ιδιωτικών πληροφοριών στα στοιχεία των εκάστοτε έξυπνων δικτύων και συσκευών με στόχο τα προαναφερθέντα.

Οι αδυναμίες μπορούν να είναι διαφορετικού είδους (π.χ. διαχείριση, οργανωτική, κ.λπ.). Παρακάτω παρέχεται μια σύντομη λίστα των συστατικών στοιχείων των ICT (InformationandCommunicationTechnology) του έξυπνου δικτύου που πρέπει να θεωρηθούν ως πηγή αδυναμίας. Πρόκειται για μια κατηγοριοποίηση των υπηρεσιών υποδομής των υπηρεσιών κοινής ωφέλειας που μπορεί να έχουν αδυναμίες στον κυβερνοχώρο.

Η λίστα είναι η εξής:

• Λειτουργικά συστήματα: γεννήτριες, μετασχηματιστές, εποπτικός έλεγχος & δεδομένα, Συστήματα Αποκέντρωσης (SCADA) και Συστήματα Διαχείρισης Ενέργειας / Διανομής

(EMS / DMS),προγραμματιζόμενους λογικούς ελεγκτές (PLC), υποσταθμούς, έξυπνους μετρητές και άλλες έξυπνες ηλεκτρικές συσκευές (IED).

• Κλασσικά συστήματα πληροφορικής: υπολογιστές, κεντρικοί υπολογιστές, εφαρμογές, βάσεις δεδομένων, ιστότοποι, ιστός, υπηρεσίες, κ.λπ., μεταξύ των οποίων περιλαμβάνονται τα στοιχεία της εταιρικής υποδομής.

• Δίκτυα και πρωτόκολλα επικοινωνιών: Ethernet, Wifi, PRIME, DLMS / COSEM, Zigbee, 4G, DNP3, κλπ.

• Τερματικά σημεία: έξυπνοι μετρητές, HY, έξυπνα τηλέφωνα και άλλες κινητές συσκευές.

Για κάθε συγκεκριμένη περίπτωση πρέπει να γίνει μια διαδικασία εντοπισμού και αναγνώρισης αδυναμιών με σκοπό τον εντοπισμό όλων των τρωτών σημείων.

Ένα σύνολο αποτυχιών που μπορεί να προκαλέσουν προβλήματα:

- Αποτυχίες ασφαλείας: Έχουν αναπτυχθεί διαδικασίες και βελτιωθεί ξανά και ξανά για τη βελτίωση της ασφάλειας. Αν και αυτές οι διαδικασίες είναι το πιο σημαντικό συστατικό της ασφάλειας παρακολούθησης της κατάστασης του βασικού εξοπλισμού και της καταγραφής / συναγερμού του, η συμμόρφωση προς τις διαδικασίες ασφάλειας μέσω ηλεκτρονικών μέσων μπορεί να ενισχύσει την ασφάλεια σε σημαντικό βαθμό και μπορεί να ωφελήσει και άλλους σκοπούς. Για παράδειγμα, η ηλεκτρονική παρακολούθηση των μέτρων ασφαλείας εντός των υποσταθμών ηλεκτρικής ενέργειας μπορεί επίσης να συμβάλλει στην αποτροπή ορισμένων εσκεμμένων επιθέσεων, όπως είναι ο βανδαλισμός και η κλοπή.
- Αποτυχίες εξοπλισμού: Αυτές είναι οι πιο κοινές και αναμενόμενες απειλές για την αξιόπιστη λειτουργία του συστήματος ηλεκτρικής ενέργειας. Σημαντικές εργασίες έχουν αναληφθεί με την πάροδο των ετών: περιττές συνιστώσες και δίκτυα, παρακολούθηση της κατάστασης του εξοπλισμού κ.λπ.
- Απροσεξία: Συχνά η απροσεξία οφείλεται στην εφησυχασμό ("κανείς δεν έχει βλάψει ποτέ εξοπλισμό σε υποσταθμό ακόμα") ή τεμπελιά ("γιατί να ασχοληθούμε να κλειδώσουμε αυτή την πόρτα για τις λίγες στιγμές που πηγαίνω στην άλλη περιοχή") ή ερεθισμός ("αυτά τα μέτρα ασφάλειας επηρεάζουν την ικανότητά μου να κάνω τη δουλειά μου"). Παραδείγματα απειλών απροσεξίας περιλαμβάνουν: ακούσια ελευθερία εισόδου σε μη εξουσιοδοτημένο προσωπικό σε πρόσβαση σε κωδικούς, κλειδιά και άλλες διασφαλίσεις ασφαλείας ή για παράδειγμα η εφαρμογή ενημερώσεων,

διορθώσεων και άλλων αλλαγών στα λειτουργικά συστήματα και τον έλεγχο εφαρμογές χωρίς προηγούμενη δοκιμή σε ελεγχόμενο περιβάλλον.

- Οι φυσικές καταστροφές: οι καταιγίδες, οι τυφώνες και οι σεισμοί μπορούν να οδηγήσουν σε αποτυχίες του συστήματος, παραβιάσεις της ασφάλειας και ευκαιρίες κλοπής, βανδαλισμού και τρομοκρατίας. [7]

Στον Πίνακα 1 παρακάτω αναφέρονται οι αδυναμίες που εντοπίζονται στα έξυπνα ηλεκτρικά δίκτυα.

Πίνακας 1. Αδυναμίες έξυπνου δικτύου

Αδυναμίες	Εξήγηση
Ασφάλεια της ιδιωτικής ζωής των χρηστών	Οι πληροφορίες που συλλέγονται από έξυπνη παρακολούθηση μπορούν να χρησιμοποιηθούν για εισβολή στην ασφάλεια των χρηστών είτε από επιθέσεις στον κυβερνοχώρο είτε από φυσική πρόσβαση
Είσοδος των έξυπνων συσκευών	Οι έξυπνες συσκευές μπορούν να χρησιμοποιηθούν για να εισβάλει ένας χάκερ στο έξυπνο ηλεκτρικό δίκτυο
Η φυσική ασφάλεια των περιουσιακών στοιχείων	Η εγκατάσταση των συσκευών σε πολύ απομακρυσμένες και ανασφαλείς περιοχές αποτελεί απειλή για τη φυσική ασφάλειά.
Η διάρκεια ζωής των συστημάτων που χρησιμοποιούνται	Η χρήση παρωχημένων συστημάτων ισχύος με τα πιο πρόσφατα συστήματα επικοινωνίας αυξάνουν την πιθανότητα της ασφάλειας-επίθεσης, επιτρέποντας τη μη εξουσιοδοτημένη πρόσβαση στις παλιές συσκευές.
Διάδοση λάθους σήματος	Το λανθασμένο σήμα που παράγεται από μια συσκευή επηρεάζει την απόδοση όλων των συσκευών που λαμβάνουν αυτό το σήμα

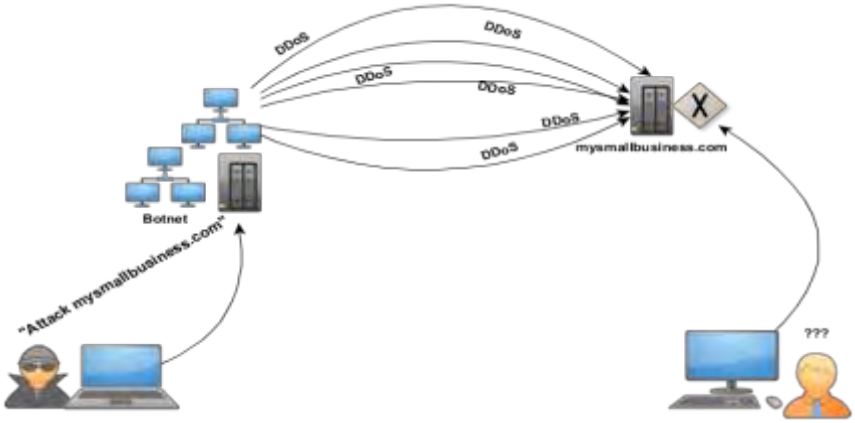
	και αλλάζει την κατάσταση τους
Επικοινωνιακό κενό μεταξύ διαφορετικών ομάδων	Το χάσμα επικοινωνίας μεταξύ διαφορετικών μηχανικών ομάδων ενδέχεται να προκαλέσει ανεπιθύμητες αλλαγές στην υποδομή καθώς και στην αύξηση αδυναμίας της αρχιτεκτονικής επικοινωνίας
Η χρήση παρωχημένου υλικού και λογισμικού συμβατό με το Διαδίκτυο Πρωτόκολλο (IP)	Οι παρωχημένες συσκευές που χρησιμοποιούνται είναι πολύ επιρρεπείς στις επιθέσεις ασφάλειας. Επίσης, το πρωτόκολλο Internet (IP) είναι συμβατό με τα περισσότερα ασύρματα πρότυπα αυξάνοντας την πιθανότητα μη εξουσιοδοτημένης πρόσβασης.
Μεγάλος αριθμός ενδιαφερόμενων μερών	Ο μεγάλος αριθμός ενδιαφερόμενων μερών αυξάνει το επίπεδο ανταγωνισμού και μπορεί να οδηγήσει σε εσωτερικές επιθέσεις.

Με βάση τις παραπάνω αδυναμίες που αναφέρθηκαν, γίνεται προφανές ότι το έξυπνο ηλεκτρικό δίκτυο είναι αρκετά ευάλωτο στους κινδύνους γενικότερα και σε διάφορους τύπους επιθέσεων που θα παρουσιαστούν στην παρακάτω ενότητα με περισσότερες λεπτομέρειες.

2.3 Τύποι επιθέσεων

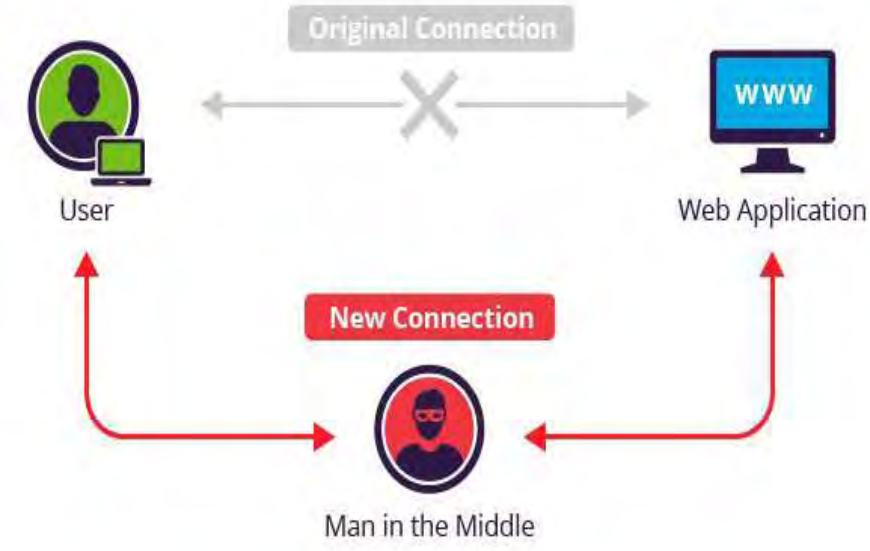
Παρακάτω παρουσιάζονται τέσσερις πολύ συχνοί τύποι επιθέσεων στο έξυπνο δίκτυο:

1. Denial-of-service (DOS) : Σε αυτήν την περίπτωση, ο επιτιθέμενος δεν επιτρέπει στην πηγή πρόσβαση στον προορισμό (Σχήμα 5). [8]



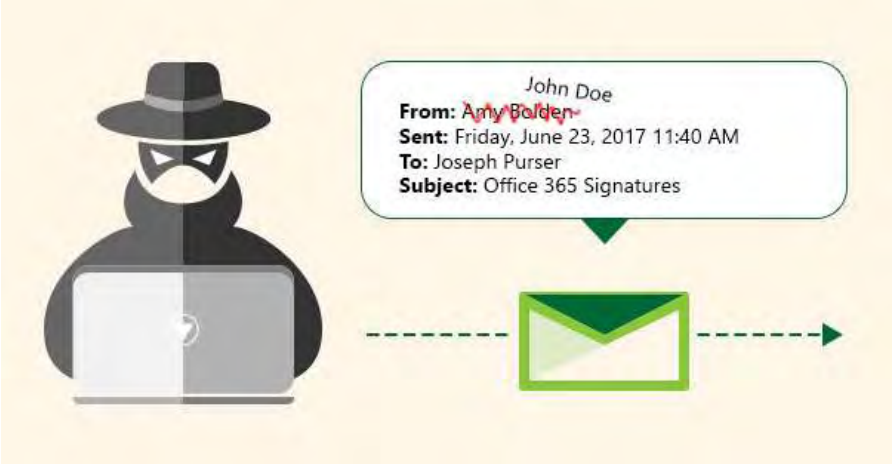
Σχήμα 5. Denial-of-service

2. Man-in-the-middle: Σε αυτήν την περίπτωση, ο επιτιθέμενος δεν επιτρέπει την νόμιμη επικοινωνία δύο νόμιμων μερών .Στην συνέχεια έχει τον έλεγχο της ροής επικοινωνίας και μπορεί να αποσπάσει ή και να αλλάξει πληροφορίες (Σχήμα 6). [9]



Σχήμα 6. Man-in-the-Middle

3. Spoofing: Σε αυτήν την περίπτωση ένα άτομο μεταμφιέζεται επιτυχώς σε ένα άλλο μέσω της παραποίησης δεδομένων, κερδίζοντας έτσι πλεονέκτημα στον έλεγχο (Σχήμα 7). [10]



Σχήμα 7. Spoofing

4. Eavesdropping: Σε αυτήν την περίπτωση, ο επιτιθέμενος παίρνει τις πληροφορίες που στέλνονται ανάμεσα σε δύο μέρη χωρίς αυτά να το γνωρίζουν.

Στον Πίνακα 2 παρακάτω αναφέρονται οι διαφορετικοί τύποι επιθέσεων ασφάλειας που μπορούν να γίνουν στο έξυπνο ηλεκτρικό δίκτυο.

Πίνακας 2. Επιθέσεις ασφάλειας

Επιθέσεις Ασφάλειας	Εξήγηση
Έγχυση κακόβολου λογισμικού	Η χρήση κακόβουλου λογισμικού για τη δυσλειτουργία των συσκευών ή των διακομιστών για την μετάδοση ευαίσθητων πληροφοριών
Εισβολή μέσω των συνδέσεων της βάσης δεδομένων	Η πρόσβαση σε κρίσιμα σημαντικά δεδομένα με στόχο την πρόκληση ζημιών σε λογική και φυσική υποδομή
Επιρροή στον εξοπλισμό των επικοινωνιών	Ο εξοπλισμός που χρησιμοποιείται για την επικοινωνία μπορεί να μπλοκαριστεί για να απενεργοποιήσει την επικοινωνία μεταξύ των συσκευών.
Δημιουργία ψευδών πληροφοριών	Η έγχυση λανθασμένων δεδομένων και σημάτων στο δίκτυο για

	πρόσβαση στις κρίσιμες συσκευές και κατά συνέχεια για πρόσβαση σε κρίσιμες πληροφορίες.
Διαθεσιμότητα δικτύου	Τα ασύρματα πρότυπα και τα πρωτόκολλα που χρησιμοποιούνται στο έξυπνο δίκτυο χρησιμοποιούνται ευρέως στο διαδίκτυο καθιστώντας τα ευάλωτα και προσβάσιμα από οποιαδήποτε απομακρυσμένη τοποθεσία.
Δυνατότητα ανάλυσης υποκλοπής	Η ικανότητα πρόσβασης και ανάλυσης των δεδομένων μπορεί να οδηγήσει σε μελλοντική εκτίμηση της τιμολόγησης ή της χρήσης ενέργειας
Έκδοση του πρωτοκόλλου ModBus	Το πρωτόκολλο ModBus που χρησιμοποιείται στα συστήματα SCADA δεν είναι έτοιμο να αντιμετωπίσει τις επιθέσεις. Επίσης είναι πολύ εύκολο να προσπελαστεί.

2.4 Παγκόσμιες δηλώσεις σχετικά με τους κινδύνους

Ναι μεν τα έξυπνα συστήματα θεωρούνται και είναι κρυπτογραφημένα, η κρυπτογράφηση συχνά αποτυγχάνει.

Για αυτόν τον λόγο και επειδή υπάρχουν πολλά προβλήματα ασφάλειας, ως «ηλίθιο» αποκάλεσε το έξυπνο δίκτυο ο πρώην διευθυντής CIA James Woolse καθώς είναι πολύ ευαίσθητο στις επιθέσεις με σκοπό την απόσπαση προσωπικών δεδομένων, την αλλαγή των χρεώσεων, την παρακολούθηση των ενοίκων.

Σύμφωνα με στοιχεία από το FBI, τέτοιου είδος επιθέσεων κοστίζουν στις εταιρείες παροχής ενέργειας 400.000.000 δολάρια ετησίως!

Οι επιθέσεις που αναφέραμε όμως είναι άκρως ρεαλιστικές. Μελέτη γνωστής εταιρείας ασφάλειας υπολογιστών έδειξε πόσο χειροτερεύουν τα πράγματα συνεχώς. «Ένα από τα πιο εντυπωσιακά αποτελέσματα της έρευνάς μας είναι η ανακάλυψη των συνεχών επιθέσεων που αντιμετωπίζουν αυτά τα κρίσιμα δίκτυα κοινής ωφέλειας. Μερικές ηλεκτρικές εταιρείες αναφέρουν χιλιάδες επιθέσεις κάθε μήνα».

Ειδικοί από το Εργαστήριο Υπολογιστών του Πανεπιστημίου Cambridge τονίζουν ότι εχθρικές κυβερνήσεις ή τρομοκράτες θα μπορούσαν να επηρεάσουν ή ακόμη και να διακόψουν την ηλεκτρική τροφοδοσία σε ένα έξυπνο δίκτυο.

“Δεν υπάρχει τρόπος να προβλέψουμε πώς θα χρησιμοποιηθούν αυτές οι τεράστιες δυνάμεις που θα συσσωρεύονται δυσανάλογα στα χέρια εταιρειών που αναζητούν οικονομικό πλεονέκτημα και κυβερνήσεων που θα επιθυμούν όλο και περισσότερο έλεγχο. Το πιο πιθανό είναι ότι η αποθήκευση δεδομένων και το Διαδίκτυο των Πραγμάτων θα κάνει πιο δύσκολο τον έλεγχο της ζωής μας, καθώς θα γινόμαστε όλο και περισσότερο διαφανείς σε ισχυρές εταιρείες και κρατικούς θεσμούς που γίνονται όλο και πιο αδιαφανείς για μας” Catherine Crump, Matthew Harwood, Αμερικανική Ένωση Πολιτικών Ελευθεριών (ACLU) [11]

“Όταν υπάρχει ένας νέος βολικός τρόπος να κάνουμε κάτι, πρέπει να εξετάσουμε την ασφάλεια. Είτε πρόκειται για πρόσβαση σε ένα σύστημα είτε σε μια φυσική τοποθεσία, οι μηχανισμοί εξουσιοδότησης πρέπει να είναι ισχυροί και δοκιμασμένοι για ευπάθειες. Για παράδειγμα, εξετάστε τα προβλήματα με την παρακολούθηση των baby monitors.“ Chris Kirby, Voices.com [12]

"Παρά τις υψηλού προφίλ επιθέσεις hacking, οι κατασκευαστές συσκευών παραμένουν ατάραχοι, εστιάζοντας στην κερδοφορία έναντι της ασφάλειας." [13]

”Αυτό που θα χάσετε είναι η ιδιωτικότητα σας. Στην πραγματικότητα είναι χειρότερα από αυτό. Δεν θα χάσετε απλά την ιδιωτικότητα σας. Θα πρέπει να βλέπετε την έννοια της ιδιωτικότητας να ξαναγράφετε κάτω από την μύτη σας ”. Περιοδικό WIRED [14]

Η πρώτη επίσημα αναφερθείσα περίπτωση παράνομης εισβολής στο έξυπνο δίκτυο στις Η.Π.Α. συνέβη τον Απρίλιο του 2009. Διαπιστώθηκε ότι έγιναν τυχαίες και επιτυχείς προσπάθειες διείσδυσης στο έξυπνο δίκτυο με στόχο την πρόκληση πολύ περισσότερων σοβαρών βλαβών. Το περιστατικό αυτό οδήγησε τις αρχές στην ανάπτυξη και την εφαρμογή κανονισμών που απαιτούνται για την αντιμετώπιση ζητημάτων ιδιωτικότητας του ευφυούς δικτύου, διατηρώντας παράλληλα την αξιοπιστία και την τεχνολογική του αποδοτικότητα. Στις ΗΠΑ, οι τεχνολογίες έξυπνων δικτύων είναι πιθανόν να απαιτούν διπλή πολιτική προστασίας της ιδιωτικής ζωής. Μία επίθεση στον κυβερνοχώρο σε ένα

ηλεκτρικό δίκτυο θα μπορούσε να συνεπάγεται μη εξουσιοδοτημένη πρόσβαση, τροποποίηση, διαγραφή ή / και κλοπή δεδομένων. Τα ζητήματα προστασίας της ιδιωτικής ζωής στο έξυπνο δίκτυο απαιτούν λεπτομερείς μελέτες και δημόσιες πληροφορίες, ώστε να μπορούν να προσαρμοστούν οι ισχύοντες νόμοι και να μπορούν με βάση αυτούς να δημιουργηθούν νέοι νόμοι. Επί του παρόντος, δεν υπάρχουν σαφώς καθορισμένοι νόμοι και κανονισμοί για την προστασία της ιδιωτικής ζωής στο έξυπνο δίκτυο. Θεωρείται ότι οι ισχύοντες νόμοι περί απορρήτου όπως ο νόμος Gramm-Leach-Bliley, ο νόμος για την προστασία του παιδιού στο Διαδίκτυο (CIPA), ο νόμος για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες (ECPA) και η προστασία που παρέχεται από την ιδιωτική ζωή στους οικείους νόμους(τέταρτη και δέκατη τέταρτη τροποποίηση του συντάγματος των Η.Π.Α.) μπορούν να τροποποιηθούν για να αντιμετωπίσουν τα σχετικά ζητήματα ιδιωτικού απορρήτου με χρήση τεχνολογίας έξυπνου δικτύου.
Υπάρχουν τρεις νομικές προσεγγίσεις για την προστασία της ιδιωτικής ζωής στο έξυπνο δίκτυο:

- Συνταγματική προστασία: καλύπτει προσωπική επικοινωνία και δραστηριότητες.
- Προστασία δεδομένων: καλύπτει συγκεκριμένα στοιχεία, όπως αριθμούς πιστωτικών καρτών και αριθμούς κοινωνικής ασφάλισης.
- Συμβατική προστασία: περιγράφεται για τις επιχειρηματικές συμβάσεις. Αξίζει να σημειωθεί ότι η εστίαση της τεχνολογίας των έξυπνων δικτύων στην Ευρώπη είναι πρωτίστως ως αποκλειστική πηγή παραγωγής ανανεώσιμης ενέργειας (σε αντίθεση με την αντίστοιχη χρήση στις ΗΠΑ που επικεντρώνεται στην ευκολία των τοπικών καταναλωτών).

Το ιταλικό έργο ENEL Telegestore είναι διαπιστευμένο ως το πρώτο και το μεγαλύτερο και έξυπνο δίκτυο έργου της Ευρώπης. Το ευφυές δίκτυο βιομηχανίας στην Ευρώπη δεν διαθέτει τη νομοθεσία και τους κανονισμούς για την προστασία της ιδιωτικής ζωής των έξυπνων δικτύων, σε αντίθεση με τις Ηνωμένες Πολιτείες που έχουν κάποιους ρυθμιστικούς φορείς και άλλες κυβερνητικές υπηρεσίες που συνεργάζονται για να εξασφαλίσουν την ιδιωτική ζωή των καταναλωτών του έξυπνου δικτύου. [15]

Πέραν από τις δηλώσεις έχουν υπάρξει και συγκεκριμένα περιστατικά όπου οι κίνδυνοι δημιούργησαν εν τέλει προβλήματα. Λαμβάνοντας υπόψη την παραγωγή ηλεκτρικής ενέργειας, τον Μάρτιο του 2008 ο πυρηνικός σταθμός Edwin I στη Γεωργία(ΗΠΑ), αναγκάστηκε να πραγματοποιήσει έκτακτη διακοπή λειτουργίας για 48 ώρες λόγω

ενημέρωσης λογισμικού. Αυτή η ενημέρωση λογισμικού εφαρμόστηκε στο σύστημα πληροφορικής που είναι επιφορτισμένο με την παρακολούθηση των χημικών ουσιών και των δεδομένων διάγνωσης από ένα από τα πρωτεύοντα συστήματα ελέγχου της εγκατάστασης. Μετά την εφαρμογή της ενημέρωσης, ο υπολογιστής επανεκκινήθηκε και αυτό οδήγησε στην έλλειψη και στο χάσιμο πληροφοριών παρακολούθησης. Το σύστημα ασφαλείας το παρερμήνευσε αυτό και σηματοδότησε ότι η στάθμη του νερού στα συστήματα ψύξης για τις ράβδους πυρηνικού καυσίμου είχε πέσει, πράγμα που προκάλεσε αυτόματη διακοπή λειτουργίας. Δεν υπήρχε κάποιος δημόσιος κίνδυνος, αλλά η εταιρεία ηλεκτρικής ενέργειας έχασε εκατομμύρια δολάρια σε έσοδα και έπρεπε να υποστεί και κάποιο ουσιαστική δαπάνη για την επαναλειτουργία.

Όσον αφορά τον τομέα διανομής και μετάδοσης, ένα από τα πιο σημαντικά περιστατικά θα μπορούσε να είναι η επίθεση που υπέστη το αμερικανικό ηλεκτρικό δίκτυο το 2009. Αξιωματούχοι των ΗΠΑ αναγνώρισαν ότι χάκερς από την Κίνα και τη Ρωσία είχαν εισβάλει στο ηλεκτρικό δίκτυο των ΗΠΑ και εγκατέστησαν κρυφό λογισμικό που θα μπορούσε να χρησιμοποιηθεί για διακοπή τροφοδοσίας.

Ο Mike Davis, σύμβουλος ασφάλειας, ασχολήθηκε με τις αδυναμίες ολόκληρης της αρχιτεκτονικής μέτρησης και ειδικότερα των έξυπνων μετρητών. Κατέδειξε ότι επιθέσεις στον κυβερνοχώρο θα μπορούσαν να χρησιμοποιηθούν για να αποκτήσουν απομακρυσμένο έλεγχο περίπου σε 15.000-22.000 σπίτια σε 24 ώρες. Για να το δείξουν, ο Mike Davis και η ομάδα του δημιούργησαν προσομοιωτή καθώς και ένα πραγματικό κομμάτι κακόβουλου λογισμικού (δηλ. ένα σκουλήκι) ικανό να αυτοαναδιπλασιαστεί και να αυτοδιεγείρεται σε μια περιοχή όπου όλα τα σπίτια είναι εξοπλισμένα με την ίδια μάρκα μετρητή. Το 2009 μια ηλεκτρική εταιρεία στο Πουέρτο Ρίκο τους ζήτησε από το FBI να βοηθήσει στη διερεύνηση εκτεταμένων περιστατικών κλοπών ισχύος που πίστευε ότι σχετίζονταν με τον έξυπνο μετρητή. Το FBI ανακάλυψε ότι πρώην υπάλληλοι κατασκευαστικής έξυπνων ηλεκτρικών μετρητών, πείραζαν έναντι μετρητών. Πιθανόν, χρησιμοποιούσαν μια οπτική σειριακή θύρα που τους επέτρεψε να συνδέσουν τους υπολογιστές τοπικά και να αλλάξουν τις ρυθμίσεις για την καταγραφή της κατανάλωσης ενέργειας. Αυτοί απλά χρειάζονταν ένα πρόγραμμα λογισμικού που θα μπορούσε να μεταφορτωθεί απευθείας από το Διαδίκτυο.[7]

Κεφάλαιο 3
Έξυπνοι μετρητές

3.1 Ορισμός έξυπνων μετρητών

Ένας έξυπνος μετρητής ηλεκτρικής ενέργειας (Σχήμα 8), είναι επί της ουσίας μια ασύρματη φορητή συσκευή νέας τεχνολογίας, η οποία έχει ως λειτουργία την παρακολούθηση και τον έλεγχο της ηλεκτρικής ενέργειας που καταναλώνεται, και τον υπολογισμό του κόστους λειτουργίας των ηλεκτρικών συσκευών που έχουμε στο σπίτι ή στην επιχείρηση σε πραγματικό χρόνο. Με την άμεση ενημέρωση μας, επιτυγχάνεται η ορθότερη χρήση και διαχείριση των συσκευών μας. Έτσι είναι εφικτή η άμεση μείωση της κατανάλωσης ενέργειας και πιθανή οικονομία στον λογαριασμό μας έως και 20%. Επειδή η κατανάλωση ενέργειας από καθημερινές συσκευές δεν είναι εφικτό να μετριέται, να ελέγχεται, να αξιολογείται και να συγκρίνεται λόγω του γεγονότος ότι υπάρχει ένας μηνιαίος ή ακόμα και διμηνιαίος λογαριασμός για όλα, για αυτό, ότι αλλαγή και να γίνει με στόχο την εξοικονόμηση ενέργειας, δεν μπορεί να είναι παρά υποθέσεις. Οι έξυπνοι μετρητές ηλεκτρικής ενέργειας, παρέχουν πλέον την δυνατότητα μέτρησης σε κάτι που θεωρούσαμε αόρατο και την δυνατότητα απόκτησης ελέγχου του ενεργειακού κόστους των συσκευών σας. Με έναν έξυπνο μετρητή ενέργειας παρέχονται στον χρήστη πληροφορίες σε οποιονδήποτε χρόνο για το σύνολο ή μεμονωμένα κομμάτια του εξοπλισμού, γίνεται σύγκριση του εξοπλισμού, αποφεύγονται διαρροές ενέργειας, αποκαλύπτονται υπερκαταναλώσεις ενέργειας, αποφεύγονται δαπανηρές αυξήσεις ζήτησης ισχύος, ακόμα και ακόμα γίνεται έλεγχος στην δραστικότητα προϊόντων εξοικονόμησης ενέργειας. Επίσης, ένα σημαντικό πλεονέκτημα είναι η προσφορά λεπτομερούς ανάλυσης της ενέργειας κάθε εξοπλισμού, οποιοδήποτε κτιρίου, ακόμα και όταν ο χρήστης δεν βρίσκεται στην επιχείρηση του, ανά πάσα στιγμή, από την άνεση μια κινητής συσκευής ή μέσω ενός προσωπικού ηλεκτρονικού υπολογιστή. Η ύπαρξη εξειδικευμένου λογισμικού δίνει την δυνατότητα να δει κάποιος πόση ενέργεια χρησιμοποίησε, να δει το προσωπικό κόστος, το περιβαλλοντικό κόστος, και αυτό για οποιαδήποτε χρονική περίοδο ζητήσετε. Μπορείτε επίσης να παρατηρηθεί η κατανάλωση και η απόδοση της ενέργειας, ανά ώρα, ημέρα ή οποιοδήποτε σενάριο σας εξυπηρετεί, καθώς επίσης και να γίνει σύγκριση μίας δεδομένης περιόδου με μία παρόμοια στο κοντινό παρελθόν. [16]

Σχήμα 8. Έξυπνοι μετρητές

Πλεονεκτήματα του έξυπνου μετρητή

- Μέτρηση σε πραγματικό χρόνο
- Εξοικονόμηση ενέργειας
- Απλή και γρήγορη εγκατάσταση
- Προηγμένη τεχνολογία

Υπάρχουν αρκετοί τύποι τέτοιων μετρητών με κυριότερους τους: [16]

- FLUKE 1750 και FLUKE 1760
- ACE 5000, ACE 6000, ACE 7000 ή ACTARIS SL7000
- Gran-Electro SS-101 και Gran-Electro SS-301
- CTC 5602 και CTC 5605
- Voltech - PM 3000
- AMPROBE DM-III
- Trinity Oracle Portable Power Analysis
- G4500 BLACKBOX Portable Power Quality Analyzer

3.2 Κίνδυνοι μέσω των έξυπνων μετρητών

Όπως όμως έχει ήδη αναφερθεί, παρά τα πλεονεκτήματα του, ο έξυπνος μετρητής είναι και ένα μέσο μέσω του οποίου μπορεί κάποιος hacker ή και γενικότερα οποιοσδήποτε και με λιγότερες γνώσεις να τον χρησιμοποιήσει για κακόβουλες πράξεις.

Για παράδειγμα μια πιθανή κακόβουλη πράξη όπως αναφέραμε είναι η αλλαγή δεδομένων και παραπλάνηση του παρόχου (αλλαγή ποσού κατανάλωσης, αλλαγή ταυτότητας καταναλωτή).

Ένας τρόπος για την αλλαγή του ποσού κατανάλωσης που δεν χρειάζεται εξειδικευμένες γνώσεις σύμφωνα με το FBI είναι η τοποθέτηση ενός ισχυρού μαγνήτη στον έξυπνο μετρητή. Ο μαγνήτης αποπροσανατολίζει την μέτρηση ενώ ταυτόχρονα η παροχή ενέργειας λειτουργεί κανονικά. Η τοποθέτηση γίνεται την νύχτα όπου μπορεί να λειτουργεί κάποια βαριά συσκευή σε θέμα κατανάλωσης (θέρμανση) έτσι ώστε να στείλει χαμηλότερη μέτρηση ενώ κατά την διάρκεια της ημέρας απομακρύνεται ο μαγνήτης όπου μπορεί να γίνει και κάποιος έλεγχος.

Ένας δεύτερος πιο εξειδικευμένος τρόπος σχετίζεται με πρώην υπαλλήλους εταιριών κατασκευής έξυπνων μετρητών, οι οποίοι τους τροποποιούν αναλόγως έτσι να ώστε να έρχεται το επιθυμητό κακόβουλο αποτέλεσμα.

Οι έξυπνοι μετρητές επίσης διαθέτουν λειτουργία απομακρυσμένου ελέγχου. Σε αυτήν την περίπτωση μπορεί κάποιος μη σχετιζόμενος με τον συγκεκριμένο έξυπνο μετρητή να πάρει τον έλεγχο του και να υποκλέψει τα προσωπικά στοιχεία του πελάτη, να τα τροποποιήσει ή και να αλλάξει τις ρυθμίσεις και προτιμήσεις του πελάτη και να προκαλέσει κάποιο υψηλότερο δυσμενές οικονομικό κόστος. [3]

Από την άλλη μεριά, ένα πλεονέκτημα του έξυπνου μετρητή μπορεί να μετατραπεί και σε κίνδυνος. Ένα παράδειγμα η μέτρηση σε πραγματικό χρόνο. Η συλλογή και επεξεργασία των προσωπικών δεδομένων των Ενόπλων Δυνάμεων, των στελεχών της Αστυνομίας και άλλων υπηρεσιών είναι πολύ ευαίσθητα θέματα.

Όσον αφορά τους έξυπνες μετρητές πλέον από μια άλλη σκοπιά.

Ισχύουν ως δεδομένα τα εξής :

- Η Κίνα είναι ο μεγαλύτερος κατασκευαστής Έξυπνων μετρητών στον κόσμο. [16]
- Το 24% του ΑΔΜΗΕ (Ανεξάρτητος Διαχειριστής Μεταφοράς Ηλεκτρικής Ενέργειας) ανήκει στην Κινεζική Κυβέρνηση, δηλαδή στο Κινεζικό Κομμουνιστικό Κόμμα.

Επίσης υπάρχουν και κάποια θέματα που δημιουργούν απορίες :

- Ποιος θα έχει πρόσβαση στον server στον οποίο θα καταλήγουν τα προσωπικά δεδομένα (Big Data) των έξυπνων μετρητών
- Οι έξυπνοι μετρητές αποτελούν εγγενή κίνδυνο για την Εθνική Ασφάλεια καθώς μέσω αυτών θα παρακολουθούνται τα στελέχη του Υπουργείου Εθνικής Άμυνας και της Αστυνομίας;
- Το γεγονός ότι το 24% του ΑΔΜΗΕ ανήκει στο ΚΚΚ αποτελεί εγγενή κίνδυνο εθνικής ασφαλείας; Στην Κίνα για παράδειγμα, το ΚΚΚ εφαρμόζει μεθόδους παρακολούθησης των Κινέζων πολιτών μέσω αλγόριθμων μέγα-δεδομένων [18].

Έλλειψη ελέγχου:

Η εφαρμογή των έξυπνων μετρητών δημιουργεί πολύπλοκες διαδικασίες επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Τα περισσότερα πρόσωπα στα οποία αναφέρονται τα δεδομένα δεν θα γνωρίζουν τη φύση αυτών των πράξεων, των οποίων οι οργανισμοί χρησιμοποιούν τα δεδομένα τους και τις πιθανές επιπτώσεις που θα μπορούσε να έχει αυτό για το ιδιωτικό τους απόρρητο. Βεβαίως, αν δεν γνωρίζουν την επεξεργασία των προσωπικών δεδομένων, τότε είναι αδύνατο να λάβουν τεκμηριωμένες αποφάσεις γι 'αυτό. Στην πράξη, μόλις εγκατασταθεί ένας έξυπνος μετρητής με ενεργοποιημένη συνδεσιμότητα, μπορεί να είναι δύσκολο για τους καταναλωτές να αποτρέψουν τη συσσώρευση δεδομένων μετρητών. Οι προμηθευτές ηλεκτρικής ενέργειας αναπτύσσουν έξυπνους μετρητές για μια αναμενόμενη διάρκεια ζωής 14 ετών κατά μέσο όρο. Ακόμη και αν οι καταναλωτές έχουν κατανοήσει αρχικά τις συνέπειες νέων συσκευών, η επεξεργασία δεδομένων μετρητών ενδέχεται να εξελίσσεται καθ 'όλη τη διάρκεια ζωής του μετρητή και μπορεί τελικά να αποτελέσει ουσιαστικό μέρος των έξυπνων κατοικιών. Αυτό μπορεί να αυξήσει ακόμη περισσότερο την πολυπλοκότητα της επεξεργασίας. Επιπλέον, οι μελλοντικές έρευνες και αναλύσεις μπορούν να επιτρέψουν την εξαγωγή λεπτομερέστερων συμπερασμάτων σχετικά με τις δραστηριότητες ενός ατόμου, χρησιμοποιώντας τα δεδομένα μετρητών.

Μαζική επιτήρηση:

Οι πληροφορίες σχετικά με την κατανάλωση ενέργειας σε πραγματικό χρόνο μπορούν να έχουν υψηλή εμπορική αξία. Εάν δεν υπάρχουν επαρκείς διασφαλίσεις για να διασφαλιστεί ότι μόνο εξουσιοδοτημένα τρίτα μέρη μπορούν να έχουν πρόσβαση και να επεξεργάζονται δεδομένα για σαφώς προσδιορισμένους σκοπούς και σύμφωνα με τον ισχύοντα νόμο περί προστασίας δεδομένων, η χρήση έξυπνης μέτρησης μπορεί να οδηγήσει στην παρακολούθηση της καθημερινής ζωής των ανθρώπων στα σπίτια τους και στην απόκτηση λεπτομερών στοιχείων όλων των ατόμων με βάση τις εγχώριες δραστηριότητές τους.

Υπό ορισμένες συνθήκες, τα προφίλ ενδέχεται να εμπλουτιστούν με δεδομένα προσωπικού χαρακτήρα που προέρχονται από έξυπνες κατοικίες και άλλες πηγές στο διαδίκτυο και εκτός σύνδεσης. Αυτά τα προφίλ θα μπορούσαν στη συνέχεια να χρησιμοποιηθούν για πολλούς άλλους σκοπούς, συμπεριλαμβανομένου του μάρκετινγκ και της διαφήμισης.

Οι υπηρεσίες επιβολής του νόμου, οι φορολογικές αρχές, οι ασφαλιστικές εταιρείες, οι ιδιοκτήτες, οι εργοδότες και άλλοι τρίτοι ενδέχεται επίσης να ενδιαφέρονται για την πρόσβαση σε προσωπικές πληροφορίες κατανάλωσης ενέργειας. Ένα δίκτυο έξυπνων μετρητών με αμφίδρομες επικοινωνίες θα μπορούσε επίσης να γίνει μέρος μιας υποδομής μαζικής επιτήρησης. Αυτό θα μπορούσε τεχνικά να επιτευχθεί με μια απλή ενημέρωση του υλικολογισμικού για να μειωθούν τα διαστήματα μέτρησης και μεταφοράς. Οι έξυπνοι μετρητές που συνδέονται με έξυπνες οικιακές συσκευές είναι πιο ευάλωτοι σε παραβιάσεις δεδομένων μετρητών.

Γενικοί κίνδυνοι που είναι κοινοί στις συσκευές IoT

Οι έξυπνοι μετρητές και οι έξυπνες οικιακές συσκευές υπάγονται στην κατηγορία των συσκευών Internet of Things (IoT), καθώς διαθέτουν σύνδεση δικτύου, αισθητήρες και χειριστήρια για να αλληλοεπιδράσουν με το τοπικό τους περιβάλλον. Κατά συνέπεια, οι έξυπνοι μετρητές και κατοικίες μοιράζονται επίσης τους κινδύνους που προέρχονται από συσκευές ή δίκτυα διαδικτύου. Γενικά, οι κίνδυνοι αυξάνονται με τον αριθμό συνδεδεμένων συσκευών που είναι ενσωματωμένες στο έξυπνο σπίτι, ειδικά εάν αυτές οι συσκευές επιτρέπουν τη σύνδεση με μη ασφαλείς δίκτυα.

Όπου οι έξυπνοι μετρητές συνδέονται με έξυπνες οικιακές συσκευές ή το διαδίκτυο και διακυβεύονται, θα μπορούσαν να βλάψουν ή να μολύνουν άλλες ευάλωτες ή ευαίσθητες συσκευές ή υπηρεσίες, όπως κινητά τηλέφωνα, υπολογιστές, κάμερες ασφαλείας, έξυπνες κλειδαριές ή δημόσιες υπηρεσίες ιστού. Αντίθετα, η μη εξουσιοδοτημένη πρόσβαση σε έξυπνες συσκευές μέτρησης μέσω άλλων συσκευών σε ένα έξυπνο σπίτι θα μπορούσε να θέσει σε κίνδυνο τις λειτουργίες του έξυπνου μετρητή, συμπεριλαμβανομένης της παροχής ενέργειας. Οι έξυπνοι μετρητές με δυνατότητα σύνδεσης στο δίκτυο ενδέχεται να υπόκεινται σε μη εξουσιοδοτημένη πρόσβαση. Οι κακοί παραγωγοί ενδέχεται να αποσπάσουν δεδομένα κατανάλωσης ή να θέσουν σε κίνδυνο το υλικολογισμικό για να καταγράφουν συστηματικά τις ψευδείς τιμές κατανάλωσης, για παράδειγμα. Προκειμένου να προστατευθούν οι καταναλωτές και το ηλεκτρικό δίκτυο ως υποδομή ζωτικής σημασίας, ορισμένες χώρες της ΕΕ απαιτούν ολοκληρωμένες πιστοποιήσεις για έξυπνους μετρητές και συναφή στοιχεία.

Για να εξασφαλιστεί υψηλό επίπεδο ασφάλειας, οι έξυπνοι μετρητές και οι οικιακές συσκευές πρέπει να ενημερώνονται τακτικά με επιδιορθώσεις ασφαλείας και αναβαθμίσεις καθ 'όλη τη διάρκεια του κύκλου ζωής τους.

Η χρήση του προτύπου αξιολόγησης αντίκτυπου προστασίας δεδομένων (DPIA) για το έξυπνο δίκτυο και τα συστήματα έξυπνης μέτρησης ως εργαλείο αξιολόγησης και λήψης αποφάσεων μπορεί να στηρίξει περαιτέρω τους φορείς εκμετάλλευσης έξυπνων δικτύων. [19]

Προστασία δεδομένων από το σχεδιασμό:

Απαιτείται από τους ελεγκτές να εφαρμόζουν τα κατάλληλα τεχνικά και οργανωτικά μέτρα τόσο κατά τον προσδιορισμό των μέσων επεξεργασίας όσο και κατά τη στιγμή της ίδιας της επεξεργασίας.

Η δυνατότητα των χρηστών να επιλέγουν μεγάλα διαστήματα μέτρησης θα μπορούσε να μειώσει την ακρίβεια των συμπερασμάτων που προέκυψαν χρησιμοποιώντας δεδομένα έξυπνου μετρητή. Οι καταναλωτές θα μπορούσαν επίσης να έχουν τη δυνατότητα να απενεργοποιήσουν και να ενεργοποιήσουν ορισμένες έξυπνες λειτουργίες του έξυπνου μετρητή τους σε ορισμένες περιπτώσεις.

Επιπλέον, η ανάπτυξη τεχνολογιών ενίσχυσης της ιδιωτικής ζωής (PETs) μπορεί να μειώσει τους κινδύνους που προκύπτουν από την εξαγωγή συμπερασμάτων από τα δεδομένα χωρίς να αλλάξει το διάστημα μέτρησης. Παραδείγματα τέτοια είναι: η κρυπτογράφηση δεδομένων μετρητή, διαφορετικές χρονικές αναλύσεις θα μπορούσαν να κρυπτογραφηθούν με διαφορετικά κλειδιά για την εξυπηρέτηση διαφορετικών σκοπών, διαφορετικών απαιτήσεων ακρίβειας και να διανεμηθούν σε βάση ανάγκης, καλύπτοντας τα πρωτόκολλα κάλυψης που επιτρέπουν την ασφαλή συσσωμάτωση δεδομένων, ομοιομορφική κρυπτογράφηση για τη συγκέντρωση δεδομένων μετρητών πολλών νοικοκυριών. [19]

Κεφάλαιο 4
Ασφάλεια

4.1 Εισαγωγή

Το σημαντικό θέμα όμως είναι να ενταχθεί κάποια ασφάλεια για την αντιμετώπιση αυτών των κινδύνων. Ο όρος ασφάλεια στους ενεργειακούς μηχανισμούς χρησιμοποιείται για εξηγήσει την ικανότητα που έχει το ηλεκτρικό δίκτυο να αντιμετωπίζει πιθανές απροσδόκητες προκλήσεις όπως για παράδειγμα μη αναμενόμενες απώλειες στοιχείων του συστήματος χάρη σε βραχυκυκλώματα για παράδειγμα. Ο όρος ασφάλεια δεν υπάρχει για να περιγράφει μόνο την αξιοπιστία του συστήματος ηλεκτρικής ισχύος αυτού καθ' αυτού, αλλά έγκειται και στην ασφάλεια επιπλέον ηλεκτρικών συστημάτων που χρησιμοποιούνται ως επιπλέον για να ενισχύσουν την ηλεκτρική ισχύ. Δηλαδή, περιέχει ακόμη την πιθανότητα να μπορεί να χαθεί πλήρως ένα μήνυμα. Επίσης ως επιπρόσθετο εμπεριέχει τη διαδικασία ανάθεσης προτεραιότητας σε ορισμένα μηνύματα όταν τα κανάλια επικοινωνίας είναι κατειλημμένα (QoS: Quality of Service). Τέλος, ο όρος ασφάλεια σε μία πιο γενική εξήγηση αναφέρεται στα μέτρα που παίρνονται με στόχο την διασφάλιση της προστασίας της πληροφορίας, την ανωνυμία της ηλεκτρονικής πληροφορίας κατά την διαδικασία μετάδοσης και της αποθήκευσης στα ψηφιακά συστήματα. Πολύ σημαντικής αξίας θεωρούνται οι πληροφορίες που σχετίζονται με τις προσωπικές πληροφορίες των πεατών0καταναλωτών όπως επίσης και οι εντολές για την χρήση του έξυπνου δικτύου. Ο όρος ασφάλεια που αναφέρθηκε ακριβώς πάνω χρειάζεται γιατί η σχεδίαση των συστημάτων των νέων αυτών τεχνολογιών είχε περισσότερο βάρος στα αποκλειστικά-ιδιωτικά λειτουργικά συστήματα που σχεδιάζονται για έλεγχο λειτουργικότητας και απόδοσης, και όχι στην ασφάλεια. Χωρίς να έχει γίνει εξέταση ασφάλειας στον κυβερνοχώρο έχουν χρησιμοποιηθεί πρωτόκολλα και τεχνολογίες που σχεδιάστηκαν για συνδεσιμότητα. Αυτά που μόλις αναφέρθηκαν συντέλεσαν αρκετά στην αύξηση των κινδύνων που αναφέρθηκαν πριν. [20]

Για να θεωρείται γενικά ένα σύστημα ασφαλές θα πρέπει να πληροί κάποιες συγκεκριμένες προδιαγραφές.

- Αρχικά είναι η εμπιστευτικότητα. Δηλαδή η πρόληψη μη εξουσιοδοτημένης αποκάλυψης πληροφοριών. Δηλαδή να μην υπάρχει ο κίνδυνος να βρεθούν οι προσωπικές πληροφορίες οποιουδήποτε χρήστη σε μη εξουσιοδοτημένα άτομα.
- Κατά συνέχεια είναι η ακεραιότητα. Δηλαδή η πρόληψη της μη εξουσιοδοτημένης

μεταβολής των πληροφοριών. Δηλαδή να μην είναι εφικτό από μη εξουσιοδοτημένα άτομα να μεταβάλουν της πληροφορίες του συστήματος.

- Και τέλος είναι η διαθεσιμότητα. Δηλαδή να είναι διαθέσιμες οι πληροφορίες χωρίς κάποια καθυστέρηση που να προκύπτει από μη εξουσιοδοτημένα άτομα.[21]

4.2 Τακτικές επίτευξης ασφάλειας στο έξυπνο δίκτυο

Για να μπορέσει να επιτευχθεί λοιπόν η επιθυμητή ασφάλεια και να ελαχιστοποιηθούν οι κίνδυνοι υπάρχουν ορισμένες τακτικές που μπορούν να το φέρουν εις πέρας.

Κλιμάκωση: με αυτόν τον τρόπο ένα σύστημα μπορεί να αυξομειώνει την χωρητικότητα του με στόχο να προστατεύσει ένα αντίστοιχο μέγεθος συστήματος αυτοματισμού του δικτύου (π.χ. περισσότερες ή λιγότερες ηλεκτρονικές συσκευές και χρήστες) με απλό και λειτουργικό τρόπο. Μέσα σε αυτήν την διαδικασία, πρέπει να γίνετε σωστή διατήρηση του επιπέδου σε όλους τους τομείς του δικτύου.

Επεκτασιμότητα: αναφέρεται σε σύστημα το οποίο θα περιλαμβάνει ειδικούς κατασκευαστικούς μηχανισμούς που θα επιτρέπουν την επέκταση του χωρίς να πρέπει να γίνουν πολλές αλλαγές. Έτσι θα μπορεί να εντάσσει εύκολα κάποια καινούργια τεχνολογία ή ένα καινούργιο σύστημα ασφαλείας καθώς οι κίνδυνοι και οι επιθέσεις αυξάνονται

Δια-λειτουργικότητα: αναφέρεται στο πόσο ικανό είναι ένα σύστημα να μπορεί να λειτουργήσει ταυτόχρονα μαζί με άλλα συστήματα. Επειδή υπάρχουν πολλές τεχνολογίες, υλικό, πρωτόκολλα ασφαλείας και επικοινωνιών, πρέπει να μπορούν να λειτουργήσουν όλα μαζί για να προστατευτεί πιο έμπιστα το σύστημα.

Μη-διεισδυτικότητα: αναφέρεται στο να μπορεί ένα σύστημα να ανακατεύεται με πολλές λειτουργίες χωρίς όμως ταυτόχρονα να μειώνεται η απόδοση του ή να θέτει σε κίνδυνο τις λειτουργίες ελέγχου. Πολλά συστήματα, είτε λόγω παλαιότητας είτε λόγω μη επένδυσης σε αυτά διαθέτουν είτε μικρό χώρο μνήμης είτε δεν έχουν δυνατή απόδοση. Άσχετα με αυτό όμως οποιοδήποτε νέο πρωτόκολλο ασφαλείας, πρέπει να εντάσσεται άμεσα και χωρίς συμβιβασμούς αξιοπιστίας

Ευελιξία: αναφέρεται στο πόσο μπορεί να προσαρμόζεται το σύστημα σε διάφορες καταστάσεις που μπορεί να πρέπει, για παράδειγμα στην αναβάθμιση και πολύ σημαντικό σε πραγματικό χρόνο λειτουργίας. Πρέπει να μπορεί να προσαρμόζεται και να επεκτείνεται με βάση νέα χαρακτηριστικά από καινούργιες τεχνολογίες, χωρίς φυσικά αυτό να επηρεάζει την προηγούμενη λειτουργικότητα ή να μειώνει την απόδοση και την ισχύ.

Επίσης θα έπρεπε να υπάρχει ένα σύστημα εντοπισμού εισβολών. Ένα σύστημα που να εντοπίζει τις εισβολές και να τις ταξινομεί κατάλληλα με βάση έναν συγκεκριμένο αλγόριθμο.

Ένας μηχανισμός εντοπισμού ανωμαλιών. Όταν κάποιος δεν γνωρίζει ακριβώς την πληροφορία, εισβάλει στην ηλεκτρονική συσκευή. Τότε θα μπορούσε να μετριέται ο αριθμός των αποτυχιών του. Σαν αποτέλεσμα, καταγράφονται αποτυχημένες προσπάθειες, και η συσκευή θα μπορούσε να έχει ένα συγκεκριμένο όριο προσπαθειών και μετά να κλειδώνει. Αν καταφέρει και εισβάλει στο σύστημα, μπορεί να προσπαθήσει να αποσυνδέσει γραμμές μεταφοράς ενέργειας ή να αλλάξει τις ρυθμίσεις των κύριων μετασχηματιστών. Μία άλλη πιθανή πράξη είναι η προσπάθεια επαναφοράς στις εργοστασιακές ρυθμίσεις, με σκοπό την διαγραφή στοιχείων και ρυθμίσεων που ήταν απαραίτητα για τη λειτουργία του συστήματος. Οι πιο κοινές πράξεις που γίνονται κακόβουλα είναι οι εξής και με βάση αυτές θα μπορούσε να ενισχυθεί το σύστημα:

- Καταμέτρηση των προσπαθειών εισβολής
- Τροποποίηση των αρχείων και των ρυθμίσεων του συστήματος όπως επίσης και της κατάστασης του

Με αυτόν τον τρόπο όταν κάποιος κακόβουλος προσπαθεί να κάνει κάτι από το παραπάνω, ο αντίστοιχος μηχανισμός θα το αντιληφθεί ότι γίνεται χωρίς κάποια εξουσιοδότηση και μπορεί να απενεργοποιήσει την αντίστοιχη συσκευή με στόχο την πρόληψη. [21]

Ο έξυπνος μετρητής είναι μια πιθανή λύση σχετικά με την προστασία των προσωπικών πληροφοριών παρά τους κινδύνους που αναφέραμε. Ο έξυπνος μετρητής μπορεί να λειτουργήσει σαν μια πύλη δικτύου ανάμεσα σε εσωτερικές και εξωτερικές οντότητες. Οι διαδικασίες που θα χρειάζονται πλέον θα γίνονται μέσω των έξυπνων ηλεκτρικών μετρητών. Είναι απαραίτητο φυσικά όμως ότι ο ίδιος ο καταναλωτής θα έχει βάλει σε κάποια σειρά προτεραιότητας της προτιμήσεις του σχετικά με τις συσκευές. Έτσι

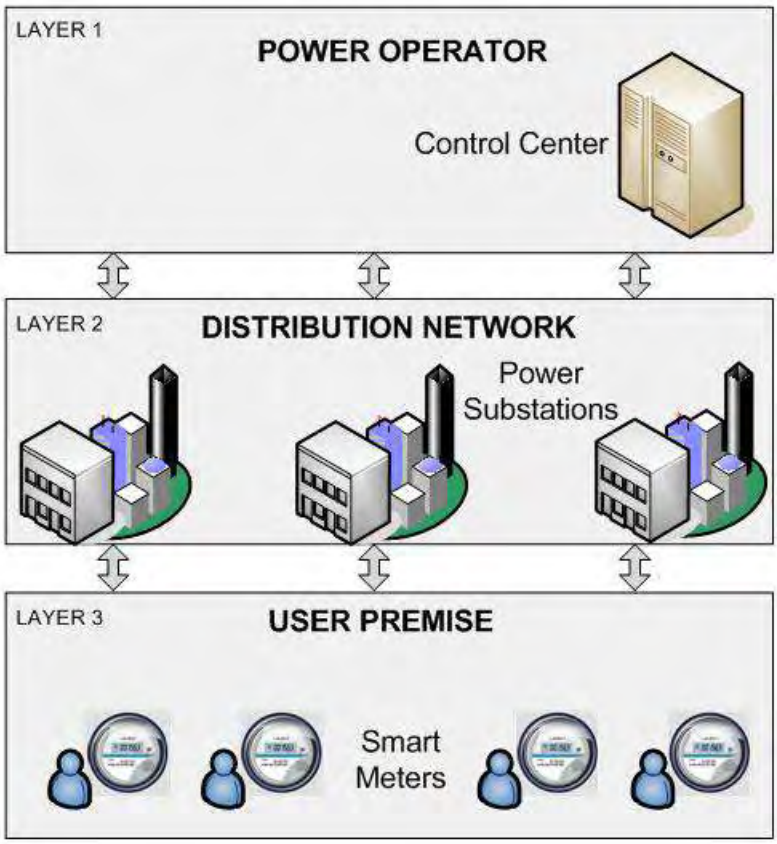
μέσω των έξυπνων μετρητών αποκρύπτονται οι προσωπικές πληροφορίες από τον πάροχο και κατά συνέχει από κάποιο κακόβουλο τρίτο άτομα που μπορεί να προσπαθήσει να τα υποκλέψει. [20], [21]

Βέβαια υπάρχουν και κάποιες δευτερεύουσες έννοιες ασφάλειας των πληροφοριακών συστημάτων:

- Εξουσιοδοτημένη χρήση (authorized use)—άτομα τα οποία έχουν συγκεκριμένη εξουσιοδότηση για να χρησιμοποιήσουν το σύστημα ή οποιαδήποτε από τις περιφερειακές συσκευές που το πλαισιώνουν.
- Αυθεντικοποίηση μηνυμάτων (message authentication)—η έννοια του να γνωρίζουμε με σιγουριά ότι το άτομο που ισχυρίζεται το σύστημα ότι έστειλε το μήνυμα είναι όντως σωστό.
- Αξιοπιστία (reliability) και σιγουριά (safety)—η ασφάλεια (security) είναι στενά συνδεδεμένη με αυτή, και αναφέρεται στο πόσο αξιόπιστο θα είναι σύστημα σε δύσκολες συνθήκες. [21]

Ας αναφερθούμε σε μια άλλη διαδικασία:
Ένα έξυπνο ηλεκτρικό δίκτυο θα μπορούσε να χωριστεί σε τρία βασικά επίπεδα: Στο υψηλότερο επίπεδο όπου υπάρχει ένα κέντρο ελέγχου. Το δεύτερο στρώμα έχει υποσταθμούς μέσα στο δίκτυο διανομής και κάθε υποσταθμός είναι υπεύθυνος για την παροχή ρεύματος σε μια περιοχή και το χαμηλότερο στρώμα έχει τους έξυπνους μετρητές που είναι τοποθετημένοι στην οθόνη του χρήστη, όπως φαίνεται στο Σχήμα 9. Η προτεινόμενη αρχιτεκτονική διατηρεί το απόρρητο των χρηστών συμπεριλαμβανομένων των καθημερινών προτύπων χρήσης ηλεκτρικής ενέργειας από τρίτους καθώς και από τον φορέα παροχής ηλεκτρικής ενέργειας. Η διαδικασία βασίζεται σε τυφλές υπογραφές. Οι τυφλές υπογραφές είναι μια μέθοδος που επιτρέπει στο πρώτο μέρος (Μέρος 1) να υπογράψει ένα μήνυμα που παράγεται από ένα δεύτερο μέρος (Μέρος 2), χωρίς να γνωρίζει το πραγματικό του περιεχόμενο. Όταν ένα τρίτο μέρος (Μέρος 3) λαμβάνει το υπογεγραμμένο μήνυμα, μπορεί να επιβεβαιώσει ότι το μήνυμα έχει υπογραφεί από το μέρος 1. Το σύστημα ανώνυμων διαπιστευτηρίων χρησιμοποιεί αυτή την τεχνική που επιτρέπει στο κέντρο ελέγχου (συμβαλλόμενο μέρος 1) να υπογράψει μια πιστοποίηση που παράγεται από έναν πελάτη (μέρος 2) χωρίς να γνωρίζει το πραγματικό του περιεχόμενο.

Σε μεταγενέστερο χρόνο, το ίδιο το κέντρο ελέγχου (Μέρος 3) μπορεί να επαληθεύσει ότι η βεβαίωση είναι πράγματι υπογεγραμμένη από το συμβαλλόμενο μέρος 1 χωρίς να γνωρίζει ποιος ζήτησε την υπογραφή ή πότε δημιουργήθηκε η υπογραφή. Η χρήση της τεχνικής της τυφλής υπογραφής σε αυτό το σχήμα έχει ως εξής: Οι πελάτες προετοιμάζουν ένα σύνολο διαπιστευτηρίων, το καθένα δηλώνει τη ζητούμενη ποσότητα ηλεκτρικής ενέργειας και ζητάει από το κέντρο ελέγχου να τα υπογράψει τυφλά ώστε ο πελάτης να μπορέσει να υποβάλει οποιαδήποτε από αυτά τα διαπιστευτήρια για το αίτημα της ηλεκτρικής ενέργειας. Δεδομένου ότι το Μέρος 1 δεν γνωρίζει το πραγματικό περιεχόμενο του μηνύματος που αποστέλλεται από το Μέρος 2, το μήνυμα επαληθεύεται χρησιμοποιώντας μια ειδική τεχνική που υιοθετείται ευρέως σε συστήματα ηλεκτρονικών μετρητών.



Σχήμα 9. Το ηλεκτρικό δίκτυο σε υποστρώματα. [15]

Υπάρχουν δύο προτεινόμενες λύσεις. Η πρώτη είναι μια έξυπνη παραλλαγή δικτύου σε μια τεχνική που χρησιμοποιείται ήδη για την προστασία ιδιωτικών πληροφοριών που συλλέγονται για βάσεις δεδομένων υγείας ή από υπηρεσίες Διαδικτύου όπως το Google και το Amazon. Αναφέρεται στην ανωνυμία δεδομένων. Προκειμένου το

έξυπνο δίκτυο να κάνει έξυπνα πράγματα, όπως η πιο ομοιόμορφη κατανομή ισχύος, πρέπει να έχει λεπτομερείς και συχνές πληροφορίες σχετικά με τη χρήση ενέργειας και μια γενική ιδέα για το ποιες γεωγραφικές περιοχές χρησιμοποιούν ενέργεια, λένε οι ερευνητές. Αλλά το βοηθητικό πρόγραμμα δεν χρειάζεται απαραίτητα να γνωρίζει σε ποιον ανήκουν τα δεδομένα αυτά. Τα ενεργειακά δεδομένα, με άλλα λόγια, δεν χρειάζεται να συνδέονται με ένα συγκεκριμένο νοικοκυριό για να είναι χρήσιμα στη διαχείριση του δικτύου. Το σύστημα της Toshiba θα αποκρύψει μια έξυπνη διεύθυνση μετρητή πριν από την αποστολή δεδομένων για την κατανάλωση ενέργειας σε βοηθητικά προγράμματα, με τον ίδιο τρόπο που ένας ανώνυμος διακομιστής μεσολάβησης Internet μπορεί να αποκρύψει τη διεύθυνση IP ενός υπολογιστή προτού στείλει δεδομένα σε άλλα δίκτυα. Το πρόβλημα με την παροχή αυτής της ευθύνης στις επιχειρήσεις είναι ότι πολλοί καταναλωτές δεν τους εμπιστεύονται, λένε οι ερευνητές. Πράγματι, η έκθεση του Απριλίου του Accenture διαπίστωσε ότι λιγότερο από το ένα τρίτο των ερωτηθέντων καταναλωτών δήλωσαν ότι εμπιστεύονται τους παρόχους ηλεκτρικής ενέργειας για να τους παρέχουν καλές συμβουλές σχετικά με τη χρήση ενέργειας. Η εμπιστοσύνη είναι ιδιαίτερα χαμηλή σε χώρες όπως η Γερμανία και το Ηνωμένο Βασίλειο, όπου οι επιχειρήσεις ηλεκτρικής ενέργειας έχουν απελευθερωθεί και οι καταναλωτές αλλάζουν τακτικά τους παρόχους, "Ο λόγος που οι πελάτες δεν εμπιστεύονται δεν είναι επειδή πιστεύουν ότι οι πάροχοι κάνουν κάτι αμφίβολο", λέει ο GregGuthridge, διευθύνων σύμβουλος της πρακτικής φροντίδας πελατών της Accenture. Αντίθετα, οι πελάτες δεν εμπιστεύονται τις επιχειρήσεις κοινής ωφέλειας επειδή έχουν ελάχιστες αλληλεπιδράσεις μαζί τους, οι περισσότερες από τις οποίες είναι δυσάρεστες - αναφέροντας μια διακοπή ρεύματος, για παράδειγμα, ή αμφισβητώντας ένα λογαριασμό υψηλής ισχύος. Ο Guthridge πιστεύει ότι οι επιχειρήσεις κοινής ωφέλειας μπορούν ακόμα να κερδίσουν την εμπιστοσύνη των καταναλωτών εάν επικοινωνούν με σαφήνεια. Οι ερευνητές της Toshiba προτείνουν την παροχή υπηρεσιών τρίτου μέρους για την ανωνυμοποίηση και τη διαχείριση λεπτομερών δεδομένων σχετικά με την κατανάλωση ενέργειας. Σε αυτή την περίπτωση, μόνο η υπηρεσία αυτή θα μπορούσε να είναι ο κατασκευαστής ενός έξυπνου μετρητή και θα ήταν σε θέση να επικοινωνήσει με τα κρυπτογραφημένα στοιχεία συλλογής δεδομένων που είναι ενσωματωμένα στο έξυπνο μετρητή, εξηγούν οι ερευνητές. Οι μόνες αναγνωρίσιμες πληροφορίες που θα μπορούσε να έχει ένα βοηθητικό πρόγραμμα απευθείας από τον έξυπνο μετρητή θα είναι οι πληροφορίες που λαμβάνει ήδη: πληροφορίες χρέωσης και μηνιαία χρήση ενέργειας. Φυσικά, αυτή η λύση απαιτεί πρωτόκολλα και τυποποίηση, λένε οι ερευνητές. Η δεύτερη λύση υιοθετεί μια εντελώς διαφορετική προσέγγιση: Προβλέπει μια εποχή στο μη-τόσο μακρινό μέλλον,

όταν πολλοί άνθρωποι θα οδηγούν τα ηλεκτρικά και plug-in υβριδικά αυτοκίνητα και με μια επιπλέον επαναφορτιζόμενη μπαταρία (ή δύο) γύρω από το σπίτι δεν θα αποτελεί καινοτομία. Οι ερευνητές της Toshiba υποδεικνύουν ότι η λειτουργία μερικών συσκευών μερικώς από μια μπαταρία και όχι απευθείας από το δίκτυο, θα αποκρύψει το γεγονός ότι αυτές οι συσκευές είναι σε χρήση. Λειτουργεί ως εξής: Εάν συνδέσετε την μπαταρία με την παροχή ηλεκτρικού ρεύματος και κατευθύνετε έξυπνα την τροφοδοσία τόσο από την μπαταρία όσο και από το δίκτυο στις συσκευές, τότε ο έξυπνος μετρητής θα καταγράψει μια πολύ διαφορετική υπογραφή φόρτισης, αυτή που δεν αναγνωρίζει συσκευές. Οι ερευνητές της Toshiba παραδέχονται ότι κάποια ηλεκτρική ενέργεια θα χαθεί στην εκτροπή, οπότε θα υπάρξει αντιστάθμιση κάποιας αποτελεσματικότητας για την προστασία της ιδιωτικής ζωής. Εξακολουθούν να υπολογίζουν τον καλύτερο τρόπο βελτιστοποίησης τόσο του κόστους όσο και της ιδιωτικής ζωής χρησιμοποιώντας ένα τέτοιο σύστημα. Από την άλλη, επισημαίνουν ότι η αποθήκευση ηλεκτρικού ρεύματος σε μια μπαταρία θα επέτρεπε στη συσκευή να φορτίζει σε περιόδους κατά τις οποίες η παραγωγή ηλεκτρισμού είναι υψηλή και η ζήτηση είναι χαμηλή, μειώνοντας τον κίνδυνο συσκότισης. Είναι μια έξυπνη ιδέα, λέει η RebeccaHerold, σύμβουλος προστασίας προσωπικών δεδομένων, η οποία είναι επικεφαλής της υποομάδας NIST smart grid privacy. "Αλλά είναι σημαντικό να αναγνωρίσουμε ότι κάθε φορά που διαθέτετε δεδομένα που αποκαλύπτουν πληροφορίες για τους ανθρώπους, πρέπει να έχετε ισχυρές πολιτικές για να καθοδηγήσετε τον τρόπο με τον οποίο αυτά χρησιμοποιούνται". [22]

4.3 Ενδεικτικοί τρόποι επίλυσης συχνών επιθέσεων που αναφέρθηκαν παραπάνω

1. Man-in-the-middle: [9]

- Εγκατάσταση Internet Security που προστατεύει από τύπους επιθέσεων MITM
- Αποφυγή απευθείας σύνδεσης σε δημόσιο δρομολογητή Wi-Fi. Εγκατάσταση και χρησιμοποίηση ενός εικονικού δικτύου (VPN). ToVPN κρυπτογραφεί την σύνδεση σε δημόσια hotspot για την προστασία των ιδιωτικών δεδομένων που στέλνονται κατά την χρήση δημόσιων δικτύων Wi-Fi, όπως είναι οι κωδικοί πρόσβασης και οι πιστωτικές κάρτες.
- Προσεκτική αντιμετώπιση των email-phishing από διαδικτυακούς εγκληματίες που ζητούν την ενημέρωση κωδικών πρόσβασης ή άλλων διαπιστευτηρίων σύνδεσης.
- Ασφάλεια οικιακού δικτυού Wi-Fi. Ισχυροί κωδικοί πρόσβασης.

2. Denial-of-Service: [8]

Μια αποτελεσματική στρατηγική πρόληψης επίθεσης κατά Denial-of-Service αρχίζει από το σχεδιασμό του δικτύου και τελειώνει με τον κωδικό της εφαρμογής. Αυτό σημαίνει ότι το πρώτο βήμα είναι η επιλογή ενός κέντρου δεδομένων που έχει την δυνατότητα να διαχειριστεί μεγάλο αριθμό επιθέσεων.

Υπάρχουν κέντρα δεδομένων και πάροχοι φιλοξενίας που ειδικεύονται στο σχεδιασμό δικτύων που είναι ανθεκτικά στις επιθέσεις Distributed Denial of Service. Ακόμη και αν ένας πάροχος έχει επαρκή χωρητικότητα, όλη αυτή η κίνηση πρέπει ακόμα να καθαριστεί για να φιλτράρει την κακή κίνηση επίθεσης μέχρι να παραμείνει μόνο η νόμιμη κυκλοφορία.

Οι περισσότερες επιθέσεις απαιτούν και τεράστιο όγκο, οπότε είναι αδύνατο να γίνει το φιλτράρισμα σε έναν διακομιστή. Απαιτεί ειδικές λίστες ελέγχου πρόσβασης (ACL) που είναι εγκατεστημένες στον εξοπλισμό δρομολόγησης και μια δέσμη συσκευών μετριασμού DDoS υψηλής χωρητικότητας που είναι βασικά τείχη προστασίας με ικανότητα 30Gbit / s η κάθε μία ειδικά σχεδιασμένη για ανίχνευση και φιλτράρισμα DDoS κυκλοφορία. Αυτό συνήθως συνεπάγεται μια τεράστια επένδυση για τον πάροχο υπηρεσιών.

Μια τέτοια εγκατάσταση θα κάνει όλους τους διακομιστές που φιλοξενούνται στο εσωτερικό του δικτύου να μην είναι επιρρεπείς σε επιθέσεις DDoS επειδή έχουν φιλτραριστεί πριν μπορέσουν να φτάσουν στους διακομιστές ή την εφαρμογή. Η ενοικίαση ή η στέγαση του υλικού σας σε μια τέτοια ασφαλή εγκατάσταση θα παρέχει ασφάλεια απέναντι σε κακόβουλες πράξεις του κυβερνοχώρου.

Εάν κάποιος δεν επιθυμεί την μεταφορά των δεδομένων σε διαφορετική εγκατάσταση, υπάρχει επίσης κάτι που ονομάζεται απομακρυσμένη πρόληψη DDoS, που καθιστά δυνατή την απομακρυσμένη προστασία των εφαρμογών από επιθέσεις με τη δρομολόγηση της κυκλοφορίας μέσω ενός κέντρου καθαρισμού DDoS που στέλνει πίσω καθαρή κυκλοφορία στην μη ασφαλισμένη τοποθεσία σας.

3. Spoofing: [10]

Παρόλο που το spoofing δεν μπορεί να προληφθεί, υπάρχουν κάποια μέτρα που μπορούν να παρθούν για την αντιμετώπιση του. Μια αρκετά κοινή άμυνα είναι το Ingress-Filtering. Είναι μια διαδικασία που εξετάσει τα εισερχόμενα πακέτα και ελέγχει τις πηγές του. Εάν δεν ταιριάζουν στα πακέτα ή φαίνονται ύποπτες τότε απορρίπτονται. Έτσι καταλήγουν να παραμένουν μόνο τα νόμιμα πακέτα.

Στον Πίνακα 3 παρακάτω αναφέρονται κάποιες επιπρόσθετες ενδεικτικές λύσεις για επιθέσεις ασφάλειας που αναφέρθηκαν παραπάνω.

Πίνακας 3. Λύσεις για επιθέσεις ασφάλειας

Αξιολόγηση των αδυναμιών	Η έγκαιρη αξιολόγηση των αδυναμιών για την σωστή πρόληψη
Εκπαίδευση των χρηστών σχετικά με την ασφάλεια	Η γνώση των χρηστών σχετικά με την διασφάλιση της ασφάλειας τους είναι απαραίτητη
Τεχνικές αυθεντικοποίησης	Η χρήση τεχνικών αυθεντικοποίησης μπορεί να επιφέρει προστασία σε πολλά επίπεδα
Εικονικό ιδιωτικό δίκτυο	Οι εγκατεστημένες συσκευές πρέπει να είναι συμβατές με το εικονικό ιδιωτικό δίκτυο
Βασική υποδομή	Η συσκευή θα πρέπει να χρησιμοποιεί δημόσιο και ιδιωτικό κλειδί για να εξασφαλιστεί η ασφαλής πρόσβαση
Επιλεκτική συσσωμάτωση δεδομένων	Οι συσκευές θα πρέπει να συλλέγουν τα δεδομένα που είναι απαραίτητα να εκτελεστεί μια συγκεκριμένη λειτουργία και να μπορέσει να απορρίψει τα περιττά δεδομένα
Μηχανικοί ασφάλειας	Η επίτευξη της ασφάλειας πρέπει να είναι μια συνεργατική προσπάθεια των τμημάτων μηχανικών
Αναβαθμισμένα συστήματα πληροφορικής	Ο χρόνος ζωής των συστημάτων πληροφορικής είναι πολύ μικρός σε σύγκριση με τα ηλεκτρικά συστήματα. Έτσι, τα

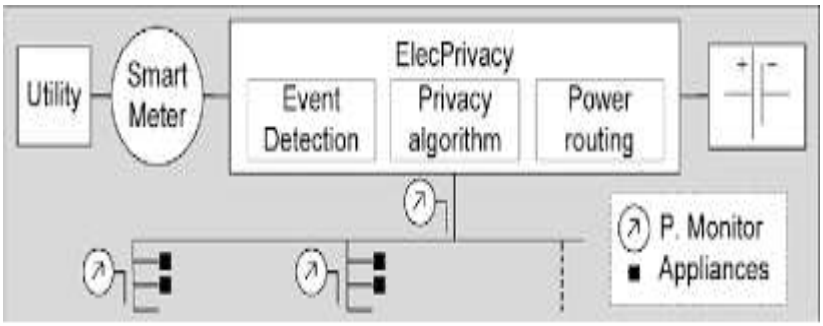
	συστήματα πληροφορικής πρέπει να είναι αναβαθμισμένο από καιρό σε καιρό.
Ασφάλεια στον σχεδιασμό	Η ασφάλεια θα πρέπει να ενσωματωθεί στο σχεδιασμό των έξυπνων δικτύων και δεν θα πρέπει να είναι ευθύνη των πωλητών.
Χρήση τρίτων μερών	Η χρήση τρίτων μερών είναι επιθυμητή για την επικοινωνία και την επίτευξη ασφάλειας

4.4 Σύστημα προστασίας προσωπικών δεδομένων “ElecPrivacy”

Ο συγκεκριμένος μηχανισμός προστασίας προσωπικών δεδομένων για την λειτουργία του εμπεριέχει μια βασική προϋπόθεση η οποία είναι η ύπαρξη μιας μονάδας αποθήκευσης ενέργειας, όπως για παράδειγμα ένα ηλεκτρικό όχημα, και έναν μηχανισμό δρομολόγησης ηλεκτρικής ενέργειας, ο οποίος λειτουργεί επιλεκτικά κάνοντας έλεγχο και αναμιγνύοντας ροές ηλεκτρικής ισχύος ενός πλήθους ηλεκτρικών πηγών με στόχο την κάλυψη της ζήτησης ενέργειας. Ένα παράδειγμα είναι η επιθυμητή χρήση της ενέργειας της μπαταρίας και έτσι να αποκρύψουμε την καταναλωτική ζήτηση μιας οικιακής συσκευής, η ενέργεια της μπαταρίας θα μειώσει τη σύνθετη αιχμή ζήτησης ισχύος.

Στο Σχήμα 10, παρουσιάζεται απλά και χωρισμένο σε κατηγορίες το παραπάνω σύστημα:

- Μηχανισμός μέτρησης: υπάρχει για να κρατάει της μετρήσεις ηλεκτρικής ενέργειας από τον έξυπνο μετρητή.
- Εντοπισμός γεγονότος: μετά την ανάλυση των προηγούμενων δεδομένων, εντοπίζει ένα πιθανό μοτίβο και αναγνωρίζει ένα πιθανό γεγονός.
- Αλγόριθμος προστασίας προσωπικών δεδομένων: υπάρχει για να αποκρύπτει ένα γεγονός που μπορεί να συνέβη.
- Δρομολόγηση ηλεκτρικής ενέργειας: είναι η ανάμιξη ενέργειας του παρόχου με μια προσωπική πηγή ενέργειας όπως για παράδειγμα μια μπαταρία.



Σχήμα 10. ElecPrivacy

Συνοψίζοντας, ο βασικός σκοπός του συστήματος αυτού είναι για αρχή ο εντοπισμός μιας πιθανής απειλής σχετικά με τα προσωπικά δεδομένα και κατά συνέχεια η απόκρισή του εκτελώντας δρομολόγηση ηλεκτρικής ενέργειας για να αποκρύψει τα φορτία των οικιακών ηλεκτρικών συσκευών. Το να μην μπορέσει να εντοπίσει κάποιος διάφορα γεγονότα από διάφορες προσωπικές ατομικές συσκευές παρέχει προστασία στην ιδιωτική του ζωή και στις προσωπικές του προτιμήσεις, δηλαδή το θεμελιώδης δικαίωμα κάθε ανθρώπου να κρατάει τις προσωπικές του επιλογές και προτιμήσεις μακριά από κάποιο άλλο άτομο. [21]

4.5 Ερευνητικό πρόγραμμα SPEAR

«Το ερευνητικό πρόγραμμα SPEAR είναι μια πλατφόρμα, ένα πολυεπίπεδο λογισμικό, που θα υλοποιήσει και θα αναπτύξει εργαλεία άμυνας απέναντι σε κυβερνοεπιθέσεις σε δίκτυα παραγωγής, διανομής και διαχείρισης ηλεκτρικής ενέργειας. Η δομή του SPEAR αποτελείται από τρία επίπεδα. Στο πρώτο επίπεδο θα υλοποιηθούν κατάλληλα συστήματα έγκαιρης και ορθής ανίχνευσης απειλών χρησιμοποιώντας καινοτόμες τεχνολογικές τεχνικές όπως τα μεγάλα δεδομένα (big data). Στο δεύτερο επίπεδο, το σύστημα SPEAR θα επεκταθεί ώστε είναι ικανό να προσελκύσει και να καταγράψει επιθετικές ενέργειες σε κατάλληλα διαμορφωμένες παγίδες που ονομάζονται βάζα με μέλι (honey pots). Με τον τρόπο αυτό, κάθε κυβερνο-επίθεση καταγράφεται ώστε να συλλεχθούν τα κατάλληλα δεδομένα για την έκθεση του επιτιθέμενου στο δικαστήριο,

ώστε να είναι σε θέση το θύμα, που έχει δεχθεί την κυβερνο-επίθεση, να διεκδικήσει αποζημίωση και να εκθέσει την κυβερνο-επίθεση. Στο τρίτο επίπεδο, το SPEAR εισάγει έναν καινοτόμο δίαυλο επικοινωνίας μεταξύ των φορέων που άπτονται των έξυπνων δικτύων, όπου ένα ανώνυμο κανάλι επικοινωνίας θα είναι ικανό να ενημερώνει όλους τους φορείς και τους οργανισμούς που σχετίζονται με τα έξυπνα δίκτυα σχετικά με τα συμβάντα κυβερνο-επιθέσεων, χωρίς να εκθέτει προσωπικά δεδομένα αλλά και τη φήμη των φορέων και των οργανισμών. Αυτό θα έχει σαν αποτέλεσμα την άμεση ενημέρωση στην περίπτωση εκδήλωσης κυβερνο-επιθέσεων σε παγκόσμια βάση, ώστε να λαμβάνονται συλλογικά και άμεσα μέτρα εναντίον τους.

«Η φάση της ψηφιοποίησης των μετρητών κατανάλωσης του ηλεκτρικού ρεύματος σε οικιακό αλλά και σε βιομηχανικό περιβάλλον, εισάγει μία νέα πρόκληση που σχετίζεται με την ευπάθεια των έξυπνων μετρητών σε κυβερνο-επιθέσεις. Κάθε έξυπνος μετρητής περιέχει μια διαδικτυακή διεπαφή, η οποία μπορεί να δεχτεί επιθέσεις από επιτιθέμενους απ' όλο τον κόσμο. Σε επίπεδο οικιακού χρήστη, ένα από τα σημαντικότερα θέματα είναι η προστασία των ηλεκτρικών οικιακών συσκευών από επιθέσεις αλλά και η αποτροπή παρεμβολών στη μέτρηση της κατανάλωσης. Θα μπορούσε για παράδειγμα ένας επιτιθέμενος από την Κίνα να παρακολουθεί έναν οικιακό ή βιομηχανικό καταναλωτή στην Κοζάνη και να προβεί σε κακόβουλες ενέργειες, όπως να αλλοιώσει τη μέτρηση κατανάλωσης (για παράδειγμα αν κάποιος καταναλώνει 50 ευρώ ρεύμα τον μήνα, με μια επίθεση στον μετρητή ο επιτιθέμενος μπορεί να αλλάξει το ποσό κατανάλωσης σε πολλές χιλιάδες ευρώ), να εκτελέσει μια κυβερνοεπίθεση στοχεύοντας σε ηλεκτρικές συσκευές όπως ένα ψυγείο ή ένα πλυντήριο ή ακόμα και να υποκλέψει ένα μοτίβο κατανάλωσης του χρήστη (ώρες και διάρκεια κατανάλωσης) και να πουλήσει αυτές τις πληροφορίες σε κάποιον τρίτο για διαφημιστικούς λόγους.

Η πλατφόρμα SPEAR προστατεύει παράλληλα τόσο τον καταναλωτή όσο και τον πάροχο ηλεκτρικής ενέργειας, διότι και οι δυο θα έχουν πλήρη έλεγχο και τα κατάλληλα εργαλεία, έτσι ώστε να προστατευθούν από κυβερνο-επιθέσεις αλλά και να λάβουν την απαραίτητη νομική κάλυψη σε περίπτωση που δεχθούν μία κυβερνο-επίθεση».

«Σύμφωνα με τις οδηγίες της Ευρωπαϊκής Επιτροπής, μέχρι το 2020 αναμένεται η

αντικατάσταση των παλιών μεθόδων μέτρησης με ψηφιακό τρόπο, δημιουργώντας «έξυπνα» σπίτια από πλευράς διαχείρισης και ελέγχου κατανάλωσης ηλεκτρικής ενέργειας. Αυτό θα οδηγήσει, σύμφωνα με τις εκτιμήσεις, σε μία μείωση 3% της μέσης κατανάλωσης ενέργειας. Επιπλέον, θα επιτρέψει την εισαγωγή νέων καινοτόμων υπηρεσιών. Λόγου χάρη, ο καταναλωτής θα έχει τη δυνατότητα με ένα κινητό τηλέφωνο να διαχειρίζεται και να ελέγχει σε πραγματικό χρόνο την κατανάλωση ρεύματος στο σπίτι του, αυτοματοποιώντας πολλές διαδικασίες και μειώνοντας την κατανάλωση ρεύματος. Πρωτοπόρες στη μετάβαση σε έξυπνα δίκτυα ηλεκτροδότησης είναι η Δανία, η Σουηδία και η Φινλανδία, ενώ η Ελλάδα, όπως και οι περισσότερες χώρες στην Ευρώπη, είναι ακόμη σε φάση σχεδιασμού.» [23]

4.6 Κρυπτογραφία

4.6.1 Εισαγωγή στην κρυπτογραφία

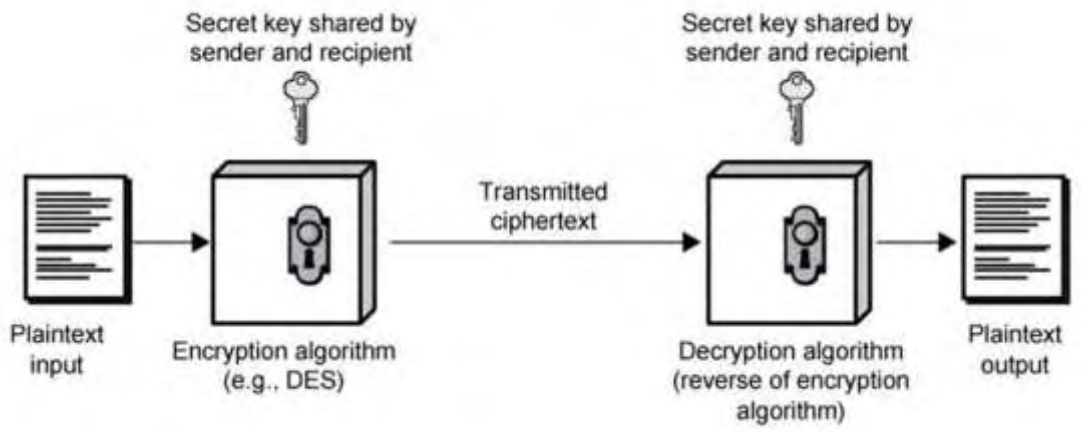
Κρυπτογραφία. Μια διαδικασία που προστατεύει τις συναλλαγές σε ένα δίκτυο όπως είναι το διαδίκτυο.

Η κρυπτογραφία είναι ένα σημαντικό εργαλείο ασφάλειας από τους κινδύνους που αφορούν τα προσωπικά δεδομένα στα έξυπνα δίκτυα. Ο ρόλος της είναι επί της ουσίας οι τεχνικές με τις οποίες θα επιτευχθεί η απόκρυψη περιεχομένου μηνυμάτων. Το νόημα είναι να δημιουργηθούν μηχανισμοί οι οποίοι θα επιτρέπουν την ανταλλαγή μηνυμάτων με ασφάλεια ανάμεσα σε δύο συναλλασσόμενα μέρη χωρίς να υπάρχει ο κίνδυνος ένα επιπλέον άτομο να έρθει σε επαφή με τα μηνύματα αυτά. Χρησιμοποιώντας την κρυπτογράφηση τα δεδομένα μετασχηματίζονται με τέτοιο τρόπο που είναι αδύνατο να διαβαστούν χωρίς την σωστή ακολουθία bits. Αυτή η ακολουθία αποκαλείται κλειδί. Η αποκρυπτογράφηση είναι η αντίστροφη διαδικασία και για την πραγματοποίηση της απαιτείται η χρήση του κλειδιού. Κάποιους μηχανισμούς που χρησιμοποιεί η κρυπτογράφηση για την διασφάλιση της ζητούμενης ασφάλειας είναι η ψηφιακή υπογραφή και η ψηφιακή χρονοσφραγίδα. Η ψηφιακή υπογραφή δηλώνει σε κάποιον το ποιος δημιούργησε τα εκάστοτε αρχεία και η ψηφιακή χρονοσφραγίδα συνδέει τα δεδομένα με την ώρα δημιουργίας τους. Επίσης η κρυπτογραφία μπορεί να γίνει με δύο διαφορετικούς τρόπους. Την συμμετρική και την ασύμμετρη. Στην συμμετρική κρυπτογραφία υπάρχει ένα κλειδί το οποίο το χρησιμοποιεί πρώτα ο αποστολέας για να

κρυπτογραφήσει το μήνυμα και κατά συνέχεια ο παραλήπτης για την αντίθετη διαδικασία. Από την άλλη μεριά στην ασύμμετρη υπάρχουν δύο διαφορετικά το ένα για την κρυπτογράφηση και το άλλο για την αποκρυπτογράφηση. Κάθε μέρος συναλλασσόμενο έχει από ένα ζεύγος κλειδιών. Το ένα είναι το δημόσιο κλειδί και το άλλο το ιδιωτικό. [24]

4.6.2 Κρυπτογραφία μυστικού κλειδιού

Οι αλγόριθμοι συμμετρικής κρυπτογραφίας έχουν ως βασίζονται στο γεγονός ότι υπάρχει ένα μοναδικό μυστικό κλειδί, το οποίο το γνωρίζουν μόνο τα δύο συναλλασσόμενα. Αυτό το κλειδί που δημιουργείται είναι για χρήση τόσο κρυπτογράφησης όσο και αποκρυπτογράφησης μηνυμάτων. (Σχήμα 11). Αυτή η διαδικασία κρυπτογραφίας (συμμετρική) δίνει εγγύηση για την εμπιστευτικότητα (confidentiality) των δεδομένων που αναφέραμε προηγουμένως αφού κρυπτογραφεί το μήνυμα με ένα μυστικό κλειδί. Κατά συνέχεια, ο παραλήπτης αποκρυπτογραφεί το μήνυμα που παράγεται με την χρήση του ίδιου κλειδιού (εξού και συμμετρική), το οποίο είναι σημαντικό να παραμείνει μυστικό μεταξύ των δύο συναλλασσόμενων μερών. Ένα βασικό πλεονέκτημα που έχουν οι συμμετρικοί αλγόριθμοι είναι ότι οι χρήστες δεν καταλαβαίνουν κάποια σημαντική χρονική καθυστέρηση λόγω της διαδικασίας κρυπτογράφησης / αποκρυπτογράφησης. Το μόνο που χρειάζεται είναι η μυστική διατήρηση του διαμοιρασμένου (shared) κλειδιού. Ενώ η συμμετρική κρυπτογράφηση είναι ικανή να εγγυηθεί την εμπιστευτικότητα που αναφέραμε, έχει πρόβλημα όμως στο να εγγυηθεί και την επιτυχημένη ανταλλαγή του κλειδιού με ασφάλεια. Επομένως, όταν τα δύο συναλλασσόμενα μέρη δεν γνωρίζονται (αποστολέας-παραλήπτης), είναι σημαντικό να υπάρχει ένα ασφαλές κανάλι επικοινωνίας για τη μεταφορά του κλειδιού. Για αυτόν τον λόγο ένα σημαντικό πρόβλημα έχει να κάνει με την αναγνώριση ή ταυτοποίηση (identification) μεταξύ του αποστολέα και του παραλήπτη. Ένα πρόβλημα σχετικά με την ταυτοποίηση αφορά το γεγονός ότι το δημόσιο κλειδί είναι προσβάσιμο με μεγάλη ευκολία και από πολύ κόσμο. Διότι και στην περίπτωση που κάποιος ναι μεν παραλαμβάνει κάποιο μήνυμα, δεν έχει την δυνατότητα να αποδείξει σίγουρα από ποιον το έχει παραλάβει. Για αυτό, ένα θέμα με υψηλή βαρύτητα είναι η διαχείριση των κλειδιών και η αρχική διανομή τους. [21]

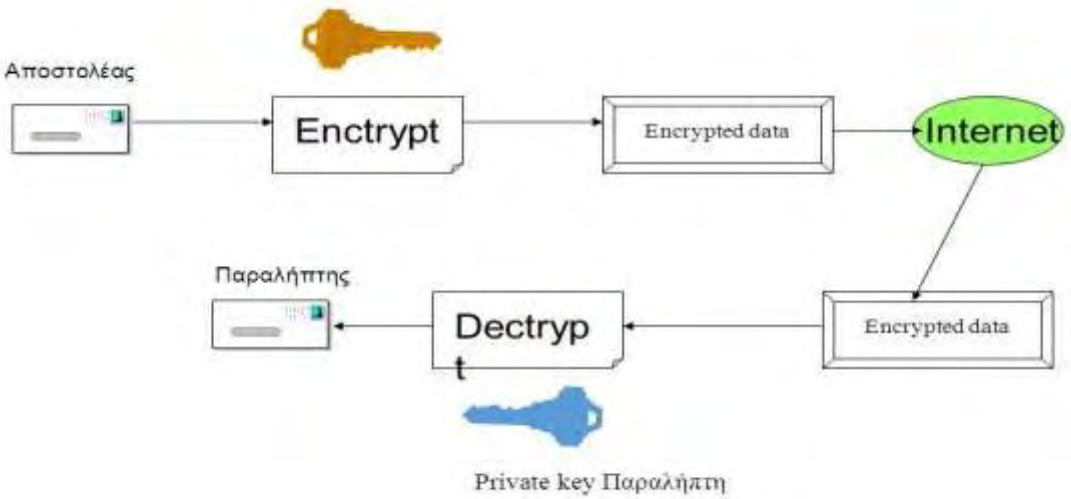


Σχήμα 11. Συμμετρική κρυπτογραφία [25]

4.6.3 Κρυπτογραφία δημόσιου κλειδιού

Αυτή η διαδικασία κρυπτογράφησης διαφέρει από την προηγούμενη γιατί πλέον τα δύο συναλλασσόμενα μέρη δεν έχουν το ίδιο μυστικό κλειδί, αλλά αντιθέτως πλέον έχουμε δυο διαφορετικά κλειδιά το κάθε ένα για διαφορετική λειτουργία. Για την διαδικασία της κρυπτογράφησης του δημοσίου κλειδιού χρειάζεται η χρήση και των δυο κλειδιών (δημόσιου και προσωπικού) (Σχήμα 12).

Σε πρώτο επίπεδο η κρυπτογράφηση γίνεται με το δημόσιο κλειδί του παραλήπτη και στέλνονται τα δεδομένα. Σε επόμενο επίπεδο όταν ο παραλήπτης τα παραλάβει, τα αποκρυπτογραφεί με το προσωπικό του κλειδί. Υπάρχει μαθηματική σχέση ανάμεσα στα δύο κλειδιά. Ένα πολύ σημαντικό πλεονέκτημα είναι δεν είναι εφικτό κάποιος να υπολογίσει το κλειδί της αποκρυπτογράφησης έχοντας στην κατοχή του μόνο το κλειδί της κρυπτογράφησης. Σημαντικό πλεονέκτημα της κρυπτογράφησης δημοσίου κλειδιού είναι ότι το δημόσιο κλειδί δίνεται ελεύθερα και αυτό έχει ως αποτέλεσμα να μπορούν να δημιουργηθούν εύκολα και με ασφάλεια κανάλια επικοινωνίας χωρίς να χρειάζεται να ενταχθεί ακόμα ένα άτομο διαμεσολάβησης που πολύ πιθανώς να μην είναι έμπιστο. Από την άλλη μεριά βέβαια ένα μείον αυτού του είδους κρυπτογράφησης είναι δεν είναι γρήγορη διαδικασία καθώς χρειάζονται παραπάνω πράξεις και υπολογισμοί συγκριτικά με την άλλη. Για αυτόν τον λόγο, για την μείωση χρόνου, γίνεται η κρυπτογράφηση δημοσίου κλειδιού για την ανταλλαγή / διανομή συμμετρικών κλειδιών και στο επόμενο στάδιο γίνεται η συμμετρική κρυπτογράφηση για την ουσιαστική επικοινωνία. [21]



Σχήμα 12. Ασύμμετρη κρυπτογραφία [26]

4.6.4 Σύνοψη της διαδικασίας της κρυπτογράφησης

Για την ολοκληρωμένη και σωστή μεταφορά ενός μηνύματος, η διαδικασία η οποία ακολουθείται είναι η εξής:

Βήμα πρώτο: Ο αποστολέας χρησιμοποιεί μια συνάρτηση κατακερματισμού στο αρχικό μήνυμα με σκοπό την παραγωγή μιας μοναδικής τιμής η οποία αποτελεί την σύνοψη του μηνύματος.

Βήμα δεύτερο: Ο αποστολέας χρησιμοποιώντας το ιδιωτικό κλειδί, κρυπτογραφεί την σύνοψη του μηνύματος και έτσι δημιουργείται η ψηφιακή υπογραφή του.

Βήμα τρίτο: Ο αποστολέας κατασκευάζει ένα τυχαίο συμμετρικό κλειδί με σκοπό την κρυπτογράφηση του επιθυμητού μηνύματος, της ψηφιακής υπογραφής και του αντιγράφου του ψηφιακού πιστοποιητικού του που περιέχει το δημόσιο κλειδί του.

Βήμα τέταρτο: Το δημόσιο κλειδί περιέχει το ψηφιακό πιστοποιητικό του παραλήπτη, το οποίο ο παραλήπτης πρέπει να διαθέτει πριν την αρχή της διαδικασίας. Για να μπορέσει να μεταδοθεί με ασφάλεια το συμμετρικό κλειδί, κρυπτογραφείται με βάση το δημόσιο κλειδί του παραλήπτη. Με αυτόν τον τρόπο, δημιουργείται ένα κρυπτογραφημένο κλειδί το οποίο αποτελεί τον ψηφιακό φάκελο και στέλνεται με το κρυπτογραφημένο μήνυμα του προηγούμενου βήματος.

Συνοψίζοντας:

Το απεσταλμένο μήνυμα προς τον παραλήπτη περιέχει το συμμετρικά κρυπτογραφημένο μήνυμα και το ασύμμετρα κρυπτογραφημένο συμμετρικό κλειδί που αναφέρθηκαν παραπάνω.

Το μήνυμα καταφθάνει στον παραλήπτη ο οποίος αποκρυπτογραφεί τον ψηφιακό φάκελο με την χρήση του ιδιωτικού κλειδιού με σκοπό να αποκτήσει το συμμετρικό κλειδί.

Κατά συνέχεια γίνεται η αποκρυπτογράφηση του με την χρήση του συμμετρικού κλειδιού μαζί με την υπογραφή και το πιστοποιητικό του αποστολέα.

Στο πιστοποιητικό που μόλις παραλήφθηκε, περιέχεται το δημόσιο κλειδί του αποστολέα με το οποίο αποκρυπτογραφείται η ψηφιακή υπογραφή. Με αυτόν τον τρόπο αποκτάται η γνήσια σύνοψη του κρυπτογραφημένου μηνύματος.

Με την χρήση της ίδιας συνάρτησης κατακερματισμού του αποστολέα δημιουργείται μια εκ νέου σύνοψη για το αποκρυπτογραφημένο μήνυμα.

Τέλος, γίνεται σύγκριση των συνόψεων μηνυμάτων που υπάρχουν.

4.7 Πρωτόκολλα προστασίας επιθέσεων

Το σύστημα SCADA (Supervisory control and data acquisition) χρησιμοποιείται ευρέως. Σε κάποιες περιπτώσεις, μερικές φορές ο «έλεγχος ταυτότητας», η «κρυπτογράφηση» και τα «τείχη προστασίας» δεν μπορούν να μετριάσουν τα ζητήματα ασφάλειας σε ένα μεγάλο SCADA δίκτυο. Επιπλέον, εστιάζοντας στη διασφάλιση ζητημάτων και λαμβάνοντας υπόψη μόνο το δίκτυο SCADA ως μια ενιαία οντότητα, δεν θα λυθεί το πρόβλημα και ως εκ τούτου, είναι σημαντικό να διασφαλιστεί η ασφάλεια στον κυβερνοχώρο για κάθε μια από τις μεμονωμένες συσκευές στο δίκτυο. Διαφορετικά πρωτόκολλα επικοινωνίας χρησιμοποιούνται μεταξύ των συσκευών SCADA για επιτυχημένη αυτοματοποίηση και λειτουργία ενός έξυπνου δικτύου. Η εξέλιξη των ιδιωτικών και βιομηχανικών πρωτοκόλλων SCADA ξεκίνησαν στις αρχές της δεκαετίας του 1980 όταν Modbus, Modbus Plus και άλλα πρωτόκολλα αναπτύχθηκαν για πρώτη φορά. Το πρωτόκολλο (DNP) εμφανίστηκε για πρώτη φορά το 1990 από την Westronic, Inc. ως ανοιχτό πρωτόκολλο. Το πρωτόκολλο DNP3 είναι βάσει του πρωτοκόλλου IEC 60870-5. Αν και το πρωτόκολλο DNP3 έχει σχεδιαστεί για αξιόπιστα δεδομένα επικοινωνίας εξακολουθεί να είναι ευάλωτο σε επιθέσεις στον κυβερνοχώρο. Επομένως, μια ασφάλεια βασισμένη για συσκευές DNP3 είναι καλή ιδέα για την προστασία του έξυπνου δικτύου από επιθέσεις στον κυβερνοχώρο. [27]

4.8 Προστασία από τοπολογικές επιθέσεις

Το έξυπνο δίκτυο είναι επίσης ευάλωτο στις τοπολογικές σοβαρές επιθέσεις στον κυβερνοχώρο. Για παράδειγμα, με βάση τις τοπολογικές γνώσεις του συστήματος ισχύος, ένας εισβολέας μπορεί να επιτεθεί στους αλγορίθμους ανίχνευσης κακών δεδομένων των εκτιμητών ρεύματος. Μια άλλη τοπολογία που βασίζεται σε επιθέσεις στον κυβερνοχώρο είναι η επίθεση στο ηλεκτρικό διακόπτη που θα προκαλέσει την απομόνωση των μονάδων παραγωγής από το ηλεκτρικό δίκτυο. Έχει αποδειχθεί ότι μπορούν να γίνουν επιθέσεις στον κυβερνοχώρο για την εμπιστευτικότητα με κατάλληλες τοπολογικές γνώσεις όπως επίσης και επιθέσεις ακεραιότητας και διαθεσιμότητας. Επομένως, προτείνεται ένα μοντέλο που βασίζεται στην ασφάλεια ροής πληροφοριών για την άμβλυνση αυτών των ζητημάτων ασφάλειας. Μια βέλτιστη στρατηγική τοποθέτησης μεταξύ των συνδέσμων ενάντια σε τυχαίες επιθέσεις στον κυβερνο-φυσικό δίκτυο αποδεικνύει ότι η στρατηγική αυτή εξασφαλίζει μια καλύτερη ασφάλεια σε σχέση με όλες τις άλλες πιθανές στρατηγικές, συμπεριλαμβανομένων στρατηγικών που χρησιμοποιούν τυχαία κατανομή, μονόδρομες διασυνδέσεις, στην περίπτωση που η τοπολογία του κυβερνοχώρου και του φυσικού δικτύου είναι άγνωστοι ο ένας στον άλλο. [27]

4.9 Χρήση συγκεντρωτικών δεδομένων

Το λογισμικό και τα δίκτυα στο δίκτυο έχουν αυξήσει τον αριθμό πιθανών σημείων εισόδου για κυβερνοεπιθέσεις. Σε περίπτωση διακοπής της επικοινωνίας και άρνησης της υπηρεσίας, η ακεραιότητα του λογισμικού, τα συστήματα και η εμπιστευτικότητα των δεδομένων διακυβεύονται. Έτσι, οι απειλές στον κυβερνοχώρο θέτουν σε κίνδυνο την εμπιστευτικότητα των δεδομένων χρήσης των καταναλωτών μαζί με την ασφάλεια και την αξιοπιστία της παροχής ηλεκτρικής ενέργειας. Οι υπεύθυνοι που χειρίζονται τα δεδομένα κατανάλωσης ηλεκτρικής ενέργειας των καταναλωτών θα πρέπει να υποχρεούνται να προστατεύουν την ιδιωτική ζωή και την ασφάλεια των πληροφοριών αυτών. Χρήσιμες μέθοδοι που υπάρχουν για την φύλαξη των προσωπικών πληροφοριών είναι η συσσωμάτωση, η κρυπτογράφηση και η στερεογραφία. Η συνάθροιση συνδυάζει δεδομένα που ανήκουν σε δύο ή περισσότερα άτομα, σε συγκεκριμένες χρονικές περιόδους και καταργεί τις προσωπικά αναγνωρίσιμες πληροφορίες. Για παράδειγμα, το λογισμικό και

τα δίκτυα στο δίκτυο έχουν αυξήσει τον αριθμό των πιθανών σημείων εισόδου για κυβερνοεπιθέσεις. Έτσι η χρήση ενέργειας από 100 σπίτια σε μια συγκεκριμένη γειτονιά θα μπορούσε να συγκεντρωθεί μαζί και να δοθούν έτσι τα απαραίτητα δεδομένα για ανάλυση ανά οικία, προστατεύοντας παράλληλα την ταυτότητα του πελάτη και τα συμπεριφορικά πρότυπα. Ένα άλλο πλεονέκτημα των συγκεντρωτικών δεδομένων είναι ότι θα μπορούσε να μειώσει τις καθυστερήσεις του δικτύου. Αυτό οφείλεται στο γεγονός ότι μεγάλες ποσότητες πληροφοριών θα μπορούσαν να παραδοθούν σε πακέτα αντί να μεταδίδονται χωριστά. Η κρυπτογράφηση ανακατεύει δεδομένα και κωδικοποιεί ένα μήνυμα που είναι γνωστό μόνο στους εξουσιοδοτημένους χρήστες. Έτσι, τα δεδομένα μπορούν να διαβαστούν μόνο από τον παραλήπτη που έχει το κλειδί για να ανοίξει τις πληροφορίες. Ενώ αυτός είναι ένας αποτελεσματικός τρόπος για την εφαρμογή μιας προσέγγισης ασφάλειας σε στρώσεις, μπορεί να είναι δαπανηρή. Αυτό οφείλεται στο γεγονός ότι τα δεδομένα πρέπει να αποθηκεύονται με μεγάλη χωρητικότητα και απαιτούνται συχνές αναβαθμίσεις. Χωρίς ικανά συστήματα, η ασφάλεια των δεδομένων μπορεί να διακυβεύεται. Τέλος, η στερεογραφία κρύβει ένα αρχείο ή ένα μήνυμα με άλλο αρχείο ή μήνυμα. Με αυτόν τον τρόπο οι πληροφορίες φαίνονται αρκετά ασήμαντες. Το San Diego Gas & Electric (SDG & E) είναι ένα παράδειγμα ενός βοηθητικού προγράμματος που μοιράζεται δεδομένα χρήσης ενώ προστατεύει την ιδιωτική ζωή των πελατών. Αφού ο καταναλωτής ηλεκτρικής ενέργειας εξουσιοδοτήσει την SDG & E να μοιραστεί δεδομένα, ένα μοναδικό αναγνωριστικό έχει οριστεί για τη μεταφορά των δεδομένων χρήσης του καταναλωτή. Αυτό σημαίνει το τρίτο μέρος έχει τις πληροφορίες που σχετίζονται με το μοναδικό αναγνωριστικό ενώ προστατεύει τις προσωπικές πληροφορίες του πελάτη. Τα τρίτα μέρη θα μπορούσαν επίσης να αναπτύξουν αποτελεσματικές ρυθμίσεις ελέγχου απορρήτου που να επιτρέπουν στους καταναλωτές να ελέγχουν την προστασία των δεδομένων τους. Για παράδειγμα, η Tendril, μια εταιρεία που συνεργάζεται με παρόχους ενέργειας σε όλο τον κόσμο, πρότεινε ότι οι καταναλωτές χρησιμοποιούν τέτοιους διαδραστικούς ελέγχους όπως αυτούς στο Facebook για τη διαχείριση των ρυθμίσεων απορρήτου. Αυτό θα επιτρέψει στους πελάτες να κάνουν εύκολα πρόσβαση στις ρυθμίσεις απορρήτου τους και να τις προσαρμόσουν ανά πάσα στιγμή. Αυτές οι προσεγγίσεις προστατεύουν τα προσωπικά δεδομένα των πελατών. Δεν πρέπει να ξεχνάμε ότι η ανώνυμη συγκέντρωση δεδομένων απαιτεί υπολογιστικό κόστος, χρόνο και προσπάθεια. Χρειάζονται πρόσθετοι πόροι για την τροποποίηση, αποθήκευση, επεξεργασία και μεταφορά μεγάλων ποσοτήτων πληροφοριών. [28]

4.10 Ασφάλεια της υποδομής της ηλεκτρικής ενέργειας από τις επιθέσεις στον κυβερνοχώρο

Υπάρχουν τουλάχιστον 27 προγράμματα στο Τμήμα Ενέργειας, Τμήμα Ασφάλειας και στης Ομοσπονδιακής Επιτροπής Ρυθμιστικής Ενέργειας (FERC) για την προστασία του δικτύου από παραβιάσεις του κυβερνοχώρου. Απειλές στον κυβερνοχώρο και επιθέσεις στο σύστημα διανομής θα μπορούσαν να έχουν συνέπειες στο σύστημα ηλεκτρικής παραγωγής, στην ευρύτερη εθνική ασφάλεια και στα οικονομικά συμφέροντα. Το σύστημα διανομής παραδίδει ηλεκτρική ενέργεια σε αγωγούς, συστήματα ύδρευσης, τηλεπικοινωνίες και σε άλλες σημαντικές υποδομές, συμπεριλαμβανομένων των κρίσιμων κυβερνητικών και στρατιωτικών εγκαταστάσεων. Αυτό σημαίνει ότι οι κυβερνοεπιθέσεις σε αυτό το σύστημα θα μπορούσαν να διαταράξουν την παροχή ηλεκτρικού ρεύματος σε τέτοιες εγκαταστάσεις, με αποτέλεσμα καταστροφικές συνέπειες για την οικονομία και την ασφάλεια. Προτεινόμενες βελτιώσεις περιλαμβάνουν καλύτερη επικοινωνία και ανταλλαγή πληροφοριών μεταξύ των οργανισμών και σαφή σχέδια για την αποκατάσταση της ισχύος μετά από μια μεγάλη διακοπή. Η διασφάλιση της ηλεκτρικής υποδομής είναι κρίσιμη για την προστασία των προσωπικών δεδομένων των καταναλωτών και των δεδομένων χρήσης. Μια λύση για την προστασία της ηλεκτρικής υποδομής από απειλές στον κυβερνοχώρο είναι η δημιουργία μιας αποθήκης όπου εκεί θα αποθηκεύονται πληροφορίες σχετικά με απειλές στον κυβερνοχώρο, όπως κακόβουλες διευθύνσεις πρωτοκόλλου Internet. Το Υπουργείο Εσωτερικής Ασφάλειας διεξάγει επί του παρόντος πιλότο για να διερευνήσει αυτή την επιλογή. Μια τράπεζα αποθήκευσης επιτρέπει την κοινή χρήση πληροφοριών σχετικά με απειλές από την κυβέρνηση, τη βιομηχανία και από τις επιχειρήσεις κοινής ωφελείας. Επιπλέον, τα δεδομένα θα αποθηκεύονται, συγκεντρώνονται και αναλύονται για να αυξήσουν την κοινή γνώση σχετικά με τις τρέχουσες και ιστορικές συνθήκες στον κυβερνοχώρο. Ο ιδιωτικός τομέας πρέπει επίσης να συνεργαστεί για να προστατεύσει τα προϊόντα του από τις απειλές στον κυβερνοχώρο. Ένα παράδειγμα είναι το πώς οι CheckPoint, Cisco, Fortinet, IntelSecurity, PaloAltoNetworks και η Symantec συνεργάζονται για την προστασία των πελατών της μέσω της ανταλλαγής πληροφοριών σχετικά με τις απειλές. Περισσότεροι εταίροι της βιομηχανίας θα πρέπει να ακολουθήσουν τις δραστηριότητές τους και να ενώσουν τις δυνάμεις τους για την προστασία των προϊόντων, των υπηρεσιών και των πελατών από απειλές στον κυβερνοχώρο. Σύμφωνα με τον RichardMroz, Πρόεδρο του Διοικητικού Συμβουλίου του Νιου Τζέρσεϋ οι δημόσιες υπηρεσίες και τα θέματα ασφάλειας και

δεδομένων είναι αλληλένδετα. Οι επιχειρήσεις κοινής ωφέλειας στο Νιου Τζέρσεϋ πρέπει να αναπτύξουν προγράμματα και διαδικασίες που να εντοπίζουν και μετριάζουν τους κινδύνους του κυβερνοχώρου, να αναφέρουν συμβάντα και ύποπτες δραστηριότητες, να δημιουργούν σχέδια αντίδρασης και ανάκαμψης και να παρέχουν προγράμματα κατάρτισης. Στην Πενσυλβανία, επιχειρήσεις κοινής ωφέλειας απαιτούνται για τη διατήρηση της ασφάλειας στον κυβερνοχώρο, την αντιμετώπιση καταστάσεων έκτακτης ανάγκης και για την αναφορά επιθέσεων στον κυβερνοχώρο που προκαλούν περισσότερα από 50.000 δολάρια σε ζημιές. Στο Τέξας, μια ανεξάρτητη οργάνωση διαχείρισης δεδομένων μετρητών καθορίζει τα πρότυπα για την ασφάλεια στον κυβερνοχώρο και η επιτροπή για τις επιχειρήσεις κοινής ωφελείας ασκούν ετήσιους ελέγχους ασφάλειας. Περισσότερα κράτη πρέπει να ζητήσουν από τις επιχειρήσεις κοινής ωφελείας να εφαρμόσουν προστατευτικά μέτρα κατά των απειλών στον κυβερνοχώρο. Οι νομοθέτες πρέπει να απαιτούν τυπικά κριτήρια απόδοσης για να διασφαλίζουν ότι τα βοηθητικά προγράμματα προστατεύονται από απειλές στον κυβερνοχώρο. Οι υπάλληλοι διανομής πρέπει επίσης να είναι εκπαιδευμένοι και διαπιστευμένοι για να ενισχύσουν τις δεξιότητές τους στον κυβερνοχώρο. Επί του παρόντος, η FERC ρυθμίζει τη μετάδοση και τη χονδρική πώληση ηλεκτρικής ενέργειας στο διακρατικό εμπόριο. Επιπλέον, οι απειλές στον κυβερνοχώρο και οι επιθέσεις στο σύστημα διανομής θα μπορούσαν να έχουν επιπτώσεις για το σύστημα ηλεκτρικής ενέργειας και για την ευρύτερη εθνική ασφάλεια και οικονομία. Διατάξεις για την ενθάρρυνση της ανταλλαγής πληροφοριών μεταξύ ομοσπονδιακών υπηρεσιών και οργανισμών, θα πρέπει να συνεχίσουν να αναπτύσσονται. [28]

4.11 Θέματα ασφαλείας για το μελλοντικό έξυπνο δίκτυο

Με στόχο το έξυπνο δίκτυο να γίνει ακόμα πιο έξυπνο, αναλαμβάνονται σημαντικές πρωτοβουλίες σε ολόκληρο τον κόσμο. Αυτά τα μέτρα θα είναι όχι μόνο για να εκσυγχρονιστεί το δίκτυο αλλά και για να βελτιωθεί η συνολική αποτελεσματικότητα του συστήματος, η σταθερότητα και προφανώς η αξιοπιστία. Αλλά τα ζητήματα ασφάλειας πρέπει να διατηρηθούν για να εξασφαλιστεί η αδιάλειπτη τροφοδοσία στους χρήστες και η προστασία του εθνικού δικτύου ηλεκτρικής ενέργειας από τρομοκρατικές επιθέσεις. Είναι σημαντικό να αναφέρουμε ότι το σωστά σχεδιασμένο αμυντικό πλαίσιο κατά των επιθέσεων στον κυβερνοχώρο πρέπει να αντιμετωπίσει όλες τις πτυχές που σχετίζονται με

το έγκλημα στον κυβερνοχώρο σε μια πολύπλοκη υποδομή ηλεκτρικού δικτύου ηλεκτρικής ενέργειας. Αυτό σημαίνει ότι δεν πρέπει να εξεταστεί μόνο το ενδεχόμενο επιθέσεων στον κυβερνοχώρο, αλλά πρέπει επίσης να αντιμετωπιστούν οι ακούσιες ανωμαλίες που σχετίζονται με τις ICT (Information and Communication Technology), π.χ., λάθη χειριστών, σφάλματα λογισμικού, αποτυχίες εξοπλισμού και προφανώς φυσικές καταστροφές και προβλήματα. Κατά τη διαδικασία μετατροπής του έξυπνου δικτύου σε πιο ευφυές, πιο αυτοματοποιημένο εισάγεται στο δίκτυο-πλέγμα. Ο κίνδυνος επιθέσεων στον κυβερνοχώρο θα αυξηθεί καθώς το δίκτυο γίνεται πιο αυτοματοποιημένο. Ειδικά, τα κέντρα ελέγχου αποτελούν τον κύριο στόχο των τρομοκρατών του κυβερνοχώρου. Τα βοηθητικά προγράμματα ενέργειας εφαρμόζουν προηγμένες τεχνικές και σχέδια ασφάλειας στον κυβερνοχώρο για την αποφυγή επιθέσεων στον κυβερνοχώρο. Τεχνικές προηγμένης ανίχνευσης και πρόληψης εισβολής μπορούν να υλοποιηθούν σε διαφορετικό σημείο εισόδου του σύνθετου δικτύου. Οι πάροχοι ενέργειας υιοθετούν επίσης διαφορετικές στρατηγικές διαχείρισης κινδύνου και προσέγγιση άμυνας κατά των επιθέσεων στον κυβερνοχώρο. Είναι προφανές ότι το έξυπνο δίκτυο παρέχει πολλά οφέλη, συμπεριλαμβανομένου του ενεργειακά αποδοτικού έξυπνου σπιτιού, πιο οικολογική τεχνολογία όπως ηλιακή και αιολική ενέργεια, αποδοτική διαχείριση από πλευράς ζήτησης και ούτω καθεξής. Προκειμένου να διασφαλιστούν αυτά τα οφέλη, τα μέτρα ασφάλειας του έξυπνου δικτύου πρέπει να διατηρηθούν. [27]

Κεφάλαιο 5
Συμπεράσματα

Το έξυπνο ηλεκτρικό δίκτυο είναι ένας μεγάλου μεγέθους κλάδος, ο οποίος έχει φυσικά και θετικά και αρνητικά χαρακτηριστικά. Με την ορθή χρήση του, μπορούν να υπάρξουν αρκετές θετικές συνέπειες όπως ο απομακρυσμένος έλεγχος έξυπνων οικιακών συσκευών μέσω έξυπνων μετρητών, η αύξηση της ενεργειακής απόδοσης και ποιότητας ισχύος, η εξοικονόμηση κόστους από τη μείωση του φορτίου αιχμής και άλλες που έχουν αναφερθεί παραπάνω. Βέβαια πέραν αυτών ελλοχεύουν και πολλοί κίνδυνοι που αφορούν την ασφάλεια και την προστασία των προσωπικών δεδομένων, που μπορούν να δημιουργήσουν προβλήματα όπως η υποκλοπή και μετατροπή αυτών, η ζημιά σε κάποιον συγκεκριμένο τομέα και η αλλαγή δεδομένων και παραπλάνηση του παρόχου. Με την σωστή χρήση του έξυπνου ηλεκτρικού δικτύου και με την σωστή ασφάλεια που μπορεί να υπάρχει μέσω μεθόδων όπως είναι η κρυπτογράφηση μπορούν να υπάρξουν σημαντικές αλλαγές προς το καλύτερο στο σημερινό ηλεκτρικό δίκτυο.

Βιβλιογραφία

[1] Ε. Χριστοφόρου<<Smart grid, smart meters καιηεφαρμογήτουςστηνΕλλάδα>>, Αθήνα, 2016Rosen R., *Anticipatory Systems Philosophical, Mathematical & Methodological Foundations*, New York, NY: Pergamon Press, 1985.

[2] Rae.gr. (2019). ΡΥΘΜΙΣΤΙΚΗ ΑΡΧΗ ΕΝΕΡΓΕΙΑΣ. [online] Available at: http://www.rae.gr/site/categories_new/consumers/know_about/electricity/history.csp.

[3] Krebs, B. (2012). FBI: Smart Meter Hacks Likely to Spread — Krebs on Security. [online] Krebsonsecurity.com. Available at: https://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/

[4] 13 Factors To Consider With Smart Home Products, https://www.forbes.com/sites/forbestechcouncil/2018/01/23/13-factors-to-consider-with- smart-home-products/#7c4544fd306a

[5] Ward, M. (2014). Smart meters can be hacked to cut power bills. [online] Bbc. Available at: https://www.bbc.com/news/technology-29643276

[6] Hahn, Adam and Manimaran Govindarasu. "Cyber Attack Exposure Evaluation Framework for the Smart Grid". IEEE Transactions on Smart Grid 2.4(2011): 835-843. December 2018

[7] Egozcue, E., Rodríguez, D., Ortiz, J., Villar, V. and Tarrafeta, L. (2012). Smart Grid Security.https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/smart-grids/smart-grids-and-smart-metering/ENISA_Annex%20II%20-%20Security%20Aspects%20of%20Smart%20Grid.pdf.

[8] JavaPipe. (2019). (Distributed) Denial of Service Attack: Definition & Prevention. [online] Available at: https://javapipe.com/blog/denial-of-service-attack/

[9] Dialogos. (2019). Τιείναιηηλεκτρονικήαπάτη «Man in the Middle» και «Man in the Browser» scam. [online] Available at: https://dialogos.com.cy/ti-einai-i-ilektroniki-apati-man-in-the-middle-kai-man-in-the-vrowser-scam/ [Accessed 19 Sep. 2019]

[10] Anon, (2019). [online] Available at: https://www.cloudflare.com/learning/ddos/glossary/ip-spoofing/

[11] Crump, Catherine, Harwood, Matthew "The Net Closes Around Us",2014

[12] Basenese,"The Best Play on the Internet of Things Trend". Wall Street Daily,2015

[13] 13 Factors To Consider With Smart Home Products, https://www.forbes.com/sites/forbestechcouncil/2018/01/23/13-factors-to-consider-with-smart-home-products/#7c4544fd306a

[14] Webb, Geoff "Say Goodbye to Privacy". WIRED,2015

[15] Pathan, A., Alcaraz, C., Badra, M. and Zeadally, S. (2013). Towards Privacy Protection in Smart Grid. pp. 1-28.

[16] Energylab.gr. (2019). Έξυπνοι μετρητές ηλεκτρικής ενέργειας | EnergyLab. [online] Available at: http://www.energylab.gr/products/energy-monitoring

[17] Sharma, J. and Kumar Jain, V. (2018). A Review on Security in Smart Grids.

[18] Largue, P. (2018). Meter market: New report finds China leading global smart meter market. [online] Smart Energy International. Available at: https://www.smart-energy.com/industry-sectors/smart-energy/china-smart-electric-meter-market/

[19] Riemann, R. (2019). Smart Meters in Smart Homes. [online] Available at: https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-2-smart-meters-smart-homes_en

[20] Wei, Dong et al. "Protecting Smart Grid Automation Systems Against Cyberattacks". IEEE Transactions on Smart Grid 2.4(2011): 782-795. December 2018

[21] Χ. Τσιράκης<<Θέματα Ασφάλειας και Συνεργατικών Υπηρεσιών σε Δίκτυα Smart Grid>>, Αθήνα, 2012

[22] Bleicher, A. (2010). Privacy on the Smart Grid.

[23] energypress.gr. (2018). SPEAR: Ένα καινοτόμο έργο ανάπτυξης συστημάτων ανίχνευσης απειλών ασφάλειας σε έξυπνα δίκτυα ηλεκτρικής ενέργειας. [online] Available at: https://energypress.gr/news/spear-ena-kainotomo-ergo-anaptyxis-systimaton-anihneysis-apeilon-asfaleias-se-exypna-diktya

[24] Menezes, P. van Oorschot, and S.A. Vanstone. "Handbook of Applied Cryptography" CRC Press. 1997

[25] Α. Γιάνναρης << Κρυπτογραφία Η επιστήμη της κρυπτογραφίας αποτελεί το σύνολο των τεχνικών και των εφαρμογών μέσω των οποίων προστατεύεται η πληροφορία που ανταλλάσσεται.>>,2017

[26] Μ. Γραμματικού <<Ασφάλεια Ηλεκτρονικού Εμπορίου>>,2014

[27] Anwar, A. and Mahmood, A. (2014). Cyber Security of Smart Grid Infrastructure. p.https://www.researchgate.net/publication/259764406_Cyber_Security_of_Smart_Grid_Infrastructure

[28] Douris, C. (2017). BALANCING SMART GRID DATA AND CONSUMER PRIVACY. [ebook] Available at: https://www.lexingtoninstitute.org/wp-content/uploads/2017/07/Lexington_Smart_Grid_Data_Privacy-2017.pdf