University of Patras
Department of Mechanical Engineering & Aeronautics
Laboratory for Manufacturing Systems and Automation
Assoc. Professor Dimitris MOURTZIS

ΑΓΓΕΛΟΠΟΥΛΟΣ ΚΩΝΣΤΑΝΤΙΝΟΣ
246690

Επιβλέπων:
Αναπληρωτής Καθηγητής
ΜΟΥΡΤΖΗΣ Δημήτριος

Πάτρα
1η Μάρτη 2019

«Ασφάλεια στο Διαδίκτυο για την τέταρτη Βιομηχανική Επανάσταση»

Περίληψη:

Με την έλευση της τέταρτης βιομηχανικής επανάστασης (Βιομηχανία 4.0) τα βιομηχανικά συστήματα μετατρέπονται σε ψηφιακά οικοσυστήματα μέσω των διαδικτυακών επικοινωνιακών τεχνολογιών για να διαμορφώσουν τα έξυπνα εργοστάσια του μέλλοντος. Η Βιομηχανία 4.0 χαρακτηρίζεται από αυξημένη ποσότητα, ποικιλία και πολυπλοκότητα των ανταλλασσόμενων δεδομένων. Οι βιομηχανίες χρησιμοποιούν διάφορα μηχανήματα, ρομπότ, υπολογιστές και διακομιστές, όλα συνδεδεμένα μεταξύ τους μέσω διαφορετικών δικτύων. Μεταξύ αυτών των μηχανών, λαμβάνει χώρα μια μαζική ανταλλαγή δεδομένων και ευαίσθητων πληροφοριών. Κάθε φορά που υπάρχει μια νέα διασύνδεση μεταξύ δικτύων και συσκευών, δημιουργεί έναν αδύναμο σύνδεσμο και χαρακτηρίζεται ως πιθανό σημείο επίθεσης. Καθώς περισσότερες συσκευές εισέρχονται στη σφαίρα του Διαδικτύου των Πραγμάτων, οι επιθέσεις που στοχεύουν στην ποικιλία των 'τελικών' Διαδικτυακών σημείων θα αυξηθούν. Ωστόσο, οι υπάρχουσες τεχνολογίες του Διαδικτύου μαστίζονται από ζητήματα ιδιωτικού απορρήτου δεδομένων και κακόβουλες παραβιάσεις που θα λειτουργήσουν ως εμπόδιο για την υιοθεσία της Βιομηχανίας 4.0. Έτσι η ανάγκη ταυτοποίησης των απαιτούμενων πρωτοκόλλων για την ασφάλεια στο κυβερνοχώρο, σε συγκεκριμένα 'τελικά' σημεία όπου ενδέχεται να προκύψουν διαρροές δεδομένων, έχει αυξηθεί σημαντικά για την αντιμετώπιση κακόβουλων συμπεριφορών. Το πραγματικό δυναμικό της Βιομηχανίας 4.0 δεν μπορεί να επιτευχθεί, εάν αυτές οι προκλήσεις δεν αντιμετωπιστούν σωστά. Σκοπός του έργου αυτού είναι να εντοπίσει και να χαρτογραφήσει τα πιθανά ευάλωτα σημεία σε ένα κοινό βιομηχανικό πρότυπο, όπου τα δεδομένα θα διασταυρώνονται κατά τη διάρκεια της συσσωμάτωσης και να προτείνει έναν ισχυρό τρόπο ασφάλισης ενός ασύρματου δικτύου αισθητήρων (WSN), εξασφαλίζοντας την ακεραιότητα και την αυθεντικότητα των δεδομένων και των ταυτοτήτων των χρηστών που περιλαμβάνονται σε ένα WSN. Τέλος, οι ευπάθειες ενός συστήματος συλλογής δεδομένων, εφαρμοζόμενο σε μία βιομηχανίας μηχανών λέιζερ, χαρτογραφούνται και παρουσιάζονται.

Λέξεις κλειδιά: **Ασφάλεια Διαδικτύου, Διαδίκτυο των Πραγμάτων (IoT), Ιδιωτικότητα, Ασύρματο Δίκτυο Αισθητήρων**

Εισαγωγή:

Η πρόοδος στις τεχνολογίες παραγωγής και επικοινωνιών έθεσε τα βασικά θεμέλια για τη μετατροπή των σημερινών βιομηχανιών σε Cyber – Physical συστήματα (CPS). Τα θεμέλια του Industry 4.0 βασίζονται στο Internet of Things (IoT), ένα δίκτυο διασυνδεδεμένων συσκευών που δημιουργούν ένα έξυπνο δίκτυο. Η ιδέα του IoT άρχισε να επηρεάζει τις βιομηχανίες όταν μειώθηκε το κόστος για την υλοποίησή της και οι διάφορες τεχνολογίες επικοινωνίας εξελίχθηκαν ταχύτατας. Τα προηγούμενα χρόνια, η γραμμή παραγωγής απαρτιζόταν μόνο από μηχανήματα που επικοινωνούσαν με έναν μόνο υπολογιστή ενσύρματα και αντάλλαζαν δεδομένα χωρίς τον κίνδυνο παρακολούθησής της σύνδεσης από τρίτους. Αν και η ποικιλία των συνδεδεμένων συσκευών και πρωτοκόλλων επικοινωνίας είναι επωφελής για τις βιομηχανίες, παρέχει μία εκτεταμένη «επιφάνεια» σημείων επίθεσης για τους αντιπάλους.

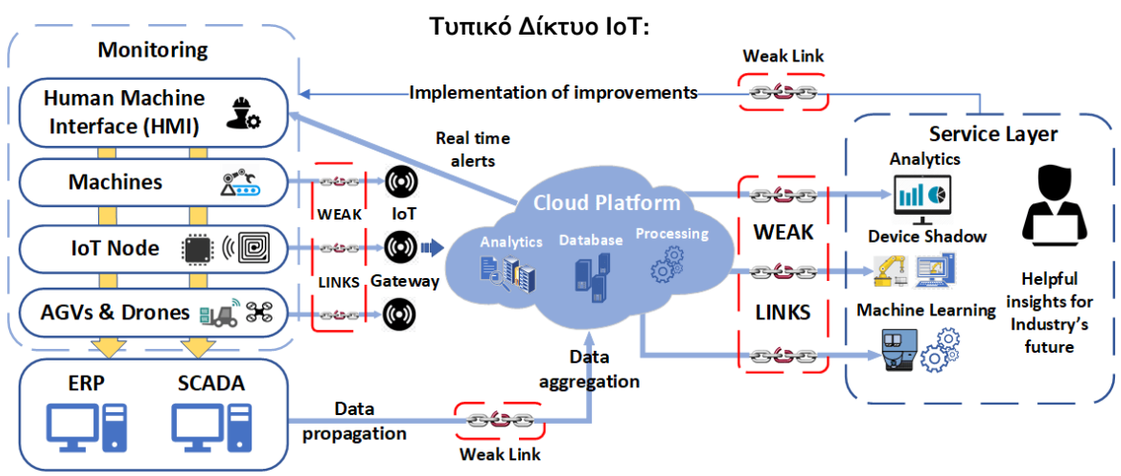
Ορισμός Προβλήματος:

Τα κύρια προβλήματα που αντιμετωπίζει αυτή τη στιγμή το Industrial Internet of Things (IIoT) είναι τα εξής:

- Οι συσκευές που χρησιμοποιούνται στις σύγχρονες βιομηχανίες είναι περιορισμένων πόρων και σχεδιάζονται με γνώμονα την προσαρμοστικότητα στα διαφορετικά πρωτόκολλα και δίκτυα και όχι την ασφάλεια.
- Τα πρωτόκολλα που χρησιμοποιούνται για την επικοινωνία των συσκευών μαστίζονται ακόμα από ζητήματα ιδιωτικού απορρήτου δεδομένων και παραβιάσεις από τρίτους ή από κακόβουλα λογισμικά.

Η είσοδος του IIoT έδωσε την δυνατότητα στους επιτιθέμενους να αλλάξουν το στόχο των επιθέσεων τους από διαρροή ή εξαγωγή δεδομένων σε απομακρυσμένο έλεγχο των μηχανών και των συσκευών που βρίσκονται στο δίκτυο.

Αρχιτεκτονική του Συστήματος:



Κατηγοριοποίηση επιθέσεων σε ένα δίκτυο IIoT και αξιολόγησή τους με βάση τις επιπτώσεις που έχουν για το δίκτυο και την Βιομηχανία

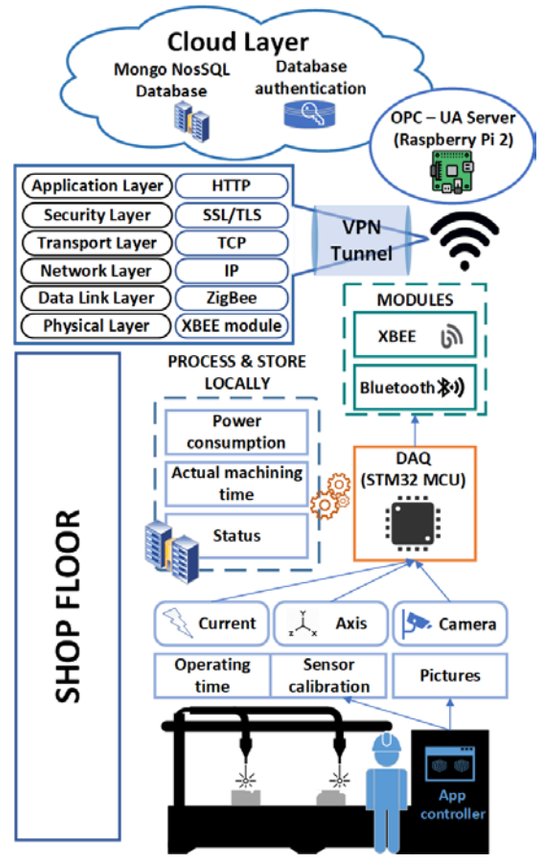
	Vulnerabilities	Possible scenarios	Impact	Intensity
Data Control	• Side channel attack [13] • Power analysis attack [13] • Password guessing attack [14]	Extraction of private key and decryption of messages	• Access/Decrypt data • Sell data as corporate espionage	High
	• Phishing [15] • Ransomware [16]	Exploiting vulnerabilities to access and encrypt crucial information	• Encrypt / Destruct data • Inaccessible network • Big loss of profits	Medium
	• Routing attack [10] • MITM attack [9] • Spoofing attack [17]	Manipulation of routing chain to exfiltrate data packets and obtain crucial information	• Access/Steal data • Falsify information	Low
Machine Control	• Transport Layer Attack [9] • Session hijacking [9] • Sniffing attack [21]	Link interception and extraction of ephemeral cookie/private key	• Unauthorized access / control to machines and actuators • Exposal of machines and employees to danger	
	• DoS / DDoS attack [18] • Power depletion attack [22]	Denial of security mechanism to bypass them and expose system flaws	• Destruction of security mechanisms • Unresponsive exploitable network	
	• Trojan/Backdoor [19]	Port sweeping to infiltrate networks and gain access to the main server	• Expose network vulnerabilities • Gain unauthorized access	

Πρωτόκολλα χρησιμοποιούμενα σε IIoT, οι ευπάθειές τους και οι λύσεις για την αντιμετώπιση

Protocols	Security mechanisms	Vulnerabilities	Solutions
Bluetooth 5.0	Secure Pairing	– Password guessing attack – DoS / DDoS attack – Trojan/Backdoor attack – MITM attacks	– Dual shared secret key – RSA or DES implementation
IEEE 802.11/Wi-Fi	WEP, AES, WPA, WPA2	– Password guessing attack – MITM attacks – DoS/DDoS attack	– Hiding SSID – Disabling Telnet/SSH services – Honeypot countermeasure – Implement Shell script code
IEEE 802.15.4/Zigbee	Link Layer encryption with AES-128, TLS	– Power depletion attack – MITM attacks – Spoofing attack – DoS/DDoS attack	– Remote alert system – Key management
6LoWPAN	Link Layer encryption with AES-128, Access control list	– Sniffing attack – Power depletion attack – DoS/DDoS/Jamming attack – Transport Layer attack – Spoofing attack	– Remote monitoring of energy – Key management system – Intrusion Detection System

Υλοποίηση σε Πραγματικό Σύστημα:

Σχεδιασμένο δίκτυο και μηχανισμοί ασφαλείας, εφαρμοσμένο σε βιομηχανία με μηχανές κοπής με λέιζερ



Συμπεράσματα:

Το IoT μετατρέπει τις βιομηχανίες, εισάγοντας πολύπλοκα συστήματα όπως CPS, αισθητήρες σύνδεσης, μηχανές και ενεργοποιητές που επικοινωνούν και ανταλλάσσουν δεδομένα για να παρέχουν ένα ευέλικτο και πλήρως συνειδητό σύστημα. Ωστόσο το εκτεταμένο «τοπίο» του IoT παρέχει περισσότερες ευκαιρίες και μεθόδους για την εκμετάλλευση ενός δικτύου που οδηγούν σε πολλές διαφορετικές απειλές. Για να μπορέσουν να υιοθετήσουν οι βιομηχανίες τη φιλοσοφία του Industry 4.0, αυτές οι απειλές θα πρέπει να αντιμετωπιστούν σωστά. Το σχεδιασμένο δίκτυό μας εφαρμόστηκε στη γραμμή παραγωγής μια βιομηχανίας, καθώς εκεί οι συσκευές σχεδιάζονται συνήθως με γνώμονα το κόστος και όχι τόσο την ασφάλεια, ώστε να επισημανθεί η σημασία και η ανάγκη της ασφάλειας σε κάθε επίπεδο πριν από την παροχή κάποιας υπηρεσίας στους χρήστες.

Δημοσιεύσεις:

Η εφαρμογή του σχεδιασμένου δικτύου αναφέρεται στην ακόλουθη δημοσίευση:

▪ Dimitris Mourtzis, Konstantinos Angelopoulos, Vasilios Zogopoulos, Mapping Vulnerabilities in the Industrial Internet of Things Landscape, 29th CIRP Design Conference, May 2019, Povoa de Varzim, Portugal