ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΣΤΗΜΩΝ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΤΜΗΜΑ ΔΙΟΙΚΗΤΙΚΗΣ ΕΠΙΣΤΗΜΗΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ

ΠΡΟΚΛΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ ΤΩΝ ΠΡΑΓΜΑΤΩΝ & ΑΝΑΔΥΟΜΕΝΕΣ ΑΠΕΙΛΕΣ ΣΤΟΝ ΤΟΜΕΑ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΡΙΑ: ΗΡΑ ΑΝΤΩΝΟΠΟΥΛΟΥ

ΧΑΡΑΛΑΜΠΙΑ ΚΥΡΙΑΚΟΠΟΥΛΟΥ

ΜΑΡΙΛΕΝΑ ΓΚΟΤΣΟΠΟΥΛΟΥ

ΠΑΤΡΑ 2021

ΠΕΡΙΛΗΨΗ

Ο στόχος αυτής της εργασίας είναι να παρουσιάσει μια επισκόπηση του Διαδικτύου των πραγμάτων και των αναδυόμενων κινδύνων στο τομέα της κυβερνοασφάλειας. Όλα τα ευρήματα βασίζονται στη βιβλιογραφία που διατίθεται για τα βασικά στοιχεία του Διαδικτύου των πραγμάτων και της ασφάλειας στον κυβερνοχώρο. Αυτό η εργασία επίσης παρέχει λεπτομερείς πληροφορίες σχετικά με τα βασικά στοιχεία του Διαδικτύου των πραγμάτων, που κυμαίνονται από το Radio Frequency Identification, το Near-Field Communication και τα Wireless Δίκτυα αισθητήρων.

Επιπλέον, η εργασία παρέχει πληροφορίες για τα διάφορα πεδία εφαρμογής που χρησιμοποιούνται από αυτά και περιγράφει τους κινδύνους ασφαλείας που αντιμετωπίζει κάθε ένα. Όλα τα γνωστά αντίμετρα, τα οποία μπορούν να προστατεύσουν το Διαδίκτυο των πραγμάτων από επιθέσεις ασφαλείας και μπορούν να παρέχουν μια ασφαλή έκδοση του Διαδικτύου των πραγμάτων.

Η ανάπτυξη καινοτόμων και πιο αποτελεσματικών μηχανισμών άμυνας κακόβουλου λογισμικού έχει θεωρηθεί ως επείγουσα απαίτηση στην κοινότητα ασφάλειας στον κυβερνοχώρο. Για την επίτευξη αυτού του στόχου, παρουσιάζουμε μια επισκόπηση των πιο ευάλωτων δυνατοτήτων σε υπάρχοντα επίπεδα υλικού, λογισμικού και δικτύου. Στην συνέχεια ακολουθούν κριτικές για τις υπάρχουσες προηγμένες τεχνικές μετριασμού και το γιατί λειτουργούν ή δεν λειτουργούν.

Αυτό η εργασία αξιολογεί τα διαθέσιμα αντίμετρα για την προστασία κάθε συνιστώσας του Διαδικτύου των πραγμάτων από κινδύνους ασφαλείας. Με βάση την τρέχουσα βιβλιογραφία, αυτή η εργασία παρέχει μια απάντηση στο ερώτημα αν το Διαδίκτυο των πραγμάτων από σήμερα μπορεί ήδη να θεωρηθεί ασφαλές.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Internet of Things, Radio Frequency Identification, Wireless Sensor Networks, Cyber Security, Emerging cyber threats, Cyber attacks and countermeasures.

Περιεχόμενα

ΕΙΣΑΓΩΓΗ

Το Διαδίκτυο των πραγμάτων μπορεί να περιγραφεί ως ένα δίκτυο που αποτελείται από διασυνδεδεμένα έξυπνα αντικείμενα. Αυτά τα αντικείμενα έχουν τη δυνατότητα να ανιχνεύουν το περιβάλλον τους και με τη σειρά τους μπορούν να μοιράζονται και να επεξεργάζονται πληροφορίες, οι οποίες μπορούν να διατίθενται σε διαφορετικές εφαρμογές.

Το «Διαδίκτυο των πραγμάτων» είναι η φράση που περιγράφει μια νέα εποχή στον χώρο των νέων τεχνολογιών. Εν συντομία, το Διαδίκτυο των πραγμάτων μπορεί να οριστεί ως η αλληλεπίδραση έξυπνων αντικειμένων που είναι συνδεδεμένα στο Διαδίκτυο. Αυτά τα αντικείμενα μπορούν να ανιχνεύσουν, να μοιραστούν και να επεξεργαστούν πληροφορίες, να τα ανεβάσουν στο cloud και να τα καταστήσουν διαθέσιμα στο χρήστη μέσω μεγάλου αριθμού διαφορετικών εφαρμογών. Παρ 'όλα αυτά αυτές οι πολλά υποσχόμενες καινοτομίες, όπως κάθε άλλη τεχνολογία, αντιμετωπίζουν πολλές προκλήσεις ασφάλειας. Το Διαδίκτυο των πραγμάτων (IoT), μπορεί να χαρακτηριστεί ως το διαδίκτυο του μέλλοντος. Από τον πρώτο καιρό που πραγματοποιήθηκε μια επιτυχημένη μμεταφορά δεδομένων μεταξύ 2 υπολογιστών που βρισκόντουσαν σε ξεχωριστά σημεία, εμφανίστηκε η ιδέα πως η δικτύωση όλων των υπολογιστών οφείλει να μεταβιβαστεί σε ένα κοινό Δίκτυο. Η ιδέα αυτή όσον αφορά τη δικτύωση των υπολογιστών και των υπολογιστικών συστημάτων έχει πλέον πραγματοποιηθεί με το γνωστό Διαδίκτυο , το οποίο στην πραγματικότητα δεν είναι τίποτε παραπάνω από την διασύνδεση πολλών δικτύων υπολογιστών μεταξύ τους. (Karlof, C., Wagner, D. 2003)

Τα θύματα κυβερνοεπιθέσεων αυξάνονται επίσης σημαντικά. Με βάση την έρευνα που διενήργησε η Symantec, η οποία περιελάμβανε συνέντευξη 20.000 ανθρώπων σε 24 χώρες, το 69% ανέφερε ότι έχει πέσει θύμα μιας επίθεσης στον κυβερνοχώρο στη διάρκεια της ζωής τους. Η Symantec υπολόγισε ότι 14 ενήλικες γίνονται θύματα μιας

επίθεσης στον κυβερνοχώρο κάθε δευτερόλεπτο ή ότι πραγματοποιούνται περισσότερες από ένα εκατομμύριο επιθέσεις κάθε μέρα.

ΚΕΦΑΛΑΙΟ 1: Το Διαδίκτυο των Πραγμάτων

Το Διαδίκτυο των πραγμάτων είναι μια φράση που χρησιμοποιείται για να περιγράψει την εισαγωγή μιας νέας εποχής του χρήση του υπολογιστή. Αλλά πώς μπορεί να οριστεί το IoT; Αναλύοντας τις δυο λέξεις κλειδιά της φράσης, το Διαδίκτυο είναι μέρος της καθημερινής ζωής των περισσότερων ανθρώπων. Παρέχει μέσα επικοινωνίας, μας επιτρέπει να αλληλεπιδρούμε και να χρησιμοποιούμε ένα δίκτυο μέσω κοινωνικών μέσων, μας παρέχει εφαρμογές και παιχνίδια για να κάνουμε την καθημερινή μας ζωή ευκολότερη και πιο ευχάριστη. Επιπλέον, γίνεται όλο και πιο εύκολα προσβάσιμο σε ένα ευρύτερο κοινό. Η άλλη λέξη κλειδί της φράσης Διαδίκτυο των Πραγμάτων μας περιγράφει έξυπνα αντικείμενα που έχουν το ακόλουθα χαρακτηριστικά.

• Τα πράγματα είναι οντότητες που μπορούν να αναγνωριστούν μοναδικά

• Μπορούν να προσδιοριστούν από τη φυσική τους φύση σε σχήμα, μέγεθος κ.λπ.

• Μπορούν να επικοινωνούν με τη λήψη και την αποστολή μηνυμάτων

• Μπορούν να εκτελέσουν βασικό έως πολύπλοκο υπολογισμό

• Μπορεί να είναι σε θέση να αισθανθούν το περιβάλλον τους (θερμοκρασία, φωτισμός κ.λπ.)

Σύμφωνα με τους Gubbi et al αυτά τα πράγματα μπορούν να αλληλεπιδρούν μεταξύ τους. Εκτός από την ανταλλαγή δεδομένων, τα περισσότερα από αυτά τα έξυπνα αντικείμενα μπορούν ακόμη και να αντιδράσουν σε γεγονότα που συμβαίνουν στο φυσικό περιβάλλον γύρω τους. Αυτές οι αντιδράσεις μπορούν να προκαλέσουν ενέργειες που μπορούν να χρησιμοποιηθούν από υπηρεσίες που είναι διαθέσιμες για τα ανθρώπινα όντα χωρίς να δίνουν καμία είσοδο στο σύστημα.Τα δεδομένα αυτά

μπορούν να αναπαραχθούν από αντικείμενα που αποτελούν μέρος της καθημερινής μας ζωής, όπως smartphones, tablets ή laptop σε αντικείμενα που συνδέονται με αντικείμενα που χρησιμοποιούμε στα σπίτια ή τα οχήματά μας, η οποία άλλη συσκευή μπορεί να συνδεθεί στο Διαδίκτυο. Η διασύνδεση των πραγμάτων επιτρέπει σε αυτήν τη νέα εποχή της τεχνολογίας να απομακρυνθεί το Διαδίκτυο από το αρχικό όραμα του και να εξελιχθεί σε κάτι αρκετά πιο περίπλοκο. Αντί να υποστηρίζει τη συνδεσιμότητα ανά πάσα στιγμή, σε οποιοδήποτε μέρος και για όλους, το Διαδίκτυο των πραγμάτων κάνει μια κίνηση από όλους προς τα πάντα.

Για την υποστήριξη αυτής της αλλαγής πρέπει να εισαχθούν διάφορα νέα στοιχεία. Σύμφωνα με τους Atzori et al (2010) η αναγνώριση ραδιοσυχνοτήτων (RFID) μπορεί να θεωρηθεί ως η κινητήρια τεχνολογία πίσω από το IoT. Τα συστήματα RFID περιλαμβάνουν μια συσκευή ανάγνωσης και πολλές ετικέτες RFID που μπορούν να συνδεθούν με αντικείμενα γύρω μας. Άλλα παραδείγματα χρήσης RFID είναι η διαχείριση της λιανικής και της εφοδιαστικής αλυσίδας, στις μεταφορές ως συστήματα έκδοσης εισιτηρίων ή σε τραπεζικές κάρτες και φορτία. Με τη βοήθεια μιας συσκευής ανάγνωσης είναι δυνατή η εξαγωγή των πληροφοριών που είναι αποθηκευμένες στις ετικέτες.

Ένα άλλο βασικό στοιχείο του IoT είναι η επονομαζόμενη επικοινωνία κοντινού πεδίου (NFC). Αυτή η τεχνολογία χρησιμοποιείται ως ηλεκτρονική υποστήριξη για συστήματα RFID και έχει αποκτήσει δημοτικότητα στις ηλεκτρονικές πληρωμές. Το NFC εξάλειψε τα προβλήματα που προέκυψαν κατά τη χρήση των συστημάτων RFID από μόνο του. Κορυφαίοι προμηθευτές, όπως η Walmart και η Tesco, που χρησιμοποίησαν το RFID για να αυτοματοποιήσουν τη λιανική τους έπρεπε να αντιμετωπίσουν τους περιορισμούς της τεχνολογίας. Ένα σημαντικό ζήτημα που αντιμετώπισε κατά τη διάρκεια αυτών των δοκιμών ήταν ότι άλλα υλικά παρενέβησαν στις ετικέτες κατά την αναγνώρισή τους. Τα συστήματα NFC λειτουργούν ασύρματα και μπορούν να συνδεθούν σε οποιοδήποτε στοιχείο. Ένα παράδειγμα συστημάτων NFC στη σημερινή εποχή είναι το iPhone X της Apple, το οποίο συνοδεύεται από NFC τεχνολογία και μπορεί να χρησιμοποιηθεί με το ApplePay. (C. M. Medaglia, A. Serbanati, 2010)

ΟΡΙΣΜΟΣ ΔΙΑΔΙΚΤΥΟΥ ΤΩΝ ΠΡΑΓΜΑΤΩΝ

Καθώς το Διαδίκτυο των πραγμάτων βρίσκεται ακόμη στα αρχικά του στάδια, υπάρχει μια ποικιλία ορισμών. Η ομάδα RFID ορίζει το IoT ως παγκόσμιο δίκτυο, το οποίο αποτελείται από αντικείμενα που μπορούν να αντιμετωπιστούν με μοναδικό τρόπο. Αυτά τα αντικείμενα μπορούν να επικοινωνούν μεταξύ τους με βάση τα διαθέσιμα τυποποιημένα πρωτόκολλα. Ένας άλλος ορισμός από το Cluster των ευρωπαϊκών ερευνητικών έργων στο Διαδίκτυο των πραγμάτων περιγράφει τα έξυπνα αντικείμενα ως συμμετέχοντες που διαδραματίζουν ενεργό ρόλο στη διαδικασία ενημέρωσης του IoT. (C. M. Medaglia, A. Serbanati, 2010)

Ο Gubbi ορίζει το Διαδίκτυο των πραγμάτων ως συσκευές που μπορούν να ανιχνεύσουν, να μοιραστούν και να επεξεργαστούν πληροφορίες που μπορούν να χρησιμοποιηθούν από καινοτόμες εφαρμογές. Ορίζουν το IoT από την άποψη του χρήστη χωρίς να το περιορίζουν σε οποιοδήποτε τυπικό πρωτόκολλο.

Όλοι αυτοί οι ορισμοί δίνουν έμφαση σε διαφορετικά μέρη που σχηματίζουν το Διαδίκτυο των πραγμάτων, από δίκτυο μέσω αντικειμένων έως χρήστες. Ο Atzori συνδυάζει αυτές τις διαφορετικές απόψεις στον ορισμό του, και ισχυρίζεται ότι το πλήρες δυναμικό του IoT βρίσκεται εκεί όπου το Διαδίκτυο και τα πράγματα είναι σημασιολογικά προσανατολισμένα.

ΕΦΑΡΜΟΓΕΣ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ ΤΩΝ ΠΡΑΓΜΑΤΩΝ

Το Διαδίκτυο των πραγμάτων μπορεί να παρέχει ένα τεράστιο αριθμό εφαρμογών που είναι πιθανό να επηρεάσουν τον τρόπο ζωής μας και να βελτιώσουν την ποιότητά του. Οι περισσότερες από τις διαθέσιμες εφαρμογές μπορούν να χωριστούν στις ακόλουθες ομάδες: μεταφορά και εφοδιαστική, υγειονομική περίθαλψη και έξυπνα και προσωπικά περιβάλλοντα. (C. M. Medaglia, A. Serbanati, 2010)

Ένας σημαντικός τομέας που μπορεί να επωφεληθεί από τις αλλαγές του IoT είναι η εφοδιαστική αλυσίδα. Χάρη στην παρακολούθηση RFID και NFC σε πραγματικό χρόνο, σε οποιοδήποτε στάδιο της αλυσίδας εφοδιασμού, είναι δυνατή. Αυτό διασφαλίζει ότι η επιχείρηση μπορεί να αντιδράσει σε οποιαδήποτε αλλαγή στην αλλαγή προσφοράς αμέσως. Αυτό επιτρέπει στις επιχειρήσεις να σχεδιάζουν πιο αποτελεσματικά την στρατηγική τους , έτσι ώστε να υπάρχει πλήρες απόθεμα ασφαλείας. (Karlof, C., Wagner, D. 2003)

Ένας άλλος τομέας που θα επηρεαστεί από τις αλλαγές του IoT είναι η μεταφορά. Τα οχήματα μπορούν να εξοπλιστούν με κάθε είδους διαφορετικούς αισθητήρες, για να διασφαλιστεί η ασφάλεια μέσω συστημάτων αποφυγής σύγκρουσης. Λαμβάνοντας υπόψη τις εταιρείες ιδιωτικών μεταφορών και εμπορευματικών μεταφορών, το IoT μπορεί να παρέχει πληροφορίες σε πραγματικό χρόνο σχετικά με την κυκλοφοριακή συμφόρηση, έτσι ώστε οι οδηγοί να μπορούν να επιλέξουν γρήγορα την βέλτιστη διαδρομή. (Mudassar Ahmad, Tanveer Younis, Muhammad Asif Habib, Rehan Ashraf, Syed Hassan Ahmed, 2019)

Ένας άλλος σημαντικός τομέας που μπορεί να επωφεληθεί από τις αλλαγές είναι ο τομέας της υγειονομικής περίθαλψης. Το IoT επιτρέπει την παρακολούθηση κινούμενων ετικετών, οι οποίες μπορούν να συνδεθούν με οποιοδήποτε άτομο ή αντικείμενο. Αυτό σημαίνει ότι θα ήταν δυνατό να ακολουθήσετε την κίνηση οποιουδήποτε αντικειμένου ή ατόμου και θα μπορούσατε να αποφύγετε τα αντικείμενα που βρίσκονται ως εμπόδια κατά τη διάρκεια μιας χειρουργικής επέμβασης ή ακόμα και την κλοπή φαρμάκων ή οργάνων. Εκτός από την παρακολούθηση, οι αισθητήρες που εμφυτεύονται αποτελούν μέρος της εξωτερικής περίθαλψης και μπορούν να χρησιμοποιηθούν για την παρακολούθηση της κατάστασης του ασθενούς σε πραγματικό χρόνο και από παντού. (Mudassar Ahmad, Tanveer Younis, Muhammad Asif Habib, Rehan Ashraf, Syed Hassan Ahmed, 2019)

Εκτός από τη μεταφορά, την εφοδιαστική αλυσίδα και τον τομέα της υγειονομικής περίθαλψης, υπάρχουν και άλλοι τομείς που μπορούν να υποστηριχθούν από το IoT,

όπως το έξυπνο περιβάλλον. Σε αυτά περιλαμβάνονται σπίτια, δάπεδα ή βιομηχανικές εγκαταστάσεις. Το IoT μπορεί να βοηθήσει στην εξοικονόμηση ενέργειας ρυθμίζοντας τα συστήματα θέρμανσης ή απενεργοποιώντας αυτόματα τις συσκευές που δεν χρησιμοποιούνται. (Mudassar Ahmad, Tanveer Younis, Muhammad Asif Habib, Rehan Ashraf, Syed Hassan Ahmed, 2019)

Ο τελευταίος τομέας που μπορεί να επωφεληθεί από τις καινοτομίες του IoT είναι ο προσωπικός τομέας. Τα συστήματα RFID μπορούν να μας βοηθήσουν να βρούμε τα χαμένα στοιχεία μας ελέγχοντας την τελευταία καταγεγραμμένη τοποθεσία. Επιπλέον, ο χρήστης θα μπορούσε να αναζητήσει λέξεις-κλειδιά και αν η συνθήκη ταιριάζει με την τοποθεσία που θα μπορούσε να βρεθεί το αντικείμενο. Αυτή η επιλογή παρακολούθησης στοιχείων μπορεί ακόμη και να χρησιμοποιηθεί για τον εντοπισμό κλοπής. Σε περίπτωση που ένα αντικείμενο, που είναι μέρος περιορισμένης περιοχής, έχει αφαιρεθεί από αυτήν την περιοχή χωρίς άδεια, μπορεί να ενεργοποιηθεί συναγερμός για να ανακοινώσει την πιθανή κλοπή. (Karlof, C., Wagner, D. 2003)

ΓΝΩΣΤΟΙ ΚΙΝΔΥΝΟΙ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ

Παρά όλα τα οφέλη που παρέχει το IoT, υπάρχουν γνωστοί κίνδυνοι που έχουν επηρεάσει τις τρέχουσες εφαρμογές IoT. Αυτό το κεφάλαιο παρέχει μερικά παραδείγματα περιστατικών που έχουν μειωθεί στους τομείς που περιγράφονται στο προηγούμενο κεφάλαιο.

Μελετώντας τον τομέα του έξυπνου περιβάλλοντος, ο Smith περιγράφει το σενάριο ενός ξενοδοχείου που αντικατέστησε τους παλιούς διακόπτες φωτός με μερικά tablet Android, έτσι ώστε οι επισκέπτες να μπορούν να ανάβουν και να σβήνουν τα φώτα των δωματίων τους χρησιμοποιώντας το tablet. Ένας επισκέπτης του ξενοδοχείου που άντρας ηλικίας να μυρίζει το Ethernet, ωστόσο, ξαφνικά μπόρεσε να χρησιμοποιήσει αυτήν τη λειτουργία για όλα τα δωμάτια του ξενοδοχείου, ανάβοντας και σβήνοντας τα φώτα στα δωμάτια των άλλων επισκεπτών.

Λαμβάνοντας υπόψη τη μεταφορά, υπήρξαν μερικά περιστατικά με αυτοκίνητα, που κυμαίνονται από το άνοιγμα ενός κλειδωμένου αυτοκινήτου και την κλοπή των ακριβών αντικειμένων του ιδιοκτήτη έως τον έλεγχο ενός αυτοκινήτου που οδηγείται στον αυτοκινητόδρομο. Άλλα περιστατικά στον τομέα των μεταφορών έχουν αναφερθεί για αεροπλάνα. Ο ερευνητής ασφαλείας Chris Roberts κατάφερε να εισέλθει στο σύστημα ελέγχου ενός αεροπλάνου, από τη θέση του μέσα στο αεροπλάνο.

Ένας άλλος τομέας που έπρεπε να αντιμετωπίσει τους κινδύνους ασφαλείας του IoT είναι ο ιατρικός τομέας. Ζητήματα ασφάλειας στο λογισμικό που χρησιμοποιείται για εμφυτευμένες αντλίες ινσουλίνης ή βηματοδότη είναι γνωστά για μεγαλύτερο χρονικό διάστημα. Ένα άλλο περιστατικό που διαπίστωσαν οι ερευνητές το 2016 ήταν η ανακάλυψη τρύπων ασφαλείας στο λογισμικό διανομής ναρκωτικών που επέτρεψε στους ανθρώπους να αποκτήσουν επιβλαβή φάρμακα. (Mudassar Ahmad, Tanveer Younis, Muhammad Asif Habib, Rehan Ashraf, Syed Hassan Ahmed, 2019)

Περαιτέρω περιστατικά με συσκευές IoT έχουν συμβεί όταν λείπει η υποδομή για την υποστήριξη της καινοτομίας. Η εκκίνηση ενός αυτοκινήτου που απαιτεί να καλέσετε στο σπίτι πριν ξεκινήσει ο κινητήρας δεν ήταν πλέον δυνατή αφού ο οδηγός έφυγε σε μια περιοχή χωρίς πλήρη ηλικία κάλυψης του κινητού. Τα σχολεία που παρέχουν δοκιμές μέσω του Διαδικτύου είχαν πρόβλημα με τη σύνδεση στο Διαδίκτυο, η οποία διέκοψε την υποβολή των αποτελεσμάτων των δοκιμών για όλους τους μαθητές. (Mudassar Ahmad, Tanveer Younis, Muhammad Asif Habib, Rehan Ashraf, Syed Hassan Ahmed, 2019)

Παρά τα οφέλη του, το IoT παρέχει μια μεγάλη επιφάνεια επιθέσεων. Τα ακόλουθα κεφάλαια δίνουν μια λεπτομερή επισκόπηση των βασικών στοιχείων, των συστημάτων RFID, των NFC και των WSN, εξηγούν τις τεχνολογίες, τις πιθανότητες και τους κινδύνους που είναι γνωστές σήμερα και παρέχουν τεχνικές λύσεις σε αυτά τα ζητήματα ασφαλείας. Η ολοκλήρωση της εργασίας θα συνοψίσει τα πιο σοβαρά ζητήματα ασφάλειας και θα δώσει μια αξιολόγηση για το πόσο ασφαλή είναι τα βασικά

στοιχεία του IoT. (Mudassar Ahmad, Tanveer Younis, Muhammad Asif Habib, Rehan Ashraf, Syed Hassan Ahmed, 2019)

ΚΕΦΑΛΑΙΟ 2: Radio Frequency Identification

Τα τελευταία χρόνια, η τεχνολογία της αναγνώρισης ραδιοσυχνοτήτων (RFID) έχει αυξηθεί σε δημοτικότητα. Σε σύγκριση με άλλες ευρέως χρησιμοποιούμενες τεχνολογίες, όπως ετικέτες γραμμικού κώδικα, το RFID δεν απαιτεί δυνατότητα παρακολούθησης. Επιπλέον, το RFID δεν αναγνωρίζει μόνο ένα αντικείμενο ή αντικείμενο από έναν συγκεκριμένο μοναδικό αριθμό, αλλά παρέχει επίσης τη δυνατότητα πρόσθετων, περιγραφικών στοιχείων. (F.T. Sheldon, V. Vishik 2010)

Τα συστήματα RFID αποτελούνται από μια βάση δεδομένων, μια συσκευή ανάγνωσης RFID και τις ετικέτες RFID που τοποθετούνται σε διάφορα στοιχεία που πρέπει να παρακολουθούνται ή να αναγνωρίζονται. Σε ένα σύστημα RFID, μια συσκευή ανάγνωσης επικοινωνεί με τη βάση δεδομένων, συνήθως μέσω ενός ασφαλούς καναλιού. Επιπλέον, η συσκευή ανάγνωσης επικοινωνεί με τις ετικέτες RFID του συστήματος. Αυτό το κανάλι θεωρείται ανασφαλές και επομένως πρέπει να εφαρμοστούν ισχυρά χαρακτηριστικά ασφαλείας. (F.T. Sheldon, V. Vishik 2010)

ΕΝΕΡΓΑ ΚΑΙ ΠΑΘΗΤΙΚΑ RFID tags

Οι ετικέτες RFID μπορούν να χωριστούν σε δύο κατηγορίες: ενεργές και παθητικές. Οι παθητικές ετικέτες RFID είναι συνήθως φθηνότερες στην τιμή, καθώς δεν περιέχουν πηγή τροφοδοσίας. Όπως οι ενεργές ετικέτες RFID, οι παθητικές αποτελούνται από κεραία και τσιπ με επικάλυψη προστατευτικού καλύμματος. Δεδομένου ότι οι παθητικές ετικέτες δεν περιέχουν πηγή ισχύος λαμβάνουν την ισχύ, απαραίτητη για

επικοινωνία, μέσω ποικίλων μαγνητικών πεδίων που προκαλούνται από μια συσκευή ανάγνωσης. Ανάλογα με τη συχνότητα με την οποία λειτουργούν οι παθητικές ετικέτες, μπορούν να φτάσουν από περίπου μισό μέτρο έως αρκετά μέτρα. (Mudassar Ahmad, Tanveer Younis, Muhammad Asif Habib, Rehan Ashraf, Syed Hassan Ahmed, 2019)

Οι ενεργές ετικέτες RFID είναι εξοπλισμένες με μια μπαταρία που παρέχει ισχύ απαραίτητη για τη μεταφορά. Αυτό τους επιτρέπει να φτάσουν σε άλλες αποστάσεις περίπου 100 μέτρων. Παρά το πλεονέκτημά τους στο εύρος, λόγω της πηγής ισχύος τους, οι ενεργές ετικέτες έχουν περιορισμένη διάρκεια ζωής και είναι πολύ πιο ακριβές σε σύγκριση με τους παθητικούς ομολόγους τους. (Mudassar Ahmad, Tanveer Younis, Muhammad Asif Habib, Rehan Ashraf, Syed Hassan Ahmed, 2019)

Οι ετικέτες RFID, για παράδειγμα, χρησιμοποιούνται από εταιρείες λιανικής για τη βελτιστοποίηση των αλυσίδων εφοδιασμού τους και μπορούν ακόμη και να βρεθούν σε ηλεκτρονικά διαβατήρια. Περαιτέρω παραδείγματα είναι οι εμφυτευμένες ετικέτες RFID σε κατοικίδια ζώα, κάρτες πρόσβασης για κλειδαριές σε κτίρια ή ορισμένοι τύποι πιστωτικών καρτών, που επιτρέπουν την ανέπαφη πληρωμή. (Mudassar Ahmad, Tanveer Younis, Muhammad Asif Habib, Rehan Ashraf, Syed Hassan Ahmed, 2019)

ΣΥΝΗΘΕΙΣ ΕΠΙΘΕΣΕΙΣ ΣΕ ΣΥΣΤΗΜΑΤΑ RFID

Οι πιο συχνές και σοβαρές επιθέσεις σε συστήματα RFID είναι ο αποσυγχρονισμός, η ανιχνευσιμότητα, η διαρροή πληροφοριών και οι επιθέσεις επανάληψης. Οι επιθέσεις αποσυγχρονισμού επιτρέπουν στους διαφημιστές να εντοπίζουν ετικέτες και να αποκαλύπτουν τη θέση τους, αποκλείοντας τη μετάδοση ενός συγκεκριμένου τύπου επικοινωνίας μεταξύ ετικέτας και αναγνώστη. (F.T. Sheldon, V. Vishik 2010)

Οι επαναλαμβανόμενες επιθέσεις επιτρέπουν στους εισβολείς να κάνουν κατάχρηση έγκυρων πληροφοριών που έχουν ληφθεί προηγουμένως. Η διαρροή πληροφοριών μπορεί να έχει σοβαρό αντίκτυπο στον χρήστη του, ο οποίος μπορεί να μην γνωρίζει καν

τη δραστηριότητα της ετικέτας. Ένας χρήστης που έχει μια ενεργή ετικέτα ακούσια μπορεί να αποκαλύψει πληροφορίες σχετικά με το ιδιοκτησία ορισμένων, συνήθως δαπανηρών προϊόντων ή χρήσης φαρμάκων. (Karlof, C., Wagner, D. 2003)

Ο αντίκτυπος τέτοιων επιθέσεων στο σύστημα είναι σοβαρός και αποτελεσματικά αντίμετρα θα εξηγηθούν στα επόμενα κεφάλαια.

ΕΠΙΘΕΣΕΙΣ ΣΕ ΒΑΣΙΚΕΣ RFID ΕΤΙΚΕΤΕΣ

Όπως προαναφέρθηκε, οι πολύ βασικές ετικέτες RFID δεν διαθέτουν κρυπτογραφία, επομένως οι hackers μπορούν απλά να συλλέξουν τα δεδομένα μιας ετικέτας ή να την κλωνοποιήσουν.

Υποθέτοντας ότι ένας εισβολέας καταφέρνει να κλωνοποιήσει μια ετικέτα συμβατή με EPC χρησιμοποιώντας μια επίθεση skimming (απάτη), η οποία αποκαλύπτει τον ηλεκτρονικό κωδικό προϊόντος της κλωνοποιημένης ετικέτας (EPC), ο εισβολέας εξακολουθεί να χρειάζεται το PIN της ετικέτας για να λάβει μια έγκυρη έξοδο της ετικέτας για να εκτελέσει τον αναγνώστη σύντροφοι. Η μόνη επιλογή για τη λήψη του απαραίτητου PIN είναι η εικασία. Λόγω του μήκους του PIN, η εικασία του σωστού PIN δεν συμβαδίζει με την πραγματική πρακτική. Καθώς οι κλώνοι που δεν συμμορφώνονται με το EPC μπορούν να εξαπατήσουν τον αναγνώστη, αποδεχόμενοι απλώς οποιοδήποτε PIN ως αληθινό, είναι σημαντικό να εντοπίσουμε τους κλώνους. (Karlof, C., Wagner, D. 2003)

Μπορεί να υπάρχουν περιστάσεις υπό τις οποίες είναι προτιμότερο να χρησιμοποιείται η ανάγνωση ως μέσο επικοινωνίας μεταξύ της ετικέτας και ενός αξιόπιστου διακομιστή. Σε αυτήν την περίπτωση, ο αναγνώστης επικοινωνεί με τον διακομιστή παρέχοντάς του ένα σύνολο PIN. Ένας εισβολέας που ο άνθρωπος θέλει να θέσει σε κίνδυνο μια συσκευή ανάγνωσης, που μπορεί να δημιουργήσει πρόσβαση σε έναν διακομιστή αλλά όχι σε μια ετικέτα, αντιμετωπίζει το ίδιο πρόβλημα με το προαναφερθέν για να κλωνοποιήσει με επιτυχία μια ετικέτα, ο εισβολέας πρέπει να

μαντέψει ποιο είναι το έγκυρο PIN. Ωστόσο, όποτε ο εισβολέας μπορεί να αποκτήσει πρόσβαση στην εν λόγω ετικέτα, είναι δυνατό να μάθετε τον έγκυρο κωδικό PIN απλώς σαρώνοντας την ετικέτα. (Karlof, C., Wagner, D. 2003)

Παρά τα προηγούμενα ζητήματα ασφαλείας, υπάρχουν περαιτέρω επιθέσεις σε βασικές ετικέτες RFID. Σε περίπτωση μη επιτρεπόμενης πρόσβασης σε μια βάση δεδομένων που αποθηκεύει PIN, ένας εισβολέας έχει τη δυνατότητα κλωνοποίησης όλων των ετικετών που επηρεάζονται επιτυχώς. Μια περαιτέρω δυνατότητα κλωνοποίησης ετικετών είναι η αντίστροφη μηχανική. Για να πετύχει ένας εισβολέας πρέπει να κλέψει την ετικέτα για να είναι σε θέση να μάθει το έγκυρο PIN που μπορεί στη συνέχεια να χρησιμοποιηθεί για τον κλώνο που αντικαθιστά το αρχικό. (Karlof, C., Wagner, D. 2003)

ΕΠΙΘΕΣΕΙΣ ΣΕ ΕΤΙΚΕΤΕΣ ΣΥΜΜΕΤΡΙΚΟΥ ΚΛΕΙΔΙΟΥ

Μια σοβαρή επίθεση σε συστήματα RFID με ετικέτες συμμετρικού κλειδιού είναι η επίθεση man-in-the-middle. Αυτή η επίθεση είναι πολύ αποτελεσματική καθώς ο εισβολέας ενεργεί απλώς χωρίς ανίχνευση μεταξύ δύο επικοινωνιακών μερών, στην περίπτωση αυτή η συσκευή ανάγνωσης και η ετικέτα, ελέγχοντας ολόκληρη τη συνομιλία. Η επίθεση man-in-the-middle αποτελεί αναπόφευκτη απειλή για τα συστήματα RFID καθώς παρακάμπτει κάθε είδους κρυπτογραφία. (Mudassar Ahmad, Tanveer Younis, Muhammad Asif Habib, Rehan Ashraf, Syed Hassan Ahmed, 2019)

ΑΝΤΙΜΕΤΡΑ ΓΙΑ ΕΠΙΘΕΣΕΙΣ ΣΕ ΒΑΣΙΚΕΣ RFID ΕΤΙΚΕΤΕΣ

Καθώς οι βασικές ετικέτες RFID στερούνται κρυπτογραφίας που εφαρμόζουν ασφαλή αντίμετρα για την επιβολή του ελέγχου ταυτότητας και τη διασφάλιση της ιδιωτικής ζωής των καταναλωτών είναι μια σημαντική πρόκληση. Τα ακόλουθα κεφάλαια θα παρέχουν πληροφορίες σχετικά με τον ελαφρύ έλεγχο ταυτότητας και τον τρόπο

απόρριψης βασικών ετικετών RFID προκειμένου να διασφαλιστεί η ιδιωτική προστασία των καταναλωτών (Mudassar Ahmad, Tanveer Younis, Muhammad Asif Habib, Rehan Ashraf, Syed Hassan Ahmed, 2019)

Ελαφρύς έλεγχος ταυτότητας

Λαμβάνοντας υπόψη τις βασικές ετικέτες RFID, το πιο δύσκολο ζήτημα ασφάλειας είναι αποτελεσματικό. Για τον εντοπισμό κλώνων εισβολέων, το λεγόμενο βασικό έλεγχο ταυτότητας περιλαμβάνει το χαρακτηριστικό της δοκιμής μιας ετικέτας στέλνοντας ένα σύνολο τυχαίων, ψευδεπίγραφων PIN, συμπεριλαμβανομένου του σωστού PIN σε τυχαίο μέρος. Εάν η απόκριση της ετικέτας είναι έγκυρη, η ετικέτα μπορεί να αποκρυφτεί ως κλώνος. Το απλούστερο πρωτόκολλο ελέγχου ταυτότητας, το οποίο υποτίθεται ότι προστατεύει επιτυχώς από τις ετικέτες κλωνοποίησης ή εξαπατά τις συσκευές ανάγνωσης, αναλαμβάνει μια αξιόπιστη συσκευή ανάγνωσης ετικετών και είναι κατάλληλη για τον πιο βασικό τύπο Ετικέτες RFID, όπως EPC. (F.T. Sheldon, V. Vishik 2010)

Αφαιρούμενες ετικέτες και καταστροφή ετικετών

Μια άλλη λύση για να αποφύγετε την αποκάλυψη πληροφοριών σχετικά με τον πάροχο μιας ετικέτας, είναι να καταστήσετε την ετικέτα άχρηστη. Επί του παρόντος, σύμφωνα με τον Juels υπάρχουν δύο πιθανά σενάρια για την επίτευξη αυτής της προσέγγισης. Μια λύση που είναι κοινή στο λιανικό εμπόριο είναι η χρήση των λεγόμενων αφαιρούμενων ετικετών που χρησιμοποιούνται συχνά ως τιμή. Αυτές οι ετικέτες μπορούν απλά να αφαιρεθούν από το αντικείμενο μόλις το αγοράσετε. (F.T. Sheldon, V. Vishik 2010)

Μια άλλη λύση που χρησιμοποιείται με μη αφαιρούμενες ετικέτες είναι η εξόντωση ετικετών. Η θανάτωση των ετικετών θεωρείται πολύ αποτελεσματική και παίζει καθοριστικό ρόλο στην ιδιωτική ζωή των καταναλωτών. Σύμφωνα με τον Jules, ένα

μελλοντικό σενάριο θα ήταν να σκοτώσει την ετικέτα αμέσως μετά την πληρωμή του αντικειμένου. Για να σκοτώσετε μια ετικέτα μια συσκευή ανάγνωσης στέλνει μια εντολή, συμπεριλαμβανομένου ενός συσχετισμένου, έγκυρου κωδικού PIN, για απενεργοποίηση της ετικέτας. (Mudassar Ahmad, Tanveer Younis, Muhammad Asif Habib, Rehan Ashraf, Syed Hassan Ahmed, 2019)

ΑΝΤΙΜΕΤΡΑ ΓΙΑ ΕΠΙΘΕΣΕΙΣ ΣΕ ΕΤΙΚΕΣ ΣΥΜΜΕΤΡΙΚΟΥ ΚΛΕΙΔΙΟΥ

Για την προστασία συστημάτων RFID από διάφορες επιθέσεις υπάρχουν διάφορα πρωτόκολλα που μπορούν να εφαρμοστούν σε συστήματα ετικετών συμμετρικού κλειδιού. Οι ετικέτες συμμετρικού κλειδιού μπορούν να εκτελούν κρυπτογραφία και, συνεπώς, έχουν καλύτερες επιλογές ασφάλειας. Οι ακόλουθες ενότητες παρέχουν μια επισκόπηση των δύο πιο αποτελεσματικών πρωτοκόλλων για την αντιμετώπιση των προβλημάτων αποσυγχρονισμού, διαρροής πληροφοριών και επιθέσεων επανάληψης. (Mudassar Ahmad, Tanveer Younis, Muhammad Asif Habib, Rehan Ashraf, Syed Hassan Ahmed, 2019)

Πρωτόκολλο ελέγχου ταυτότητας χαμηλού κόστους και υψηλής ασφάλειας

Οι Van Deursen και Radomirović περιγράφουν ένα πρωτόκολλο ελέγχου ταυτότητας που εισήχθη από τους Ha, Moon, Nieto και Boyd. Η ασφάλεια του πρωτοκόλλου βασίζεται στην υπόθεση ότι η σύνδεση μεταξύ της συσκευής ανάγνωσης και της βάσης δεδομένων είναι ασφαλής. Επιπλέον, συνοψίζεται ότι η επικοινωνία μεταξύ ετικέτας και συσκευής ανάγνωσης δεν μπορεί να θεωρηθεί ως θεραπεία, λόγω της υποκλοπής.

Σε αυτό το κρατικό πρωτόκολλο, η ετικέτα περιέχει ένα μυστικό αναγνωριστικό καθώς και μια τιμή, είτε 0 είτε 1, που δείχνει την επιτυχία της προηγούμενης εκτέλεσης. Εκτός από την κατοχή μυστικού αναγνωριστικού, η συσκευή ανάγνωσης διατηρεί επιπλέον το αναγνωριστικό της προηγούμενης εκτέλεσης και το

κατακερματισμό της τρέχουσας ταυτότητας. Η ανάγνωση δημιουργεί έναν μοναδικό αριθμό που χρησιμοποιείται μόνο μία φορά (nonce) και τον στέλνει στην ετικέτα. Εκεί, η ετικέτα δημιουργεί έναν τέτοιο αριθμό επίσης. Επιπλέον, εάν η προηγούμενη εκτέλεση ήταν επιτυχής, οδηγώντας στην τιμή της ετικέτας 0, η ετικέτα αποστέλλει μια απάντηση, συμπεριλαμβανομένου του κατακερματισμένου αναγνωριστικού και του μη. Επιπλέον, η ετικέτα ορίζει την κατάστασή της σε 1. (F.T. Sheldon, V. Vishik 2010)

Σε περίπτωση προηγούμενης αποτυχημένης εκτέλεσης, η ετικέτα διατηρεί την κατάστασή της σε 1 και αποστέλλει, εκτός από την nonce, τη λειτουργία κατακερματισμού του αναγνωριστικού της, nonce και της συσκευής ανάγνωσης nonce. Για να αποδεχτεί την ετικέτα, ο αναγνώστης πρέπει να ελέγξει την απόκριση της ετικέτας, εξαιρουμένης της μη ετικέτας. Εάν η απόκριση, που αποτελείται είτε από το hash του τρέχοντος ID, είτε από την κατακερματισμένη λειτουργία του ID, το nonce της ετικέτας και το nonce του αναγνώστη, ή την κατακερματισμένη λειτουργία του προηγούμενου αναγνωριστικού, το nonce της ετικέτας και το nonce του αναγνώστη , ταιριάζει με οποιαδήποτε από τις τιμές που η συσκευή ανάγνωσης διατηρεί την ετικέτα θεωρείται αποδεκτή. (F.T. Sheldon, V. Vishik 2010)

Μετά την επαλήθευση, η συσκευή ανάγνωσης ενημερώνει τις τιμές που κατέχει και στέλνει την τιμή της κατακερματισμένης λειτουργίας του προηγούμενου αναγνωριστικού της και της μη ετικέτας στην ετικέτα. Εάν η απόκριση είναι ίση με την κατακερματισμένη λειτουργία του αναγνωριστικού της ετικέτας και αν η ετικέτα ενημερώσει το αναγνωριστικό της στην τιμή της κατακερματισμένης λειτουργίας του αναγνωριστικού της και της συσκευής ανάγνωσης. Επιπλέον, δείχνει επιτυχημένη εκτέλεση αυτής της εκτέλεσης ρυθμίζοντας την κατάσταση σε 0. (F.T. Sheldon, V. Vishik 2010)

Πρωτόκολλο Lee Asano Kim

Οι Lee, Asano και Kim τονίζουν τη σημασία της ανιχνευσιμότητας και της αντι-κλωνοποίησης. Η ανιχνευσιμότητα εμποδίζει έναν εισβολέα να εντοπίσει πληροφορίες που εκπέμπει μια ετικέτα, οι οποίες στη συνέχεια μπορούν να χρησιμοποιηθούν για να ανακαλύψουν συγκεκριμένα μοτίβα που αποκαλύπτουν τα μυστικά δεδομένα μιας ετικέτας, όπως το αναγνωριστικό της. (Lee, S., Asano, T., & Kim, K. 2006)

Το πρωτόκολλό τους βασίζεται στην υπόθεση ότι και οι δύο, η ετικέτα και η συσκευή ανάγνωσης, μπορούν να αποθηκεύσουν συγκεκριμένες μεταβλητές σε διαφορετικές μνήμες. Κάθε ετικέτα περιέχει έναν μοναδικό, τυχαίο αριθμό που αποθηκεύεται μόνιμα για σκοπούς ελέγχου ταυτότητας που αναφέρεται ως αναγνωριστικό της ετικέτας. (Lee, S., Asano, T., & Kim, K. 2006)

Σε περίπτωση που το αναγνωριστικό της ετικέτας ταιριάζει με το αναγνωριστικό που είναι αποθηκευμένο στη βάση δεδομένων, στην ετικέτα εκχωρείται μια νέα τιμή μετά από κάθε επιτυχημένο έλεγχο ταυτότητας. Επιπλέον, η ετικέτα και ο αναγνώστης μπορούν να αποθηκεύσουν έναν δεύτερο ψευδοτυχαίο αριθμό που θα αποθηκευτεί μόνο όσο διαρκεί η διαδικασία ελέγχου ταυτότητας, για να διασφαλιστεί ότι κάθε περίοδος σύνδεσης έχει διαφορετική αναγνώριση για την αποφυγή επιθέσεων επανάληψης. Η βάση δεδομένων που επικοινωνεί με τις συσκευές ανάγνωσης αποθηκεύει το τρέχον αναγνωριστικό κάθε ετικέτας καθώς και την προηγούμενη. (Lee, S., Asano, T., & Kim, K. 2006)

Η διαδικασία ελέγχου ταυτότητας του πρωτοκόλλου μπορεί να περιγραφεί ως εξής. Ο αναγνώστης στέλνει έναν τυχαίο αριθμό, που ισχύει για τον τρέχοντα γύρο, στην ετικέτα. Η ετικέτα στέλνει τον ίδιο τύπο αριθμού στον αναγνώστη. Επιπλέον, η ετικέτα δημιουργεί μια συνάρτηση κατακερματισμού τον αριθμό που λαμβάνεται από τον αναγνώστη, τον δικό του αριθμό και το αναγνωριστικό του και στέλνει αυτό το κατακερματισμό στον αναγνώστη. (Lee, S., Asano, T., & Kim, K. 2006)

Η βάση δεδομένων, την οποία επικοινωνεί ο αναγνώστης, ελέγχει ότι το αναγνωριστικό της ετικέτας ταιριάζει με το κατακερματισμό ενός από τα πεδία της βάσης δεδομένων. Η βάση δεδομένων ενημερώνει τα πεδία της σε περίπτωση που ο κατακερματισμός ταιριάζει με το αναγνωριστικό της ετικέτας. (Lee, S., Asano, T., & Kim, K. 2006)

Σε αυτήν την περίπτωση, το αναγνωριστικό της τρέχουσας ετικέτας αποθηκεύεται στο πεδίο για το προηγούμενο αναγνωριστικό της ετικέτας και ο κατακερματισμός χρησιμεύει ως το νέο αναγνωριστικό. Από τον τυχαίο αριθμό του αναγνώστη, το κατακερματισμό της ετικέτας και το μόνιμο αναγνωριστικό της ετικέτας, η βάση δεδομένων υπολογίζει μια νέα τιμή χρησιμοποιώντας μια συνάρτηση κατακερματισμού και στέλνει αυτόν τον αριθμό στον αναγνώστη. Με τη βοήθεια αυτού του αριθμού, ο αναγνώστης ενημερώνει το αναγνωριστικό της ετικέτας στο κατακερματισμό του αριθμού που λαμβάνεται από τη βάση δεδομένων. (Lee, S., Asano, T., & Kim, K. 2006)

ΚΕΦΑΛΑΙΟ 3: Near-Field Communication

Το Near-Field Communication (NFC) είναι μια τεχνολογία που χρησιμοποιείται κατά την αναγνώριση ραδιοσυχνοτήτων (RFID). Το NFC επιτρέπει στις συσκευές να αλληλεπιδρούν μεταξύ τους χρησιμοποιώντας μια ασύρματη σύνδεση μικρής εμβέλειας. Το NFC επιτρέπει την επικοινωνία τοποθετώντας απλώς τις εν λόγω συσκευές η μία κοντά στην άλλη επιτρέποντας τη μετάδοση δεδομένων. Σε τεχνικούς όρους, αυτό σημαίνει ότι οι συσκευές εκτελούν χειραψία. (Smith, S. 2017)

Σύμφωνα με τους Haselsteiner και Breitfuß οι συσκευές και ο τρόπος επικοινωνίας τους μπορούν να διαιρεθούν ανάλογα με την κατάσταση των συσκευών. Σε σύγκριση με τα παθητικά τους μέρη, οι ενεργές συσκευές είναι εξοπλισμένες με πηγή ισχύος. Σε περίπτωση που και οι δύο συσκευές είναι ενεργές, το πεδίο ραδιοσυχνοτήτων δημιουργείται από τη συσκευή αποστολής δεδομένων. Εάν μόνο μία από τις συσκευές είναι ενεργή και η άλλη παθητική συσκευή, το πεδίο ραδιοσυχνοτήτων δημιουργείται

μόνο από την ενεργή συσκευή. Κατά την εκτέλεση χειραψίας, η ενεργή συσκευή, που συνήθως αναφέρεται ως εκκινητής, στέλνει ένα μήνυμα στη δεύτερη συσκευή που μπορεί είτε να είναι ενεργή είτε παθητική. Βάσει αυτού του μηνύματος, η δεύτερη απάντηση απαντά και η σύνδεση δημιουργείται.

Το NFC λέγεται ότι είναι πολύ φιλικό προς το χρήστη, καθώς δεν χρειάζεται να διαμορφώσετε τις συσκευές πριν χειροκίνητα. Η τοποθέτηση των συσκευών μεταξύ τους αρκεί για να δημιουργηθεί σύνδεση σε πολύ σύντομο χρονικό διάστημα, συνήθως εντός χιλιοστών του δευτερολέπτου. Επιπλέον, το NFC μπορεί να χρησιμοποιηθεί με άλλες ασύρματες τεχνολογίες, όπως WiFi, ZigBee και Bluetooth. (Smith, S. 2017)

ΠΙΘΑΝΟΙ ΚΙΝΔΥΝΟΙ ΚΑΙ ΡΙΣΚΑ

Παρά τα προαναφερθέντα πλεονεκτήματα, το NFC είναι επιρρεπές σε διάφορες επιθέσεις που μπορεί να έχουν σοβαρές επιπτώσεις στο σύστημα. Αυτές οι απειλές βασίζονται σε κοινά ζητήματα ασφάλειας δικτύου, όπως η υποκλοπή ή η λεγόμενη επίθεση άρνησης υπηρεσίας. Οι ακόλουθες ενότητες παρέχουν μια λεπτομερή επισκόπηση όλων των κοινών απειλών που αφορούν την ασφάλεια. (Smith, S. 2017)

Eavesdropping

Το Eavesdropping είναι ένα ζήτημα ασφάλειας που επηρεάζει όλες τις ασύρματες τεχνολογίες. Καθώς το NFC επικοινωνεί μέσω κυμάτων ραδιοσυχνοτήτων, η υποκλοπή αποτελεί απειλή για το NFC. Συνήθως, δύο συσκευές επικοινωνίας δεν απέχουν περισσότερο από 10 cm μεταξύ τους. Παρά τη μικρή απόσταση, ένας εισβολέας που λαμβάνει και αποκωδικοποιεί το σήμα μπορεί να παρακολουθεί την επικοινωνία, ανεξάρτητα από το πόσο μικρή είναι η απόσταση. (Smith, S. 2017)

Ωστόσο, σύμφωνα με τους Haselsteiner και Breitfuß δεν είναι δυνατόν να προβλεφθεί πόσο κοντά πρέπει να είναι ένας εισβολέας για τη λήψη του σήματος. Αυτό εξαρτάται από διάφορες παραμέτρους και των δύο, της συσκευής αποστολής και λήψης. Μεταξύ

άλλων, αυτές οι παράμετροι καλύπτουν τα χαρακτηριστικά των κεραιών των συσκευών αποστολής και λήψης, την ποιότητα των συσκευών γενικά και τη θέση της εγκατάστασης του συστήματος. (Smith, S. 2017)

Επιπλέον, ένας εισβολέας πρέπει να εξετάσει τη λειτουργία της συσκευής αποστολής. Μια συσκευή που δημιουργεί το δικό της πεδίο ραδιοσυχνοτήτων, μια λεγόμενη ενεργή συσκευή, είναι πολύ πιο εύκολο να παρακολουθεί κανείς από μια συσκευή που χρησιμοποιεί το πεδίο άλλης συσκευής. Αυτό συμβαίνει μόνο επειδή η εμβέλεια μιας ενεργής συσκευής είναι δέκα φορές μεγαλύτερη. (Smith, S. 2017)

Denial of Service

Μια επίθεση άρνησης υπηρεσίας γίνεται διαταράσσοντας την ανταλλαγή δεδομένων μεταξύ των συσκευών, έτσι ώστε τα δεδομένα που αποστέλλονται από τη συσκευή αποστολής να μην μπορούν να αποκωδικοποιηθούν από τη δεύτερη συσκευή. Συνήθως αυτό γίνεται "πλημμυρίζοντας" την επικοινωνία. (Smith, S. 2017)

Data Insertion

Οι εισαγωγές δεδομένων είναι πάντοτε δυνατές όταν η συσκευή απάντησης είναι πιο αργή στην απάντηση από τη συσκευή του εισβολέα. Σε αυτήν την περίπτωση, ο εισβολέας μπορεί να στείλει τα πλαστά δεδομένα πριν από την αποστολή των πραγματικών έγκυρων δεδομένων. Σε περίπτωση που τα δεδομένα του εισβολέα και τα έγκυρα δεδομένα αποστέλλονται ταυτόχρονα, θα προκύψει ένα ελάττωμα στα δεδομένα. (Smith, S. 2017)

Man-in-the-Middle attack

Σύμφωνα με τον Haselsteiner και τον Breitfuß, η επίθεση «man-in-the-middle» είναι δυνατή μόνο θεωρητικά. Ωστόσο, για λόγους πληρότητας, ένα θεωρητικό σενάριο θα περιγραφεί παρακάτω. Υπάρχουν δύο ρυθμίσεις που πρέπει να ληφθούν υπόψη. Η πρώτη συνομιλία αποτελείται από τη χρήση ενεργής και παθητικής λειτουργίας, ενώ η δεύτερη προϋποθέτει και τα δύο μέρη σε ενεργή λειτουργία. (Smith, S. 2017)

Σε ενεργή-παθητική λειτουργία, το ενεργό μέρος δημιουργεί το πεδίο ραδιοσυχνοτήτων και στέλνει τα δεδομένα στο δεύτερο μέρος. Ένας εισβολέας μπορεί να παρακολουθεί την επικοινωνία και να καθιστά αδύνατη τη μετάδοση διαταράσσοντας τη μετάδοση. Μόλις διαδοθεί η μετάδοση, ο εισβολέας στέλνει τα δεδομένα, αντικαθιστώντας το πρωτότυπο, στο δεύτερο μέρος. Για να πετύχει ο εισβολέας πρέπει να δημιουργήσει ένα πεδίο ραδιοσυχνοτήτων. Καθώς το προηγούμενο πεδίο ραδιοσυχνοτήτων του αποστολέα είναι ακόμη ενεργό, ο εισβολέας θα πρέπει να ευθυγραμμίσει τέλεια και τα δύο ενεργά πεδία για να πετύχει, γεγονός που καθιστά αδύνατη την επίθεση σε ενεργή-παθητική λειτουργία. (Smith, S. 2017)

Η δεύτερη πιθανότητα της επίθεσης man-in-the-middle περιλαμβάνει και τα δύο μέρη επικοινωνίας χρησιμοποιώντας ενεργό τρόπο. Και πάλι, όπως στον ενεργό-παθητικό τρόπο που περιγράφηκε προηγουμένως, ο εισβολέας διαταράσσει τη μετάδοση. Σε σύγκριση με την προηγούμενη ρύθμιση, στην ενεργή λειτουργία το μέρος αποστολής πρέπει να απενεργοποιήσει το πεδίο ραδιοφώνου για το δεύτερο μέρος να λάβει τα δεδομένα. Αυτό επιτρέπει στον εισβολέα να ενεργοποιήσει το δικό του ραδιοφωνικό πεδίο για να στείλει τα πλαστά δεδομένα. Σε αυτή τη ρύθμιση και τα δύο μέρη ακούνε την επικοινωνία περιμένοντας την απάντηση του άλλου μέρους. Αυτό καθιστά αδύνατο για τον εισβολέα να στείλει τα πλαστά δεδομένα χωρίς κανένα από τα μέρη να παρατηρήσει ότι τα δεδομένα αποστέλλονται από κάποιον άλλο. Και πάλι, σύμφωνα με τον Haselsteiner και τον Breitfuß, η ρύθμιση που περιγράφηκε προηγουμένως καθιστά αδύνατη την επίθεση man-in-the-middle.

SECURITY IMPLEMENTATIONS

Αυτό το κεφάλαιο παρουσιάζει μια επισκόπηση των πιο αποτελεσματικών εφαρμογών ασφαλείας σε συστήματα NFC. Επιπλέον, θα παρέχει ένα παράδειγμα για το πώς να ασφαλίσετε το κανάλι μεταξύ δύο συσκευών. (Smith, S. 2017)

Eavesdropping

Δεν υπάρχει κανένα αντίμετρο στο ίδιο το NFC που θα μπορούσε να αποτρέψει ένα σύστημα από μια επίθεση υποκλοπής. Η μόνη αποτελεσματική εφαρμογή ασφάλειας είναι το λεγόμενο ασφαλές κανάλι που θα περιγραφεί λεπτομερώς στην ενότητα Secure channel. (Smith, S. 2017)

Denial of Service

Οι επιθέσεις άρνησης υπηρεσίας είναι πολύ εύκολο να εντοπιστούν. Η ισχύς που απαιτείται για αλλοιώσεις δεδομένων είναι εξαιρετικά υψηλότερη, ώστε οι συσκευές NFC να μπορούν να ανιχνεύσουν την αύξηση. Σε περίπτωση που διαπιστωθεί σημαντική αύξηση της ισχύος, το NFC μπορεί να απενεργοποιηθεί με έναν απλό διακόπτη που περιλαμβάνεται σε κάθε συσκευή. (Smith, S. 2017)

Data Insertion

Για να αποτρέψετε έναν εισβολέα να αντικαταστήσει έγκυρα δεδομένα με πλαστά δεδομένα, υπάρχουν διάφορες χώρες. Μία δυνατότητα αποτροπής της επίθεσης είναι η άμεση απάντηση της συσκευής απάντησης χωρίς καθυστέρηση για να βεβαιωθείτε ότι ο εισβολέας δεν έχει χρόνο να απαντήσει με πλαστά δεδομένα. Ένα άλλο αντίμετρο που θα μπορούσε να ανιχνεύσει και να αποτρέψει μια επίθεση, είναι ότι ενώ το κανάλι για μετάδοση μεταξύ των δύο συσκευών είναι ανοιχτό, οι συσκευές ακούνε το κανάλι. Σε περίπτωση που ένας εισβολέας εισάγει δεδομένα, θα μπορούσε να ακουστεί στο κανάλι. Η τελευταία επιλογή για την αποτροπή μιας επίθεσης εισαγωγής δεδομένων είναι το λεγόμενο ασφαλές κανάλι που θα καταγραφεί στην ενότητα Secure channel. (Smith, S. 2017)

Man-in-the-Middle attack

Λόγω των δυσκολιών τόσο στον ενεργό-παθητικό όσο και στον ενεργό τρόπο, σύμφωνα με τους Haselsteiner και Breitfuß είναι αδύνατο να εκτελεστεί μια επίθεση

man-in-the-middle. Ωστόσο, λόγω του μόνιμα δημιουργημένου πεδίου ραδιοσυχνοτήτων, μια επίθεση στην ενεργή παθητική λειτουργία είναι λιγότερο πιθανό να πετύχει, έτσι ώστε για λόγους ασφαλείας συνιστάται η χρήση αυτής της ρύθμισης. (Smith, S. 2017)

Secure channel

Ένα ασφαλές κανάλι μεταξύ δύο συσκευών NFC είναι αρκετά εύκολο να δημιουργηθεί και μπορεί να προστατεύσει τα δεδομένα που αποστέλλονται από τροποποιήσεις. Καθώς είναι σχεδόν αδύνατο να εκτελεστεί μια επίθεση man-in-the-middle, η οποία περιγράφεται στην ενότητα Επίθεση Man-in-the-Middle, δεν απαιτούνται περαιτέρω προστατευτικά μέτρα για την εγκατάσταση. Γενικά, ένα ασφαλές κανάλι βασίζεται σε ένα πρωτόκολλο βασικής συμφωνίας όπως το τυπικό Diffie-Hellmann. Σε αυτό το πρωτόκολλο, και τα δύο μέρη που επικοινωνούν διαθέτουν ένα μυστικό κλειδί, γνωστό μόνο σε αυτούς, το οποίο εγγυάται την ασφαλή μετάδοση δεδομένων. (Smith, S. 2017)

ΚΕΦΑΛΑΙΟ 4: Wireless Sensor Networks

Τα ασύρματα δίκτυα αισθητήρων (WSN) είναι ένα άλλο βασικό στοιχείο του Διαδικτύου των πραγμάτων. Χρησιμοποιούνται σε πολλές εφαρμογές, συμπεριλαμβανομένων στρατιωτικών εφαρμογών, περιβαλλοντικών εφαρμογών, εφαρμογών υγείας, οικιακών εφαρμογών ή άλλων εμπορικών προϊόντων. (F.T. Sheldon, V. Vishik 2010)

Οι στρατιωτικές εφαρμογές περιλαμβάνουν, μεταξύ άλλων, επιτήρηση πεδίου μάχης, εκτίμηση ζημιών και εντοπισμό επιθέσεων. Σε περιβαλλοντικές εφαρμογές, τα WSN χρησιμοποιούνται για την παρακολούθηση των κινήσεων των ζώων, την παρακολούθηση της Γης, συμπεριλαμβανομένων των δασικών πυρκαγιών ή ανίχνευσης

πλημμυρών, ή για γεωγραφική έρευνα. Οι εφαρμογές υγείας χρησιμοποιούν WSN για παρακολούθηση των διεργασιών στα νοσοκομεία, παρακολούθηση και ανίχνευση ανθρώπινων φυσιολογικών δεδομένων ή παρακολούθηση της χορήγησης φαρμάκων στα νοσοκομεία. Μικρές οικιακές συσκευές, όπως ηλεκτρικές σκούπες ή φούρνοι μικροκυμάτων, μπορούν να περιέχουν κόμβους αισθητήρα για να διασφαλίσουν τον αυτοματισμό του σπιτιού που χρησιμοποιείται στις εφαρμογές στο σπίτι, με βάση την αλληλεπίδραση αυτών των συσκευών. Παραδείγματα άλλων εμπορικών εφαρμογών που χρησιμοποιούν WSN είναι παρακολούθηση και ανίχνευση οχημάτων, έλεγχος ρομπότ αυτοματισμού ή κεντρικός έλεγχος κλιματισμού κτιρίων γραφείων. (C. M. Medaglia, A. Serbanati, 2010)

Τα ασύρματα δίκτυα αισθητήρων αποτελούνται συνήθως από δύο μέρη: τους λεγόμενους σταθμούς βάσης και έναν τεράστιο αριθμό κόμβων αισθητήρων. Οι κόμβοι αισθητήρα αποτελούνται και πάλι από τα ακόλουθα τέσσερα μέρη: Μια μονάδα ισχύος, μια μονάδα μετάδοσης, μια μονάδα επεξεργασίας και μια μονάδα ανίχνευσης. (Mudassar Ahmad, Tanveer Younis, Muhammad Asif Habib, Rehan Ashraf, Syed Hassan Ahmed, 2019)

Συνήθως η μονάδα ισχύος είναι το μόνο συστατικό που παρέχει ισχύ σε όλα τα άλλα συστατικά του κόμβου. Μπορεί είτε να αποτελείται από μία μόνο μπαταρία είτε από οποιαδήποτε συσκευή συλλογής ενέργειας, όπως ηλιακά κύτταρα. Η μονάδα μετάδοσης συνδέει τον κόμβο στο δίκτυο αλληλεπιδρώντας συνεχώς με τη μονάδα επεξεργασίας. Η μονάδα επεξεργασίας αποτελείται από δύο συστατικά, έναν επεξεργαστή και έναν αποθηκευτικό χώρο. Αυτή η μονάδα αλληλεπιδρά με όλες τις άλλες μονάδες, τη λήψη και την επεξεργασία πληροφοριών που υποστηρίζονται από τη μονάδα ισχύος. Η μονάδα ανίχνευσης αποτελείται και πάλι από δύο δευτερεύοντα στοιχεία: ένας αισθητήρας και ένας μετατροπέας που μετατρέπει τις αναλογικές εισόδους σε ψηφιακές, ως εκ τούτου αναφέρεται ως μετατροπέας αναλογικού σε ψηφιακό (ADC). (Mudassar Ahmad, Tanveer Younis, Muhammad Asif Habib, Rehan Ashraf, Syed Hassan Ahmed, 2019)

ΚΑΤΗΓΟΡΙΕΣ ΕΙΣΒΟΛΕΩΝ ΣΕ WSN

Υπάρχουν δύο τύποι εισβολέων που μπορούν να αποτελέσουν απειλή για τα ασύρματα δίκτυα αισθητήρων. Οι επιτιθέμενοι Mote-class μπορούν να αποκτήσουν πρόσβαση σε WSN χρησιμοποιώντας έναν συγκεκριμένο αριθμό κακόβουλων κόμβων που έχουν παρόμοιες δυνατότητες με τους κόμβους μέσα στο δίκτυο. Ο δεύτερος τύπος εισβολέων είναι οι λεγόμενοι εισβολείς τάξης φορητού υπολογιστή. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Οι επιτιθέμενοι στην κατηγορία φορητών υπολογιστών είναι πολύ πιο ισχυροί από τους επιτιθέμενους στην κατηγορία mote. Ενώ οι επιτιθέμενοι της κατηγορίας mote μπορούν να εκτελέσουν επιθέσεις στο άμεσο περιβάλλον τους, ο επιτιθέμενος στην κατηγορία φορητών υπολογιστών θα μπορούσε να επιτεθεί σε ολόκληρο το δίκτυο. Οι επιτιθέμενοι στην κατηγορία φορητών υπολογιστών χρησιμοποιούν πιο ισχυρές συσκευές, οι οποίες συνήθως έχουν τη χωρητικότητα και τα στοιχεία ενός φορητού υπολογιστή ή μιας παρόμοιας συσκευής, συμπεριλαμβανομένου του υψηλού εύρους ζώνης και ενός ισχυρού ενεργειακού πόρου. Εκτός από την προηγούμενη διάκριση, οι εισβολείς μπορούν να ταξινομηθούν ανάλογα με την πρόσβασή τους στο δίκτυο καθώς και εάν μια επίθεση είναι ενεργή ή παθητική. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Οι ενεργές επιθέσεις περιλαμβάνουν τροποποίηση ή δημιουργία ροών δεδομένων, ενώ παθητικές επιθέσεις χρησιμοποιούνται για την παρακολούθηση αυτών των ροών. Οι εξωτερικές επιθέσεις εκτελούνται από κόμβους που δεν αποτελούν μέρος του WSN. Οι εσωτερικές επιθέσεις από την άλλη πλευρά πραγματοποιούνται χρησιμοποιώντας κόμβους που ανήκουν στο WSN. Για να επιτύχει επιθέσεις εσωτερικών, ο εισβολέας πρέπει να κρατήσει το βασικό υλικό για να θέσει σε κίνδυνο τον κόμβο του αισθητήρα. Μόλις τεθεί σε κίνδυνο ο κόμβος του αισθητήρα, οι επιτιθέμενοι στην τάξη του φορητού υπολογιστή μπορούν να επιτεθούν σε ολόκληρο το WSN. (F.T. Sheldon, V. Vishik 2010)

ΕΠΙΘΕΣΕΙΣ ΣΕ ΔΙΚΤΥΑ ΑΙΣΘΗΤΗΡΩΝ

Τα ασύρματα δίκτυα αισθητήρων είναι ευάλωτα σε διαφορετικούς τύπους επιθέσεων που θα περιγράφονται λεπτομερώς στα επόμενα κεφάλαια. Οι επιθέσεις συμβαίνουν σε διαφορετικά επίπεδα του στρώματος στοίβας protocol τα οποία μπορούν να περιγραφούν ως εξής. Το φυσικό στρώμα ασχολείται με τη μετάδοση ροών δεδομένων, την ανίχνευση σήματος και την κρυπτογράφηση δεδομένων και αντιμετωπίζει επιθέσεις εμπλοκής και μετριασμού. Το επίπεδο σύνδεσης δεδομένων είναι υπεύθυνο για την πολυπλεξία αυτών των ροών δεδομένων, για την ανίχνευση πλαισίων δεδομένων και για τη διασφάλιση συνδέσεων από σημείο σε σημείο ή από σημείο σε σημείο. Οι κοινές επιθέσεις είναι εξάντληση πόρων και αδικία. Το επίπεδο δικτύου εξασφαλίζει την προώθηση πακέτων και αντιστοιχίσεων διευθύνσεων. Οι επιθέσεις που συμβαίνουν σε επίπεδο δικτύου είναι οι ακόλουθες: πλαστογράφηση, αλλοίωση ή επανάληψη δρομολόγησης σε σχηματισμό, επιλεκτική προώθηση, sinkholes, επίθεση Sybil, wormholes και επιθέσεις HELLO-flood. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Το επίπεδο μεταφοράς εξασφαλίζει μια αξιόπιστη μεταφορά πακέτων και το επίπεδο εφαρμογής είναι υπεύθυνο για τη διαχείριση αιτημάτων δεδομένων που αντιμετωπίζουν επιθέσεις όπως πλημμύρες και αποσυγχρονισμός. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Jamming

Το jamming, που συχνά αναφέρεται ως ραδιοσυμπίεση, είναι μια μέθοδος που χρησιμοποιείται για την επίθεση ασύρματων δικτύων παρεμβαίνοντας στις ραδιοσυχνότητες του δικτύου. Οι αντίπαλοι που έχουν μια ισχυρή πηγή που χρησιμοποιούνται για παρεμβολές επιθέσεων μπορούν να διαταράξουν ένα ολόκληρο δίκτυο. Αυτό είναι ακόμη δυνατό αν η πηγή είναι λιγότερο ισχυρή, αλλά η

ραδιοσυμπίεση κατανέμεται τυχαία. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Tampering

Λόγω του χαμηλού κόστους των κόμβων αισθητήρων, η παραβίαση είναι μια άλλη πιθανή επίθεση σε δίκτυα αισθητήρων. Οι εισβολείς που μπορούν να αποκτήσουν φυσική πρόσβαση σε έναν κόμβο μπορούν να εξαγάγουν τις πληροφορίες του κόμβου και επιπλέον να δημιουργήσουν έναν κόμβο του οποίου ο εισβολέας έχει τον πλήρη έλεγχο. (F.T. Sheldon, V. Vishik 2010)

Resource exhaustion

Οι εισβολείς μπορούν να εξαντλήσουν έναν κόμβο και τους γύρω κόμβους τους προκαλώντας συγκρούσεις μεταξύ της μετάδοσης δεδομένων μεταξύ πολλαπλών κόμβων. Εάν η αναμετάδοση δεδομένων δεν καλύπτεται και το δίκτυο προσπαθεί συνεχώς να μεταδίδει αυτά τα πακέτα, οι ενεργειακοί πόροι των επηρεαζόμενων κόμβων θα εξαντληθούν. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Unfairness

Το Unfairness περιλαμβάνει την προηγούμενη επίθεση επιπέδου συνδέσμου και μπορεί να θεωρηθεί ήπια μορφή επίθεσης DoS. Σε μια επίθεση αδικίας ένας αντίπαλος προσπαθεί να κάνει τους κόμβους να χάσουν την προθεσμία μετάδοσης που μπορεί να επηρεάσει και να αποδυναμώσει ολόκληρο το δίκτυο. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Spoofing, Altering and Replaying

Ο σκοπός της πλαστογράφησης, της αλλαγής και της αναπαραγωγής πληροφοριών δρομολόγησης είναι να διαταράξει την κίνηση του δικτύου. Οι αναφερόμενες επιθέσεις

μπορούν να περιλαμβάνουν τα εξής: δημιουργία βρόχων δρομολόγησης, επέκταση ή συντόμευση διαδρομών, διαμερισμός δικτύου ή δημιουργία μηνυμάτων λανθασμένων σφαλμάτων. (F.T. Sheldon, V. Vishik 2010)

Selective forwarding

Σε μια επίθεση επιλεκτικής προώθησης, οι εισβολείς κάνουν χρήση της υπόθεσης ότι οι κόμβοι συνήθως προωθούν τα μηνύματα με πιστό τρόπο. Σε αυτήν την επίθεση οι αντίπαλοι χρησιμοποιούν κακόβουλους κόμβους για να ρίξουν ορισμένα μηνύματα που σημαίνει ότι δεν προωθούνται περαιτέρω. Για να περιορίσετε την υποψία και να αποφύγετε ότι οι γύρω κόμβοι επιλέγουν άλλη διαδρομή, σε περίπτωση που καταλήξουν στο συμπέρασμα ότι το πρωτότυπο έχει αποτύχει, οι εισβολείς ενδέχεται να επιλέξουν να τροποποιήσουν ή να πιέσουν μόνο μερικά πακέτα και προωθήστε τα υπόλοιπα. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Οι εισβολείς έχουν δύο δυνατότητες να επιτύχουν αυτήν την επίθεση. Μπορούν είτε να είναι μέρος της διαδρομής μετάδοσης δεδομένων είτε να ακούσουν τη ροή μετάδοσης μέσω γειτονικών κόμβων. Παρόλο που είναι δυνατές και οι δύο μορφές επίθεσης, η πρώτη επιλογή είναι πιο αποτελεσματική και πιο εύκολη στην εκτέλεση. (F.T. Sheldon, V. Vishik 2010)

Sinkhole attacks

Ο στόχος μιας επίθεσης με καταβόθρες είναι να διασφαλίσει ότι όλη η κίνηση μιας συγκεκριμένης περιοχής του δικτύου ρέει μέσω ενός συμβιβασμένου κόμβου στον οποίο ο επιτιθέμενος έχει πλήρη έλεγχο. Για να δημιουργήσει μια καταβόθρα, ο εισβολέας πρέπει να διασφαλίσει ότι ο κόμβος φαίνεται ελκυστικός στους γύρω κόμβους του, προσομοιώνοντας τους κόμβους να είναι μια διαδρομή υψηλής ποιότητας προς ένα σταθμό βάσης. Αυτό διασφαλίζει ότι οι κόμβοι χρησιμοποιούν την καταβόθρα για την προώθηση πακέτων που υποτίθεται ότι φτάνουν στο σταθμό

βάσης. Χρησιμοποιώντας αυτήν την επίθεση, οι αντίπαλοι μπορούν εύκολα να καταστείλουν ή να τροποποιήσουν τα πακέτα δεδομένων. (F.T. Sheldon, V. Vishik 2010)

The Sybil attack

Αυτή η μορφή επίθεσης χρησιμοποιείται συχνά στη γεωγραφική δρομολόγηση. Σε μια επίθεση Sybil ένας αντίπαλος περιλαμβάνει έναν κόμβο που εμφανίζεται ως πολλαπλές ταυτότητες. Σε μια τοποθεσία, οι κόμβοι του συστήματος δρομολόγησης αλλάζουν τις συντεταγμένες τους με τους γειτονικούς τους κόμβους σε πληροφορίες γεωγραφικής διαδρομής, αποδεχόμενοι συνήθως οποιοδήποτε σύνολο συντεταγμένων. Αυτό προκαλεί ότι ο αντίπαλος μπορεί να βρίσκεται σε πολλά μέρη κάθε φορά. (F.T. Sheldon, V. Vishik 2010)

Wormholes

Οι εισβολείς χρησιμοποιούν σκουληκότρυπες για να διοχετεύουν μηνύματα από ένα μέρος του δικτύου σε ένα άλλο. Οι επιθέσεις στο Wormhole περιλαμβάνουν συνήθως δύο απομακρυσμένους κόμβους που ένας εισβολέας έχει τον πλήρη έλεγχο της προώθησης μηνυμάτων μεταξύ τους. Εάν ένας αντίπαλος καταφέρει να τοποθετήσει μια σκουληκότρυπα κοντά σε σταθμό βάσης και πείσει κόμβους που συνήθως είναι πολλαπλοί λυκίσκοι για να είναι πολύ πιο κοντά, ο εισβολέας θα μπορούσε να διακόψει τη δρομολόγηση σε ολόκληρο το δίκτυο. Οι επιθέσεις του Wormhole μπορούν να χρησιμοποιηθούν σε συνδυασμό με άλλες επιθέσεις για να κάνουν την επίθεση πιο ισχυρή. Αυτές οι επιθέσεις περιλαμβάνουν υποκλοπή, επιλεκτική προώθηση, καταβόθρες ή την επίθεση Sybil. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

HELLO flood attack

Σε μια επίθεση πλημμύρας HELLO οι αντίπαλοι κάνουν κατάχρηση του γεγονότος ότι στα περισσότερα πρωτόκολλα δρομολόγησης οι κόμβοι χρησιμοποιούν πακέτα HELLO για να ανακοινωθούν στους γειτονικούς κόμβους τους. Αυτό περιλαμβάνει την υπόθεση ότι αυτοί οι κόμβοι βρίσκονται εντός του φυσιολογικού εύρους μεταξύ τους. Οι επιτιθέμενοι που στέλνουν αυτά τα πακέτα HELLO, παρά το ότι βρίσκονται σε φυσιολογικό εύρος, μπορούν να κάνουν άλλους κόμβους να είναι ότι αυτοί είναι οι κόμβοι αποστολής γείτονες. Οι γειτονικοί κόμβοι θα μεταδώσουν τα πακέτα δεδομένων τους στον κόμβο στέλνοντας τα πακέτα HELLO, αλλά, δεδομένου ότι είναι εκτός εμβέλειας ραδιοφώνου, το πακέτο δεν θα φτάσει ποτέ στον προορισμό τους, γεγονός που καθιστά αδύνατη για την καθαρή εργασία να διατηρήσει την κατάστασή της. (F.T. Sheldon, V. Vishik 2010)

De-synchronisation

Σε μια επίθεση αποσυγχρονισμού, ένας αντίπαλος στέλνει συνεχώς πλαστά πακέτα σε έναν κεντρικό υπολογιστή, που προσπαθεί να ζητήσει την αναμετάδοση αυτών των χαμένων πλαισίων. Αυτό μπορεί να κάνει τον οικοδεσπότη να σπαταλήσει ενέργεια, προσπαθώντας να ανακτήσει από ψευδή λάθη, σε περίπτωση που ο εισβολέας καταφέρει να αποτρέψει εντελώς την ανταλλαγή δεδομένων. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

ΑΝΤΙΜΕΤΡΑ

Σύμφωνα με τους Karlof και Wagner οι περισσότερες επιθέσεις που προέρχονται από το εξωτερικό του WSN μπορούν να αποφευχθούν με την εφαρμογή κρυπτογράφησης επιπέδου σύνδεσης χρησιμοποιώντας ένα κοινό κλειδί μεταξύ των κόμβων και του σταθμού βάσης.

Ωστόσο, αυτό το αντίμετρο δεν παρέχει προστασία ενάντια σε επιθέσεις εκ των έσω. Οι ακόλουθες ενότητες θα επικεντρωθούν σε αντίμετρα για τους μηχανισμούς επίθεσης που περιγράφηκαν προηγουμένως σε WSN και θα παρουσιάσουν διάφορες λύσεις στις πιο κοινές σε επιθέσεις εναντίον WSN. (F.T. Sheldon, V. Vishik 2010)

Jamming

Υπάρχουν δύο γνωστοί μηχανισμοί άμυνας κατά της παρεμβολής: μετακίνηση συχνότητας και διάδοση κώδικα. Η μετάβαση με συχνότητα συνεπάγεται ταχεία αλλαγή συχνότητας κατά τη μετάδοση σημάτων, γεγονός που καθιστά αδύνατο για έναν εισβολέα να μπλοκάρει την άγνωστη συχνότητα. Η διάδοση κώδικα χρησιμοποιείται για τον ίδιο σκοπό, αλλά, καθώς το σήμα διαδίδεται, αυτός ο αμυντικός μηχανισμός απαιτεί μεγαλύτερη ποσότητα ενέργειας. Λόγω του χαμηλού κόστους των WSN και των περιορισμένων ενεργειακών πόρων και οι δύο αμυντικοί μηχανισμοί δεν μπορούν να εφαρμοστούν. (C. M. Medaglia, A. Serbanati, 2010)

Tampering

Όπως το μπλοκάρισμα, ο μετριασμός είναι μια επίθεση που συμβαίνει στο φυσικό στρώμα. Λόγω του χαμηλού κόστους των WSN, δεν υπάρχει γνωστό αποτελεσματικό αντίμετρο που θα μπορούσε να εφαρμοστεί στο σχεδιασμό των τρέχοντων WSN. Προκειμένου να προστατευθούν τα WSN από επιθέσεις στο φυσικό στρώμα, όλα τα συστήματα ασφαλείας πρέπει να εξετάσουν αυτήν την αδυναμία. (C. M. Medaglia, A. Serbanati, 2010)

Resource exhaustion

Υπάρχουν δύο αντίμετρα που χρησιμοποιούνται για την αποφυγή εξάντλησης πόρων. Το πρώτο αντίμετρο αποτρέπει την εξάντληση ενέργειας επιτρέποντας στο WSN να αγνοήσει αιτήματα που βρίσκονται εκτός των ορίων ρυθμού στο επίπεδο MAC. Η δεύτερη λύση εισάγει ένα χρονικό διάστημα στο οποίο επιτρέπεται η μετάδοση

σημάτων και εμποδίζει το WSN να συνεχίζει να μεταδίδει συνεχώς τα κατεστραμμένα δεδομένα. Αυτή η λύση αναφέρεται συχνά ως πολυπλεξία διαίρεσης χρόνου. (C. M. Medaglia, A. Serbanati, 2010)

Unfairness

Προς το παρόν δεν υπάρχει καμία λύση που να μπορεί να αποτρέψει εντελώς τους WSN από επιθέσεις αθέμιτου χαρακτήρα. Η χρήση μικρότερων χρονικών πλαισίων για μεταδόσεις μπορεί να μειώσει τον αντίκτυπο των επιθέσεων αδικίας στο WSN, ωστόσο η ίδια η επίθεση δεν μπορεί να αποφευχθεί καθώς οι εισβολείς μπορούν να αναμεταδώσουν πολύ γρήγορα το κακόβουλο υλικό. (C. M. Medaglia, A. Serbanati, 2010)

Spoofing, Altering and Replaying

Μια αποτελεσματική λύση για να αποτρέψετε τα WSN από πλαστογράφηση, τροποποίηση και αναπαραγωγή πληροφοριών είναι να προσθέσετε έναν κωδικό ελέγχου ταυτότητας μηνύματος και μια χρονική σήμανση στο μήνυμα. Αυτό επιτρέπει την επαλήθευση των ληφθέντων δεδομένων και επιπλέον αποφεύγει την αναπαραγωγή των πληροφοριών. (C. M. Medaglia, A. Serbanati, 2010)

Selective forwarding and sinkhole attacks

Η επιλεκτική επίθεση και οι επιθέσεις καταβόθρας από εξωτερικό εισβολέα μπορούν να αποφευχθούν πλήρως εφαρμόζοντας κρυπτογράφηση κοινόχρηστου κλειδιού. Αυτό το αντίμετρο διασφαίζει ότι ο αντίπαλος δεν μπορεί πλέον να συμμετάσχει στο WSN. Ωστόσο, το αντίμετρο δεν είναι αποτελεσματικό για τους εσωτερικούς εισβολείς. (C. M. Medaglia, A. Serbanati, 2010)

The Sybil attack

Καθώς οι επιθέσεις που προέρχονται από το WSN δεν μπορούν να αποφευχθούν, είναι σημαντικό να επαληθεύσετε τις ταυτότητες των κόμβων για να εντοπίσετε πιθανές

μεταμφιέσεις. Λόγω των περιορισμών των WSN, οι παραδοσιακές προσεγγίσεις, όπως η κρυπτογράφηση δημόσιου κλειδιού, δεν είναι εφικτές. Μια πιθανή λύση για να ξεπεραστεί το πρόβλημα των επιθέσεων Sybil σε WSNs είναι η εφαρμογή μοναδικών, μετρικών κλειδιών που μοιράζονται μεταξύ των κόμβων και του σταθμού βάσης. Αυτά τα κλειδιά επιτρέπουν στους γειτονικούς κόμβους να επαληθεύσουν την ταυτότητά τους και να δημιουργήσουν ένα κοινόχρηστο κλειδί που περιορίζει την επικοινωνία του στους γειτονικούς κόμβους που έχουν επικυρωθεί. Είναι σημαντικό να σημειωθεί ότι ο αριθμός των πλήκτρων ανά κόμβο πρέπει να περιορίζεται από το σταθμό βάσης για να αποτρέψει τους αντιπάλους να δημιουργήσουν ένα κοινό κλειδί με κάθε κόμβο. Σε περίπτωση που ένας κόμβος υπερβαίνει τον δεδομένο αριθμό κοινόχρηστων κλειδιών με γειτονικούς κόμβους, θα σταλεί ένα μήνυμα σφάλματος για την ανακοίνωση του προβλήματος. (C. M. Medaglia, A. Serbanati, 2010)

Wormholes

Τα περισσότερα υπάρχοντα πρωτόκολλα δεν προστατεύουν από επιθέσεις τύπου wormhole, γεγονός που καθιστά πολύ δύσκολη την προστασία των WSN από αυτήν τη μορφή επίθεσης, ειδικά όταν χρησιμοποιούνται σε συνδυασμό με άλλες επιθέσεις. Ο μόνος τύπος πρωτοκόλλου που είναι ανθεκτικός στις σκουληκότρυπες είναι το πρωτόκολλο γεωγραφικής δρομολόγησης. Σε αυτόν τον τύπο πρωτοκόλλου η τοπολογία του WSN δεν κατασκευάζεται από το σταθμό βάσης αλλά από την κυκλοφορία που φτάνει στη φυσική θέση του σταθμού βάσης. Οι τοπολογίες που κατασκευάζονται με αυτόν τον τρόπο λαμβάνουν υπόψη τη φυσική απόσταση μεταξύ γειτονικών κόμβων και μπορεί να αποκαλυφθούν κόμβοι που βρίσκονται πέρα από το εύρος ραδιοφώνου. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

HELLO flood attack

Ένα πιθανό αντίμετρο για τις επιθέσεις πλημμύρας HELLO είναι ένα πρωτόκολλο ελέγχου ταυτότητας μεταξύ γειτονικών κόμβων που επαληθεύει τις ταυτότητες των κόμβων χρησιμοποιώντας το σταθμό βάσης. Προτού ένας αντίπαλος μπορεί να

χρησιμοποιήσει μια επίθεση πλημμύρας HELLO, πρέπει να καθοριστεί ένας έλεγχος ταυτότητας με όλους τους γειτονικούς κόμβους. Εάν ο αριθμός των γειτονικών κόμβων είναι πάνω από ένα ορισμένο όριο, ο σταθμός βάσης ενδέχεται να εντοπίσει τον εισβολέα. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

De-synchronisation

Οι επιθέσεις αποσυγχρονισμού μπορούν να αποφευχθούν με τον έλεγχο ταυτότητας των πακέτων που αποστέλλονται μεταξύ των δύο κεντρικών υπολογιστών, εμποδίζοντας τον εισβολέα να στείλει πλαστά πακέτα. (F.T. Sheldon, V. Vishik 2010)

ΣΥΜΠΕΡΑΣΜΑΤΑ ΓΙΑ ΕΠΙΘΕΣΕΙΣ ΚΑΙ ΑΝΤΙΜΕΤΡΑ

Οι προαναφερθείσες επιθέσεις σε ασύρματα δίκτυα αισθητήρων έχουν δείξει ότι η κρυπτογράφηση στο επίπεδο σύνδεσης, η επαλήθευση ταυτότητας και ο έλεγχος ταυτότητας είναι αποτελεσματικά αντίμετρα έναντι εξωτερικών εισβολέων. Εάν εφαρμοστεί σωστά, τα WSN μπορούν να προστατευτούν από επιθέσεις Sybil, επιθέσεις HELLO, επιλεκτική προώθηση, πλαστογράφηση και αποσυγχρονισμό. Επιθέσεις που εκτελούνται από ισχυρούς αντιπάλους από το εσωτερικό του WSN, ωστόσο αποτελούν σημαντική απειλή για το δίκτυο, καθώς υπάρχει Δεν είναι γνωστό κανένα αποτελεσματικό αντίμετρο που θα μπορούσε να προστατεύσει από αυτές τις επιθέσεις. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Οι πιο δύσκολες επιθέσεις που προκαλούνται από το εσωτερικό του δικτύου είναι η επίθεση με καταβόθρες. Για την προστασία των WSN από τους εσωτερικούς εισβολείς, πρέπει να εξεταστούν περαιτέρω αντίμετρα στην κρυπτογραφία. Τα πρωτόκολλα ασφαλούς δρομολόγησης πρέπει να προσαρμοστούν στις ανάγκες και τους περιορισμούς των WSN. Επί του παρόντος, μόνο το πρωτόκολλο γεωγραφικής δρομολόγησης μπορεί να προστατεύσει το δίκτυο αισθητήρων από εσωτερικές επιθέσεις, όπως η επίθεση σκουληκότρυπας. Σύμφωνα με τον Karlof και τον Wagner να

σχεδιάσουν ένα πρωτόκολλο δρομολόγησης, το οποίο μπορεί να ξεπεράσει τα τρέχοντα ζητήματα ασφαλείας, παραμένει ένα ανοιχτό πρόβλημα που πρέπει να λυθεί για να χρησιμοποιηθούν περίεργα τα WSN για πολλές εφαρμογές. (F.T. Sheldon, V. Vishik 2010)

Αξιολογώντας τους κινδύνους ασφαλείας των συστημάτων RFID, μπορούμε να πούμε ότι, όσο χαμηλότερες είναι οι τιμές, τόσο υψηλότερα είναι τα θέματα ασφαλείας. Οι βασικές ετικέτες RFID χαμηλού κόστους δεν μπορούν να εμποδίσουν τους εισβολείς να εξάγουν τις πληροφορίες μιας ετικέτας, αποκαλύπτοντας τα δεδομένα της στον αντίπαλο ενώ η ετικέτα θεωρείται ενεργή. Σε περίπτωση που ένας εισβολέας μπορεί να αποκτήσει φυσική πρόσβαση σε μια ετικέτα, δεν υπάρχει αντίμετρο ασφαλείας που να εμποδίζει τον εισβολέα να κλωνοποιήσει την ετικέτα, καθώς όλα τα απαραίτητα για την επιτυχία στοιχεία αποκαλύπτονται από την ετικέτα. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Παρόλο που το προτεινόμενο ελαφρύ πρωτόκολλο ελέγχου ταυτότητας μπορεί να ανιχνεύσει κλώνους, σαρώνοντάς τους, προς το παρόν δεν υπάρχει διαθέσιμο πρωτόκολλο που θα μπορούσε να προστατεύσει τα συστήματα RFID, με βασικές ετικέτες χαμηλού κόστους, από την αποκάλυψη των δεδομένων του. Ένα αποτελεσματικό αντίμετρο για να ξεπεραστεί αυτό το ελάττωμα ασφαλείας είναι η εξόντωση ετικετών. Μόλις καταστραφεί μια ετικέτα, δεν μπορεί πλέον να αποκαλύψει τις πληροφορίες της, καθώς οι εισβολείς δεν μπορούν να παρακολουθήσουν το στοιχείο στο οποίο είναι συνδεδεμένη η ετικέτα. Αυτό διασφαλίζει ότι οι, συχνά ευαίσθητες πληροφορίες του αντικειμένου, όπως η περιγραφή του προϊόντος ή η τιμή, δεν πέφτουν σε λάθος χέρια, καθώς αυτές οι πληροφορίες πρέπει να παραμείνουν ιδιωτικές για να διασφαλίσουν την ασφάλεια του κατόχου. (F.T. Sheldon, V. Vishik 2010)

Ωστόσο, μπορεί να μην είναι πάντα δυνατό να απορρίψετε τις ετικέτες ενός συστήματος όταν το αντικείμενο βρίσκεται στα χέρια ενός ατόμου. Για συστήματα, που απαιτούν μια ετικέτα για να παραμείνει ζωντανή για όλη τη διάρκεια ζωής ενός αντικειμένου ή προϊόντος, το οποίο μπορεί να χρησιμοποιηθεί σε αλυσίδες ενοικίασης,

συμπεριλαμβανομένων ενοικίασης αυτοκινήτων ή βιβλιοθηκών, προς το παρόν δεν υπάρχει γνωστό αποτελεσματικό αντίμετρο. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Τα συστήματα RFID που χρησιμοποιούν ετικέτες συμμετρικού κλειδιού έχουν περισσότερες διαθέσιμες επιλογές ασφάλειας λόγω της υποστηριζόμενης κρυπτογραφίας. Παρά τις ευπάθειες που εντοπίστηκαν στα τρέχοντα αντίμετρα, το πρωτόκολλο των Lee, Asano και Kim παρέχει βελτιωμένη ασφάλεια, η οποία μπορεί να ξεπεράσει τα ελαττώματα ασφαλείας που είναι γνωστά σε άλλα πρωτόκολλα. Συνοψίζοντας, μπορεί να ειπωθεί ότι τα συστήματα RFID που χρησιμοποιούν ετικέτες συμμετρικού κλειδιού μπορούν να θεωρηθούν ασφαλή, ενώ τα βασικά αντίστοιχά τους δεν έχουν σχεδόν καθόλου ασφάλεια απέναντι σε πιθανές επιθέσεις. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Η τεχνολογία της επικοινωνίας κοντινού πεδίου είναι ευάλωτη σε όλες τις επιθέσεις που αντιμετωπίζουν οι περισσότερες ασύρματες τεχνολογίες, που κυμαίνονται από την υποκλοπή των παρεμβολών δεδομένων έως τις επιθέσεις άρνησης υπηρεσίας. Παρά αυτά τα ζητήματα ασφάλειας, με την εισαγωγή του ασφαλούς καναλιού, το NFC παρέχει ένα αποτελεσματικό αντίμετρο που μπορεί να διασφαλίσει την ασφαλή μετάδοση δεδομένων. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Παρ 'όλα αυτά, υπάρχει ο κίνδυνος επίθεσης άρνησης εξυπηρέτησης για τον οποίο επί του παρόντος δεν υπάρχει γνωστό αποτελεσματικό αντίμετρο, που θα εξασφάλιζε τη διάθεση της συσκευής ή του συστήματος. Παρά την επίθεση DoS, το NFC παρέχει τις απαραίτητες εφαρμογές ασφαλείας για να θεωρήσει αυτήν την τεχνολογία μια σταθερή και ασφαλή βάση για το IoT. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Όπως τα συστήματα RFID, τα WSN αντιμετωπίζουν το πρόβλημα της ανταγωνιστικότητας που τους αναγκάζει να λειτουργούν με κόμβους χαμηλού κόστους που περιορίζουν τον ενεργειακό τους πόρο. Τα WSN δεν μπορούν να προστατεύσουν από επιθέσεις στο φυσικό στρώμα, όπως μπλοκαρίσματα ή παραβίαση, λόγω των

σπάνιων πηγών τους. Παρ 'όλα αυτά, όχι μόνο οι περιορισμοί υλικού διαδραματίζουν ρόλο σε αυτό το ελάττωμα ασφαλείας, αλλά και οι περιβαλλοντικοί περιορισμοί, όπως ο θόρυβος, καθιστούν πιο πιθανό να εμφανιστούν επιθέσεις στο φυσικό στρώμα. (F.T. Sheldon, V. Vishik 2010)

Όχι μόνο το φυσικό στρώμα αντιμετωπίζει προσβολές για το οποίο δεν είναι γνωστό το τρέχον αντίμετρο, αλλά και το στρώμα ζεύξης μπορεί να θεωρηθεί αδύναμο μέρος. Τα αποτελέσματα μιας επίθεσης τύπου unfairness, που λειτουργεί ως επίθεση DoS, προκειμένου να καταστεί το δίκτυο μη διαθέσιμο, μπορούν να μειωθούν αν και δεν εμποδίζεται.

Αν και η αποτελεσματική κρυπτογραφία μπορεί να προστατεύσει το WSN από εξωτερικές επιθέσεις, κανένα αντίμετρο δεν μπορεί να προστατεύσει το δίκτυο όταν η επίθεση προέρχεται από το εσωτερικό. Αυτές οι επιθέσεις αποτελούν σημαντική απειλή για την ασφάλεια ολόκληρου του δικτύου. (F.T. Sheldon, V. Vishik 2010)

Λαμβάνοντας υπόψη το IoT από σήμερα, μπορεί να συναχθεί το συμπέρασμα ότι τα αντίμετρα για την αποτροπή επιθέσεων του IoT, που οδηγούν σε ζητήματα ασφαλείας που επηρεάζουν τους χρήστες του, γίνονται πιο αποτελεσματικά. Ο έλεγχος ταυτότητας και η κρυπτογραφία μπορούν να προστατεύσουν τα βασικά στοιχεία του IoT RFID και του NFC από σοβαρές επιθέσεις, ωστόσο, δεν ισχύουν για τα WSN. (C. M. Medaglia, A. Serbanati, 2010)

Συμπερασματικά μπορούμε να πούμε ότι, αρκεί να μην υπάρχουν αποτελεσματικοί μηχανισμοί ασφαλείας που να μπορούν να προστατεύσουν τα WSN από σοβαρές επιθέσεις, το IoT από σήμερα δεν μπορεί να θεωρηθεί 100% ασφαλές.

ΚΕΦΑΛΑΙΟ 5: CYBER SECURITY

Η ασφάλεια στον κυβερνοχώρο αφορά την κατανόηση των ζητημάτων των διαφορετικών κυβερνοεπιθέσεων και την επινόηση αμυντικών στρατηγικών (δηλαδή αντιμέτρων) που διατηρούν το απόρρητο, την ακεραιότητα και τη διαθεσιμότητα οποιωνδήποτε ψηφιακών και τεχνολογιών πληροφοριών.

• Εμπιστευτικότητα είναι ο όρος που χρησιμοποιείται για την αποτροπή της αποκάλυψης πληροφοριών σε μη εξουσιοδοτημένα άτομα ή συστήματα.

• Ακεραιότητα είναι ο όρος που χρησιμοποιείται για την αποτροπή οποιασδήποτε τροποποίησης / διαγραφής με μη εξουσιοδοτημένο τρόπο. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Πολλοί ειδικοί στην κυβερνοασφάλεια πιστεύουν ότι το κακόβουλο λογισμικό είναι η βασική επιλογή όπλου για την πραγματοποίηση κακόβουλων προθέσεων για την παραβίαση της ασφάλειας στον κυβερνοχώρο. Το κακόβουλο λογισμικό αναφέρεται σε μια ευρεία κατηγορία επιθέσεων που φορτώνονται σε ένα σύστημα, συνήθως χωρίς τη γνώση του νόμιμου κατόχου, για να θέσουν σε κίνδυνο το σύστημα προς όφελος ενός αντιπάλου. Ορισμένες υποδειγματικές τάξεις κακόβουλου λογισμικού περιλαμβάνουν ιούς, worms, δούρειους ίππους, spyware και εκτελέσιμα bot. Το κακόβουλο λογισμικό μολύνει τα συστήματα με διάφορους τρόπους όπως για παράδειγμα την διάδοση ίου από μολυσμένα μηχανήματα, εξαπατώντας τον χρήστη να ανοίξει μολυσμένα αρχεία ή δελεάζοντας τους χρήστες να επισκεφθούν ιστότοπους διάδοσης κακόβουλου λογισμικού. Σε πιο συγκεκριμένα παραδείγματα μόλυνσης από κακόβουλο λογισμικό, το κακόβουλο λογισμικό μπορεί να φορτωθεί σε μια μονάδα USB που έχει εισαχθεί σε μια μολυσμένη συσκευή και στη συνέχεια να μολύνει κάθε άλλο σύστημα στο οποίο στη συνέχεια εισάγεται αυτή η συσκευή. (M.Tehranipoor, C. Wang , 2011.)

Το Malware διαδίδεται από συσκευές και εξοπλισμούς που περιέχουν ενσωματωμένα συστήματα και υπολογιστική λογική. Εν ολίγοις, το malware εισάγεται σε οποιοδήποτε σημείο του κύκλου ζωής του συστήματος. Τα θύματα κακόβουλου λογισμικού μπορούν

να κυμαίνονται από συστήματα τελικών χρηστών, διακομιστές, συσκευές δικτύου (δηλ. Δρομολογητές, διακόπτες κ.λπ.) και συστήματα ελέγχου διεργασιών, όπως εποπτικός έλεγχος και απόκτηση δεδομένων (SCADA). Ο πολλαπλασιασμός και η εξειδίκευση του ταχέως αυξανόμενου αριθμού κακόβουλου λογισμικού αποτελεί μείζονα ανησυχία στο Διαδίκτυο σήμερα. Παραδοσιακά, επιθέσεις κακόβουλου λογισμικού σημειώθηκαν σε ένα μόνο σημείο της επιφάνειας μεταξύ εξοπλισμού υλικού, λογισμικού ή επιπέδου εκμετάλλευσης εκμεταλλευόμενων υφιστάμενων τρωτών σημείων σχεδιασμού και υλοποίησης σε κάθε επίπεδο. Αντί να προστατεύει κάθε περιουσιακό στοιχείο, η περιμετρική αμυντική στρατηγική έχει χρησιμοποιηθεί κυρίως για να βάλει ένα τείχος (firewall) έξω από όλους τους εσωτερικούς πόρους για να προστατεύσει τα πάντα μέσα από οποιαδήποτε ανεπιθύμητη εισβολή από έξω. (F.T. Sheldon, V. Vishik 2010)

Η πλειονότητα του περιμετρικού αμυντικού μηχανισμού χρησιμοποιεί λογισμικό τείχους προστασίας και έχει εγκατεστημένη εφαρμογή για ιούς σε συστήματα πρόληψης ή και ανίχνευσης εισβολής. Κάθε κίνηση που προέρχεται από έξω παρακολουθείται και εξετάζεται για να διασφαλιστεί ότι δεν υπάρχει κακόβουλο λογισμικό που διεισδύει στους εσωτερικούς πόρους. Η γενική αποδοχή αυτού του περιμετρικού μοντέλου υπεράσπισης έχει συμβεί επειδή είναι πολύ πιο εύκολο και φαινομενικά λιγότερο δαπανηρό να ασφαλιστεί μία περίμετρος από ότι είναι να εξασφαλιστεί ένας μεγάλος όγκος εφαρμογών ή μεγάλος αριθμός εσωτερικών δικτύων. Για να δοθεί πιο συγκεκριμένη πρόσβαση σε ορισμένες εσωτερικές πηγές, οι μηχανισμοί ελέγχου πρόσβασης έχουν χρησιμοποιηθεί σε συνδυασμό με τον περιμετρικό αμυντικό μηχανισμό. (F.T. Sheldon, V. Vishik 2010)

Εκτός από τον έλεγχο υπεράσπισης και τον έλεγχο πρόσβασης, προστίθεται και επιπλέον προστασία για τον εντοπισμό ή την τιμωρία για τυχόν κακή συμπεριφορά. Ωστόσο, οι συνδυασμένες προσπάθειες της στρατηγικής περιμετρικής άμυνας έχουν αποδειχθεί ολοένα και πιο αναποτελεσματικές καθώς βελτιώνεται η εξέλιξη και η πολυπλοκότητα του κακόβουλου λογισμικού. Το κακόβουλο λογισμικό που εξελίσσεται πάντα φαίνεται να βρίσκει κενά για να παρακάμψει εντελώς την άμυνα της περιμέτρου. (F.T. Sheldon, V. Vishik 2010)

Αρχικά περιγράφονται λεπτομερώς οι πιο κοινές επιθέσεις στα τρία διαφορετικά επίπεδα του υπάρχοντος συστήματος πληροφοριών που χωρίζονται σε επίπεδα υλικού, λογισμικού και δικτύου. Στη συνέχεια συζητάμε τα πλεονεκτήματα και τα μειονεκτήματα των πιο αντιπροσωπευτικών μηχανισμών άμυνας που έχουν χρησιμοποιηθεί σε αυτά τα επίπεδα. Το κακόβουλο λογισμικό εξελίσσεται με το χρόνο αξιοποιώντας νέες προσεγγίσεις και εκμεταλλευόμενο τα ελαττώματα στην αναδυόμενη τεχνολογία για να αποφύγει τον εντοπισμό. (C. M. Medaglia, A. Serbanati, 2010)

Εν συνεχεία περιγράφουμε μια σειρά από νέα μοτίβα επιθέσεων κακόβουλου λογισμικού που υπάρχουν στις αναδυόμενες τεχνολογίες. Αναγνωρίζοντας τις αναδυόμενες τεχνολογίες, εστιάζουμε σε μερικές από αυτές που έχουν αλλάξει τον τρόπο με τον οποίο ζούμε την καθημερινή μας ζωή. Αυτές περιλαμβάνουν τα κοινωνικά μέσα, το υπολογιστικό νέφος, και φυσικά η τεχνολογία smartphone που αποτελεί υποδομή ζωτικής σημασίας. Συζητάμε για τα μοναδικά χαρακτηριστικά της καθεμιάς από αυτές τις αναδυόμενες τεχνολογίες και πώς το κακόβουλο λογισμικό μπορεί και χρησιμοποιεί τα μοναδικά χαρακτηριστικά τους για να πολλαπλασιαστεί. (F.T. Sheldon, V. Vishik 2010)

Για παράδειγμα, τα μέσα κοινωνικής δικτύωσης, όπως οι ιστότοποι κοινωνικής δικτύωσης και ιστολόγια, αποτελούν πλέον αναπόσπαστο μέρος του τρόπου ζωής μας, καθώς πολλοί άνθρωποι κάνουν δημοσιεύσεις που αφορούν τα γεγονότα της ζωής τους, μοιράζονται νέα, καθώς και κάνουν διαδικτυακούς φίλους. Αντιμετωπίζοντας τη δυνατότητά τους να συνδέουν εκατομμύρια ανθρώπους με μία κίνηση, οι εισβολείς χρησιμοποιούν λογαριασμούς κοινωνικών μέσων για να κάνουν φίλους ανυποψίαστους χρήστες και να τους χρησιμοποιήσουν ως οχήματα για την αποστολή ανεπιθύμητων μηνυμάτων στους φίλους του θύματος, ενώ το μηχάνημα του θύματος επανατοποθετείται σε ένα μέρος του botnet. (F.T. Sheldon, V. Vishik 2010)

Το πρότυπο υπολογιστικού νέφους επιτρέπει την χρήση πόρων υπολογιστών, όπως βοηθητικά προγράμματα, όπου οι χρήστες πληρώνουν μόνο για τη χρήση χωρίς να χρειάζεται να δημιουργήσουν εκ των προτέρων κόστος ή να απαιτούν οποιεσδήποτε

δεξιότητες στη διαχείριση σύνθετων υπολογιστικών υποδομών. Η αυξανόμενη συλλογή δεδομένων που συγκεντρώνεται στις υπηρεσίες αποθήκευσης cloud προσελκύει τους χρήστες κακόβουλων λογισμικών. Τον Ιούνιο του 2012, οι χρήστες κακόβουλων λογισμικών έθεσαν σε κίνδυνο την υπηρεσία μετριασμού της Κατανεμημένης άρνησης υπηρεσίας (DDoS) στο CloudFlare χρησιμοποιώντας ελαττώματα στην υπηρεσία αυτόματου τηλεφωνητή της AT&T για τους χρήστες κινητών τους. Παρομοίως, η υπηρεσία ανάκτησης λογαριασμού της Google για τους χρήστες του Gmail. Με την αύξηση κατά 2 δισεκατομμύρια χρήστών smartphone έως το 2015, η σημαντική αύξηση του κακόβουλου λογισμικού για κινητά αποτέλεσε μεγάλο πρόβλημα τα τελευταία χρόνια. Για παράδειγμα, ο αριθμός των μοναδικών ανιχνεύσεων λογισμικού για Android αυξήθηκε παγκοσμίως κατά 16 φορές το 2013 από το προηγούμενο έτος. Υπάρχουν επίσης αυξανόμενες ανησυχίες για απειλές στον κυβερνοχώρο για τις κρίσιμες υποδομές, όπως είναι τα δίκτυα ηλεκτρικής ενέργειας και συστήματα υγειονομικής περίθαλψης που δύναται να χρησιμοποιηθούν στην τρομοκρατία, το σαμποτάζ και τον πόλεμο πληροφοριών. Εκτός από τη διερεύνηση εκμετάλλευσης μέσω των μοναδικών χαρακτηριστικών στις επιλεγμένες αναδυόμενες τεχνολογίες, συζητάμε επίσης γενικά μοτίβα επίθεσης κακόβουλου λογισμικού που εμφανίζονται σε αυτά για να κατανοήσουμε τις μεθόδους και τις τάσεις των επαναληπτικών επιθέσεων. (F.T. Sheldon, V. Vishik 2010)

Τέλος, αναφέρονται παρατηρήσεις ως προς το πού κατευθύνονται οι μελλοντικές ερευνητικές κατευθύνσεις. Αυτές περιλαμβάνουν: (1) ανησυχίες για την προστασία της ιδιωτικής ζωής για την αύξηση του όγκου των προσωπικών πληροφοριών που εισάγονται στο Διαδίκτυο, (2) απαίτηση να υπάρχει νέα γενιά ασφαλούς Διαδικτύου από το μηδέν με προσεκτική εξέταση των υποκειμένων προτύπων ανάπτυξης και χρήσης που δεν συνέβαιναν με το Διαδίκτυο που χρησιμοποιούμε σήμερα, (3) αξιόπιστο σύστημα του οποίου η θεμελιώδης αρχιτεκτονική είναι διαφορετική από την αρχή του για να αντέχει από το συνεχώς εξελισσόμενο κακόβουλο λογισμικό, (4) να είναι σε θέση να εντοπίζει την πηγή επιθέσεων με την ανάπτυξη παγκόσμιου συστήματος διαχείρισης ταυτότητας κλίμακας και τεχνικών ανίχνευσης , και τέλος (5) μεγάλη έμφαση στην χρησιμοποιήσιμη

ασφάλεια για να δοθούν στα άτομα έλεγχοι ασφαλείας που μπορούν να κατανοήσουν και να ελέγξουν. (C. M. Medaglia, A. Serbanati, 2010)

ΚΕΦΑΛΑΙΟ 6: ΤΟ ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ ΩΣ ΕΡΓΑΛΕΙΟ ΕΠΙΘΕΣΗΣ

Τον πρώτο καιρό δημιουργίας του, το κακόβουλο λογισμικό δημιουργήθηκε απλώς ως πείραμα συχνά για να επισημάνει τις ευπάθειες ασφαλείας ή, σε ορισμένες περιπτώσεις, να εξουδετερώσει τις τεχνικές ικανότητες. Σήμερα, το κακόβουλο λογισμικό χρησιμοποιείται κυρίως για την κλοπή ευαίσθητων προσωπικών, οικονομικών ή επιχειρηματικών πληροφοριών προς όφελος άλλων. Για παράδειγμα, το κακόβουλο λογισμικό χρησιμοποιείται συχνά για τη στόχευση κυβερνητικών ή εταιρικών ιστότοπων για τη συλλογή πληροφοριών που προστατεύονται ή για τη διακοπή της λειτουργίας τους. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Σε άλλες περιπτώσεις, το κακόβουλο λογισμικό χρησιμοποιείται επίσης κατά ατόμων για να αποκτήσουν προσωπικές πληροφορίες, όπως αριθμούς κοινωνικής ασφάλισης ή αριθμούς πιστωτικών καρτών. Από την άνοδο της ευρυζωνικής πρόσβασης στο Διαδίκτυο που είναι φθηνότερη και γρηγορότερη, το κακόβουλο λογισμικό έχει σχεδιαστεί όλο και περισσότερο όχι μόνο για την ανάκτηση των πληροφοριών αλλά αυστηρά για σκοπούς κέρδους. Για παράδειγμα, η πλειονότητα των διαδεδομένων κακόβουλων προγραμμάτων έχουν σχεδιαστεί για να ελέγχει τους υπολογιστές των χρηστών για εκμετάλλευση της μαύρης αγοράς, όπως η αποστολή ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου ή η παρακολούθηση των συμπεριφορών περιήγησης στον ιστό του χρήστη και η εμφάνιση ανεπιθύμητων διαφημίσεων. (C. M. Medaglia, A. Serbanati, 2010)

Με βάση την έκθεση της ομάδας Anti-Phishing, το 2013 αναφέρθηκαν συνολικά 27 εκατομμύρια νέα λογισμικά. Η έκθεση περιγράφει σχετικές αναλογίες των νέων τύπων δειγμάτων κακόβουλου λογισμικού που εντοπίστηκαν κατά το δεύτερο εξάμηνο του

2013 που αναφέρθηκαν από την ομάδα Anti-Phishing. Σύμφωνα με αυτήν την αναφορά, οι χρήστες κακόβουλων λογισμικών συνέχισαν να λογοδοτούν για τις περισσότερες από τις απειλές όσον αφορά την καταμέτρηση κακόβουλου λογισμικού καθώς ο αριθμός αυξάνεται θεαματικά. Το 2010, οι Trojans αναφέρθηκαν ότι αποτελούσαν το 60% όλων των κακόβουλων προγραμμάτων. Το 2011, το ποσοστό έχει ανέβει στο 73%. Το τρέχον ποσοστό δείχνει ότι σχεδόν τρεις στους τέσσερις νέους malware που δημιουργήθηκαν ήταν Trojans και επίσης δείχνει ότι αποτελούν το κύριο όπλο της επιλογής για εγκληματίες στον κυβερνοχώρο προκειμένου να πραγματοποιούν εισβολές σε ένα δικτύο και κλοπές δεδομένων.

Ανεπιθύμητο περιεχόμενο: Το ανεπιθύμητο περιεχόμενο αναφέρεται στην αποστολή άσχετων, ακατάλληλων και ανεπιθύμητων μηνυμάτων σε χιλιάδες ή εκατομμύρια παραλήπτες. Το Spam αποδείχθηκε μια εξαιρετικά κερδοφόρα αγορά, καθώς το spam αποστέλλεται ανώνυμα χωρίς να απαιτείται ιδιαίτερο κόστος πέρα από τη διαχείριση των λιστών αλληλογραφίας. Λόγω του τόσο χαμηλού εμποδίου εισόδου, οι spammers είναι πολυάριθμοι και ο όγκος των ανεπιθύμητων emails έχει αυξηθεί πάρα πολύ. Το έτος 2022, το εκτιμώμενο ποσοστό για τα μηνύματα spam είναι περίπου επτά τρισεκατομμύρια. Αυτό το σχήμα περιλαμβάνει το κόστος που συνεπάγεται η απώλεια παραγωγικότητας και απάτης και επιπλέον χωρητικότητα που απαιτείται για την αντιμετώπιση του ανεπιθύμητου περιεχομένου. Σήμερα, η πιο ευρέως αναγνωρισμένη μορφή spam είναι email spam. Σύμφωνα με την έκθεση της ομάδας εργασίας για την κατάχρηση μηνυμάτων, μεταξύ 88–92% των μηνυμάτων email που στάλθηκαν το πρώτο εξάμηνο του 2016 έφεραν ανεπιθύμητα μηνύματα. (F.T. Sheldon, V. Vishik 2010)

Ηλεκτρονικό ψάρεμα: Το ηλεκτρονικό ψάρεμα (phishing) είναι ένας τρόπος απόπειρας απόκτησης ευαίσθητων πληροφοριών, όπως το όνομα χρήστη, ο κωδικός πρόσβασης ή τα στοιχεία πιστωτικής κάρτας, ζητώντας τα με μια απλή ερώτηση ως αξιόπιστος φορέας. Οι περισσότερες απάτες ηλεκτρονικού ψαρέματος βασίζονται στο να εξαπατήσουν έναν χρήστη να επισκεφτεί έναν κακόβουλο ιστότοπο που ισχυρίζεται ότι προέρχεται από νόμιμες επιχειρήσεις και εταιρείες. Ο ανυποψίαστος χρήστης εισάγει ιδιωτικές πληροφορίες στον ιστότοπο του κακόβουλου ιστότοπου, ο οποίος στη συνέχεια

χρησιμοποιείται από κακόβουλους εγκληματίες. Οι περισσότερες μέθοδοι ηλεκτρονικού ψαρέματος χρησιμοποιούν κάποια μορφή τεχνικής απάτης που έχει σχεδιαστεί για τη δημιουργία συνδέσμου σε ένα ηλεκτρονικό ταχυδρομείο (και πλαστογραφημένο ιστότοπο) που φαίνεται να ανήκουν σε έναν νόμιμο οργανισμό, όπως είναι μια γνωστή τράπεζα. Οι ορθογραφικές διευθύνσεις URL ή η χρήση υποτομέων είναι συνηθισμένα κόλπα που χρησιμοποιούνται από τους phishers. Η έκθεση της Anti-Phishingtechnical ανέφερε ότι, υπήρχε μια ορατή τάση των phishers το 2013 να κρύβουν τις προθέσεις τους, αποφεύγοντας τη χρήση προφανών κεντρικών υπολογιστών IP για να φιλοξενήσουν τις πλαστές σελίδες σύνδεσης. Αντ 'αυτού, οι phishers προτιμούσαν να φιλοξενούν έναν παραβιασμένο τομέα για να αποφύγουν τον εντοπισμό. Αναφέρεται ότι σημειώθηκε πτώση 16% στον αριθμό των διευθύνσεων URL ηλεκτρονικού ψαρέματος που περιείχαν το όνομα της πλαστογραφημένης εταιρείας στη διεύθυνση URL. Αυτές οι συνδυασμένες τάσεις δείχνουν πώς οι phishers προσαρμόζονται καθώς οι χρήστες γίνονται ολο και πιο ενημερωμένοι και γνωρίζουν περισσότερα σχετικά με τα χαρακτηριστικά ενός τυπικού phishing. (M.Tehranipoor, C. Wang , 2011.)

Drive-by Downloads: Τα Drive-by Downloads αντιμετωπίζουν τις ακούσιες λήψεις κακόβουλου λογισμικού από το Διαδίκτυο και χρησιμοποιούνται ολοένα και περισσότερο από τους εισβολείς για γρήγορη διάδοση κακόβουλου λογισμικού. Λήψεις Drive-by συμβαίνουν σε διάφορες καταστάσεις. Για παράδειγμα, όταν ένας χρήστης επισκέπτεται έναν ιστότοπο, ενώ βλέπει ένα μήνυμα email από τον χρήστη ή όταν οι χρήστες κάνουν κλικ σε ένα παραπλανητικό αναδυόμενο παράθυρο. Ωστόσο, οι πιο δημοφιλείς λήψεις με κίνηση πραγματοποιούνται κατά πολύ όταν επισκέπτεστε ιστότοπους. Ένας αυξανόμενος αριθμός ιστοσελίδων έχει μολυνθεί με διάφορους τύπους κακόβουλου λογισμικού. Σύμφωνα με την έρευνα της Osterman Research, 11 εκατομμύρια παραλλαγές κακόβουλου λογισμικού ανακαλύφθηκαν έως το 2010 και το 90% αυτών των κακόβουλων προγραμμάτων προέρχεται από κρυφές λήψεις από δημοφιλείς και συχνά αξιόπιστους ιστότοπους. Πριν πραγματοποιηθεί μια λήψη, απαιτείται πρώτα ένας χρήστης να επισκεφθεί τον κακόβουλο ιστότοπο. Για να παρασύρουν τον χρήστη να επισκεφτεί έναν ιστότοπο με κακόβουλο περιεχόμενο, οι

εισβολείς θα στείλουν ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου που περιέχουν συνδέσμους προς τον ιστότοπο. Όταν ο ανυποψίαστος επισκέπτης επισκέπτεται τον κακόβουλο ιστότοπο, γίνεται λήψη και εγκατάσταση κακόβουλου λογισμικού στο μηχάνημα του θύματος χωρίς τη γνώση του χρήστη. Για παράδειγμα, το περίφημο σκουλήκι Storm χρησιμοποιεί το δικό του δίκτυο από πολλαπλούς μολυσμένους υπολογιστές και αποστέλλει μηνύματα spam που περιέχουν συνδέσμους σε τέτοιες σελίδες επίθεσης. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

ΚΕΦΑΛΑΙΟ 7: ΕΚΜΕΤΑΛΛΕΥΣΗ ΥΦΙΣΤΑΜΕΝΩΝ ΤΡΩΤΩΝ ΣΗΜΕΙΩΝ

Όταν το κακόβουλο λογισμικό εγκατασταθεί στο σύστημα του θύματος, οι εγκληματίες του κυβερνοχώρου θα μπορούσαν να χρησιμοποιήσουν πολλές διαφορετικές πτυχές των υφιστάμενων ευπαθειών του συστήματος του θύματος για να τα χρησιμοποιήσουν στις εγκληματικές τους δραστηριότητες. Εξετάζουμε τις πιο ευάλωτες υφιστάμενες ευπάθειες σε υλικό, λογισμικό και συστήματα δικτύου. Ακολουθεί η συζήτηση για τις υπάρχουσες προσπάθειες που έχουν προταθεί για τον περιορισμό των αρνητικών επιπτώσεων από τις εκμεταλλεύσεις. (F.T. Sheldon, V. Vishik 2010)

Hardware: Το Hardware είναι η πιο προνομιακή οντότητα και έχει τη μεγαλύτερη ικανότητα χειρισμού ενός υπολογιστικού συστήματος. Αυτό είναι το επίπεδο όπου έχει τη δυνατότητα να δώσει στους επιτιθέμενους σημαντική ευελιξία και δύναμη για να ξεκινήσουν κακόβουλες επιθέσεις ασφαλείας, εάν το λογισμικό υποβιβάζεται. Συγκρίνεται με επιθέσεις επιπέδου λογισμικού όπου υπάρχουν πολλές ενημερώσεις κώδικα ασφαλείας, εργαλεία ανίχνευσης εισβολών και σαρωτές προστασίας από ιούς για την τακτική ανίχνευση κακόβουλων επιθέσεων, πολλές από τις επιθέσεις που βασίζονται σε υλικό έχουν τη δυνατότητα να ξεφύγουν από αυτήν την ανίχνευση. Εκμεταλλευόμενοι την έλλειψη υποστήριξης εργαλείων στην ανίχνευση υλικού, οι επιθέσεις με βάση το υλικό έχουν αναφερθεί ότι αυξάνονται. Μεταξύ διαφορετικών

τύπων κακής χρήσης υλικού, το υλικό Trojan (trojanware) είναι από τα πιο συνηθισμένα κακόβουλα λογισμικά υλικού. (Fadi Al-Turjman, 2019)

Τα Trojanware είναι κακόβουλα και κρυφά τροποποιήσιμα. Είναι κατασκευασμένα σε ηλεκτρονικές συσκευές, όπως IntegrityCircuits (IC) στο υλικό. Το υλικό Trojan έχει διάφορες διαβαθμίσεις που προκαλούν διαφορετικούς τύπους ανεπιθύμητων αποτελεσμάτων. Ένα υλικό Trojan ενδέχεται να προκαλέσει την αποδοχή εισόδου μιας μονάδας εντοπισμού σφαλμάτων που θα πρέπει να απορριφθούν. Ένας Trojan ενδέχεται να εισάγει περισσότερα buffer στις διασυνδέσεις του chip και ως εκ τούτου καταναλώνει περισσότερη ισχύ, η οποία με τη σειρά της θα μπορούσε να εξαντλήσει γρήγορα την μπαταρία. Σε πιο σοβαρή περίπτωση, οι Trojan Denial-of-Service (DoS) αποτρέπουν τη λειτουργία μιας λειτουργίας ή ενός πόρου. Ένα DoS Trojan ακυρώνει τη μονάδα στόχου για να εξαντλήσει τους περιορισμένους πόρους όπως το εύρος ζώνης (Bandwidth), τον υπολογισμό και την ισχύ της μπαταρίας. Θα μπορούσε επίσης να καταστρέψει, να απενεργοποιήσει ή να αλλάξει τη διαμόρφωση της συσκευής, για παράδειγμα, προκαλώντας στον επεξεργαστή να αγνοήσει τη διακοπή από ένα συγκεκριμένο περιφερειακό μηχάνημα. (Fadi Al-Turjman, 2019)

Οι παράνομοι κλώνοι του υλικού γίνονται πηγή εκμετάλλευσης βάσει υλικού, καθώς οι πιθανότητες να περιέχουν κακόβουλο backdoor αυξάνονται. Η πιθανότητα παραγωγής μη αυθεντικού υλικού έχει αυξηθεί με μια νέα τάση σε εταιρείες πληροφορικής που προσπαθούν να μειώσουν το κόστος πληροφορικής τους μέσω εξωτερικής ανάθεσης και εξαγοράς μη αξιόπιστου υλικού από διαδικτυακούς ιστότοπους. (Fadi Al-Turjman, 2019)

Οι Karri et al. αναφέρουν πώς το σημερινό μοντέλο πληροφορικής της εξωτερικής ανάθεσης έχει συμβάλει στην αυξημένη πιθανότητα παραγωγής παραποιημένων εξαρτημάτων υλικού από μη αξιόπιστα εργοστάσια στις ξένες χώρες. Παρομοίως, αποδεικνύεται επίσης ότι οι εταιρείες πληροφορικής αγοράζουν συχνά μη αξιόπιστο υλικό, όπως chipset και δρομολογητές από διαδικτυακούς ιστότοπους δημοπρασιών ή μεταπωλητές, οι οποίοι με τη σειρά τους ενδέχεται να περιέχουν επιβλαβείς ιούς που

βασίζονται σε υλικό. Αυτές οι πρακτικές δεν είναι μόνο προβληματικές για εταιρείες πληροφορικής που λειτουργούν σε αλλοιωμένο υλικό με πιθανή είσοδο backdoor, αλλά αυξάνει επίσης την πιθανότητα διαρροής του αρχικού σχεδιασμού και των λεπτομερειών εσωτερικών καταστάσεων του συστήματος σε μη εξουσιοδοτημένο προσωπικό. (M.Tehranipoor, C. Wang , 2011.)

Οι επιθέσεις πλευρικών καναλιών συμβαίνουν όταν οι εισβολείς αποκτούν πληροφορίες σχετικά με τις εσωτερικές καταστάσεις ενός συστήματος με την εξέταση φυσικών πληροφοριών της συσκευής, όπως η κατανάλωση ενέργειας, η ηλεκτρομαγνητική ακτινοβολία και οι πληροφορίες χρονισμού των δεδομένων εντός και εκτός της CPU. Τα ευαίσθητα δεδομένα μπορούν να διαρρεύσουν μέσω των αποτελεσμάτων τέτοιων επιθέσεων καναλιού. Έχει αναφερθεί μια προσέγγιση που εξετάζει έναν τρόπο διαρροής του μυστικού κλειδιού κρυπτογραφικού αλγορίθμου ως αποτέλεσμα της ανάλυσης ραδιοσυχνοτήτων. Έχουν προταθεί διάφορες τεχνικές για την αποτροπή επιθέσεων σε επίπεδο υλικού. Οι ανθεκτικές συσκευές στις παραβιάσεις υλικού έχουν γίνει ένα σημαντικό θέμα λόγω της κρίσιμης σημασίας του ως σημείο εισόδου στη συνολική ασφάλεια του συστήματος. Το TrustedPlatform Module (TPM) παρέχει κρυπτογραφικά πρωτόγονα και προστατευμένο χώρο αποθήκευσης μαζί με τη λειτουργικότητα ανταλλαγής αποδεικτικών στοιχείων ανθεκτικών σε απομακρυσμένους διακομιστές. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Ο όρος Trusted Computing Base (TCB) έχει οριστεί για τα μέρη ενός συστήματος, το σύνολο όλων των στοιχείων υλικού και λογισμικού, ώστε να είναι κρίσιμο για τη συνολική ασφάλεια του συστήματος. Το TCB δεν πρέπει να περιέχει σφάλματα ή ευπάθειες που συμβαίνουν στο εσωτερικό, επειδή αυτό ενδέχεται να θέσει σε κίνδυνο την ασφάλεια ολόκληρου του συστήματος. Μια διεξοδική και αυστηρή εξέταση της βάσης του κώδικα πραγματοποιείται μέσω ελέγχου λογισμικού υποβοηθούμενης από έναν υπολογιστή ή επαλήθευσης προγράμματος για τη διασφάλιση της ασφάλειας του TCB. Σε ένα υδατογράφημα υλικού, οι πληροφορίες ιδιοκτησίας ενσωματώνονται και αποκρύπτονται στην περιγραφή ενός κυκλώματος που αποτρέπει το αντικείμενο του κεντρικού υπολογιστή από παράνομη παραποίηση. Το Hardware Obfuscation είναι μια

τεχνική για την τροποποίηση της περιγραφής ή της δομής του ηλεκτρονικού υλικού αποσκοπώντας στην απόκρυψη της σκόπιμης λειτουργίας του. Αυτές οι τεχνικές χρησιμοποιούνται για να αποτρέψουν τους αντιπάλους από την απόκτηση του αρχικού σχεδιασμού ή την παραχάραξη / κλωνοποίηση σημαντικών τμημάτων του υλικού όπως οι μονάδες IC. Μερικά από τα αντίμετρα που πρέπει να εφαρμοστούν απέναντι στις πλευρικές επιθέσεις καναλιού περιλαμβάνουν εισαγωγή θορύβων, έτσι ώστε οι φυσικές πληροφορίες να μην μπορούν να εμφανιστούν άμεσα, φιλτράρισμα ορισμένων τμημάτων φυσικών πληροφοριών και δημιουργία / τύφλωση που επιδιώκει να αφαιρέσει οποιαδήποτε συσχέτιση μεταξύ των δεδομένων εισόδου και των εκπομπών πλευρικών καναλιών. (F.T. Sheldon, V. Vishik 2010)

Ελαττώματα λογισμικού: Το σφάλμα λογισμικού είναι ο κοινός όρος που χρησιμοποιείται για να περιγράψει ένα σφάλμα, ένα ελάττωμα, ένα λάθος σε ένα πρόγραμμα υπολογιστή όπως το εσωτερικό λειτουργικό σύστημα, τα εξωτερικά προγράμματα οδήγησης διασύνδεσης I / O και λοιπές εφαρμογές. Οι επιθέσεις στον κυβερνοχώρο χρησιμοποιούν τα σφάλματα λογισμικού προς όφελός τους για να προκαλέσουν στα συστήματα ακούσιους τρόπους διαφορετικούς από την αρχική τους ρύθμιση. Η πλειοψηφία των επιθέσεων στον κυβερνοχώρο εξακολουθεί να συμβαίνει μέσα από την εκμετάλλευση των τρωτών σημείων του λογισμικού που προκαλούνται από σφάλματα λογισμικού αλλά και σχεδίασης. Η εκμετάλλευση βάσει λογισμικού συμβαίνει όταν εκμεταλλεύονται συγκεκριμένες δυνατότητες στοίβας και διεπαφής λογισμικού. Οι περισσότερες ευπάθειες λογισμικού συμβαίνουν ως αποτέλεσμα της εκμετάλλευσης σφαλμάτων λογισμικού στη μνήμη, της επικύρωσης της εισόδου χρήστη, τις συνθήκες αγώνα και των δικαιωμάτων πρόσβασης ενός χρήστη. Οι παραβιάσεις της ασφάλειας μνήμης εκτελούνται από τους εισβολείς για να τροποποιήσουν το περιεχόμενο της τοποθεσίας μνήμης. Η πιο παραδειγματική τεχνική είναι υπερχείλιση buffer. Η υπερχείλιση του buffer συμβαίνει όταν ένα πρόγραμμα προσπαθεί να αποθηκεύσει περισσότερα δεδομένα σε ένα buffer από ό, τι επρόκειτο να κρατήσει. Δεδομένου ότι τα buffer δημιουργούνται για να περιέχουν μια πεπερασμένη ποσότητα δεδομένων, η εξωπληροφορία μπορεί να ξεχειλίζει σε γειτονικά buffer, καταστρέφοντας

ή αντικαθιστώντας τα έγκυρα δεδομένα που διατηρούνται σε αυτά. Επιτρέπει στους χρήστες κακόβουλων λογισμικών να παρεμβαίνουν στον υπάρχοντα κώδικα διαδικασίας. Η επικύρωση εισόδου είναι η διαδικασία διασφάλισης πως τα δεδομένα εισαγωγής ακολουθούν ορισμένους κανόνες. (M.Tehranipoor, C. Wang , 2011.)

Η εσφαλμένη επικύρωση δεδομένων μπορεί να οδηγήσει σε καταστροφή δεδομένων, όπως φαίνεται στην SQL injection. Το SQL injection είναι μια από τις πιο γνωστές τεχνικές που εκμεταλλεύονται ένα σφάλμα προγράμματος στο λογισμικό ενός ιστότοπου. Ένας εισβολέας εισάγει εντολές SQL από τον Ιστό είτε για να αλλάξει το περιεχόμενο της βάσης δεδομένων είτε για να απορρίψει τις πληροφορίες της βάσης δεδομένων όπως πιστωτικές κάρτες ή κωδικούς πρόσβασης. Ο εισβολέας εκμεταλλεύεται ένα ελάττωμα σε μια διαδικασία όπου η έξοδος της εξαρτάται από την εκτίμηση άλλων εξόδων. Ο χρόνος ελέγχου έως τον χρόνο χρήσης είναι ένα σφάλμα που προκαλείται από αλλαγές σε ένα σύστημα μεταξύ του ελέγχου της κατάστασης και της χρήσης των αποτελεσμάτων αυτού του ελέγχου. Ονομάζεται επίσης εκμετάλλευση σφάλματος κατάστασης αγώνα. Η σύγχυση προνομίων είναι πράξη εκμετάλλευσης ενός σφάλματος αποκτώντας αυξημένη πρόσβαση σε πόρους που συνήθως προστατεύονται από μια εφαρμογή ή χρήστη. Το αποτέλεσμα είναι ότι οι εισβολείς με περισσότερα προνόμια εκτελούν μη εξουσιοδοτημένες ενέργειες, όπως η πρόσβαση σε προστατευμένα μυστικά κλειδιά. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Στην κοινότητα προγραμματισμού, έχουν ξεκινήσει ορισμένα έργα που είναι αφιερωμένα στην αύξηση του κύριου στόχου της ασφάλειας. Όχι μόνο για την επίλυση εγγενών κοινών αδυναμιών ασφαλείας αλλά πρωταρχικό μέλημα αυτών των έργων είναι η παροχή νέων ιδεών σε μια προσπάθεια δημιουργίας ενός ασφαλούς υπολογιστικού περιβάλλοντος. Σε μια πρακτική ασφαλούς κωδικοποίησης που βασίζεται στην αναθεώρηση κώδικα, οι μηχανικοί λογισμικού εντοπίζουν κοινά σφάλματα προγραμματισμού που οδηγούν σε ευπάθειες λογισμικού, καθιερώνουν τυποποιημένα πρότυπα ασφαλούς κωδικοποίησης, εκπαιδεύουν προγραμματιστές λογισμικού και προωθούν την νέα πρακτική στην ασφαλή κωδικοποίηση. Η πρακτική ασφαλούς κωδικοποίησης βασίζεται σε μια γλώσσα προγραμματισμού, σε αυτήν

αναπτύσσονται τεχνικές για να διασφαλιστεί ότι τα προγράμματα μπορούν να μην παραβιάζονται από εισβολείς. (F.T. Sheldon, V. Vishik 2010)

Οι πιο ευρέως χρησιμοποιούμενες τεχνικές περιλαμβάνουν ανάλυση και μετασχηματισμό. Μια γνωστή μορφή ανάλυσης είναι ο «έλεγχος τύπου» όπου το πρόγραμμα εντοπίζει τυχόν μη ασφαλή τύπο αντικειμένων πριν από την εκτέλεση του προγράμματος. Μια άλλη γνωστή μορφή μετασχηματισμού του προγράμματος είναι η προσθήκη ελέγχων χρόνου εκτέλεσης όπου το πρόγραμμα είναι εξοπλισμένο με κατάλληλο λογισμικό που εμποδίζει να γίνει οποιαδήποτε παραβίαση πολιτικής. Η απόκρυψη κώδικα είναι μια διαδικασία παραγωγής πηγαίου κώδικα ή μηχανικού κώδικα που έχει δημιουργηθεί προκειμένου να είναι δύσκολο να κατανοηθεί για τον άνθρωπο. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Οι προγραμματιστές συχνά αποκρύπτουν τον κώδικα για να αποκρύψουν τον σκοπό ή τη λογική του για να αποτρέψουν οποιαδήποτε πιθανότητα με αντίστροφη μηχανική. Έχει προταθεί επίσης κύκλος Secure design και Development, ο οποίος παρέχει ένα σύνολο τεχνικών σχεδιασμού που επιτρέπει την αποτελεσματική επαλήθευση, δηλαδή ότι ένα κομμάτι του στοιχείου του συστήματος είναι απαλλαγμένο από πιθανά ελαττώματα από τον αρχικό του σχεδιασμό. Αν και δεν είναι απλές προσεγγίσεις, οι επίσημες μέθοδοι παρέχουν τη δυνατότητα διερεύνησης του σχεδιασμού και εντοπισμού τρωτών σημείων ασφαλείας. Έχουν αναπτυχθεί εργαλεία και τεχνικές για τη διευκόλυνση της επαλήθευσης των κριτικών ιδιοτήτων ασφαλείας. Αυτά τα εργαλεία και οι τεχνικές βοηθούν στη μετάφραση υψηλότερου επιπέδου στόχων ασφαλείας σε μια συλλογή από ατομικές ιδιότητες προς επαλήθευση. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Υποδομη Δικτυου Και Ευπαθεια Πρωτοκολλου:

Το πρωτόκολλο του πρώιμου δικτύου αναπτύχθηκε για να υποστηρίζει κάτι εντελώς διαφορετικό από το περιβάλλον που έχουμε σήμερα σε πολύ μικρότερη κλίμακα και

συχνά δεν λειτουργεί σωστά σε πολλές καταστάσεις που χρησιμοποιείται σήμερα. Οι αδυναμίες στα πρωτόκολλα δικτύου είναι περίπλοκες όταν τόσο οι διαχειριστές συστήματος όσο και οι χρήστες έχουν περιορισμένη γνώση της υποδομής δικτύωσης. Παραδείγματος χάριν, οι διαχειριστές ενός συστήματος δεν χρησιμοποιούν ένα αποτελεσματικό σχήμα κρυπτογράφησης, δεν εφαρμόζουν τις συνιστώμενες ενημερώσεις εγκαίρως ή ξεχνούν να εφαρμόσουν φίλτρα ασφαλείας ή πολιτικές. Μία από τις πιο κοινές επιθέσεις δικτύου συμβαίνει όταν οι εισβολείς εκμεταλλευόμενοι τους περιορισμούς των πρωτοκόλλων δικτύου που χρησιμοποιούνται συνήθως στο Internet Protocol (IP), Transmission Control Protocol (TCP) ή Domain Name System (DNS). Το IP είναι το κύριο πρωτόκολλο του επιπέδου δικτύου. Παρέχει τις απαραίτητες πληροφορίες για τη δρομολόγηση πακέτων μεταξύ δρομολογητών και υπολογιστών του δικτύου. Το αρχικό πρωτόκολλο IP δεν είχε κανένα μηχανισμό για τον έλεγχο της αυθεντικότητας και του απορρήτου των δεδομένων που μεταδίδονται. Αυτό επέτρεψε την υποκλοπή ή την αλλαγή των δεδομένων κατά τη μετάδοσή τους μέσω άγνωστου δικτύου μεταξύ δύο συσκευών. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Αντιμετωπίζοντας το πρόβλημα, το IPSec αναπτύχθηκε για να παρέχει κρυπτογράφηση της κίνησης IP. Για πολλά χρόνια, το IPSec έχει χρησιμοποιηθεί ως μια από τις κύριες τεχνολογίες για τη δημιουργία ενός εικονικού ιδιωτικού δικτύου (VPN) το οποίο δημιουργεί ένα ασφαλές κανάλι στο Διαδίκτυο μεταξύ ενός απομακρυσμένου υπολογιστή και ενός αξιόπιστου δικτύου (δηλαδή, εταιρικό intranet). Το TCP υπάρχει στην κορυφή του IP για να μετατρέψει το πακέτο σε αξιόπιστο (δηλαδή να κάνει αναμετάδοση χαμένων πακέτων) και να πραγματοποιήσει την παράδοση των πακέτων. Το SSL αναπτύχθηκε αρχικά για να παρέχει ασφάλεια από άκρο σε άκρο, σε αντίθεση τα υπόλοιπα είναι το μόνο πρωτόκολλο που βασίζεται σε στρώματα, μεταξύ δύο υπολογιστών που βρίσκονται πάνω από το πρωτόκολλο ελέγχου μετάδοσης (TCP). Το SSL / TLS χρησιμοποιείται συνήθως με http για τη δημιουργία https για ασφαλείς ιστοσελίδες. Ο διακομιστής ονόματος τομέα (DNS) είναι το πρωτόκολλο που μεταφράζει τα ονόματα κεντρικών υπολογιστών που διαβάζονται από τον άνθρωπο σε διευθύνσεις πρωτοκόλλου διαδικτύου (IP) 32-bit. Βασικά λειτουργεί ως βιβλίο καταλόγου για το

Διαδίκτυο που λέει στους δρομολογητές των οποίων η διεύθυνση IP θα κατευθύνει πακέτα όταν ο χρήστης δίνει μια διεύθυνση URL. Επειδή οι απαντήσεις DNS δεν είναι επικυρωμένες, ένας εισβολέας ενδέχεται να είναι σε θέση να στείλει κακόβουλα μηνύματα DNS για την πλαστοπροσωπία ενός διακομιστή Internet. Μια άλλη σημαντική ανησυχία για το DNS είναι η διαθεσιμότητά του. Επειδή μια επιτυχημένη επίθεση κατά της υπηρεσίας DNS θα μπορούσε να δημιουργήσει μια σημαντική διακοπή της επικοινωνίας στο Διαδίκτυο, το DNS ήταν ο στόχος πολλών επιθέσεων Denial-of-Service (DoS). (Fadi Al-Turjman, 2019)

Η κρυπτογραφία είναι αποτελεί ένα εργαλείο για την προστασία των δεδομένων που μεταδίδουν μεταξύ των χρηστών κρυπτογραφώντας το δεδομένα, έτσι ώστε μόνο οι χρήστες με κατάλληλα κλειδιά να μπορούν να αποκρυπτογραφήσουν τα δεδομένα. Η κρυπτογραφία είναι ο πιο συχνά χρησιμοποιούμενος μηχανισμός προστασίας δεδομένων. Μια έρευνα που πραγματοποιήθηκε από το Ινστιτούτο Ασφάλειας Υπολογιστών το 2008 αποκάλυψε ότι το 72% των εταιρειών χρησιμοποίησαν κρυπτογράφηση για τα δεδομένα τους κατά τη μεταφορά δεδομένων. Πέραν της προστασίας των σημερινών εξελιγμένων εισβολέων που εκμεταλλεύονται τους περιορισμούς των υπαρχόντων αλγορίθμων κρυπτογραφίας, αυξάνονται και άλλο τα επίπεδα ασφαλείας. Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των ΗΠΑ (NIST) ανακοίνωσε πρόσφατα τη διακοπή του SHA-1 και τη χρήση του Advanced Hash Standard (ASH) από το 2011. Η δυνατότητα χρήσης κρυπτογράφησης βάσει ταυτότητας είναι μια ενεργή ερευνητική ατζέντα για εφαρμογές που απαιτούν κρυπτογράφηση υψηλής ταχύτητας. για να αποφευχθεί η χρήση αργού κλειδιού RSA 2048 bit, καθώς και η μη πρακτική συμμετοχή της αξιόπιστης αρχής πιστοποίησης. (Fadi Al-Turjman, 2019)

Η κβαντική κρυπτογραφία είναι μια αναδυόμενη τεχνολογία στην οποία δύο μέρη παράγουν ταυτόχρονα κοινόχρηστο, κρυπτογραφημένο υλικό χρησιμοποιώντας τη μετάδοση κβαντικών καταστάσεων φωτός. Οι εξειδικευμένοι εισβολείς χρησιμοποιούν σήμερα μια εξελιγμένη τεχνική που συγκαλύπτει κακόβουλα ωφέλιμα φορτία κυκλοφορίας που μοιάζουν πιο αντιπροσωπευτικά ωφέλιμα φορτία κίνησης. Επιπλέον, ο μεγάλος όγκος ροής δεδομένων σε δίκτυα υψηλής χωρητικότητας απαιτεί νέες τεχνικές

ανάλυσης για τον υπολογισμό και την απεικόνιση της αβεβαιότητας που συνδέεται με τα σύνολα δεδομένων. Αυτή η πρόκληση δημιούργησε μια νέα περιοχή έρευνας όπου απαιτείται η συνδυασμένη ομάδα δεξιοτήτων από επαγγελματίες του δικτύου και την κοινότητα οπτικοποίησης για να συλλάβει την επισκεψιμότητα του δικτύου με καλύτερες τεχνικές οπτικοποίησης. Η οπτική παρουσίαση των δεδομένων στη συνέχεια αναλύεται από ειδικούς δικτύου με γνώση εις βάθος στον τομέα του συστήματος δικτύωσης. (Fadi Al-Turjman, 2019)

ΚΕΦΑΛΑΙΟ 8: ΑΝΑΔΥΟΜΕΝΕΣ ΑΠΕΙΛΈΣ

Οι επιθέσεις στον κυβερνοχώρο στον κυβερνοχώρο εξελίσσονται με το χρόνο αξιοποιώντας νέες προσεγγίσεις. Τις περισσότερες φορές, οι εγκληματίες στον κυβερνοχώρο τροποποιούν τις υπάρχουσες υπογραφές κακόβουλου λογισμικού για να εκμεταλλευτούν τα ελαττώματα που υπάρχουν στις νέες τεχνολογίες. Σε άλλες περιπτώσεις, απλώς εξερευνούν μοναδικά χαρακτηριστικά των νέων τεχνολογιών για να βρουν κενά για την ένεση κακόβουλου λογισμικού. Αξιοποιώντας τα πλεονεκτήματα των νέων τεχνολογιών Internet με εκατομμύρια και δισεκατομμύρια ενεργούς χρήστες, οι εγκληματίες στον κυβερνοχώρο χρησιμοποιούν αυτές τις νέες τεχνολογίες για να προσεγγίσουν έναν μεγάλο αριθμό θυμάτων γρήγορα και αποτελεσματικά. Επιλέγουμε τέσσερις τέτοιες ανερχόμενες τεχνολογικές εξελίξεις που περιλαμβάνουν: κοινωνικά μέσα, υπολογιστικό νέφος, τεχνολογία smartphone και την κρίσιμη υποδομή, ως ενδεικτικά παραδείγματα για την εξερεύνηση απειλών σε αυτές τις τεχνολογίες. (M.Tehranipoor, C. Wang , 2011.)

Κοινωνικά μέσα: Τα κοινωνικά μέσα, όπως το Facebook και το Twitter, έχουν δείξει εκρηκτική ανάπτυξη τα τελευταία χρόνια. Στο τέλος του 2015, υπήρχαν περισσότεροι από 750 εκατομμύρια ενεργοί λογαριασμοί χρηστών στο Twitter, ενώ ο αριθμός αυξάνεται εκθετικά στο Facebook φτάνοντας σχεδόν το 1 δισεκατομμύριο χρήστες. Οι ιστότοποι κοινωνικής δικτύωσης ήταν πολύ δημοφιλείς και έγιναν η προτιμώμενη

μέθοδος επικοινωνίας για τις περισσότερες νέες γενιές. Κάθε ένας από αυτούς τους ιστότοπους κοινωνικών μέσων παρέχει συνήθως εργαλεία όπου οι χρήστες μοιράζονται τις προσωπικές τους πληροφορίες (π.χ. όνομα, διεύθυνση, φύλο, ημερομηνία γέννησης, προτίμηση στη μουσική και την ταινία), φωτογραφίες, ιστορίες και διάδοση συνδέσμων. Οι εισβολείς εκμεταλλεύονται την τρέλα των κοινωνικών μέσων ως ένα νέο μέσο εκκίνησης ύπουλων επιθέσεων. Έως το τέλος του 2013, η συλλογή Kaspersky Lab περιείχε περισσότερα από 89.000 κακόβουλα αρχεία που σχετίζονται με ιστότοπους κοινωνικών μέσων. Μια έκθεση που δημοσιεύθηκε από την εταιρεία ασφάλειας δεδομένων και προστασίας δεδομένων Sophos αποκάλυψε μια ανησυχητική αύξηση των επιθέσεων εναντίον των χρηστών των ιστότοπων της κοινωνικής media. Σύμφωνα με την έκθεσή τους, περίπου το 65% των χρηστών στα κοινωνικά δίκτυα έχουν λάβει spam. Με την απεριόριστη πρόσβαση στο προφίλ των χρηστών, οι εισβολείς μπορούν να αποκτήσουν περαιτέρω τις πληροφορίες σχετικά με τα εταιρικά και εμπορικά μυστικά. Στην έρευνα που διενήργησε η Sophos, περίπου το 60% των εταιρειών ανησυχούν ότι οι υπάλληλοί τους παρέχουν υπερβολικά πολλές πληροφορίες στα κοινωνικά δίκτυα, ενώ περίπου το 65% των εταιρειών πιστεύουν ότι η χρήση κοινωνικών δικτύων αποτελεί μεγάλη απειλή για τις εταιρείες. (Fadi Al-Turjman, 2019)

Το σκουλήκι Koobface που διαδίδεται σε ιστότοπους κοινωνικών μέσων το 2011 είναι η πιο γνωστή περίπτωση κακόβουλου λογισμικού που αξιοποιεί τον πολλαπλασιασμό των ιστότοπων κοινωνικών μέσων. Αξιοποιώντας το οπλοστάσιο του, το botnet Koobface αυτοματοποιεί τη δημιουργία νέων λογαριασμών κοινωνικών μέσων που χρησιμοποιούνται για τη φιλία ανυποψίαστων χρηστών, με τη σειρά τους ανεπιθύμητους συνδέσμους που ανακατευθύνουν σε κακόβουλα προγράμματα. Οι λογαριασμοί κοινωνικής δικτύωσης που πέφτουν θύματα μιας τέτοιας επίθεσης μετατρέπονται σε οχήματα για αποστολή ανεπιθύμητων μηνυμάτων στους φίλους τους, ενώ το μηχάνημα του θύματος μολύνεται και αυτό. (Fadi Al-Turjman, 2019)

Ο Thomas και ο Nicol δημιούργησαν έναν εξομοιωτή ζόμπι που μπόρεσε να διεισδύσει στο botnet Koobface και εντόπισε παραπλανητικούς και παραβιασμένους λογαριασμούς κοινωνικών δικτύων που χρησιμοποιήθηκαν για τη διανομή κακόβουλων συνδέσμων σε

περισσότερους από 224.000 χρήστες κοινωνικών δικτύων, δημιουργώντας πάνω από 165.000 κλικ. Ανακάλυψαν την αναποτελεσματικότητα των τρεχουσών υπηρεσιών μαύρης λίστας που προσφέρονται από φορείς εκμετάλλευσης κοινωνικών δικτύων για το φιλτράρισμα ιών μέσω των πιο σημαντικών υπηρεσιών μαύρης λίστας. Υποστήριξαν ότι αυτές οι υπηρεσίες μαύρης λίστας αναγνωρίζουν μόνο το 26% των απειλών και χρειάζονται κατά μέσο όρο 4 ημέρες για να απαντήσουν, ενώ διαπίστωσαν ότι το 82% των επισκεπτών στο spam του Koobface συμβαίνουν εντός των πρώτων 2 ημερών από τη δημοσίευση ενός συνδέσμου, αφήνοντας την πλειονότητα των χρηστών κοινωνικής δικτύωσης ευάλωτες. Ένα άλλο δημοφιλές κακόβουλο λογισμικό γίνεται με τη χρήση σημαντικού αριθμού λογαριασμών Twitter ή Facebook που δεν είναι νόμιμοι ή δεν χρησιμοποιούνται. Οι εγκληματίες του κυβερνοχώρου γίνονται πολύ πιο περίπλοκοι στις προσπάθειές τους να εμφανιστούν ως αξιόπιστοι χρήστες. Στη συνέχεια, οι εγκληματίες παραπλανούν τον ιστότοπο κοινωνικών δικτύων σε «φιλία» ή ακολουθώντας τους και κάνοντας κλικ στις ενημερώσεις κατάστασής τους που συχνά οδηγούν σε κακόβουλους ιστότοπους. Σε μια άλλη μελέτη, φαίνεται ότι ένας μεγάλος αριθμός κακόβουλου λογισμικού εξαπλώθηκε αφού έκανε κλικ για περιεχόμενο σχετικά με "δημοφιλή" θέματα μέσω Twitter. (M.Tehranipoor, C. Wang , 2011.)

Οι ιστότοποι κοινωνικής δικτύωσης έχουν επίσης αυξήσει την προστασία της ιδιωτικής ζωής λόγω του συγκεντρωτισμού των μαζικών ποσών των δεδομένων των χρηστών, της οικειότητας των προσωπικών πληροφοριών που συλλέγονται και της διαθεσιμότητας ενημερωμένων δεδομένων τα οποία είναι σταθερά επισημασμένα και μορφοποιημένα. Αυτό καθιστά τους ιστότοπους κοινωνικής δικτύωσης έναν ελκυστικό στόχο για μια ποικιλία οργανισμών που επιδιώκουν να συγκεντρώσουν μεγάλες ποσότητες δεδομένων χρηστών, ορισμένοι για νόμιμους σκοπούς και μερικοί για κακόβουλους. Στις περισσότερες περιπτώσεις, η εξαγωγή δεδομένων παραβιάζει την προσδοκία απορρήτου των χρηστών. Εξετάστηκε η προστασία των προσωπικών δεδομένων των χρηστών που διατηρούνται στις υπηρεσίες παροχής κοινωνικής δικτύωσης. Ο Lucas πρότεινε μια εφαρμογή Facebook για κρυπτογράφηση και αποκρυπτογράφηση ευαισθητοποιημένων δεδομένων χρησιμοποιώντας JavaScript από την πλευρά του

πελάτη. Αυτή η αρχιτεκτονική διασφαλίζει ότι τα δεδομένα δεν φθάνουν ποτέ στους παρόχους υπηρεσιών κοινωνικού δικτύου σε μια μη κρυπτογραφημένη μορφή που τους εμποδίζει να παρατηρήσουν και να συσσωρεύσουν τις πληροφορίες που μεταδίδουν οι χρήστες μέσω του τότε δικτύου. Θέματα και εργαλεία σχετικά με την ευαισθητοποίηση σχετικά με την προστασία της ιδιωτικής ζωής που μπορούν να βοηθήσουν τους χρήστες να ορίσουν τη ρύθμιση απορρήτου τους πιο έξυπνα. Για παράδειγμα, οι Fang και LeFevre πρότειναν οδηγό απορρήτου. Ο οδηγός ζητά επανειλημμένα από τον χρήστη να εκχωρήσει "ετικέτες" απορρήτου σε επιλεγμένους φίλους και χρησιμοποιεί αυτήν την είσοδο για την κατασκευή ενός ταξινομητή, χρησιμοποιώντας ένα μοντέλο μηχανικής εκμάθησης, το οποίο με τη σειρά του μπορεί να χρησιμοποιηθεί για την αυτόματη εκχώρηση προνομίων στους υπόλοιπους φίλους του χρήστη. Η διαίσθηση για το σχεδιασμό προκύπτει από την παρατήρηση ότι οι πραγματικοί χρήστες συλλάβουν τις προτιμήσεις απορρήτου τους, των οποίων οι φίλοι θα πρέπει να μπορούν να βλέπουν ποιες πληροφορίες, με βάση το σύνολο κανόνων που θέτουν και χρησιμοποιούν επανειλημμένα στη ρύθμιση των περισσότερων φίλων. (Fadi Al-Turjman, 2019)

Cloud Computing: Η αποτελεσματικότητα της μεταφοράς δεδομένων και εφαρμογών στο cloud συνεχίζει να προσελκύει καταναλωτές που αποθηκεύουν τα δεδομένα τους στο DropBox και το iCloud, χρησιμοποιούν το Gmail και το Live mail για να χειρίζονται email και να παρακολουθούν τη ζωή τους χρησιμοποιώντας υπηρεσίες όπως το Evernote και το Mint.com. Το cloud computing είναι αναμφισβήτητα μια από τις πιο σημαντικές τεχνολογικές αλλαγές που έχουν γίνει τα τελευταία χρόνια. Το γεγονός ότι η δυνατότητα χρήσης υπολογιστών με παρόμοιο τρόπο με τη χρήση ενός βοηθητικού προγράμματος φέρνει επανάσταση στον κόσμο των υπηρεσιών πληροφορικής και διατηρεί το μεγάλο δυναμικό. Οι πελάτες, είτε μεγάλες είτε μικρές επιχειρήσεις, προσελκύονται από τις υποσχέσεις ευελιξίας του cloud, του μειωμένου κόστους κεφαλαίου και των βελτιωμένων πόρων πληροφορικής. Οι εταιρείες πληροφορικής μετατοπίζονται από την παροχή της δικής τους υποδομής πληροφορικής αξιοποιώντας τις υπηρεσίες υπολογισμού που παρέχονται από το cloud για τις ανάγκες τους στην τεχνολογία πληροφοριών. (Fadi Al-Turjman, 2019)

Το cloud computing παρέχει μοναδικά χαρακτηριστικά που διαφέρουν από τις παραδοσιακές προσεγγίσεις. Τα πέντε βασικά χαρακτηριστικά του cloud computing περιλαμβάνουν αυτοεξυπηρέτηση κατ 'απαίτηση, πανταχού παρούσα πρόσβαση στο δίκτυο, ανεξάρτητη τοποθέτηση πόρων, γρήγορη ελαστικότητα και μετρημένη εξυπηρέτηση, όλα προσανατολισμένα στη χρήση σύννεφων χωρίς ραφή και διαφάνεια. Η δημοσκόπηση πόρων αναφέρεται στην ικανότητα όπου δεν διατίθενται πόροι σε έναν χρήστη αλλά αντ 'αυτού συγκεντρώνονται για να εξυπηρετούν πολλούς καταναλωτές. Πόροι, είτε σε επίπεδο εφαρμογής, κεντρικού υπολογιστή ή δικτύου, εκχωρούνται και εκχωρούνται εκ νέου ανάλογα με τις ανάγκες σε αυτούς τους καταναλωτές. Κατά παραγγελία, η αυτοεξυπηρέτηση αναφέρεται όπου οι χρήστες μπορούν να εκχωρήσουν στους εαυτούς τους πρόσθετους πόρους, όπως αποθήκευση ή επεξεργαστική ισχύ αυτόματα, χωρίς ανθρώπινη παρέμβαση. Αυτό είναι συγκρίσιμο με τον αυτόματο υπολογιστικό υπολογιστή όπου το σύστημα υπολογιστή είναι ικανό αυτοδιαχείρισης. Μαζί με την αυτοδιάθεση πόρων, το cloud computing χαρακτηρίζεται από την ικανότητα εντοπισμού και απελευθέρωσης πόρων όσο το δυνατόν γρηγορότερα, ο όρος συχνά ονομάζεται «ελαστικότητα». Αυτό επιτρέπει στους καταναλωτές να κλιμακώσουν τους πόρους που χρειάζονται ανά πάσα στιγμή για να αντιμετωπίσουν τα μεγάλα φορτία και τις χρήσεις, και στη συνέχεια να μειωθούν επιστρέφοντας τους πόρους στην ομάδα όταν τελειώσουν. Η μετρημένη υπηρεσία, που συχνά ονομάζεται και πληρωμή καθώς πηγαίνετε, επιτρέπει στο cloud να προσφέρεται ως βοηθητικό πρόγραμμα όπου οι χρήστες πληρώνουν με βάση την κατανάλωση. (M.Tehranipoor, C. Wang , 2011.)

Το cloud computing είναι επίσης ένα μοντέλο ολοκλήρωσης που παρέχει διάφορους πόρους σε πελάτες σε διαφορετικά επίπεδα του συστήματος και χρησιμοποιεί διαφορετικούς πόρους. Σε γενικές γραμμές, η αρχιτεκτονική ενός περιβάλλοντος υπολογιστικού νέφους μπορεί να χωριστεί σε 4 επίπεδα: το επίπεδο υλικού (συμπεριλαμβανομένων των κέντρων δεδομένων), το επίπεδο υποδομής, το επίπεδο πλατφόρμας και το επίπεδο εφαρμογής. (C. M. Medaglia, A. Serbanati, 2010)

• Επίπεδο υλικού: Αυτό το επίπεδο είναι υπεύθυνο για τη διαχείριση των φυσικών πόρων του cloud, συμπεριλαμβανομένων φυσικών διακομιστών, δρομολογητών,

διακοπτών, συστημάτων ισχύος και ψύξης Στην πράξη, το επίπεδο υλικού εφαρμόζεται συνήθως σε κέντρα δεδομένων. Ένα κέντρο δεδομένων περιέχει συνήθως χιλιάδες διακομιστές που είναι οργανωμένοι σε «ράφια» και διασυνδέονται μέσω διακοπτών, και δρομολογητών. Τυπικά ζητήματα στο επίπεδο υλικού περιλαμβάνουν τη διαμόρφωση υλικού, την ανοχή σφαλμάτων, τη διαχείριση της κυκλοφορίας, τη διαχείριση πόρων ισχύος και ψύξης. (C. M. Medaglia, A. Serbanati, 2010)

• Επίπεδο υποδομής: Αυτό το επίπεδο είναι επίσης γνωστό ως επίπεδο εικονικοποίησης. Το επίπεδο υποδομής δημιουργεί μια ομάδα πόρων αποθήκευσης και υπολογισμού, διαχωρίζοντας τους φυσικούς πόρους χρησιμοποιώντας τεχνολογίες εικονικοποίησης όπως το Xen, η εικονική μηχανή με βάση τον πυρήνα και το VMware. Το επίπεδο υποδομής είναι ένα ουσιαστικό συστατικό του cloud computing, καθώς πολλά βασικά χαρακτηριστικά, όπως η δυναμική εκχώρηση πόρων, διατίθενται μόνο μέσω τεχνολογιών εικονικοποίησης. (C. M. Medaglia, A. Serbanati, 2010)

• Επίπεδο πλατφόρμας: Χτισμένο πάνω από το επίπεδο υποδομής, το επίπεδο πλατφόρμας αποτελείται από λειτουργικά συστήματα και πλαίσια εφαρμογής. Ο σκοπός του επιπέδου πλατφόρμας είναι να ελαχιστοποιήσει το βάρος της ανάπτυξης εφαρμογών απευθείας σε κοντέινερ VM. Για παράδειγμα, το Google App Engine λειτουργεί στο επίπεδο της πλατφόρμας για να παρέχει υποστήριξη API για την υλοποίηση της λογικής αποθήκευσης, βάσης δεδομένων και επιχειρήσεων των τυπικών εφαρμογών ιστού. (C. M. Medaglia, A. Serbanati, 2010)

• Το επίπεδο εφαρμογής: Στο υψηλότερο επίπεδο της ιεραρχίας, το επίπεδο εφαρμογής αποτελείται από τις πραγματικές εφαρμογές cloud. Διαφορετικές από τις παραδοσιακές εφαρμογές, οι εφαρμογές cloud μπορούν να αξιοποιήσουν τη δυνατότητα αυτόματης κλιμάκωσης για να επιτύχουν καλύτερη απόδοση, διαθεσιμότητα και χαμηλότερο λειτουργικό κόστος. (C. M. Medaglia, A. Serbanati, 2010)

Ωστόσο, στην πράξη, τα cloud προσφέρουν υπηρεσίες που μπορούν να ομαδοποιηθούν σε τρεις κατηγορίες: λογισμικό ως υπηρεσία (SaaS), πλατφόρμα ως υπηρεσία (PaaS) και υποδομή ως υπηρεσία (IaaS). Οι εφαρμογές που εκτελούνται ή

αναπτύσσονται για πλατφόρμες υπολογιστών cloud δημιουργούν διάφορες προκλήσεις ασφάλειας και απορρήτου ανάλογα με τα υποκείμενα μοντέλα παράδοσης και ανάπτυξης. Στο IaaS, ο πάροχος cloud παρέχει ένα σύνολο εικονικοποιημένων στοιχείων υποδομής όπως εικονικές μηχανές (VM) και χώρο αποθήκευσης στον οποίο οι πελάτες μπορούν να δημιουργήσουν και να εκτελέσουν εφαρμογές. Η εφαρμογή τελικά θα βρίσκεται στο VM και στο εικονικό λειτουργικό σύστημα. Το PaaS επιτρέπει σε περιβάλλοντα προγραμματισμού να έχουν πρόσβαση και να χρησιμοποιούν πρόσθετα μπλοκ δόμησης εφαρμογών. Τέτοια περιβάλλοντα προγραμματισμού έχουν ορατό αντίκτυπο στην αρχιτεκτονική εφαρμογών, όπως περιορισμοί στους οποίους η εφαρμογή μπορεί να ζητήσει υπηρεσίες από ένα λειτουργικό σύστημα. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Τέλος, στο SaaS, οι πάροχοι cloud ενεργοποιούν και παρέχουν λογισμικά εφαρμογών ως υπηρεσίες κατ 'απαίτηση. Η πολλαπλή μίσθωση είναι ένα χαρακτηριστικό μοναδικό για τα σύννεφα που επιτρέπει στους παρόχους cloud να διαχειρίζονται αποτελεσματικότερα τη χρήση πόρων διαχωρίζοντας μια εικονικοποιημένη, κοινόχρηστη υποδομή μεταξύ διαφόρων πελατών. Για παράδειγμα, για την απομόνωση δεδομένων πολλαπλών μισθωτών, το Salesforce.com χρησιμοποιεί έναν συγγραφέα ερωτημάτων σε επίπεδο βάσης δεδομένων, ενώ η Amazon χρησιμοποιεί υπεύθυνους εποπτείας σε επίπεδο υλικού. Η οπτικοποίηση είναι μια σημαντική τεχνολογία ενεργοποίησης σε αυτόν τον τομέα που βοηθά την αφηρημένη υποδομή και πόρους να διατίθενται πελάτες ως μεμονωμένα VM. Παρέχοντας ισχυρή απομόνωση, διαμεσολαβημένη κοινή χρήση και ασφαλείς επικοινωνίες μεταξύ ενεργών ερευνητικών περιοχών του VMsare. Η πιθανή λύση έχει προταθεί η χρήση ενός ευέλικτου μηχανισμού ελέγχου πρόσβασης που διέπει τις δυνατότητες ελέγχου και κοινής χρήσης του VM. Επειδή οι πελάτες αποκτούν και χρησιμοποιούν στοιχεία λογισμικού από διαφορετικούς παρόχους, τα κρίσιμα ζητήματα περιλαμβάνουν την ασφαλή σύνθεσή τους και τη διασφάλιση ότι οι πληροφορίες που διαχειρίζονται αυτές οι υπηρεσίες είναι καλά προστατευμένες. Για παράδειγμα, ένα περιβάλλον PaaS ενδέχεται να περιορίσει την πρόσβαση σε καλά καθορισμένα μέρη του συστήματος

αρχείων, απαιτώντας έτσι μια λεπτομερή υπηρεσία εξουσιοδότησης. (C. M. Medaglia, A. Serbanati, 2010)

Η διαχείριση εμπιστοσύνης και η ολοκλήρωση πολιτικής είναι ένας ενεργός τομέας έρευνας στο cloud computing ως το μοντέλο outsourcing του cloud, όπου οι πάροχοι cloud ελέγχουν και διαχειρίζονται τα δεδομένα και τις υπηρεσίες του χρήστη, αναγκάζουν τους πελάτες να έχουν σημαντική εμπιστοσύνη στην τεχνική επάρκεια του παρόχου τους. Σε περιβάλλοντα υπολογιστικού νέφους, οι αλληλεπιδράσεις μεταξύ διαφορετικών τομέων εξυπηρέτησης που βασίζονται σε απαιτήσεις υπηρεσίας είναι επίσης δυναμικές, παροδικές και εντατικές. Έτσι, έχει προταθεί μια ανάπτυξη του έργου εμπιστοσύνης που επιτρέπει την αποτελεσματική καταγραφή ενός γενικού συνόλου παραμέτρων που απαιτείται για τη δημιουργία εμπιστοσύνης και για τη διαχείριση των εξελισσόμενων απαιτήσεων εμπιστοσύνης και αλληλεπίδρασης / κοινής χρήσης. Η ολοκλήρωση πολιτικής του cloud είναι ένας άλλος ενεργός τομέας έρευνας για την αντιμετώπιση προκλήσεων όπως η σημασιολογική ετερογένεια, η ασφαλής διαλειτουργικότητα και η διαχείριση της εξέλιξης πολιτικής. Επιπλέον, οι συμπεριφορές των πελατών μπορούν να εξελιχθούν γρήγορα, επηρεάζοντας έτσι τις καθιερωμένες αξίες εμπιστοσύνης. Αυτό υποδηλώνει την ανάγκη για ένα ολοκληρωμένο, βασισμένο στην εμπιστοσύνη, ασφαλές πλαίσιο διαλειτουργικότητας που βοηθά στη δημιουργία, τη διαπραγμάτευση και τη διατήρηση της εμπιστοσύνης για την προσαρμοστική υποστήριξη της ολοκλήρωσης της πολιτικής. (M.Tehranipoor, C. Wang , 2011.)

Smartphones*:* Τα smartphone, σε συνδυασμό με τη βελτίωση των ασύρματων τεχνολογιών, έχουν γίνει μια ολοένα και πιο εξελιγμένη συσκευή υπολογιστή και επικοινωνίας που μεταφέρεται εύκολα από άτομα καθ 'όλη τη διάρκεια της ημέρας. Η σύγκλιση της αυξανόμενης ισχύος των επιχειρήσεων, της εξατομίκευσης και της κινητικότητας τους καθιστά ένα ελκυστικό μέσο σχεδιασμού και οργάνωσης της εργασίας και της ιδιωτικής ζωής των ατόμων. Σύμφωνα με, ο τεράστιος όγκος των χρηστών κινητών τηλεφώνων σε όλο τον κόσμο δείχνει μια τρέχουσα ανάγκη για

προληπτικά μέτρα ασφάλειας για κινητά. Υποτίθεται ότι πάνω από 4,5 δισεκατομμύρια χρησιμοποιούν κινητό τηλέφωνο κάθε μέρα και εκτιμάται ότι θα αναπτυχθούν 2 δις smartphone μέχρι το 2013. Πέρα από τα απλά μηνύματα SMS, αυξάνεται το επίπεδο ευαίσθητων πληροφοριών στα smartphone. Με τις εταιρείες, αυτές οι τεχνολογίες προκαλούν βαθιές αλλαγές στην οργάνωση των συστημάτων πληροφοριών και ως εκ τούτου αποτελούν πηγή νέων κινδύνων. Καθώς τα smartphone συλλέγουν και συγκεντρώνουν αυξανόμενο αριθμό ευαίσθητων πληροφοριών, η πρόσβαση πρέπει να ελέγχεται για την προστασία του απορρήτου του χρήστη και της πνευματικής ιδιοκτησίας της εταιρείας. Αυτές οι εντυπωσιακές αυξήσεις στην τεχνολογία των κινητών έχουν δημιουργήσει έναν ελκυστικό στόχο για εγκληματίες στον κυβερνοχώρο. Οι ανησυχίες για την ασφάλεια στα κινητά είναι διαφορετικά από τα παραδοσιακά προβλήματα ασφάλειας σε υπολογιστές και υπολογιστές λόγω της ενσωματωμένης φύσης τους και του διαφορετικού λειτουργικού περιβάλλοντος. Ο Mulliner παραθέτει τις ακόλουθες λειτουργίες που είναι μοναδικές για φορητούς υπολογιστές.

• *Κινητικότητα*: Αυτό είναι το πιο σημαντικό χαρακτηριστικό των κινητών τηλεφώνων. Δεδομένου ότι οι χρήστες κινητών μπορούν να τους μεταφέρουν οπουδήποτε, οι πιθανότητες κλοπής, απώλειας ή σωματικής συμπεριφοράς αυξάνονται σε σύγκριση με τις σταθερές συσκευές.

• *Ισχυρή εξατομίκευση*: Ως προσωπική συσκευή, οι κινητές συσκευές συνήθως δεν κοινοποιούνται σε πολλούς χρήστες.

• *Ισχυρή συνδεσιμότητα*: Τα κινητά τηλέφωνα χρησιμοποιούνται συνήθως για σύνδεση με άλλες συσκευές μέσω ασύρματων δικτύων (ή ασύρματου Διαδικτύου) για ανταλλαγή δεδομένων.

• *Σύγκλιση τεχνολογίας*: Σήμερα πολλές κινητές λειτουργίες ενσωματώνονται στα κινητά τηλέφωνα, όπως παιχνίδια, κοινή χρήση βίντεο και δεδομένων και περιήγηση στο Διαδίκτυο.

• *Περιορισμένοι πόροι και μειωμένες δυνατότητες*: Σε σύγκριση με τις σταθερές συσκευές, οι φορητές συσκευές έχουν τέσσερις βασικούς περιορισμούς: α)

περιορισμένη διάρκεια ζωής της μπαταρίας, β) περιορισμένη ισχύς υπολογιστών, γ) πολύ μικρό μέγεθος οθόνης, και δ) πλήκτρα πολύ μικρού μεγέθους για εισόδους. Αυτά τα όρια φέρνουν τις προκλήσεις στη δημιουργία τεχνολογίας ασφάλειας για κινητά.

Υπάρχουν διάφορα διαφορετικά είδη επιθέσεων που στοχεύουν να εκμεταλλευτούν τον πολλαπλασιασμό της φορητής υπολογιστικής. Οι επιθέσεις που σχετίζονται με την επικοινωνία προέρχονται από ατέλειες στο σχεδιασμό και τη διαχείριση της υποδομής κινητής επικοινωνίας. Ο εισβολέας μπορεί να προσπαθήσει να σπάσει την κρυπτογράφηση του δικτύου κινητής τηλεφωνίας. Το δίκτυο GSM (Παγκόσμιο Σύστημα Επικοινωνίας Mo-bile) χρησιμοποιεί σήμερα δύο παραλλαγές αλγορίθμων γνωστών ως A5 / 1 και A5 / 2, οι οποίες είναι γνωστές ως πιο δύσκολες. Δεδομένου ότι ο αλγόριθμος κρυπτογράφησης δημοσιοποιήθηκε, αποδείχθηκε ότι είναι δυνατόν να σπάσει την κρυπτογράφηση σε περίπου 6 ώρες. Ένας εισβολέας μπορεί να προσπαθήσει να παρακολουθήσει τις επικοινωνίες Wi-Fi για να αντλήσει πληροφορίες (π.χ. όνομα χρήστη, κωδικός πρόσβασης). Αυτοί οι τύποι επιθέσεων δεν είναι μοναδικοί για τα smartphone, αλλά είναι πολύ ευάλωτοι σε αυτές τις επιθέσεις επειδή πολύ συχνά το Wi-Fi είναι το μόνο μέσο επικοινωνία που πρέπει να έχουν πρόσβαση στο Διαδίκτυο. Έχουν μελετηθεί ζητήματα ασφαλείας που σχετίζονται με το Bluetooth σε κινητές συσκευές και έχουν δείξει ορισμένα προβλήματα. Για παράδειγμα, το Cabir είναι ένα σκουλήκι που εξαπλώνεται μέσω σύνδεσης Bluetooth. Το σκουλήκι αναζητά κοντινά τηλέφωνα με Bluetooth σε δυνατότητα εντοπισμού και αποστέλλεται στη συσκευή προορισμού. Ο χρήστης πρέπει να αποδεχτεί το εισερχόμενο αρχείο και να εγκαταστήσει το πρόγραμμα. Μετά την εγκατάσταση, το σκουλήκι μολύνει το μηχάνημα. Για την αποφυγή επιθέσεων που σχετίζονται με την επικοινωνία, η κίνηση δικτύου που ανταλλάσσεται με τηλέφωνα μπορεί να παρακολουθείται όπως παρακολούθηση σημείων δρομολόγησης δικτύου ή παρακολούθηση της χρήσης πρωτοκόλλων δικτύου κινητής τηλεφωνίας. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Ένας άλλος τύπος επιθέσεων προέρχεται από τις ευπάθειες σε εφαρμογές λογισμικού κινητής τηλεφωνίας, ειδικά εκμεταλλευόμενοι το πρόγραμμα περιήγησης στο κινητό. Ακριβώς όπως τα κοινά προγράμματα περιήγησης στο Web, τα προγράμματα

περιήγησης ιστού για κινητά επεκτείνονται από την καθαρή πλοήγηση στον ιστό με widget και πρόσθετα τα οποία χρησιμοποιούν πολλοί εισβολείς ως μέσα για τη διάδοση κακόβουλων προγραμμάτων. Το jailbreaking του iPhone βασίστηκε εξ ολοκλήρου σε ευπάθειες στο πρόγραμμα περιήγησης ιστού με βάση την υπερχείλιση buffer που βασίζεται σε στοίβα σε μια βιβλιοθήκη που χρησιμοποιείται από το πρόγραμμα περιήγησης ιστού. Η ευπάθεια στο πρόγραμμα περιήγησης ιστού για Android ανακαλύφθηκε τον Οκτώβριο του 2009 εκμεταλλευόμενη την ξεπερασμένη και ευάλωτη βιβλιοθήκη. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Οι κακόβουλοι εισβολείς στοχεύουν κινητά τηλέφωνα ως μέσο για την εξάπλωση κακόβουλου λογισμικού. Και οι δύο αναφορές απειλών για την ασφάλεια στον κυβερνοχώρο και οι αναφορές απειλών της Symantec τα τελευταία δύο χρόνια προειδοποιούν ότι ο αυξανόμενος αριθμός κακόβουλων ειδών δημιουργείται ειδικά για κινητά τηλέφωνα, όπως η στόχευση τηλεφώνων που βασίζονται σε Android Android και Apple iPhone. Για τον έλεγχο της διάδοσης του κακόβουλου λογισμικού, οι εταιρείες κινητής τηλεφωνίας προσφέρουν μια κεντρική δημόσια αγορά συμπληρωμένη με μια διαδικασία έγκρισης προτού φιλοξενήσουν την εφαρμογή. Η κεντρική αγορά συμβάλλει στην κατάργηση οποιασδήποτε εφαρμογής, εάν βρεθεί ύποπτη πριν από τη λήψη τους από τους χρήστες. Για παράδειγμα, η Apple υιοθετεί μια διαδικασία ελέγχου για να διασφαλίσει ότι όλες οι εφαρμογές συμμορφώνονται με τους κανόνες της Apple προτού μπορούν να προσφερθούν μέσω του App Store. Η Apple εγκρίνει μια εφαρμογή με υπογραφή κώδικα με κλειδιά κρυπτογράφησης. Η πρόσβαση στις εφαρμογές μέσω App Store είναι ο μόνος τρόπος για την εγκατάσταση εφαρμογών από συσκευές iPhone. Παρόμοια με την Apple, το Android διαθέτει επίσης μια δημόσια αγορά για τη φιλοξενία εφαρμογών. Ωστόσο, σε αντίθεση με την Apple, η εφαρμογή Android μπορεί να υπογραφεί. Το Android χρησιμοποιεί πλήθος πηγών για να αξιολογήσει τις εφαρμογές από τους χρήστες. Με βάση τα παράπονα των χρηστών, οι εφαρμογές μπορούν να απομακρυνθούν από την αγορά και να τις αφαιρέσουν επίσης από τη συσκευή. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Μια άλλη προσέγγιση που υιοθέτησαν οι εταιρείες κινητής τηλεφωνίας για την προστασία των πλατφορμών κινητής τηλεφωνίας που βρίσκονται στην ιδέα ενός sandboxing. Το Sandboxing διαχωρίζει διαφορετικές διαδικασίες, αποτρέποντάς τους να αλληλεπιδρούν και να βλάπτουν ο ένας τον άλλον, περιορίζοντας έτσι αποτελεσματικά κάθε πιθανότητα εμφύτευσης κακόβουλου κώδικα και προσπερνώντας τις τρέχουσες διαδικασίες από την πραγματοποίηση επιβλαβών δραστηριοτήτων. Το Apple iOS επικεντρώνεται στον περιορισμό της πρόσβασης στο API του για εφαρμογές από το Apple Store, ενώ το Android χρησιμοποιεί το sandboxing σε υποκείμενο πυρήνα Linux. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Κρίσιμη υποδομή:

Τα κρίσιμα συστήματα υποδομής που αποτελούν τη σωστή γραμμή μιας σύγχρονης κοινωνίας και η αξιόπιστη και ασφαλής λειτουργία τους έχουν πρωταρχική σημασία για την εθνική ασφάλεια και την οικονομική ζωτικότητα. Αναλυτικότερα, το κυβερνοσύστημα αποτελεί τη ραχοκοκαλιά των κρίσιμων υποδομών ενός έθνους, πράγμα που σημαίνει ότι ένα σημαντικό συμβάν ασφαλείας στα κυβερνοσυστήματα θα μπορούσε να έχει σημαντικό αντίκτυπο στις αξιόπιστες και ασφαλείς λειτουργίες των φυσικών συστημάτων που βασίζονται σε αυτό. Τα πρόσφατα ευρήματα, όπως τεκμηριώνονται σε κυβερνητικές εκθέσεις, δείχνουν την αυξανόμενη απειλή φυσικών επιθέσεων και κυβερνοεπιθέσεων σε αριθμό και πολυπλοκότητα σε ηλεκτρικά δίκτυα και άλλα κρίσιμα συστήματα υποδομής. Η ασφάλεια στον κυβερνοχώρο που σχετίζεται με την κρίσιμη υποδομή επιδιώκει να περιορίσει τις ευπάθειες αυτών των δομών και συστημάτων.

• Τρομοκρατία από άτομο ή ομάδες που στοχεύουν σκόπιμα κρίσιμες υποδομές για πολιτικό κέρδος. Στην επίθεση στο Mumbai του Νοεμβρίου 2008, ο κεντρικός σταθμός της Βομβάης και το ξενοδοχείο Taj είχαν στοχευτεί σκόπιμα.

• Σαμποτάζ από άτομο ή ομάδες όπως πρώην υπάλληλοι, πολιτικές ομάδες εναντίον κυβερνήσεων, από περιβαλλοντικές ομάδες για το «καλό» του περιβάλλοντος, για

παράδειγμα η κατάσχεση του Διεθνούς αερολιμένα της Μπανγκόκ από διαδηλωτές. (M.Tehranipoor, C. Wang , 2011.)

• Πόλεμος πληροφόρησης – για ιδιωτική εισβολή ή για προσωπικό κέρδος ή χώρες που ξεκινούν επιθέσεις για να μαζέψουν πληροφορίες και να καταστρέψουν επίσης την υποδομή μιας χώρας. Για παράδειγμα, μια σειρά επιθέσεων στον κυβερνοχώρο που έπληξαν τον ιστότοπο των Εσθονικών οργανώσεων, συμπεριλαμβανομένου του Εσθονικού κοινοβουλίου, των τραπεζών, των υπουργείων, των εφημερίδων και των ραδιοτηλεοπτικών φορέων, εν μέσω της σειράς της χώρας με τη Ρωσία σχετικά με τη μετεγκατάσταση της σοβιετικής εποχής και των τάφων πολέμου. Μια καταστροφή ή ένας τυφώνας ή πολλά ακόμα φυσικά γεγονότα που καταστρέφουν κρίσιμες υποδομές όπως αγωγούς πετρελαίου, νερό και ηλεκτρικά δίκτυα. (M.Tehranipoor, C. Wang , 2011.)

Η κρίσιμη προστασία της υποδομής είναι δυσκολότερη από την προστασία της τεχνολογίας πληροφοριών και επικοινωνιών (ΤΠΕ), λόγω της πολυπλοκότητας διασύνδεσης αυτών των υποδομών, η οποία μπορεί να οδηγήσει σε διαφορετικά είδη προβλημάτων. Σκεφτείτε το ηλεκτρικό δίκτυο, στο οποίο οι γεωγραφικά διεσπαρμένοι τόποι παραγωγής διανέμουν ισχύ μέσω διαφορετικών σταθμών στάθμης τάσης (από υψηλότερη σε χαμηλότερη τάση) έως ότου η ενέργεια ρέει τελικά στα σπίτια μας. Τόσο οι τόποι παραγωγής και διανομής ελέγχονται συνήθως από συστήματα εποπτικού ελέγχου και απόκτησης δεδομένων (SCADA), τα οποία συνδέονται εξ αποστάσεως με κέντρα παρακολούθησης και με τα εταιρικά δίκτυα (intranets) των εταιρειών που διαχειρίζονται τις υποδομές. Το intranets συνδέεται με το Διαδίκτυο για να διευκολύνει, για παράδειγμα, την επικοινωνία με τους ρυθμιστές ισχύος και τους τελικούς πελάτες. Αυτοί οι σύνδεσμοι δημιουργούν μια διαδρομή για εξωτερικούς εισβολείς. Η πρόσβαση των χειριστών σε συστήματα SCADA εξ αποστάσεως για εργασίες συντήρησης και οι προμηθευτές εξοπλισμού διατηρούν συνδέσμους προς τα συστήματα μέσω μόντεμ. Η χρήση των παλαιών δομών που μαστίζονται από τρωτά σημεία πρόκειται να προσθέσει μια άλλη διάσταση και θα πρέπει να προταθούν λύσεις

για την προστασία της κρίσιμης υποδομής. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Καθώς η έρευνα για το κρίσιμο σύστημα είναι αρκετά νέα, οι ερευνητές εξακολουθούν να προσπαθούν να κατανοήσουν τη φύση των κρίσιμων συστημάτων υποδομής. Αυτό περιλαμβάνει την κατανόηση της κρίσιμης σημασίας στο σύστημα, την κατανόηση της αλληλεξάρτησης μεταξύ συστημάτων και υποδομών και τον εντοπισμό και τον ποσοτικό προσδιορισμό των συνεπειών των επιθέσεων στα κρίσιμα συστήματα. Λόγω της στενής εξάρτησης αυτών των συστημάτων και εκατομμυρίων χρηστών στην καθημερινή τους ζωή, είναι σημαντικό η κρίσιμη υποδομή να λειτουργεί σε 24-7 βάσεις χωρίς καμία κάμψη. Έχουν προταθεί αυτοδιαγνωστικές τεχνικές που χρησιμοποιούν καρδιακούς παλμούς, απόκριση πρόκλησης, ενσωματωμένη παρακολούθηση κρίσιμων λειτουργιών και ανίχνευση ανωμαλιών της διαδικασίας που μπορούν να συλλάβουν τυχόν σημάδια μη λειτουργικών λειτουργιών. Ένα άλλο σχετικό θέμα ενδιαφέροντος είναι η ανάπτυξη συστημάτων αυτοθεραπείας για την επιδίωξη αυτοματοποιημένης και συντονισμένης απόκρισης και ανάκαμψης επίθεσης. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Άλλοι αναδυόμενοι τομείς:

Η ασφάλεια στον κυβερνοχώρο σε ενσωματωμένα συστήματα και αισθητήρες είναι τα θέματα που έχουν λάβει όλο και μεγαλύτερη προσοχή από τη βιομηχανία και τον ακαδημαϊκό χώρο τα τελευταία χρόνια λόγω της αυξημένης χρήσης τους σε κάθε πτυχή της ζωής μας. Για παράδειγμα, οι ενσωματωμένες μικρές συσκευές που εισάγονται σε αυτοκίνητα, οικιακές συσκευές, κινητό τηλέφωνο και εξοπλισμό ήχου / βίντεο, γίνονται όλο και περισσότερο μέρος της ζωής μας. Ομοίως, οι αισθητήρες βλέπουν ευρύτερη έρευνα και εμπορικές αναπτύξεις σε στρατιωτικές, επιστημονικές και εμπορικές εφαρμογές, συμπεριλαμβανομένης της παρακολούθησης των βιολογικών οικοτόπων, της γεωργίας και των βιομηχανικών διαδικασιών. (M.Tehranipoor, C. Wang , 2011.)

Οι ανησυχίες για την ασφάλεια σε αυτούς τους τομείς διαφέρουν από τα παραδοσιακά προβλήματα ασφάλειας στον προσωπικό υπολογιστή και στους υπολογιστές επιχειρήσεων λόγω του διαφορετικού ενσωματωμένου χαρακτήρα τους και του λειτουργικού τους περιβάλλοντος. Τα ενσωματωμένα συστήματα και οι αισθητήρες είναι συχνά εξαιρετικά ευαίσθητα στο κόστος, απαιτώντας τους να χρησιμοποιούν μικρότερους επεξεργαστές που έχουν περιορισμένο χώρο για γενικά έξοδα ασφαλείας, για παράδειγμα για την αποθήκευση ενός μεγάλου κλειδιού κρυπτογράφησης. Επομένως, οι περισσότερες λύσεις για την ασφάλεια των επιχειρήσεων δεν λειτουργούν στον κόσμο του ενσωματωμένου συστήματος. Τα ενσωματωμένα συστήματα και οι αισθητήρες περιορίζονται σε πόρους σε ενέργεια, μνήμη, υπολογιστική ταχύτητα και εύρος ζώνης επικοινωνίας λόγω του μικρού μεγέθους τους. Έχουν ένα πολύ αδύναμο όριο φυσικής εμπιστοσύνης. Για παράδειγμα, εγκαθίστανται σε κατοίκους και εμπορικά ακίνητα, εκτός πεδίου, ή μεταφέρονται από τον άνθρωπο στα χέρια ή τις τσέπες τους, κάτι που επιτρέπει πολλές διαφορετικές φυσικές επιθέσεις. Χρησιμοποιούν μια στενή σύνδεση μεταξύ υλικού και λογισμικού συχνά χωρίς τη θωράκιση ενός λειτουργικού συστήματος. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Η διαφορετική ενσωματωμένη φύση των ενσωματωμένων συστημάτων και αισθητήρων έχει δημιουργήσει διαφορετικά σύνολα ευπάθειας ασφαλείας. Παράδειγμα, η περιορισμένη ισχύς της μπαταρίας σε ενσωματωμένα συστήματα τα καθιστά ευάλωτα σε επιθέσεις που εξαντλούν αυτόν τον πόρο. Η εγγύτητα των ενσωματωμένων συστημάτων σε έναν πιθανό εισβολέα δημιουργεί ευπάθειες για επιθέσεις όπου φυσικές Η πρόσβαση στο σύστημα είναι απαραίτητη. Αυτό επιτρέπει στους επιτιθέμενους να εκτελούν επιθέσεις που εμπλέκονται στην εξέταση της χρήσης του φυσικού συστήματος, του δείγματος, των επιθέσεων ανάλυσης ισχύος ή των επιθέσεων στο σύστημα διαύλου. Τα ενσωματωμένα συστήματα πρέπει να λειτουργούν σε λογικές περιβαλλοντικές συνθήκες. Λόγω του ιδιαίτερα εκτεθειμένου περιβάλλοντος λειτουργίας των ενσωματωμένων συστημάτων, υπάρχει πιθανότητα

ευπάθειας για επιθέσεις που υπερθερμαίνουν το σύστημα (ή προκαλούν άλλες περιβαλλοντικές ζημίες). (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Οι εισβολείς επαναπρογραμματίζουν ένα κλεμμένο σύστημα em-bedded για να τα χρησιμοποιήσουν για περαιτέρω κατάχρηση. Τα συνηθισμένα αντίμετρα ασφαλείας για την αποτροπή μη εξουσιοδοτημένης πρόσβασης μέσω ελέγχου ταυτότητας χρήστη, τεχνικές διατήρησης της ακεραιότητας δεδομένων μέσω κρυπτογραφιών και μηχανισμών άμυνας δικτύου αποτελούν ενεργό τομέα ενδιαφέροντος στον τομέα. Ωστόσο, η αποτροπή επιθέσεων που πραγματοποιούνται με εξέταση ή αλλαγή του φυσικού συστήματος είναι αρκετά μοναδική, για παράδειγμα τεχνικές όπως η κάλυψη, οι μέθοδοι παραθύρου και η εισαγωγή εικονικής εντολής στον κώδικα / αλγόριθμο έχουν προταθεί. Δεδομένου ότι η συνδεσιμότητα δικτύου μέσω ασύρματης ή ενσύρματης πρόσβασης είναι όλο και πιο συχνή για τα ενσωματωμένα συστήματα για τη βελτίωση της συλλογής και ενημέρωσης δεδομένων, τα τρωτά σημεία που εκμεταλλεύονται τέτοια συνδεσιμότητα δικτύου, όπως η εξάπλωση ιών και η χρήση καλωδίων, έχουν γίνει μια άλλη πηγή αυξανόμενης ανησυχίας στον τομέα. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Ο πόλεμος στον κυβερνοχώρο αναφέρεται σε πολιτικά υποκινούμενα πειρατεία για να κάνουν σαμποτάζ και κατασκοπεία. Στο βιβλίο Cyber Ware, ο πόλεμος cyber ορίστηκε ως «ενέργειες ενός έθνους-κράτους για διείσδυση σε υπολογιστές ή δίκτυα άλλου έθνους με σκοπό την πρόκληση ζημιών ή διαταραχών» Οι περισσότερες ανησυχίες για τον πόλεμο στον κυβερνοχώρο επικεντρώνονται στις παραβιάσεις της εθνικής ασφάλειας και στη σαμποτάζ των κρίσιμων υποδομών του έθνους. (M.Tehranipoor, C. Wang , 2011.)

Η προηγούμενη υπόθεση αφορά τη διεθνή κατασκοπεία όπου διαβαθμισμένες πληροφορίες που ενδέχεται να παραβιάζουν την εθνική ασφάλεια έχουν πρόσβαση παράνομα ή τροποποιούνται από μη εξουσιοδοτημένα άτομα. Η τελευταία περίπτωση αφορά πολλές πιθανές διαταραχές της κρίσιμης υποδομής του έθνους, όπως το δίκτυο

ηλεκτρικού δικτύου και το σύστημα μεταφοράς. Το 2009, πραγματοποιήθηκε μια προσομοιωμένη άσκηση με την ονομασία «cyber storm» από το Υπουργείο Εσωτερικής Ασφάλειας των ΗΠΑ. Ο σκοπός της άσκησης ήταν να δοκιμάσει την άμυνα του έθνους των ΗΠΑ ενάντια στην ψηφιακή κατασκοπεία. Η άσκηση Cyber Storm υπογράμμισε τα κενά και τα μειονεκτήματα της υπεράσπισης στον κυβερνοχώρο του έθνους. Έκτοτε, οι ερευνητές έχουν προτείνει μια σειρά από νέες προτεραιότητες όσον αφορά τη στρατηγική στον τομέα της άμυνας στον κυβερνοχώρο. Η αναγνώριση των κρίσιμων συστημάτων των ΗΠΑ έχει προταθεί για την αναγνώριση συστημάτων με δυνατότητα σύνδεσης στο Διαδίκτυο που είναι κρίσιμα για την υπεράσπιση του κυβερνοχώρου σε εθνικό επίπεδο και τυχόν αλληλεξαρτήσεις μεταξύ των συστημάτων. Έχουν προταθεί διάφορες στρατηγικές για την προστασία των κρίσιμων υποδομών των ΗΠΑ με τον εντοπισμό και την αποκατάσταση της ευπάθειας του συστήματος. (C. M. Medaglia, A. Serbanati, 2010)

ΣΥΜΠΕΡΑΣΜΑΤΑ

Οι αυξανόμενες απειλές έχουν βρεθεί σε αναδυόμενες τεχνολογίες, όπως τα μέσα κοινωνικής δικτύωσης, το cloud computing, η τεχνολογία smartphone και η υποδομή κρίσιμης σημασίας, αξιοποιώντας συχνά τα μοναδικά χαρακτηριστικά τους. Περιγράψαμε χαρακτηριστικά καθενός από τις αναδυόμενες τεχνολογίες και διάφορους τρόπους διάδοσης κακόβουλου λογισμικού σε αυτές τις νέες τεχνολογίες. Στη συνέχεια, συζητάμε για ένα κοινό σύνολο γενικών επιθέσεων που βρίσκονται στην αναδυόμενη τεχνολογία. Για παράδειγμα, καθώς οι περισσότερες από αυτές τις αναδυόμενες τεχνολογίες προσφέρουν υπηρεσίες μέσω διαδικτύου, ορισμένες από τις κοινές επιθέσεις εκμεταλλεύονται όλο και περισσότερο την ασφάλεια του προγράμματος περιήγησης μέσω κακόβουλου λογισμικού που κρύβεται μέσα σε επεκτάσεις ή ευπάθειες υπάρχουν σε γλώσσες δέσμης ενεργειών για πρόσβαση σε εμπιστευτικά δεδομένα.

Οι εισβολείς αλλάζουν επίσης τη μάχη τους από την επιφάνεια εργασίας σε άλλες πλατφόρμες, όπως κινητά τηλέφωνα, tablet PC και VoIP για να αποφύγουν τον

εντοπισμό. Ειδικά τα κινητά αυξήθηκαν απότομα τα τελευταία χρόνια με τον αυξανόμενο αριθμό χρηστών κινητών συσκευών και την πολυπλοκότητα των εφαρμογών για κινητά. Οι απάτες που χρησιμοποιούν την κοινωνική μηχανική αυξάνονται. Δημοφιλείς ιστότοποι κοινωνικής δικτύωσης όπως το Facebook, το Twitters και άλλοι έχουν χρησιμοποιηθεί όλο και περισσότερο ως μηχανισμοί παράδοσης για να κάνουν τους ανυποψίαστους χρήστες να εγκαταστήσουν ή να διαδώσουν κακόβουλο λογισμικό. Έχουν αναφερθεί περισσότερες οργανωμένες επιθέσεις μέσω της χρήσης botnets.

Καθώς ο αντίκτυπος αυτών των ζημιών είναι πολύ μεγαλύτερος από τις επιμέρους επιθέσεις, υπάρχει αυξανόμενη ανησυχία για την αποτροπή των botnets. Τα πρόσφατα στατιστικά στοιχεία δείχνουν επίσης ότι υπάρχει ένας αυξανόμενος αριθμός διαδικτυακών επιθέσεων προσαρμοσμένων σε ένα συγκεκριμένο σύστημα, για παράδειγμα σύστημα εντολών και ελέγχου, χρησιμοποιώντας γνώσεις και προσωπικό.

Επεξηγήσαμε επίσης πιθανές μελλοντικές ερευνητικές κατευθύνσεις. Καθώς όλο και περισσότεροι άνθρωποι είναι συνδεδεμένοι μέσω του Διαδικτύου, έχουν προταθεί όλα τα επίπεδα των χρηστών, συμπεριλαμβανομένων τόσο των εμπειρογνωμόνων όσο και των μη ειδικών στο υπολογιστικό σύστημα και η επινόηση ενός μηχανισμού ασφαλείας ανάλογα με τα επίπεδα εμπιστοσύνης τους. Η διαφύλαξη του απορρήτου των χρηστών έχει τονιστεί από πολλούς εμπειρογνώμονες ασφάλειας ως σημαντική μελλοντική έρευνα που θα διεξαχθεί καθώς ο αριθμός των προσωπικών πληροφοριών μέσω του Διαδικτύου έχει επεκταθεί ταχέως τα τελευταία χρόνια.

Αντί να προσπαθήσουμε να επιδιορθώσουμε ένα συγκεκριμένο πρόβλημα στο υπάρχον Διαδίκτυο και στα συστήματα υπολογιστών σταδιακά, έχουν προταθεί πιο καινοτόμες προσεγγίσεις για να δούμε «μια μεγαλύτερη εικόνα» ή να πιστεύουμε ότι «έξω από το κουτί», πολλές αποδείξεις δείχνουν ότι η ικανότητα της σημερινής σύγχρονης τεχνολογίας διαποτίζει και να μην κλιμακώνονται πλέον χρησιμοποιώντας παραδοσιακές σταδιακές προσεγγίσεις. Οι εξελίξεις του ασφαλούς Διαδικτύου επόμενης γενιάς και αξιόπιστων συστημάτων έχουν προταθεί ως σημαντικοί τομείς

έρευνας για να εξετάσουν το μέλλον. Η ανάπτυξη τεχνικών διαχείρισης ταυτότητας παγκόσμιας κλίμακας και τεχνικών ανίχνευσης για να εντοπιστεί ο αντίπαλος έχει επίσης αποκτήσει την προσοχή ως ένα σημαντικό ζήτημα που πρέπει να αντιμετωπιστεί στο μέλλον.

ΜΕΛΛΟΝΤΙΚΕΣ ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΕΡΕΥΝΑ

Με την τεράστια αύξηση της διαθεσιμότητας του Διαδικτύου και την πρόοδο των συσκευών με δυνατότητα σύνδεσης στο Διαδίκτυο, ένας αυξανόμενος αριθμός χρηστών χρησιμοποιούν το Διαδίκτυο σε όλες τις πτυχές της ζωής τους, εκθέτοντας συχνά εξαιρετικά ευαίσθητες προσωπικές πληροφορίες χωρίς να συνειδητοποιούν τις συνέπειες της κατάχρησης δεδομένων. Υποθέτουμε ότι τα ζητήματα που αφορούν το απόρρητο των τελικών χρηστών θα συνεχίσουν να αυξάνονται συνεχώς στο μέλλον, σύμφωνα με τον αυξανόμενο όγκο προσωπικών πληροφοριών μέσω του Διαδικτύου. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Επιπλέον, τα ζητήματα χρηστικότητας κερδίζουν περισσότερη προσοχή ως ένας τρόπος για να παρέχεται ένας μηχανισμός ασφαλείας που εστιάζει στον τελικό χρήστη, όπου οι χρήστες μπορούν να τα μάθουν και να τα χρησιμοποιήσουν διαισθητικά, χωρίς πολυπλοκότητα, για να προστατεύσουν τα δεδομένα τους. Βασίζεται σε σταδιακά «μπαλώματα» που διορθώνουν τα τρέχοντα ζητήματα ασφάλειας και απορρήτου και στη συνέχεια προχωρά στο επόμενο βήμα. Μερικοί πιστεύουν ότι αυτή η σταδιακή προσέγγιση δεν λειτούργησε καλά και δεν θα είναι σε θέση να καλύψει μελλοντικές ανάγκες, δεδομένου ότι το αρχικό Διαδίκτυο εφευρέθηκε για ένα πολύ διαφορετικό περιβάλλον από τον τρόπο που χρησιμοποιείται σήμερα. Μια προσέγγιση για να σκεφτείς «έξω από το κουτί» χωρίς να βασίζεσαι στο τρέχον υπολογιστικό σύστημα και στο Διαδίκτυο, αλλά έχει προταθεί να ξεκινήσεις κάτι εκ νέου για καλύτερη χρήση των ταχέως αναπτυσσόμενων απαιτήσεων του Διαδικτύου. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Η ανώνυμη φύση του Διαδικτύου έχει οριστεί ως πηγή της αυξανόμενης επίθεσης στον κυβερνοχώρο και είναι δύσκολο να εντοπιστεί. Οι τεχνικές διαχείρισης ταυτότητας και ανίχνευσης παγκόσμιας κλίμακας έχουν καταστεί ενεργός τομέας της έρευνας ως στρατηγικό σχέδιο για την αποτροπή αυξανόμενου αριθμού επιτιθέμενων στον κυβερνοχώρο στο μέλλον, ειδικά όταν εμπλέκεται η κρίσιμη υποδομή. Εξετάζουμε λεπτομερέστερα αυτές τις μελλοντικές ερευνητικές κατευθύνσεις στις ακόλουθες ενότητες. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Εστίαση στο απόρρητο:

Τα τελευταία χρόνια, το απόρρητο έχει γίνει ένα κρίσιμο ζήτημα στην ανάπτυξη συστημάτων πληροφορικής με την εξάπλωση των δικτυακών συστημάτων και του Διαδικτύου. Τώρα, το Διαδίκτυο χρησιμοποιείται σε όλες τις πτυχές της ζωής μας απαιτώντας αυξανόμενο όγκο προσωπικών πληροφοριών που πρέπει να εισαχθούν στον κυβερνοχώρο. Σύμφωνα με την ετήσια έκθεση της JP Morgan, οι παγκόσμιες πωλήσεις ηλεκτρονικού εμπορίου αυξήθηκαν με ετήσιο ρυθμό 18,5% φθάνοντας τα 954 δισεκατομμύρια δολάρια έως το 2015. Αυτή η αύξηση των διαδικτυακών αγορών υποδηλώνει ότι οι χρήστες του Διαδικτύου γίνονται πιο άνετοι να μοιράζονται τα ευαίσθητα οικονομικά τους στοιχεία, όπως αριθμούς πιστωτικών καρτών. διευθύνσεις αποστολής. Ομοίως, οι επαγγελματικοί ιστότοποι και οι ιστότοποι κοινωνικής δικτύωσης που συνδέουν άτομα με παρόμοια ενδιαφέροντα στο διαδίκτυο έχουν σημειώσει ραγδαία ανάπτυξη την τελευταία δεκαετία. Το LinkedIn, ένας επαγγελματικός ιστότοπος δικτύωσης που ιδρύθηκε τον Μάιο του 2003, έχει 250 εκατομμύρια χρήστες έως τον Ιανουάριο του 2015. Το Facebook, που κυκλοφόρησε τον Φεβρουάριο του 2004, έχει φτάσει το 1 δισεκατομμύριο ενεργούς χρήστες από τον Σεπτέμβριο του 2013. Αυτοί οι αριθμοί δείχνουν ότι οι άνθρωποι αισθάνονται όλο και πιο άνετα να βάζουν προσωπικά στοιχεία για τον εαυτό τους στο διαδίκτυο Τα άτομα φαίνονται επίσης πιο πρόθυμα να μιλήσουν για το τι θεωρούν εισβολή της ιδιωτικής

ζωής όταν ασχολούνται με διαδικτυακές δραστηριότητες. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Καθώς αυξάνεται ο όγκος των πληροφοριών στο Διαδίκτυο, οι πιθανότητες εμφάνισης συμβιβασμού της ιδιωτικής ζωής αυξάνονται επίσης. Για παράδειγμα, παρακολουθούνται οι διαδικτυακές επισκέψεις μεμονωμένων ατόμων για τη διείσδυση των πληροφοριών και την αποστολή διαφημίσεων βάσει του ιστορικού περιήγησης. Οι μέθοδοι συμβιβασμού μπορεί να κυμαίνονται από τη συλλογή στατιστικών στοιχείων για τους χρήστες, έως πιο κακόβουλες πράξεις όπως η διάδοση του spyware. Οι εγκληματίες του κυβερνοχώρου χρησιμοποιούν τους ιστότοπους κοινωνικής δικτύωσης για να κλέψουν προσωπικές πληροφορίες για να χρησιμοποιήσουν υπέρβαση παραβίασης και κλοπή ταυτότητας. Για να αποφευχθεί τέτοια διαρροή απορρήτου, αρκετοί ιστότοποι κοινωνικής δικτύωσης παρέχουν μέτρα απορρήτου. Για παράδειγμα, το Facebook παρέχει μια ρύθμιση απορρήτου για όλους τους εγγεγραμμένους χρήστες. Οι διαθέσιμες ρυθμίσεις στο Facebook περιλαμβάνουν τη δυνατότητα αποκλεισμού ορισμένων ατόμων από το να βλέπουν το προφίλ κάποιου, τη δυνατότητα επιλογής «φίλων» και τη δυνατότητα περιορισμού των ατόμων που έχουν πρόσβαση στις φωτογραφίες και τα βίντεο. Οι ρυθμίσεις απορρήτου είναι επίσης διαθέσιμες σε άλλους ιστότοπους κοινωνικής δικτύωσης, όπως το Google Plus και το Twitter. Τα παιδιά και οι έφηβοι είναι πολύ ευαίσθητα στην κακή χρήση του Διαδικτύου και τελικά διακινδυνεύουν την ιδιωτική τους ζωή. Υπάρχει μια αυξανόμενη ανησυχία μεταξύ των γονέων των οποίων τα παιδιά αρχίζουν πλέον να χρησιμοποιούν το Facebook και άλλα κοινωνικά μέσα σε καθημερινή βάση. Οι πρακτικές συλλογής πληροφοριών ιστότοπου είναι μια άλλη αυξανόμενη ανησυχία καθώς τα νεαρά άτομα είναι πιο ευάλωτα και δεν γνωρίζουν το γεγονός ότι όλες οι πληροφορίες και η περιήγησή τους μπορούν και μπορούν να παρακολουθούνται κατά την επίσκεψή τους σε ξεχωριστό ιστότοπο. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Ο στόχος της ασφάλειας που σχετίζεται με την προστασία της ιδιωτικής ζωής είναι να επιτρέψει στους χρήστες και τους οργανισμούς να εκφράζουν καλύτερα, να προστατεύουν και να ελέγχουν την εμπιστευτικότητα των προσωπικών τους

πληροφοριών, ακόμα και όταν επιλέγουν (ή απαιτούν) να τις κοινοποιήσουν σε άλλους. Μια έρευνα σε αυτό το πεδίο αφορά τον τρόπο πρόσβασης και αποκάλυψης δεδομένων ενώ προστατεύεται το απόρρητο. Πραγματοποιούνται πολλές έρευνες για τη διερεύνηση του τρόπου επιλεκτικής αποκάλυψης των δεδομένων, του τρόπου προστασίας των δεδομένων που κοινοποιούνται από τους ανθρώπους και του τρόπου απολύμανσης των δεδομένων . Ένα άλλο ρεύμα έρευνας που πραγματοποιήθηκε σε αυτόν τον τομέα αφορούσε την ανάπτυξη πλαισίου προδιαγραφών για τη δημιουργία και ενίσχυση της πολιτικής απορρήτου. Η ανάπτυξη μιας σειράς προδιαγραφών για την παροχή εγγυήσεων απορρήτου, όπως γλώσσες για τον καθορισμό πολιτικών απορρήτου, προδιαγραφές για παραβιάσεις της ιδιωτικής ζωής και εντοπισμός παραβιάσεων της ιδιωτικής ζωής είναι ένας ενεργός τομέας έρευνας. Η οικοδόμηση τεχνικών για την πολιτική δεδομένων για τη συλλογή δεδομένων, την κοινή χρήση δεδομένων και τη μετάδοση και την αντιμετώπιση παραβιάσεων απορρήτου είναι άλλοι ενεργοί τομείς έρευνας σε αυτήν την κατηγορία. (R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, 2010)

Ασφαλές internet επόμενης γενιάς:

Εδώ δεν υπάρχει αμφιβολία ότι το Διαδίκτυο ήταν ένα κοινωνικό φαινόμενο που έχει αλλάξει και συνεχίζει να αλλάζει τον τρόπο με τον οποίο επικοινωνούν οι άνθρωποι, λειτουργούν οι επιχειρήσεις, πώς αντιμετωπίζονται οι καταστάσεις έκτακτης ανάγκης και ο στρατός λειτουργεί μεταξύ άλλων. Το Διαδίκτυο είναι εύθραυστο και οι συνεχώς υπό αδιάκοπες επιθέσεις που κυμαίνονται από εκμεταλλεύσεις λογισμικού έως άρνηση υπηρεσίας. Ένας από τους κύριους λόγους για αυτές τις ευπάθειες ασφαλείας είναι ότι η αρχιτεκτονική του Διαδικτύου και τα υποστηρικτικά πρωτόκολλά της σχεδιάστηκαν κυρίως για ένα καλοήθη και αξιόπιστο περιβάλλον, με ελάχιστη ή καθόλου προσοχή σε θέματα ασφαλείας. Αυτή η υπόθεση σαφώς δεν ισχύει πλέον για το σημερινό Διαδίκτυο, το οποίο συνδέει εκατομμύρια ανθρώπους, υπολογιστές και εταιρείες σε έναν σύνθετο ιστό που καλύπτει ολόκληρο τον κόσμο. (Karlof, C., Wagner, D. 2003)

Τα τελευταία 30 χρόνια, το Διαδίκτυο υπήρξε πολύ επιτυχημένο χρησιμοποιώντας μια σταδιακή προσέγγιση όπου ένα σύστημα μετακινείται από τη μια κατάσταση στην άλλη με σταδιακά μπαλώματα. Ωστόσο, ορισμένοι πιστεύουν ότι ολόκληρη η τεχνολογία Διαδικτύου έχει φτάσει σε ένα σημείο όπου οι άνθρωποι δεν μπορούν να πειραματιστούν νέες ιδέες για την τρέχουσα αρχιτεκτονική. Για παράδειγμα, ένα μοντέλο παράδοσης βέλτιστης προσπάθειας IP δεν θεωρείται πλέον επαρκές χωρίς πρόσθετη διασφάλιση ασφάλειας. Η δρομολόγηση δεν βασίζεται πλέον σε αλγοριθμική βελτιστοποίηση, αλλά μάλλον πρέπει να ασχοληθεί με τη συμμόρφωση με την πολιτική για να φιλοξενήσει ένα ευρύ φάσμα εφαρμογών. Τα πρωτόκολλα που έχουν σχεδιαστεί χωρίς ανησυχία για την ενεργειακή απόδοση δεν μπορούν να ενσωματώσουν ενεργειακά συνειδητά ενσωματωμένα δίκτυα συστημάτων όπως τα δίκτυα αισθητήρων. Οι αρχικές προβλέψεις σχετικά με την κλίμακα του Διαδικτύου έχουν από καιρό ακυρωθεί, οδηγώντας στην τρέχουσα κατάσταση της έλλειψης διευθύνσεων IP. (C. M. Medaglia, A. Serbanati, 2010)

Έχει προταθεί ένα νέο παράδειγμα αρχιτεκτονικού σχεδιασμού που περιγράφεται ως «σχέδιο καθαρού σχιστόλιθου». Ωστόσο, ο «σχεδιασμός καθαρών πλακών» είναι να σχεδιάσει το σύστημα από το μηδέν χωρίς να συγκρατείται από το υπάρχον σύστημα, παρέχοντας την ευκαιρία να έχουμε μια αμερόληπτη ματιά στο πρόβλημα. χώρος. Ωστόσο, η κλίμακα του τρέχοντος Διαδικτύου απαγορεύει οποιεσδήποτε αλλαγές, και είναι εξαιρετικά δύσκολο να πείσει τους ενδιαφερόμενους να πιστεύουν σε έναν καθαρό σχεδιασμό και να το υιοθετήσουν. Υπάρχει υπερβολικά μεγάλος κίνδυνος που εμπλέκεται στη διαδικασία. Ο μόνος τρόπος για τον μετριασμό αυτών των κινδύνων και για να προσελκύσουμε τα ενδιαφερόμενα μέρη είναι μέσω πραγματικής επικύρωσης διαδικτύου τέτοιων σχεδίων που δείχνουν την ανωτερότητά τους έναντι των υφιστάμενων συστημάτων. Οι εταιρείες χρηματοδότησης της έρευνας, σε όλο τον κόσμο, έχουν συνειδητοποιήσει αυτήν την επιτακτική ανάγκη και μια παγκόσμια προσπάθεια για την ανάπτυξη της επόμενης γενιάς Internet πραγματοποιείται. Το Εθνικό Ίδρυμα Επιστημών (NSF) ήταν από τα πρώτα που ανακοίνωσαν το πρόγραμμα aGENI (Παγκόσμιο Περιβάλλον για Καινοτομίες Δικτύωσης) για την ανάπτυξη μιας

υποδομής για την ανάπτυξη και τη δοκιμή ιδεών δικτύωσης που αναπτύχθηκαν στο πλαίσιο του προγράμματος FIND (Future Internet Design). Η προσπάθεια του NSF ακολουθήθηκε από το πρόγραμμα FIRE (Future Internet Research and Experimentation) που υποστηρίζει πολλά έργα δικτύωσης επόμενης γενιάς στο πλαίσιο του 7ου προγράμματος-πλαισίου της Ευρωπαϊκής Ένωσης, το πρόγραμμα AKARI στην Ιαπωνία και πολλά άλλα παρόμοια προγράμματα στην Κίνα, την Αυστραλία, την Κορέα και άλλα μέρη του κόσμου. (Karlof, C., Wagner, D. 2003)

Η ιδέα «σχεδιασμός καθαρού κράτους» μπορεί να προσεγγιστεί σε διάφορους τομείς. Στον τομέα της ασφάλειας του Διαδικτύου, οι μηχανισμοί ασφάλειας τοποθετούνται ως πρόσθετη επικάλυψη πάνω από την αρχική αρχιτεκτονική και όχι ως μέρος της αρχιτεκτονικής του Διαδικτύου. Αυτό περιλαμβάνει προτάσεις και έργα που σχετίζονται με πολιτικές ασφαλείας, σχέσεις εμπιστοσύνης, ονόματα και ταυτότητες, κρυπτογραφία, anti-spam, anti-serangan και απόρρητο. Όσον αφορά τους νέους μηχανισμούς για την παράδοση περιεχομένου μέσω του Διαδικτύου, καθώς το Διαδίκτυο επόμενης γενιάς είναι έτοιμο να δει μια τεράστια αύξηση του όγκου του περιεχομένου που παρέχεται μέσω του Διαδικτύου, προτείνονται νεότερα πρότυπα για τη δικτύωση με την παράδοση περιεχομένου στο κέντρο της αρχιτεκτονικής αντί για τη σύνδεση μεταξύ φιλοξενίας, όπως στην τρέχουσα αρχιτεκτονική. Η αμφισβητούμενη έρευνα δικτύου εστιάζει ειδικά σε ετερογενή περιβάλλοντα δικτύωσης όπου η συνεχής σύνδεση από άκρο σε άκρο δεν μπορεί να θεωρηθεί όπως φαίνεται στα ασύρματα ad hoc δίκτυα. Οι συζητήσεις σε αυτόν τον τομέα σχετίζονται με δύο σημαντικές προοπτικές των μελλοντικών απαιτήσεων σχεδιασμού Διαδικτύου: Ενεργειακή απόδοση Σχεδιασμός και εφαρμογή πρωτοκόλλου και ομοσπονδία ετερογενών δικτύων δικτύωσης. Ένας άλλος τομέας είναι το πλαίσιο διαχείρισης και ελέγχου. Το τρέχον Διαδίκτυο λειτουργεί σε ένα προσαρμοσμένο πλαίσιο διαχείρισης και ελέγχου που δεν παρέχει αποτελεσματική διαχείριση και αντιμετώπιση προβλημάτων. Οι προτάσεις για το μελλοντικό Διαδίκτυο σε αυτόν τον τομέα διαφέρουν από πλήρως κεντρικές ιδέες διαχείρισης έως πιο επεκτάσιμες και κατανεμημένες ιδέες. (C. M. Medaglia, A. Serbanati, 2010)

Αξιόπιστα συστήματα

Τα περισσότερα από τα σημερινά συστήματα είναι κατασκευασμένα από αναξιόπιστα συστήματα παλαιού τύπου που χρησιμοποιούν ανεπαρκείς αρχιτεκτονικές, πρακτικές ανάπτυξης και εργαλεία. Ως εκ τούτου, δεν είναι κατάλληλα για να αντιμετωπίσουν τις επιθέσεις στον κυβερνοχώρο. Τα πράγματα χειροτερεύουν καθώς οι σύγχρονες συσκευές είναι τα ίδια δίκτυα συστημάτων και εξαρτημάτων. Πρέπει να αλληλεπιδράσουν με πολύπλοκους τρόπους με άλλα συστατικά και συστήματα, προκαλώντας μερικές φορές απροσδόκητη και δυνητικά δυσμενή συμπεριφορά. Ιστορικά, πολλά συστήματα ισχυρίστηκαν ότι διαθέτουν αξιόπιστη βάση υπολογιστών (TBC) που υποτίθεται ότι παρείχε μια κατάλληλη βάση για την προστασία των κρίσιμων στοιχείων. Για παράδειγμα, αναπτύχθηκαν κωδικοί διόρθωσης σφαλμάτων για να ξεπεραστούν τα αναξιόπιστα μέσα επικοινωνίας και αποθήκευσης. Η κρυπτογράφηση έχει χρησιμοποιηθεί για να αυξήσει την εμπιστευτικότητα και την ακεραιότητα παρά τα ασφαλή κανάλια επικοινωνίας. Ομοίως, τα τείχη προστασίας έχουν χρησιμοποιηθεί για την προστασία εσωτερικών περιουσιακών στοιχείων από εξωτερικές επιθέσεις. Ωστόσο, η ιδέα να έχουμε μια συγκεκριμένη λύση σε ένα συγκεκριμένο πρόβλημα δεν ήταν επιτυχής λόγω της συνεχούς εξέλιξης των επιθέσεων.

Ο όρος αξιόπιστα συστήματα έχουν οριστεί από το Υπουργείο Εσωτερικής Ασφάλειας (DHS) στις ΗΠΑ ως μακροπρόθεσμος στόχος που δείχνει ένα υπολογιστικό σύστημα που είναι εγγενώς ασφαλές, διαθέσιμο και αξιόπιστο, παρά τις περιβαλλοντικές διαταραχές, τα ανθρώπινα σφάλματα χρήστη και χειριστή και τις επιθέσεις από εχθρικά μέρη. Προς αυτόν τον στόχο, ο συγγραφέας υποστηρίζει την απαίτηση για ασφαλείς συνδυασμούς υλικού και λογισμικού ως ουσιαστικό στοιχείο για ένα αξιόπιστο σύστημα. Στην πρόταση, τα συστήματα και οι συσκευές μοιράζονται αποδεδειγμένες και τυπικές πληροφορίες εμπιστοσύνης που επιβεβαιώνουν την αξιοπιστία τους, γενικές λύσεις υλικού ασφάλειας με εγγύηση ασφάλειας σε όλα τα επίπεδα και συστήματα που μπορούν να προσδιορίσουν εάν θα εμπιστεύονται μια

συσκευή, ένα πακέτο λογισμικού ή ένα δίκτυο που βασίζεται σε δυναμικά αποκτημένες πληροφορίες ριζωμένη σε υλικό και πολιτικές ασφαλείας καθορισμένες από το χρήστη. Προς αυτόν τον στόχο, πολλά ερευνητικά έργα έχουν παρασυρθεί στους τομείς της αξιόπιστης τεχνικής απομόνωσης, του διαχωρισμού και της εικονικοποίησης σε υλικό και λογισμικό, αναλύσεις που θα μπορούσαν να απλοποιήσουν σημαντικά την αξιολόγηση της αξιοπιστίας πριν τεθούν σε λειτουργία εφαρμογές, ισχυρές αρχιτεκτονικές που παρέχουν αυτοδοκιμή και αυτοδιάγνωση, αυτοδιάρθρωση, συμβιβαστική αντοχή και αυτοματοποιημένη αποκατάσταση.

Τεχνικές διαχείρισης ταυτότητας και ανίχνευσης παγκόσμιας κλίμακας

Η διαχείριση ταυτότητας είναι το έργο του ελέγχου πληροφοριών σχετικά με τους χρήστες σε υπολογιστές. Τέτοιες πληροφορίες περιλαμβάνουν πληροφορίες που πιστοποιούν την ταυτότητα ενός χρήστη, πληροφορίες που περιγράφουν πληροφορίες και ενέργειες στις οποίες επιτρέπεται η πρόσβαση ή / και η εκτέλεση. Περιλαμβάνει επίσης τη διαχείριση περιγραφικών πληροφοριών σχετικά με το χρήστη και πώς και από ποιον μπορούν να προσπελαστούν και να τροποποιηθούν αυτές οι πληροφορίες. Οι διαχειριζόμενες οντότητες συνήθως περιλαμβάνουν χρήστες, υλικό και πόρους δικτύου και ακόμη και εφαρμογές. Υπάρχουν πολλές τρέχουσες προσεγγίσεις στη διαχείριση ταυτότητας. Για παράδειγμα, πολλοί ιστότοποι χρησιμοποιούν διαδικασία σύνδεσης με συνδυασμό ονόματος χρήστη και κωδικού πρόσβασης για την προβολή μόνο κατάλληλων χρηστών για είσοδο στην υπηρεσία.

Ωστόσο, πολλές από αυτές τις εργασίες δεν είναι ακόμη πλήρως διαλειτουργικές με άλλες υπηρεσίες σε διαφορετικούς οργανισμούς και επεκτάσιμες. Απευθύνονται μόνο σε μία χρήση ή περιορίζονται με άλλους τρόπους. Έχει επισημανθεί ότι λόγω της έλλειψης επαρκούς διαχείρισης ταυτότητας είναι εξαιρετικά δύσκολο να εντοπιστεί η κλοπή ταυτότητας. Η διαχείριση ταυτότητας παγκόσμιας κλίμακας αφορά τον εντοπισμό και τον έλεγχο ταυτότητας οντοτήτων όπως άτομα, συσκευές υλικού, κατανεμημένοι αισθητήρες και εφαρμογές λογισμικού κατά την πρόσβαση σε κρίσιμη

τεχνολογία πληροφοριών συστήματα από οπουδήποτε. Η παγκόσμια κλίμακα Theterm έχει ως στόχο να τονίσει τη διεισδυτική φύση των ταυτοτήτων, λόγω της αυξανόμενης χρήσης κινητών τηλεφώνων και ενσωματωμένων αισθητήρων σε παντού της καθημερινής μας ζωής. Αυτό συνεπάγεται επίσης την ύπαρξη ταυτοτήτων σε ομοσπονδιακά συστήματα που μπορεί να είναι πέρα από τον έλεγχο οποιουδήποτε μεμονωμένου οργανισμού. Σε συνδυασμό με την ανάπτυξη της διαχείρισης παγκόσμιας ταυτότητας, μια τεχνική απόδοσης επίθεσης θα μπορούσε να βοηθήσει στον προσδιορισμό της ταυτότητας ή της θέσης ενός εισβολέα ή ενός ενδιάμεσου επιτιθέμενου.

Στην τεχνική φιλτραρίσματος Ingress, αναλύονται οι διευθύνσεις IP προέλευσης όλων των εισερχόμενων πακέτων στο δρομολογητή της εταιρείας. Τυχόν πακέτα που περιέχουν ύποπτες διευθύνσεις IP πηγής ύποπτων ή αποκλεισμένων. Ομοίως, οι τεχνικές φιλτραρίσματος Egress φιλτράρουν κάθε κυκλοφορία εξερχόμενων επιθέσεων. Η σήμανση είναι μια άλλη συνήθως χρησιμοποιούμενη τεχνική ανίχνευσης. Ένα σημάδι, συνήθως μια διεύθυνση IP ή οι άκρες της διαδρομής που διέσχισε το πακέτο για να φτάσει στο δρομολογητή, εισάγεται σε ένα πακέτο και στη συνέχεια χρησιμοποιείται για τον εντοπισμό της πηγής της επίθεσης. Ωστόσο, επικρίνεται ότι οι περισσότερες τρέχουσες μέθοδοι ανίχνευσης λειτουργούν καλά μόνο για μια μόνο συνεταιριστική άμυνα και οι εξειδικευμένοι επιτιθέμενοι αποφεύγουν εύκολα τα πιο πρόσφατα χρησιμοποιούμενα συστήματα παρακολούθησης, τροποποιώντας τις επικεφαλίδες διευθύνσεις IP. Η ανάπτυξη ενός συστήματος ανίχνευσης παγκόσμιας κλίμακας με έναν αμυντικό μηχανισμό που μπορεί να εντοπίσει και μπλοκ εξελισσόμενες υπογραφές πακέτων παρατίθενται λύσεις που απαιτούνται για το μελλοντικό υπολογιστικό περιβάλλον.

Η τεχνική Provenance είναι μια άλλη αξιοσημείωτη που έχει αναδυθεί και παρέχει τη δυνατότητα εντοπισμού των αλλαγών χρόνου ζωής και του μετασχηματισμού πόρων που σχετίζονται με τον υπολογιστή, όπως υλικό, λογισμικό, έγγραφα, βάση δεδομένων, δεδομένα και άλλες οντότητες. Η προέλευση στοχεύει στην παροχή καλών γνώσεων σχετικά με τις πηγές και τους ενδιάμεσους επεξεργαστές των δεδομένων. Αυτό

συμβάλλει στην πρόσβαση στην αξιοπιστία και την αξιοπιστία των δεδομένων κατά τη διαδικασία λήψης αποφάσεων. Προς αυτόν τον στόχο, έχουν προταθεί διάφορες ιδέες. Στον τομέα της γενεαλογίας δεδομένων, οι ερευνητές προτείνουν τη χρήση κατευθυνόμενων γραφημάτων για τη σύνδεση μεταξύ των ιστορικών εξαρτήσεων των δεδομένων μέσω του κύκλου ζωής των δεδομένων. Οι εξελίξεις του εργαλείου προτείνονται επίσης για να βοηθήσουν στην ανίχνευση και τον εντοπισμό του πού πηγαίνουν οι πόροι και του τρόπου χρήσης τους. Σε άλλους τομείς, οι ερευνητές προτείνουν ότι απαιτείται η ανάπτυξη τεχνικών για την παρακολούθηση των αρχικών πηγών οποιωνδήποτε μεταγενέστερων αλλαγών, όπως τροποποιήσεις σε πόρους καθ 'όλη τη διάρκεια του κύκλου ζωής των δεδομένων. Προτείνεται ότι τα τρέχοντα συστήματα ελέγχου έκδοσης ή οι τεχνικές που χρησιμοποιούνται στη μετάφραση φυσικής γλώσσας και τη συμπίεση αρχείων θα μπορούσαν να είναι χρήσιμα για την ανάπτυξη απαιτούμενων τεχνικών σε αυτόν τον τομέα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1) Karlof, C., Wagner, D. 2003. *Secure routing in wireless sensor networks: Attacks and countermeasures.*

2) Lee, S., Asano, T., & Kim, K. 2006. *RFID mutual authentication scheme based on synchronized secret information*.

3) Smith, S. 2017. *The Internet of Risky Things. Trusting the Devices That Surround Us.*

4) Want, R. 2006. *An Introduction to RFID Technology. Pervasive Computing*, IEEE 5.1.

5) Fadi Al-Turjman 2019. *Security in IoT-Enabled Spaces*.

6) Carlo Maria Medaglia, Alexandru Serbanati, 2010. *An Overview of Privacy and Security Issues in the Internet of Things.*

7) Mudassar Ahmad, Tanveer Younis, Muhammad Asif Habib, Rehan Ashraf, Syed Hassan Ahmed, 2019. *A Review of Current Security Issues in Internet of Things*

8) Internet Security Threats Report. Symantec,http://www.symantec.com/threatreport/, last accessed: June 2013.

9) M.Tehranipoor, C. Wang, Introduction to Hardware Security and Trust, Springer, 2011.

10) H.Mouratidis, Secure by design: Developing secure software systems from the group up, Intern. J. Secure Software Eng. 2 (3) (2011) 23–41.

11) W. Stallings, Cryptography and Network Security Principles and Practices, third edition, Pearson Educations, 2010.

12) F.T. Sheldon, V. Vishik, Moving toward trustworthy systems: R&D essentials, IEEE Comput. Mag. (2010)

13) T. Rubya, N. Prema Latha, B. Sangeetha, A survey on recent security trends using quantum cryptography, IJCSE 3 (8) 2011

14) N. Potlapally, Hardware security in practice: Challenges and opportunities, in: HOST 2011

15) R.Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, Trustworthy hardware: Identifying and classifying hardware trojans, IEEE Comput. 43 (10) 2010