Τμήμα Μηχανικών Πληροφορικής & Τηλεπικοινωνιών,
Πανεπιστήμιο Δυτικής Μακεδονίας,
Καραμανλή & Λυγερής, 501000, Κοζάνη, Ελλάδα

Η ΑΡΧΙΤΕΚΤΟΝΙΚΗ SPEAR

Μία Καινοτόμα Προσέγγιση Προστασίας του Έξυπνου Ενεργειακού Δικτύου

SPEAR

European Union's Horizon 2020 Framework Programme
For Research and Innovation

Παναγιώτης Σαρηγιαννίδης, Γεώργιος Κακαμούκας, Δημήτριος Πλιάτσιος, Παναγιώτης Ράδογλου-Γραμματίκης και Άννα Τριανταφύλλου

2018

Περιεχόμενα

Περίληψη

Καθώς η κοινωνία μας εξαρτάται σε μεγάλο βαθμό από τις κρίσιμες υποδομές (Ενέργεια, Υγεία, Οικονομία, κ.λπ.), απαιτείται η ανάπτυξη νέων τεχνολογικών λύσεων για την έγκαιρη ανίχνευση και πρόληψη ζητημάτων ασφάλειας στον τομέα των Τεχνολογιών Πληροφορίας και Επικοινωνίας (ΤΠΕ). Ακριβέστερα, η ανίχνευση και η κατάλληλη έγκαιρη απόκριση σε κυβερνοεπιθέσεις, ειδικότερα από πηγές επιθέσεων με σημαντικά κίνητρα και υψηλή χρηματοδότηση, αποτελεί σημαντική πρόκληση. Μία από τις πιο ευάλωτες περιπτώσεις κρίσιμων υποδομών είναι το έξυπνο ενεργειακό πλέγμα ή δίκτυο, καθώς πιθανές δυσλειτουργίες μπορούν να οδηγήσουν σε κρίσιμες καταστάσεις, όπως απώλειες ανθρώπινων ζωών, αδυναμία πρόσβασης και χειρισμού της ηλεκτρικής ενέργειας, καθώς και σοβαρές οικονομικές επιπτώσεις. Το έξυπνο ενεργειακό δίκτυο αποτελεί το νέο τεχνολογικό άλμα στον τομέα της ηλεκτρικής ενέργειας, παρέχοντας καλύτερη διαχείριση ενέργειας, υψηλότερη απόδοση, μεγαλύτερη αξιοπιστία καθώς και δυνατότητες αυτοΐασης. Καθώς η συγκεκριμένη τεχνολογία εξαπλώνεται με ραγδαίους ρυθμούς, τα κίνητρα των επιτιθέμενων αυξάνονται αντίστοιχα. Ωστόσο, οι τρέχουσες λύσεις ασφάλειας δεν λαμβάνουν υπόψη τις δυνατότητες της ανάλυσης και οπτικοποίησης μεγάλων δεδομένων, ενώ ταυτόχρονα δεν παρέχουν διαδικασίες συλλογής αποδεικτικών στοιχείων για επιθετικές ενέργειες, οι οποίες θα ήταν κρίσιμες για δικαστικές αποφάσεις.

Το ερευνητικό πρόγραμμα H2020-DS-07-2016-2017 Secure and PrivatE smArt gRid (SPEAR), το οποίο συντονίζεται από το Πανεπιστήμιο Δυτικής Μακεδονίας (ΠΔΜ), στοχεύει στην υλοποίηση κατάλληλων λύσεων ασφάλειας στο έξυπνο ενεργειακό δίκτυο, εστιάζοντας σε καινοτόμες διαδικασίες ανίχνευσης και πρόληψης εισβολών. Αναλυτικότερα, το πρόγραμμα SPEAR εισάγει μία αρχιτεκτονική καινοτομία τριών επιπέδων, διασφαλίζοντας τις ανάγκες της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων και των υπηρεσιών. Σκοπός του πρώτου επιπέδου είναι η υλοποίηση ενός Συστήματος Διαχείρισης Πληροφοριών και Δεδομένων (System Information Event Management - SIEM) το οποίο ονομάζεται SPEAR-SIEM και στοχεύει στην ανάλυση και στη βέλτιστη διαχείριση πολλαπλών πληροφοριών, ανιχνεύοντας πιθανά πρότυπα απειλών και ενεργοποιώντας τα κατάλληλα αντίμετρα. Το δεύτερο επίπεδο, εστιάζει στην υλοποίηση ενός πλαισίου επεξεργασίας δεδομένων και θέσπισης ενεργειών, οι οποίες θα δύναται να χρησιμοποιηθούν σε δικαστικές

διαδικασίες. Το συγκεκριμένο πλαίσιο ονομάζεται SPEAR Forensic Readiness Framework (SPEAR-FRF) και θα περιλαμβάνει καινοτόμες διαδικασίες προσέλκυσης επιτιθέμενων, όπως παγίδες εισβολών (honeypots) προσαρμοσμένες στο έξυπνο ενεργειακό δίκτυο. Τέλος, το τρίτο επίπεδο αποτελεί ένα ανώνυμο κανάλι επικοινωνίας μεταξύ παρόχων και διανομής ενέργειας στην Ευρώπη, με στόχο την ανταλλαγή πληροφοριών για ζητήματα ασφάλειας στον κυβερνοχώρο. Συμπερασματικά, η αρχιτεκτονική του προγράμματος SPEAR εστιάζει στην υλοποίηση ενός συνεργατικού πλαισίου από εταιρίες παροχής και διανομής ηλεκτρικής ενέργειας, κατασκευαστικές επιχειρήσεις, πανεπιστήμια, ερευνητικά κέντρα και μικρομεσαίες επιχειρήσεις, δημιουργώντας και επικυρώνοντας παράλληλα νέες δυνατότητες στον τομέα της ασφάλειας του έξυπνου ενεργειακού δικτύου διάμεσου τεσσάρων πιλοτικών εφαρμογών.

Abstract

As our society is becoming increasingly dependent on Critical Infrastructure (CI), new technologies are needed to increase our detection and response capabilities. Detecting and responding to cyberattacks by a highly motivated, skilled and well-funded attacker has been proven highly challenging. One of the most vulnerable and high-impact CI is the smart grid since the collapse of an energy production utility may cause human lives, millions of euros, denial of a very important and common good such as energy and days or even months of recovering. Smart Grid is considered as the next-generation power system, which promises self-healing, resilience, sustainability and efficiency to the energy CI. As the smart grid paradigm is reaching every house and building, the potential of attracting cyber-attackers towards getting access to the underlying systems and networks is getting larger. Most of the present security solutions neglect the added-value that high-efficiency analytics and visualisation could bring in the today's smart grid arsenal, while underestimate the trade-off between the forensic effectiveness user privacy.

The H2020-DS-07-2016-2017 Secure and PrivatE smArt gRid (SPEAR) project, which is coordinated by the University of Western Macedonia, comes to provide effective solutions in detecting, responding and taking countermeasures against advanced cyber threats and attacks targeted to modern smart grids. SPEAR proposes a three-tier platform, where each part has different yet complementary role. The first-tier builds an advanced all-in-one, Security Information and Event Management (SIEM) tool, called SPEAR SIEM. The second-tier intends to provide a rigorous forensic framework, called SPEAR Forensic Readiness Framework (SPEAR-FRF), able to collect necessary information from the smart grid systems directly from the SPEAR SIEM tool. Innovative techniques are employed behind the implementation of the SPEAR-FRF, such as the design and the deployment of Advanced Metering Infrastructure (AMI) honeypots, for attracting attackers and capturing the necessary attacks traces and the implementation of an effective privacy-preserving framework. SPEAR goes beyond by inaugurating an anonymous and secure communication channel between all energy operators in EU in the third-tier. An EU-wide collaborative framework is introduced that will foster Situational Awareness (SA) by forming a common and robust defence line against threats and attacks, while validating the SPEAR architecture in four realistic

and rigorous use cases, where power plants, energy operators, energy stakeholders, universities and Small and Medium-sized Enterprises (SMEs) will cooperate to demonstrate the SPEAR platform.

1. Εισαγωγή

Σήμερα, η χρήση των έξυπνων συσκευών και του διαδικτύου έχει καταστεί αναγκαία σε πολλές πτυχές της καθημερινής ζωής. Τα έξυπνα «πράγματα» κάνουν τη ζωή μας ευκολότερη, αποτελώντας τη βάση για την ανάπτυξη νέων τεχνολογιών και την αναβάθμιση κρίσιμων υποδομών της κοινωνίας (ενέργεια, υγεία, οικονομία, κ.λπ.). Αυτή η ραγδαία τεχνολογική εξέλιξη είναι φυσικό να συνοδεύεται από αδυναμίες. Τα τελευταία χρόνια έχουν διεξαχθεί πολλαπλές επιθέσεις στον κυβερνοχώρο, με κοινωνικά και πολιτικά κίνητρα [1]. Παρόλα αυτά, πριν από μια δεκαετία, μια διαδικτυακή επίθεση δεν θα μπορούσε να έχει αντίκτυπο σε μια ανθρώπινη ζωή. Καθώς η κοινωνία μας εξαρτάται σε μεγάλο βαθμό από τις κρίσιμες υποδομές, απαιτείται η ανάπτυξη νέων τεχνολογικών λύσεων για την έγκαιρη ανίχνευση και πρόληψη ζητημάτων ασφάλειας στον τομέα των Τεχνολογιών Πληροφορίας και Επικοινωνίας (ΤΠΕ). Ακριβέστερα, η ανίχνευση και η κατάλληλη έγκαιρη απόκριση σε κυβερνοεπιθέσεις, ειδικότερα από πηγές επιθέσεων με σημαντικά κίνητρα και υψηλή χρηματοδότηση, αποτελεί σημαντική πρόκληση.

Μία από τις πιο ευάλωτες περιπτώσεις κρίσιμων υποδομών είναι το έξυπνο ενεργειακό πλέγμα ή δίκτυο. Το έξυπνο ενεργειακό δίκτυο (ESG) είναι η εξέλιξη του παραδοσιακού δικτύου ηλεκτρικής ενέργειας, στηριζόμενο στην αμφίδρομη ροή ηλεκτρικής ενέργειας και πληροφοριών, εστιάζοντας στην αποτελεσματικότερη παραγωγή, διαμοιρασμό, αλλά και έλεγχο της ηλεκτρικής ενέργειας [2]. Το ESG χρησιμοποιεί καινοτόμα προϊόντα και υπηρεσίες μαζί με έξυπνες τεχνολογίες παρακολούθησης, ελέγχου, επικοινωνίας και αυτοεξυπηρέτησης στοχεύοντας στην άμεση ανταπόκριση σε μεταβολές ζήτησης της ηλεκτρικής ενέργειας. Στόχος του ESG είναι να παρέχει αξιοπιστία μέσω της παρακολούθησης σε πραγματικό χρόνο, αλλά και αποτελεσματικότητα στη διαχείριση της ενέργειας για υψηλότερη απόδοση. Παρόλα αυτά, εξαιτίας της μεγάλης κλίμακάς του, διαθέτει πολλά τρωτά σημεία. Πιθανές δυσλειτουργίες μπορούν να οδηγήσουν σε κρίσιμες καταστάσεις, όπως απώλειες ανθρώπινων ζωών, αδυναμία πρόσβασης και χειρισμού της ηλεκτρικής ενέργειας, καθώς και σοβαρές οικονομικές επιπτώσεις [3]. Προκειμένου να ενισχυθεί το επίπεδο ασφαλείας του ESG και να αντιμετωπιστούν αυτά τα κρίσιμα σημεία ευπάθειας, θα πρέπει να εγκατασταθούν πιο προηγμένες τεχνικές ανίχνευσης ανωμαλιών. Το ρόλο αυτό αναλαμβάνει η αρχιτεκτονική SPEAR.

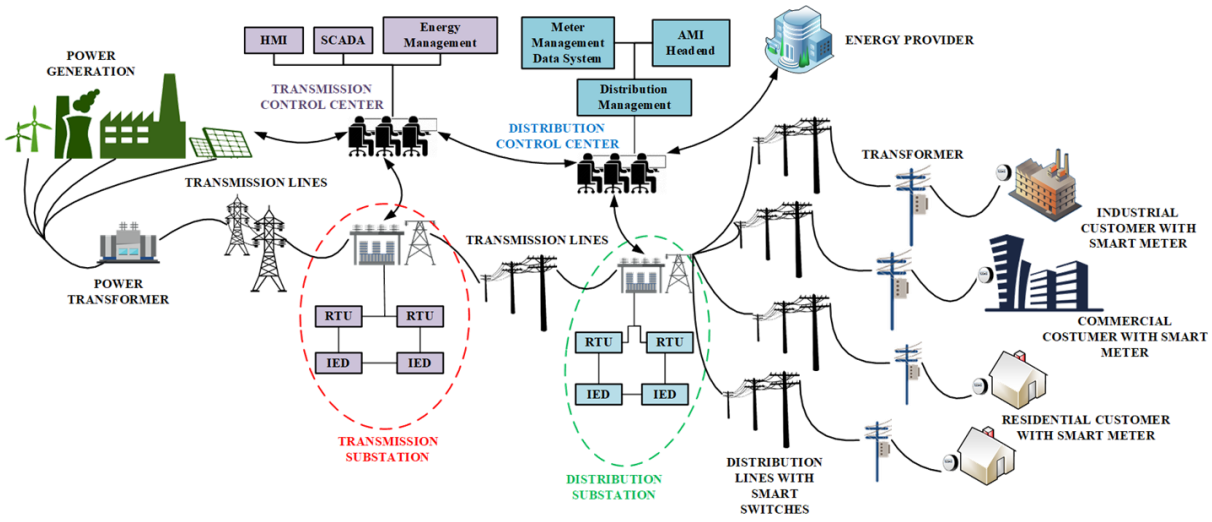
Στην ακόλουθη ενότητα, θα πραγματοποιηθεί μια μελέτη της αρχιτεκτονικής, της λειτουργίας και των τρωτών σημείων ασφάλειας ενός έξυπνου ενεργειακού δικτύου. Έπειτα, θα ακολουθήσει μια αναλυτική παρουσίαση της αρχιτεκτονικής SPEAR και μια σύντομη αναφορά στις εφαρμογές αξιολόγησή της. Συνοψίζοντας, θα προβληθεί η συνεισφορά και το επίπεδο καινοτομίας που προσφέρεται μέσω της νέας αυτής πλατφόρμας για την ασφάλεια των έξυπνων ενεργειακών δικτύων.

2. Προκλήσεις ασφαλείας για τα Έξυπνα Ενεργειακά Δίκτυα

Η αρχιτεκτονική ενός ESG ορίζει διαφορετικά επίπεδα αρμοδιοτήτων και επικοινωνίας, γεγονός που το καθιστά όχι μόνο αποτελεσματικό αλλά και ευέλικτο στη διαχείριση. Στην ουσία, ένα έξυπνο ενεργειακό δίκτυο αποτελείται από πολλαπλά κέντρα ελέγχου. Κάθε κέντρο ελέγχου περιλαμβάνει διακομιστές SCADA, συστήματα διαχείρισης ενέργειας (EMS) και διεπαφές ανθρώπων-μηχανών (HMI). Το SCADA είναι ένα δίκτυο επικοινωνίας εντός του ESG, το οποίο αποτελείται από δύο υποσυστήματα, το σύστημα διαχείρισης ενέργειας (EMS) και το σύστημα διαχείρισης διανομής (DMS). Πρόκειται για ένα σύστημα που συνδυάζει εξαρτήματα υλικού και λογισμικού. Το SCADA περιλαμβάνει μια κύρια μονάδα τερματικού (MTU), η οποία τοποθετείται σε κεντρική θέση. Περιλαμβάνει επίσης εξοπλισμό επικοινωνίας, όπως τηλεφωνική γραμμή, ραδιόφωνο, καλώδιο ή δορυφόρο, και ένα ή περισσότερα απομακρυσμένα τερματικά (RTU) ή προγραμματιζόμενους λογικούς ελεγκτές (PLC) που τοποθετούνται διάσπαρτα σε περιοχές. Το κεντρικό, έξυπνο μέρος ενός ESG είναι η Υποδομή Προηγμένης Μέτρησης (ΥΠΜ) - (Advanced Metering Infrastructure - AMI). Η ΥΠΜ είναι υπεύθυνη για τη συλλογή, την ανάλυση και την επεξεργασία δεδομένων που σχετίζονται με τη παρακολούθηση της ροής ενέργειας στο σύστημα. Στο Σχήμα 1 παρουσιάζεται η συνολική αρχιτεκτονική ενός έξυπνου ενεργειακού δικτύου, περιλαμβάνοντας τρία βασικά υποσυστήματα:

1. *Έξυπνο σύστημα Υποδομής* : το οποίο είναι υπεύθυνο για την ενέργεια, την πληροφόρηση και την επικοινωνία του έξυπνου δικτύου. Το σύστημα αυτό υποστηρίζει την ανεπτυγμένη παραγωγή, μεταφορά και κατανάλωση ενέργειας, την ανεπτυγμένη μέτρηση, παρακολούθηση και διαχείριση ενέργειας και τις ανεπτυγμένες τεχνολογίες επικοινωνίας.

2. *Έξυπνο σύστημα Διαχείρισης* : το οποίο είναι υπεύθυνο για τις υπηρεσίες διαχείρισης και ελέγχου της ενέργειας, με στόχους την βελτίωση της ενεργειακής απόδοσης, των χαρακτηριστικών της ζήτησης, την μείωση του κόστους και τον έλεγχο των εκπομπών.
3. *Έξυπνο σύστημα Προστασίας* : το οποίο είναι υπεύθυνο για την αξιόπιστη χρήση του δικτύου, προστασία από πιθανές βλάβες, καθώς και άλλες υπηρεσίες ασφαλείας.



Σχήμα 1 Αρχιτεκτονική Έξυπνου Ενεργειακού Δικτύου

Λαμβάνοντας υπόψη την τεράστια κλίμακα του δικτύου, λογικό είναι να υπάρχουν τρωτά σημεία ασφαλείας. Παρόλα αυτά, πιθανές δυσλειτουργίες μπορούν να επιφέρουν σοβαρές επιπτώσεις. Τρωτά σημεία ασφαλείας των ESGs είναι τα ακόλουθα:

- Έξυπνες συσκευές διαχείρισης ως σημεία εισόδου επίθεσης στο δίκτυο.
- Μη εξουσιοδοτημένη πρόσβαση στη υποδομή προηγμένης μέτρησης (Advanced Metering Infrastructure)
- Απόκτηση πρόσβασης στο σύστημα εποπτικού ελέγχου και απόκτησης δεδομένων (Supervisory Control And Data Acquisition - SCADA)
- Έλλειψη ασφαλείας στην ανταλλαγή μηνυμάτων των συστημάτων αυτοματισμού υποσταθμών (Substation Automation Systems)
- Η χρήση διευθύνσεων IP στις έξυπνες συσκευές

Τα δεδομένα που μεταφέρονται διαμέσων του ESG περιέχουν ευαίσθητες πληροφορίες, οι οποίες, εάν δεν προστατεύονται αποτελεσματικά, θέτουν σε κίνδυνο την αποτελεσματικότητα και την ακεραιότητα των υποσυστημάτων. Παρά το γεγονός, ότι υπάρχει ένα επίπεδο ασφάλειας και ελέγχου πρόσβασης σε πληροφορίες και συσκευές, δεν είναι αρκετό για να διασφαλιστεί η ακεραιότητα των δεδομένων στα έξυπνα ενεργειακά δίκτυα. Εξαιτίας του μεγέθους και της πολυπλοκότητας των δικτύων, πολλές αδυναμίες προβάλλονται ως πιθανά σημεία εισόδου για επιθέσεις. Μια εμπεριστατωμένη έρευνα για μοντέλα επιθέσεων στον κυβερνοχώρο για περιβάλλοντα ESG παρουσιάζεται στο [4]. Η καινοτόμα αρχιτεκτονική SPEAR στοχεύει στην ανίχνευση και απόκριση των επιθέσεων αυτών στον κυβερνοχώρο με τη χρήση νέων τεχνολογιών και δυνατοτήτων, παρέχοντας ολοκληρωμένες, ισχυρές και αποτελεσματικές λύσεις ασφάλειας για έξυπνα περιβάλλοντα. Σύμφωνα με τις NIST SP 800-53 [5] και NIST SP 800-82 [6], μέχρι στιγμής δεν έχει γίνει σωστή ενημέρωση σχετικά με τις δυνατοτήτες και τις αδυναμίες των έξυπνων συσκευών και μετρητών ενέργειας σε ευρωπαϊκό επίπεδο. Η αρχιτεκτονική SPEAR θα καλύψει αυτό το κενό γνώσης και θα παρέχει τη δυνατότητα εύρεσης αποδείξεων διαδικτυακής επίθεσης για χρήση σε δικαστική διαμάχη, αυξάνοντας έτσι την αξιοπιστία για τη λειτουργία των έξυπνων ενεργειακών δικτύων σε όλη την Ευρώπη.

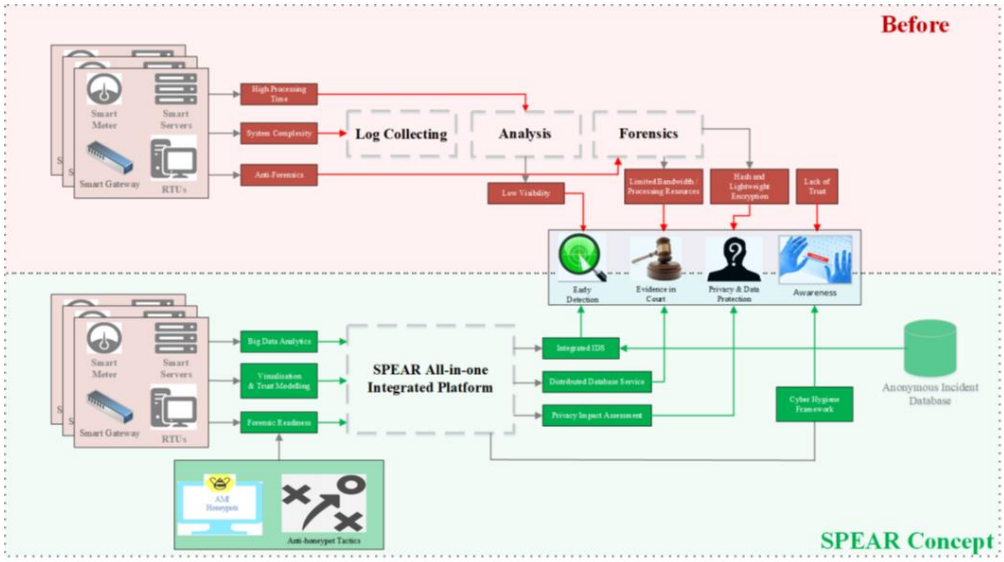
3. Αρχιτεκτονική SPEAR

Το ερευνητικό πρόγραμμα H2020-DS-07-2016-2017 Secure and PrivatE smArt gRid (SPEAR), το οποίο συντονίζεται από το Πανεπιστήμιο Δυτικής Μακεδονίας (ΠΔΜ), στοχεύει στην υλοποίηση κατάλληλων λύσεων ασφάλειας στο έξυπνο ενεργειακό δίκτυο, εστιάζοντας σε καινοτόμες διαδικασίες ανίχνευσης και πρόληψης εισβολών.
Βασικοί του στόχοι του SPEAR, όπως αποτυπώνονται στο Σχήμα 2, είναι οι ακόλουθοι:

- Έγκαιρη ανίχνευση εξελισσόμενων επιθέσεων ασφάλειας μέσω ανάλυσης δεδομένων, προηγμένης ανίχνευσης ανωμαλιών με οπτικές δυνατότητες και ενσωματωμένη διαχείριση εμπιστοσύνης έξυπνων κόμβων.
- Ανάπτυξη ενός προηγμένου πλαισίου εγκληματολογικής ετοιμότητας με χρήση παγίδων εισβολής (honeypots), οι οποίες αναγνωρίζουν τα ίχνη επίθεσης και

συλλέγουν τα απαραίτητα νομικά στοιχεία για το δικαστήριο, διατηρώντας ταυτόχρονα τις προσωπικές πληροφορίες του χρήστη [7].

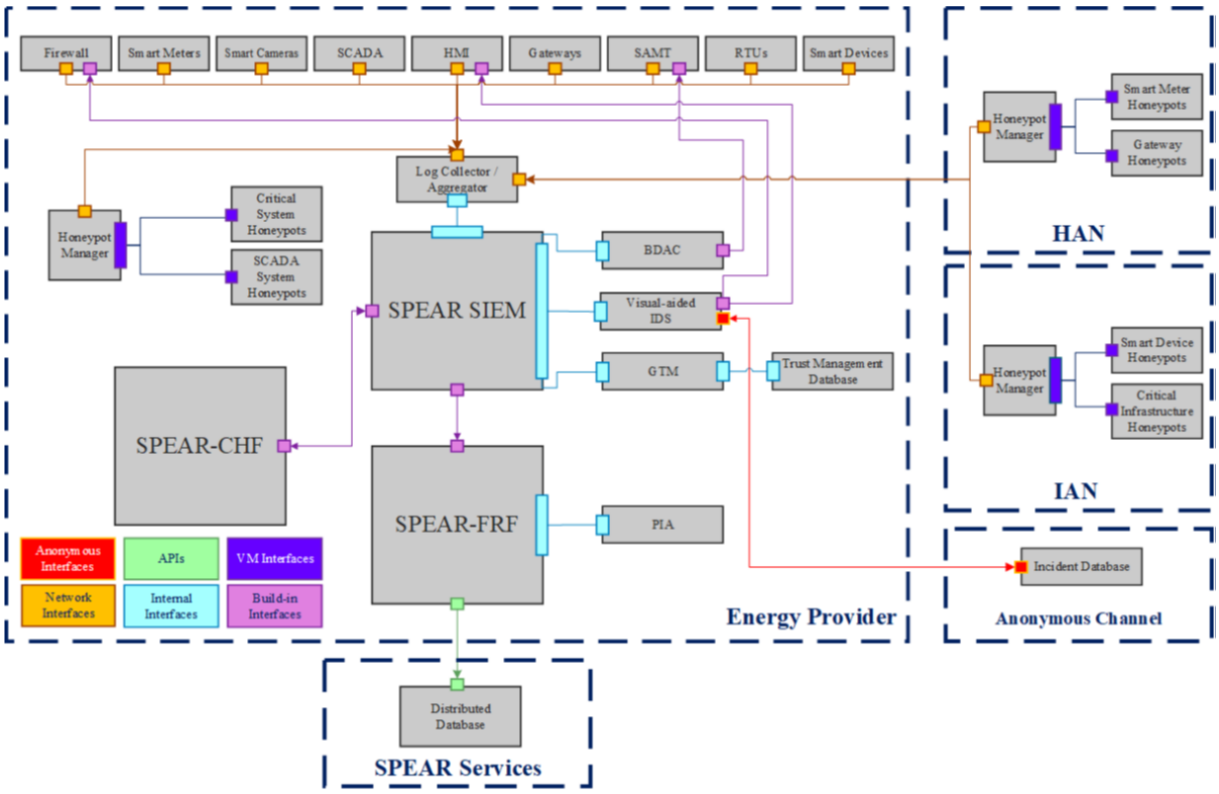
- Εφαρμογή ενός ανώνυμου καναλιού για έξυπνα ενεργειακά δίκτυα στοχεύοντας στην αύξηση εμπιστοσύνης για την ανταλλαγή ευαίσθητων πληροφοριών σχετικά με περιστατικά επιθέσεων στο κυβερνοχώρο.
- Ενδυνάμωση της συνεργασίας με ευρωπαϊκούς και παγκόσμιους οργανισμούς ασφάλειας, φορείς προτυποποίησης, βιομηχανικές ομάδες και φορείς εκμετάλλευσης έξυπνων ενεργειακών δικτύων.
- Δημιουργία ανταγωνιστικών επιχειρηματικών μοντέλων για τη χρήση των εφαρμοσμένων εργαλείων ασφάλειας σε φορείς εκμετάλλευσης έξυπνων ενεργειακών δικτύων και συντελεστών σε ολόκληρη την Ευρώπη.



Σχήμα 2: Βασικοί στόχοι της αρχιτεκτονικής SPEAR

Το πρόγραμμα SPEAR εισάγει μία καινοτόμα αρχιτεκτονική τριών επιπέδων, διασφαλίζοντας τις ανάγκες της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων και των υπηρεσιών. Σύμφωνα με το Σχήμα 3, το πρώτο επίπεδο είναι η υλοποίηση ενός Συστήματος Διαχείρισης Πληροφοριών και Δεδομένων (System Information Event Management - SIEM) το οποίο ονομάζεται SPEAR-SIEM. Το δεύτερο επίπεδο, εστιάζει στην υλοποίηση ενός πλαισίου επεξεργασίας δεδομένων και θέσπισης ενεργειών, οι οποίες θα δύναται να χρησιμοποιηθούν σε δικαστικές διαδικασίες. Το συγκεκριμένο πλαίσιο ονομάζεται SPEAR Forensic Readiness Framework (SPEAR-FRF) και θα περιλαμβάνει καινοτόμες διαδικασίες προσέλκυσης

επιτιθέμενων, όπως παγίδες εισβολών προσαρμοσμένες στο έξυπνο ενεργειακό δίκτυο, είτε εσωτερικά στα κεντρικά συστήματα ελέγχου, είτε στα δίκτυα . Τέλος, το τρίτο επίπεδο αποτελεί ένα πλαίσιο πρωτοκόλλων ασφάλειας, συστάσεων και πολιτικών, που θα χαρακτηρίζονται ως SPEAR Cyber Hygiene Framework (SPEAR-CHF), βασιζόμενα στην διεξοδική ανάλυση κινδύνου μετά από εντατικές δοκιμές επίθεσης στα συστήματα άμυνας των τελικών χρηστών στο έξυπνο ενεργειακό δίκτυο. Στα πλαίσια αυτού, αναπτύσσεται ένα ανώνυμο κανάλι επικοινωνίας μεταξύ παρόχων και διανομής ενέργειας στην Ευρώπη, με στόχο την ανταλλαγή πληροφοριών για ζητήματα ασφάλειας στον κυβερνοχώρο.

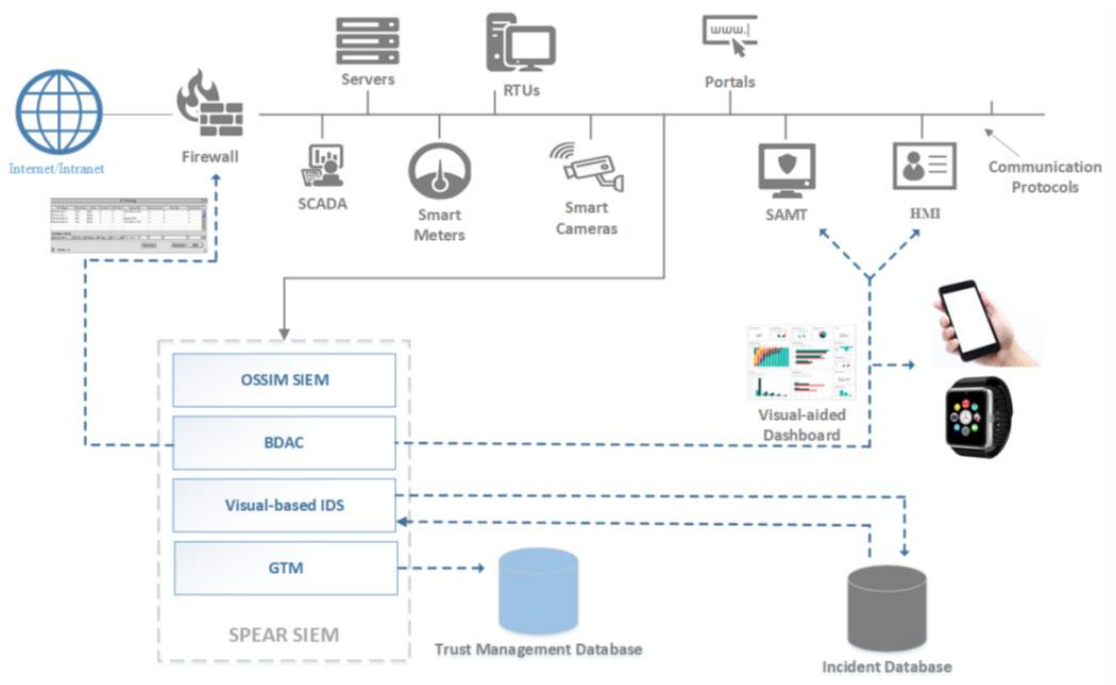


Σχήμα 3: Αρχιτεκτονική SPEAR

3.1 System Information Event Management (SIEM)

Με βάση την αρχιτεκτονική SPEAR, το εργαλείο SIEM, ως μέθοδος παρακολούθησης, συλλογής και ανάλυσης καταγραφών και συμβάντων δικτύων, συστημάτων και λειτουργικών συστημάτων, εξελίσσεται εξασφαλίζοντας αποτελεσματική ανάλυση των αρχείων καταγραφής συλλογής και των ιχνών για την επέκταση των δυνατοτήτων

των συμβατικών εργαλείων SIEM, από άποψη βαθιάς επιθεώρησης πακέτων, ανάλυσης απειλών και ανάλυσης πρωτοκόλλου. Για να επιτύχει αυτούς τους φιλόδοξους στόχους, το SPEAR SIEM βασίζεται σε έναν συλλέκτη καταγραφής ανοιχτού κώδικα βασισμένο στον μηχανισμό OSSIM του AlienVault, ο οποίος συγκεντρώνει τα ίχνη του συστήματος και του δικτύου από όλα τα στοιχεία του έξυπνου ενεργειακού δικτύου (π.χ. SCADA συστήματα, πύλες, εσωτερικοί έξυπνοι μετρητές, συσκευές και αισθητήρες και RTU) και από όλα τα προεγκατεστημένα στοιχεία ασφαλείας (π.χ. τείχος προστασίας, μονάδες διαχείρισης ασφάλειας και εργαλείο - SAMT) και τροφοδοτεί το στοιχείο SPEAR-SIEM χρησιμοποιώντας διασυνδέσεις δικτύου (π.χ. Ethernet).



Σχήμα 4: SPEAR SIEM Tool

Όπως παρουσιάζεται στα Σχήματα 3 και 4, το SPEAR-SIEM περιλαμβάνει τα ακόλουθα στοιχεία:

- Big Data Analytics (BDAC)
- Visual IDS
- Grid Trusted Module (GTM)

Το BDAC επεκτείνει τις δυνατότητες του SPEAR-SIEM υιοθετώντας αναλύσεις πολλαπλών δεδομένων για την ανίχνευση ανωμαλιών με την εφαρμογή αποφάσεων συσχετισμού και μηχανικής μάθησης στα αρχεία καταγραφής που συλλέγονται από τον

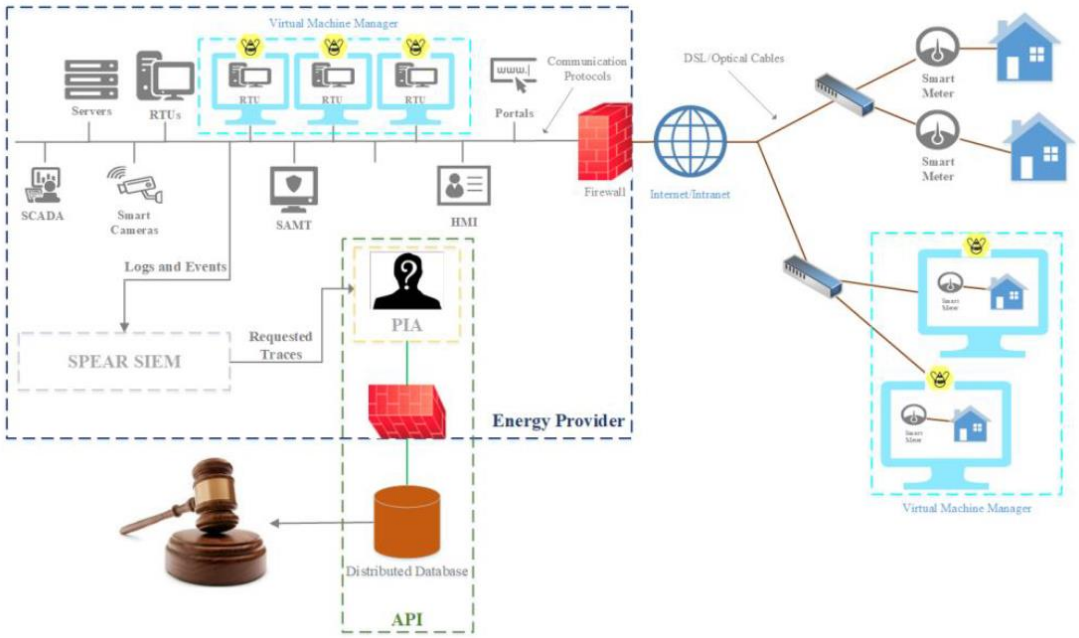
συλλέκτη. Το BDAC ενισχύεται επίσης από το στοιχείο GTM, το οποίο είναι εξοπλισμένο με αλγόριθμους διαχείρισης εμπιστοσύνης κατά την εφαρμογή φιλτραρίσματος βασιζόμενο στη φήμη των κόμβων (συσκευές, μετρητές, διεπαφές και πύλες) που συνδέονται με το έξυπνο ενεργειακό δίκτυο. Η βασική υπηρεσία που παρέχει το GTM είναι η ανίχνευση επιθέσεων από το εσωτερικό σύστημα ελέγχου. Σε περίπτωση ανίχνευσης μιας επίθεσης, εντοπίζει την επικίνδυνή IP διεύθυνση και την αντίστοιχη συσκευή, ειδοποιώντας το κεντρικό σύστημα ασφάλειας. Επιπρόσθετα, η χρήση οπτικών εργαλείων και οθονών για την παρακολούθηση συστημάτων ανίχνευσης επιθέσεων (Visual-based IDS tools) αποτελεί ένα ακόμη βοηθητικό στοιχείο του SPEAR-SIEM, στοχεύοντας στην άμεσο εντοπισμό και παρέμβαση σε περίπτωση σφάλματος ή επίθεσης. Όλα αυτά τα στοιχεία συνθέτουν ένα αποτελεσματικό και γρήγορο εργαλείο για την αντιμετώπιση ακόμη και υψηλού επιπέδου επιθέσεων.

3.2 SPEAR Forensic Readiness Framework (FRF)

Το SPEAR-FRF, ως το δεύτερο επίπεδο της αρχιτεκτονικής, εφαρμόζει μια διαδικασία εκτίμησης των επιπτώσεων στην ιδιωτικότητα (Privacy Impact Assessment - PIA) με βάση τα εγγεγραμμένα ίχνη επισκεψιμότητας από τα honeypots, αποσκοπώντας στον εντοπισμό και στη μείωση των κινδύνων ιδιωτικού απορρήτου [8]. Το SPEAR-FRF, όπως παρουσιάζεται στο Σχήμα 5, συντελεί αποτελεσματικά στη δημιουργία ενός πλαισίου επεξεργασίας δεδομένων και θέσπισης ενεργειών για χρήση σε δικαστικές διαδικασίες [9], χρησιμοποιώντας τη μεθοδολογία OSCAR διασφαλίζοντας έτσι την ορθή συλλογή των αναγκαίων εγκληματολογικών πληροφοριών [10].

Τα honeypots, είναι συστήματα που έχουν καθιερωθεί ως ένας αντιπερισπασμός για την προσέλκυση επιτιθέμενων στον κυβερνοχώρο. Στόχος τους είναι η ανίχνευση και η μελέτη των προσπαθειών για απόκτηση μη εξουσιοδοτημένης πρόσβασης σε συστήματα πληροφοριών. Η ιδέα του honeypot έχει χρησιμοποιηθεί σε συστήματα ανίχνευσης επιθέσεων γενικού σκοπού για μεγάλο χρονικό διάστημα και επίσης προτείνονται για την προστασία των συστημάτων SCADA [11]. Πράγματι, φαίνεται ότι τα honeypots που έχουν σχεδιαστεί για τη συλλογή δεδομένων σε βιομηχανικά έξυπνα περιβάλλοντα είναι αρκετά χρήσιμα, καθώς προσελκύουν πολλές επιθέσεις στον κυβερνοχώρο, π.χ. 4000 επιθέσεις σε μόνο 3 ημέρες. Παρόλα αυτά, τα τυπικά

honeypots δεν είναι κατάλληλα για συστήματα έξυπνων ενεργειακών δικτύων δεδομένου ότι δεν καλύπτονται ακόμη ορισμένες εξειδικευμένες απαιτήσεις που σχετίζονται με τα συστήματα SCADA στα συστήματα βιομηχανικού ελέγχου.



Σχήμα 5: SPEAR-FRF

Η καινοτομία των SPEAR honeypots έγκειται στην χρήση τους εκτός των εγκαταστάσεων του προμηθευτή ενέργειας, δηλαδή στην Υποδομή Προηγμένης Μέτρησης (AMI Honeypots). Ένα βοηθητικό πρόγραμμα ενέργειας συλλέγει χρήσιμες πληροφορίες από τους έξυπνους μετρητές που βρίσκονται κοντά στα (έξυπνα) σπίτια ή σε βιομηχανικούς χώρους (π.χ. δίκτυο διανομής ενέργειας) μέσω κατάλληλων στρατηγικών υλοποίησης και ανάπτυξης. Τα honeypots διακρίνονται σε δύο βασικές κατηγορίες: χαμηλής αλληλεπίδρασης και υψηλής αλληλεπίδρασης. Ένα honeypot υψηλής αλληλεπίδρασης θα ήταν μέσα σε ένα πραγματικό σύστημα / συσκευή και θα έδινε στον επιτιθέμενο τη δυνατότητα να αλληλεπιδράσει με αυτό. Από την άλλη πλευρά, ένα honeypot χαμηλής αλληλεπίδρασης θα μιμούνταν απλά το σύστημα / συσκευή, πείθοντας απλά τον εισβολέα που αλληλεπιδράσει με τον πραγματικό πόρο [12]. Το SPEAR θα στηριχθεί στο έργο Conpot [13], όπου μελετήθηκε η υλοποίηση ενός χαμηλής διαδραστικότητας honeypot σε σύστημα SCADA για την υποστήριξη

διαφόρων υπηρεσιών όπως HTTP, το πρωτόκολλο Simple Network Management Protocol (SNMP) και άλλα πρωτόκολλα σειριακής επικοινωνίας.

Πιο συγκεκριμένα, στα πλαίσια της αρχιτεκτονικής SPEAR, αναπτύσσεται ένα σύνολο honeypots υποδυόμενα RTU συσκευές για δύο κύριους λόγους [14]. Αρχικά, διότι αποκρύπτουν την πραγματική υποδομή RTU και έπειτα διότι παγιδεύουν τον εισβολέα συλλέγοντας τις απαραίτητες πληροφορίες που παραδίδονται στο σύστημα SIEM. Επίσης, η ανάπτυξη εσωτερικών honeypots θα βοηθήσει στην συλλογή σημαντικών εγκληματολογικών πληροφοριών, από εσωτερικές επιθέσεις, δηλαδή απειλές που προέρχονται από το εσωτερικό σύστημα ελέγχου (π.χ. αφήνοντας USB μονάδες δίσκου που περιέχουν κακόβουλο λογισμικό σε στρατηγικές τοποθεσίες, έτσι ώστε να εγκαταστήσετε ένα backdoor στο IT / smart υποδομή δικτύου).

3.3 SPEAR - Cyber Hygiene Framework (CHF)

Το SPEAR-CHF αποσκοπεί στην παροχή πρωτοκόλλων, πολιτικών και κανόνων προστασίας για τον εντοπισμό και την αντιμετώπιση κινδύνων πριν από την ενεργοποίησή τους. Το πλαίσιο αυτό, θα περιλαμβάνει ένα κατάλογο πιθανών απειλών στον κυβερνοχώρο όσον αφορά την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα δεδομένων. Για κάθε απειλή στον κυβερνοχώρο θα σχεδιαστεί μια ενότητα κατάρτισης τόσο για το προσωπικό της βιομηχανίας, όσο και για τους καταναλωτές ενέργειας. Για παράδειγμα, για μια επίθεση Man in the Middle, θα παρέχεται μια λεπτομερής ενότητα μάθησης, εξηγώντας τον τύπο της επίθεσης, τις αναμενόμενες συνέπειες και τους τρόπους ανίχνευσής της χρησιμοποιώντας το λογισμικό ανάλυσης καταγραφής. Επιπλέον, θα σχεδιαστεί ένας οδηγός για το πώς μπορεί να εκτεθεί αμέσως αυτή η απειλή. Επίσης, προβλέπονται ανάλογα σχέδια για επιπλέον ενέργειες, εάν η επίθεση γίνει ισχυρότερη.

Στα πλαίσια αυτών των κανονισμών για τη διατήρηση της εμπιστευτικότητας και ακεραιότητας των πληροφοριών, προτείνεται η ανάπτυξη του SPEAR-RI (Repository of Incidents), μιας κατανεμημένης βάσης δεδομένων για τη καταγραφή επιθέσεων. Το SPEAR-RI θα παρέχει ανώνυμα κανάλια διασύνδεσης (Anonymous Incident Communication Channel - AICC) μεταξύ όλων των φορέων εκμετάλλευσης έξυπνων ενεργειακών δικτύων. Η ανάπτυξή του θα γίνει σύμφωνα με παρόμοιους οργανισμούς

της ΕΕ (EE-ISAC [15] και ESMIG [16]). Το SPEAR στοχεύει στην προώθηση της ιδέας για αξιοποίηση ενός δικτύου εμπιστοσύνης, όπου οι ευαίσθητες πληροφορίες ανταλλάσσονται μεταξύ ινστιτούτων από ένα ανώνυμο κανάλι και το περιεχόμενο είναι διαθέσιμο σε όλα τα μέλη, χωρίς όμως κανείς να ξέρει ποιος είναι ο αποστολέας. Για τη υλοποίηση του καναλιού και της βάσης δεδομένων θα υιοθετηθούν τεχνολογίες υψηλής αξιοπιστίας για εμπιστευτικότητα, όπως η τεχνική *κ* βαθμού ανωνυμίας [17] [18]. Επίσης, θα υλοποιηθούν τεχνικές για την εξασφάλιση της ανωνυμίας των συντελεστών, όπως το σχήμα ψηφιακών υπογραφών [19] [20]. Για παράδειγμα, ένα περιστατικό ασφάλειας στον κυβερνοχώρο καταγράφεται στο SPEAR-RI, χωρίς να γίνεται γνωστό ποιος είναι το θύμα και πού συνέβη το περιστατικό ασφαλείας. Ωστόσο, οι τεχνικές λεπτομέρειες της επίθεσης θα είναι διαθέσιμες σε όλους ώστε να λάβουν έγκαιρα αντίμετρα. Οι εμπλεκόμενοι εταίροι θα σχεδιάσουν και θα εφαρμόσουν τη διασύνδεση του SPEAR-RI με όλα τα συστήματα SPEAR SIEM μέσω των συστημάτων ανίχνευσης επιθέσεων με οπτική παρακολούθηση. Επίσης, θα αναπτυχθεί μια κατάλληλη δικτυακή διεπαφή, όπου κάθε φορέας εκμετάλλευσης έξυπνων ενεργειακών δικτύων ή εμπειρογνώμονας ασφάλειας των μελών της ομάδας του αντίστοιχου έξυπνου ενεργειακού δικτύου θα μπορεί να μεταφορτώσει το περιστατικό ανώνυμα, διανέμοντας χρήσιμες πληροφορίες κώδικα, ενημερώσεις και διορθώσεις.

4. Εφαρμογές αρχιτεκτονικής SPEAR

Στα πλαίσια της ανάπτυξης των υποδομών της πλατφόρμας SPEAR, τέσσερα διαφορετικά σενάρια επιλέχθηκαν για την αξιολόγηση της.

1. *Εφαρμογή σε μονάδα υδροηλεκτρικής ενέργειας (Hydro Power Plant).*

   Η εφαρμογή της πλατφόρμα σε μια μονάδα υδροηλεκτρικής ενέργειας συνδυάζει τα παρακάτω μοναδικά χαρακτηριστικά

   i. αντιπροσωπεύει ένα παράδειγμα ανανεώσιμης ενέργειας που βρίσκεται στη νοτιοανατολική Ευρώπη,
   ii. η λειτουργία του εργοστασίου απαιτεί ανώτατες τεχνικές δεξιότητες και γνώσεις αποτελώντας ένα εργοστάσιο υψηλής τεχνολογίας όπου τυχόν ευπάθειες θα μπορούσαν να βλάψουν τα κύρια στοιχεία της υποδομής έξυπνου ενεργειακού δικτύου ·

iii. εξαιτίας του υψηλού κόστους παραγωγής υδροηλεκτρικής ενέργειας, το σενάριο έχει αυξημένο αντίκτυπο όσον αφορά τις αποτυχίες του υλικού και

iv. αποτελεί έναν οδηγό για την επικύρωση της αρχιτεκτονικής SPEAR για την εξασφάλιση των ανανεώσιμων πηγών ενέργειας έξυπνων δικτύων.

2. *Εφαρμογή σε υποσταθμό του έξυπνου ενεργειακού δικτύου (Substation)*

   Το παρόν σενάριο χρήσης θα επικυρώσει τον τρόπο με τον οποίο η προβαλλόμενη ανθεκτικότητα των RTUs, θα αποτελέσει παράδειγμα κατά τη λήψη επιθέσεων στον κυβερνοχώρο. Μέσω του παρόντος σεναρίου θα προβληθεί πόσο ανθεκτικό είναι το σύστημα άμυνας του SPEAR εναντίον των διαφόρων επιθέσεων στον κυβερνοχώρο των υποσταθμών με αυτόματα συστήματα.

3. *Εφαρμογή σε οικιακά και βιομηχανικά δίκτυα (IAN - HAN)*

   Η αποτελεσματικότητα και η απόδοση της πλατφόρμας SPEAR θα μελετηθεί μέσω των εγκαταστάσεων της Δημόσιας Επιχείρησης Ηλεκτρισμού (ΔΕΗ), στοχεύοντας στην αντιμετώπιση επιθέσεων στον κυβερνοχώρο σε βιομηχανικά δίκτυα (IAN) και οικιακά δίκτυα (HAN). Ένα βιομηχανικό δίκτυο (IAN) καλύπτει την περιοχή που περιλαμβάνει τον εξοπλισμό του παρόχου ενέργειας, όπως γεννήτριες, αντλίες νερού, στρόβιλοι και ηλεκτρικά συστήματα σε μια εξωτερική περιοχή. Από την άλλη μεριά, ένα οικιακό δίκτυο (HAN) ορίζει μια περιοχή μεταξύ των καταναλωτών και των διαχειριστών συστημάτων, όπου βρίσκονται οι έξυπνοι μετρητές και οι πύλες λειτουργίας [21]. Οι έξυπνες συσκευές παρέχουν πολύτιμες πληροφορίες σχετικά με την κατάσταση λειτουργίας του εξοπλισμού στο βιομηχανικό δίκτυο, όπως και για την κατανάλωση ενέργειας των χρηστών στα οικιακά δίκτυα. Τα δύο αυτά είδη δικτύων είναι ζωτικής σημασίας για την αξιοπιστία του έξυπνου ενεργειακού δικτύου.

4. *Εφαρμογή σε έξυπνο σπίτι (Smart Home*)

   Στο παρόν σενάριο, η διεξαγωγή εκτεταμένων δοκιμών της πλατφόρμας SPEAR θα πραγματοποιηθεί στο Έξυπνο Σπίτι του Εθνικού Κέντρου Έρευνας και Τεχνολογικής Ανάπτυξης (ΕΚΕΤΑ). Στόχος θα είναι η ανίχνευση επιθέσεων σε ένα έξυπνο σπίτι, όπου έχουν ήδη εγκατασταθεί συσκευές του Διαδικτύου των Πραγμάτων (IoT) και πολυαισθητηριακά δίκτυα. Επίσης, θα περιλαμβάνεται ένα σύστημα φωτοβολταϊκών (PV) 10kW για παραγωγή

ενέργειας, υποστηρίζοντας στρατηγικές απόκρισης στην ζήτηση και άλλες υπηρεσίες του έξυπνου μετρητή ενέργειας. Ο γενικός στόχος του σεναρίου είναι να δείξει ότι οι τεχνολογίες της πλατφόρμας SPEAR μπορούν να διασφαλίσουν τη διαθεσιμότητα, την ακεραιότητα και την εμπιστευτικότητα των έξυπνων ενεργειακών δικτύων.

5. Καινοτομία και συνεισφορά του προγράμματος SPEAR

Το πρόγραμμα SPEAR θα αναπτύξει ένα ολοκληρωμένο πλαίσιο για τους εμπλεκόμενους φορείς των έξυπνων ενεργειακών δικτύων ώστε να εγγυάται η ασφαλής και συνεχής τους λειτουργία. Μια στοχευμένη διαδικτυακή επίθεση σε κρίσιμη υποδομή, μπορεί να έχει μεγάλες επιπτώσεις σε πολλαπλούς κοινωνικούς τομείς. Με γνώμονα την κεντρική του πρόκληση, το πρόγραμμα SPEAR θα ωφελήσει σε μεγάλο βαθμό την κοινωνία στο σύνολό της, ενώ παράλληλα θα έχει θετικό περιβαλλοντικό αντίκτυπο μέσω του περιορισμού των φυσικών πόρων και της καλύτερης εξισορρόπησης του φόρτου του δικτύου. Το SPEAR θα μειώσει ριζικά τον χρόνο ανίχνευσης και απόκρισης των εξελιγμένων επιθέσεων στον κυβερνοχώρο μέσω της αποτελεσματικής επεξεργασίας των συλλεγόμενων δεδομένων, χρησιμοποιώντας τεχνικές απεικόνισης και αναλύσεις μεγάλου όγκου δεδομένων. Μέσω των εργαλείων του θα συμβάλει θετικά στην παραγωγή και στις πωλήσεις των εμπλεκόμενων φορέων, οδηγώντας στην εξοικονόμηση ενεργειών υψηλού κόστους για τυχόν επισκευές. Επιπρόσθετα, το SPEAR θα επηρεάσει σημαντικά τον τρόπο με τον οποίο θα ανταλλάσσονται οι ευαίσθητες πληροφορίες, παρέχοντας μια πανευρωπαϊκή ανώνυμη διασύνδεση των διαχειριστών των έξυπνων ενεργειακών δικτύων και επιτρέποντας στους φορείς εκμετάλλευσης να επωφεληθούν από την κοινή χρήση και την εισαγωγή καινοτόμων επιχειρηματικών σεναρίων. Όσον αφορά την προστασία των δεδομένων και την ιδιωτική ζωή, το SPEAR αναμένεται να ενισχύσει σημαντικά την εμπιστοσύνη των πολιτών έναντι στις κρίσιμες υποδομές. Αυτό θα βοηθήσει τους προμηθευτές ενέργειας να παραμείνουν ανταγωνιστικοί παράλληλα στην ευημερία του κοινωνικού συνόλου. Τέλος, το SPEAR θα συμμετάσχει ενεργά στην καταπολέμηση των παραγόντων απειλής συλλέγοντας και διαφυλάσσοντας εγκληματολογικές

πληροφορίες που μπορούν να χρησιμοποιηθούν ως αποδεικτικά στοιχεία στο δικαστήριο.

Επίλογος

Η βασική πρόκληση του προγράμματος SPEAR είναι η ανάπτυξη μιας νέας προσέγγισης / αρχιτεκτονικής τριών επιπέδων για την προστασία των κρίσιμων υποδομών της σημερινής κοινωνίας που θα οδηγήσει στην εξέλιξη των έξυπνων δικτύων ως προς την αντιμετώπιση του συνεχώς αυξανόμενου αριθμού απειλών στον κυβερνοχώρο. Το μοντέλο αρχιτεκτονικής του SPEAR βασίζεται σε τεχνικές αναγνώρισης, τεχνικές ανίχνευσης ιχνών μιας επίθεσης, εργαλεία μηχανικής μάθησης, τεχνολογίες μεγάλου όγκου δεδομένων, τεχνικές θεωρητικής μοντελοποίησης και απεικόνισης, τεχνικές χρονικής σήμανσης και πρωτόκολλα επικοινωνίας που θα παρέχουν μια ασφαλή πλατφόρμα για αποτελεσματική πρόληψη, ανίχνευση και απόκριση σε εξελιγμένες επιθέσεις στον κυβερνοχώρο καθώς και την αποτελεσματική ανταλλαγή κρίσιμων πληροφοριών. Συνολικά, το πρόγραμμα SPEAR θα προσφέρει το κατάλληλο πλαίσιο για να παραμείνει η ευρωπαϊκή βιομηχανία ανταγωνιστική στα συστήματα προστασίας των κρίσιμων υποδομών αλλά και στον γενικό τεχνολογικό χώρο. Σκοπός του είναι η ανάπτυξη μιας καινοτόμου πλατφόρμας ασφάλειας, ιδιωτικότητας και συνδεσιμότητας που θα προστατεύει κρίσιμες υποδομές από επιθέσεις στον κυβερνοχώρο και θα διευκολύνει την ανώνυμη την ανταλλαγή ευαίσθητων πληροφοριών, τη δημιουργία νέων ευκαιριών εξέλιξης και οικονομικής ανάπτυξης.

Βιβλιογραφία

[1] N. Corporation, «Information Management - What constitutes a cyber attack?,» 2018. [Ηλεκτρονικό]. Available: http://www.nec.com/en/global/solutions/safety/info_management/cyberattack.html.

[2] S. Tan, D. De, W.Z. Song, J. Yang και S.K. Das, «Survey of Security Advances in Smart Grid: A Data Driven Approach,» *IEEE Communications Surveys & Tutorials*, τόμ. 19, αρ. 1, pp. 397-422, 2017.

[3] E. N. a. I. S. A. (ENISA), «Annex II. Security aspects of the smart grid,» 2012.

[4] P. Eder-Neuhauser, T. Zseby, J. Fabini και G. Vormayr, «Cyber-attack models for smart grid environments,» *Sustainable Energy, Grids and Networks*, τόμ. 12, p. 10 – 29, 2017.

[5] «NIST SP 800-53,» [Ηλεκτρονικό]. Available: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf.

[6] «NIST SP 800-82,» [Ηλεκτρονικό]. Available: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf.

[7] K. Wang, M. Du, Y. Sun, A. Vinel και Y. Zhang, «Attack Detection and Distributed Forensics in Machine-to-Machine Networks,» *IEEE Network*, τόμ. 30, αρ. 6, pp. 49-55, 2016.

[8] S. Perumal, N. M. Norwawi και V. Raman, «Internet of Things (IoT) digital forensic investigation model: Top-down forensic approach methodology,» *Fifth International Conference on Digital Information Processing and Communications (ICDIPC)*, pp. 19-23, 2015.

[9] M. Baykara, R. Das και G. Tuna, «Cryptolog: A new approach to provide log security for digital forensics,» *IU-JEEE*, τόμ. 17, αρ. 2, pp. 3453-3462, 2017.

[10] S. Davidoff και J. Ham, «Network Forensics – Tracking Hackers Through Cyberspace,» *Prentice Hall*, p. 17, 2012.

[11] P. Fairley, «Internet-exposed energy control systems abound,» 2014.

[12] A. Jicha, M. Patton και H. Chen, «SCADA honeypots: An in-depth analysis of Conpot,» *IEEE Conference on Intelligence and Security Informatics (ISI)*, pp. 196-198, 2016.

[13] [Ηλεκτρονικό]. Available: http://conpot.org/.

[14] Q. D. La, T. Q. S. Quek, J. Lee, S. Jin και H. Zhu, «Deceptive Attack and Defense Game in Honeypot-Enabled Networks for the Internet of Things,» *IEEE Internet of Things Journal*, τόμ. 30, αρ. 6, pp. 1025-1035, Dec 2016.

[15] EE-ISAC, «European energy - information sharing and analysis,» 2018. [Ηλεκτρονικό]. Available: http://www.ee-isac.eu/.

[16] ESMIG, «Esmig - who we are page,» 2018. [Ηλεκτρονικό]. Available: http://esmig.eu/.

[17] D. Boneh, X. Boyen και H. Shacham, «Short Group Signatures,» *CRYPTO*, 2004.

[18] J. Camenisch και J. Groth, «Group signatures: Better efficiency and new theoretical aspects,» *In Security in Communication Networks 2004*, τόμ. 3352 of LNCS, 2005.

[19] P. Samarati, Pierangela και S. Latanya, «Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression - Technical report,» *SRI International*, 1998.

[20] S. Latanya, «k-anonymity: A model for protecting privacy,» *International Journal of Uncertainty*, Τόμ. %1 από %2Fuzziness and Knowledge-Based Systems 10.05, pp. 557-570, 2002.

[21] U.S. NETL, «Advanced metering infrastructure - White paper,» Feb 2008.