234 – Ασφάλεια & Ιδιωτικότητα στο Διαδίκτυο του Μέλλοντος

Ασφάλεια Υπολογισμού στις Ακμές (Edge Computing Security)

Κυριάκος Κρητικός
Αναπλ. Καθηγητής
Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

Περίγραμμα

- Εισαγωγή
- Αρχιτεκτονική
- Ζητήματα Ασφάλειας
- Τρωτότητες
- Είδη Επιθέσεων
- Αντίμετρα
- Προκλήσεις & Μελλοντική Έρευνα

Εισαγωγή

- Χιλιάδες IoT συσκευές μπορεί να αναπτυχθούν στα πλαίσια μιας μεγάλης πόλης
- Επίσης, εκατομμύρια IoT συσκευές είναι διασυνδεδεμένες στο διαδίκτυο
- Αν και οι ορισμένες από αυτές τις συσκευές έχουν κάποιες υπολογιστικές δυνατότητες, σε καμία περίπτωση δεν μπορούν να φέρουν εις πέρας πολύπλοκες υπολογιστικές εργασίες
  - Πχ. έξυπνες ταξιδιωτικές διευθετήσεις
- Επομένως, υπάρχει η ανάγκη για μια πανίσχυρη υπολογιστική πλατφόρμα που θα συμπληρώνει τις IoT συσκευές και θα εκμεταλλεύεται τα δεδομένα που παράγουν προς ολοκλήρωση των πολύπλοκων υπολογιστικών εργασιών

Εισαγωγή

- Το υπολογιστικό νέφος είναι μια τέτοια πλατφόρμα που συγκεντρώνει τεράστια υπολογιστική ισχύ ενώ επιτρέπει την απεριόριστη κλιμάκωση των εφαρμογών
- Όμως, επειδή είναι κεντρικοποιημένη και εξαρτάται από το διαδίκτυο, έχει περιορισμένο εύρος ζώνης ενώ η χρήση της οδηγεί σε μεγάλες καθυστερήσεις λόγω της απόστασης των κέντρων δεδομένων από τους τελικούς χρήστες & συσκευές
- Επομένως, δεν μπορεί να καλύψει τις ανάγκες διαφόρων ειδών εφαρμογών (πχ. έξυπνα συστήματα μεταφοράς ή ενέργειας)

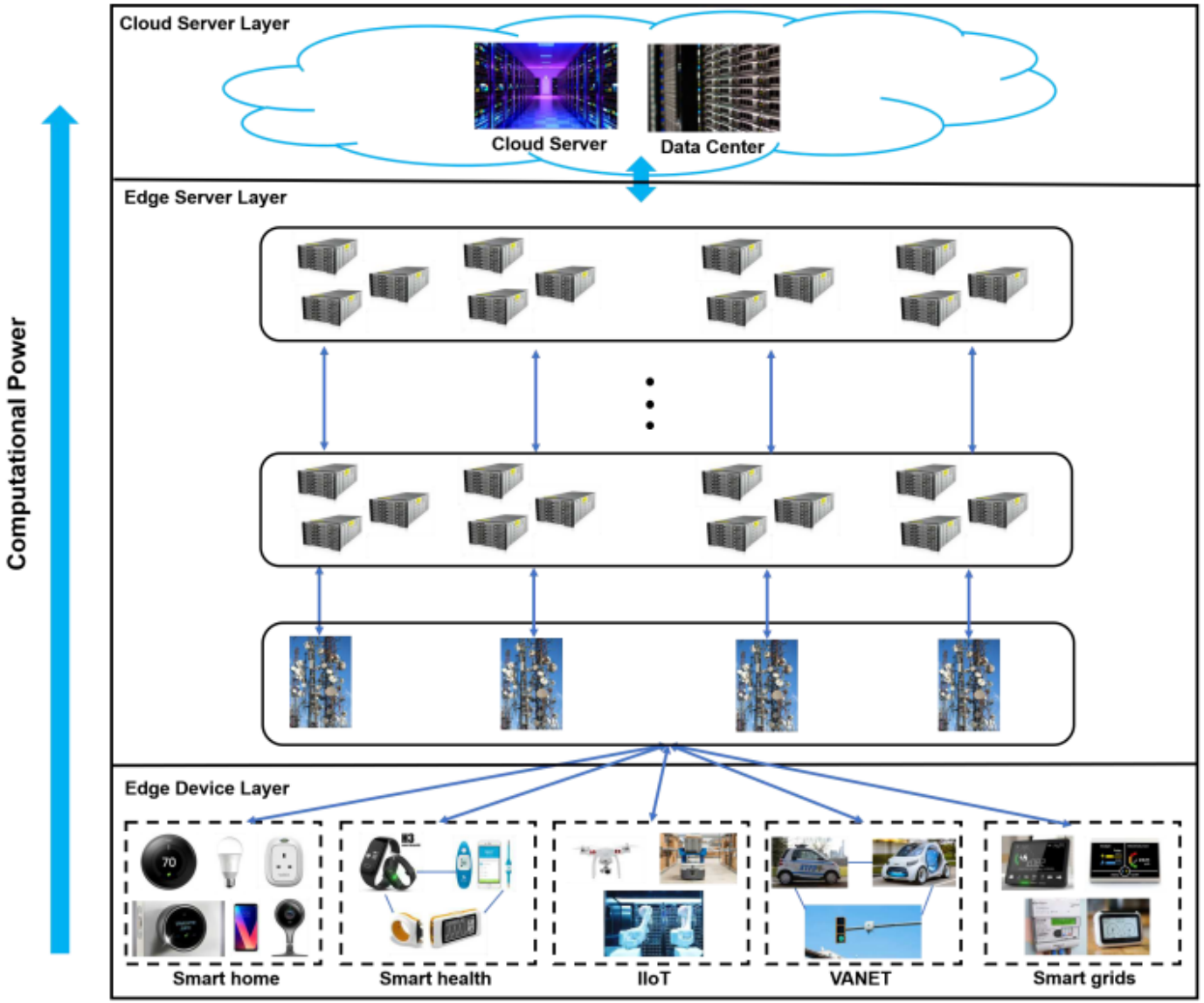
Εισαγωγή

- Το πρόβλημα αυτό επιλύεται μέσω της εισαγωγής μιας επέκτασης του υπολογιστικού νέφους όπου εξυπηρετητές στην ακμή του δικτύου, κοντά στις τελικές συσκευές, είναι σε θέση να πραγματοποιήσουν υπολογιστικές εργασίες, επιτρέποντας την διενέργεια υπολογισμών σε τοπικό επίπεδο
- Με αυτό τον τρόπο μειώνεται στο ελάχιστο η καθυστέρηση ενώ η χρήση πολλαπλών τέτοιων εξυπηρετητών που είναι κατανεμημένοι επιτρέπει την επιζητούμενη αύξηση του εύρους ζώνης
- Επίσης, επιτυγχάνεται επίγνωση θέσης ενώ καλύπτονται και σενάρια κινητικότητας
- Η επέκταση αυτή ονομάζεται υπολογισμός στις ακμές του δικτύου (edge computing)

Αρχιτεκτονική

- Αποτελείται από 3 επίπεδα
  - Επίπεδο συσκευών ακμής (Edge Device Layer – EDL)
  - Επίπεδο εξυπηρετητών ακμής (Edge Server Layer – ESL)
  - Επίπεδο εξυπηρετητών νέφους (Cloud Server Layer – CSL)

Αρχιτεκτονική



Πηγή: [1]

Επίπεδο Συσκευών Ακμής

- Αποτελείται από συσκευές ακμής που διαχωρίζονται σε IoT συσκευές και κινητές συσκευές
  - Οι IoT συσκευές είναι ελαφριές και συνδέονται με εξυπηρετητές ακμών (2ο επίπεδο) μέσω ασυρμάτων πρωτοκόλλων (πχ. 4G/5G, WiFi, Bluetooth)
    - Βασίζονται σε ΛΣ πραγματικού χρόνου (Real-Time Operating Systems) που δεν επιτρέπουν τον προγραμματισμό
    - Παραδείγματα: συσκευές έξυπνου σπιτιού, παρακολούθησης υγείας, έξυπνες κάρτες αποθηκών
  - Οι κινητές συσκευές έχουν καλύτερα ΛΣ (πχ. Android) που επιτρέπουν τον προγραμματισμό εφαρμογών
    - Παραδείγματα: κινητά τηλέφωνα, τάμπλετ και κεντρικοί ελεγκτές έξυπνων οχημάτων
- Οι συσκευές ακμής διεκπεραιώνουν λειτουργίες διαίσθησης (sensing), ενεργοποίησης (actuation) και ελέγχου (control)

Επίπεδο Εξυπηρετητών Ακμής

- Το επίπεδο αυτό είναι ιεραρχικό με 3 υπο-επίπεδα
- Όσο ανεβαίνουμε προς τα πάνω, έχουμε εξυπηρετητές ακμής με ακόμη περισσότερες δυνατότητες
- Το χαμηλότερο επίπεδο περιλαμβάνει κυρίως ασύρματους σταθμούς βάσης (base stations) & σημεία πρόσβασης (access points)
  - Κύρια ευθύνη: λήψη δεδομένων από συσκευές ακμής και προώθησή τους στο επόμενο υπο-επίπεδο με χρήση διαφορετικών ασύρματων διεπαφών

Επίπεδο Εξυπηρετητών Ακμής

- Στο μεσαίο υπο-επίπεδο πραγματοποιείται η εκτέλεση υπολογιστικών εργασιών (πχ. επεξεργασίας & ανάλυσης δεδομένων)
  - Αν, όμως, κάποια λειτουργία είναι αρκετά βαριά, τότε προωθείται (εκφόρτωση εργασιών) σε ένα εξυπηρετητή στο υψηλότερο υπο-επίπεδο
- Στο υψηλότερο υπο-επίπεδο βρίσκονται οι εξυπηρετητές με τις μεγαλύτερες υπολογιστικές ικανότητες
- Εν γένει, οι εξυπηρετητές στα 2 υψηλότερα υπο-επίπεδα αναλαμβάνουν διάφορα είδη εργασιών όπως ταυτοποίηση, εξουσιοδότηση, αναλυτική δεδομένων, αποθήκευση δεδομένων & εκφόρτωση εργασιών
- Όταν ολοκληρωθούν οι εργασίες, τα αποτελέσματα προωθούνται πίσω σε αντίστροφη πορεία

Επίπεδο Εξυπηρετητών Νέφους

- Περιλαμβάνει πανίσχυρους εξυπηρετητές που μπορούν να φέρουν εις πέρας πολύπλοκες & βαριές εργασίες
- Αυτές εκφορτώνονται από εξυπηρετητές ακμών του μεσαίου επιπέδου

Ζητήματα Ασφάλειας

- Αν και ο υπολογισμός στις ακμές του δικτύου φέρει αρκετά πλεονεκτήματα, αυξάνει από την άλλη μεριά την συνολική επιφάνεια των επιθέσεων διότι η κατανομή του συστήματος μεγαλώνει ενώ το επίπεδο ασφάλειας ανά επίπεδο ή μεμονωμένη μονάδα μπορεί να είναι ετερογενές
- Εν γένει, τα ζητήματα ασφάλειας που αφορούν αυτό το είδος υπολογισμού μπορούν να ιδωθούν υπό το πρίσμα 4 γωνιών

Ζητήματα Ασφάλειας

- Αδύναμη Υπολογιστική Δύναμη (Weak Computation Power)
  - Οι συσκευές ακμής δεν έχουν την ίδια δυναμικότητα με εξυπηρετητές νέφους
    - Περισσότερο ευάλωτες σε υπάρχουσες γνωστές επιθέσεις
  - Επίσης, έχουν εύθραυστα συστήματα προστασίας

Ζητήματα Ασφάλειας

- Άγνοια Επιθέσεων (Attack Unawareness)
  - Πολλές IoT συσκευές δεν έχουν γραφικές διεπαφές (UIs), αν και ορισμένες μπορεί να περιλαμβάνουν απλές LED οθόνες
  - Επομένως, οι χρήστες τους δεν θα μπορούν να καταλάβουν αν οι συσκευές τους έχουν πέσει θύμα επίθεσης
    - Πχ. έχουν παραβιαστεί ή ακόμη και κλείσει

Ζητήματα Ασφάλειας

- Ετερογένειες πρωτοκόλλων και λειτουργικών συστημάτων (OS & protocol heterogeneity)
  - Αυτή η μεγάλη διαφοροποίηση χωρίς ύπαρξη κάποιας προτυποποίησης εμποδίζει τον σχεδιασμό ενιαίου και ολοκληρωμένου μηχανισμού προστασίας

Ζητήματα Ασφάλειας

- Μη εκλεπτυσμένος έλεγχος πρόσβασης (coarse-grained access control)
  - Τα κλασικά μοντέλα πρόσβασης (πχ. RBAC) εστιάζουν σε 4 βασικά δικαιώματα
    - Μη εγγραφή & ανάγνωση, μόνο ανάγνωση, μόνο εγγραφή, εγγραφή & ανάγνωση
  - Συνήθως αναθέτουν τα δικαιώματα αυτά σε ρόλους χρηστών
  - Όμως, τα συστήματα & εφαρμογές προγραμματισμού στις ακμές του δικτύου είναι αρκετά πολύπλοκα και απαιτούν εκλεπτυσμένη πρόσβαση
    - Ποιος μπορεί να έχει πρόσβαση σε ποια συσκευή για να κάνει τί και πότε και πώς
    - Αυτό απαιτεί την εφαρμογή μοντέλων πρόσβασης, όπως ABAC, που είναι πιο δύσκολο, πολύπλοκο και κοστοβόρο να εφαρμοστούν σε τέτοια περιβάλλοντα

Βασικές Τρωτότητες

- Ουσιαστικά 5 είναι οι κύριες αιτίες που προετοιμάζουν τον χώρο για την διενέργεια των επιθέσεων λόγω των τρωτοτήτων που εισάγουν
  - Σχεδιαστικά σφάλματα στο επίπεδο των πρωτοκόλλων επικοινωνίας
  - Σφάλματα στο επίπεδο της υλοποίησης
  - Τρωτότητες στο επίπεδο του κώδικα
  - Συσχετίσεις δεδομένων
  - Έλλειψη εκλεπτυσμένου ελέγχου πρόσβασης

Σχεδιαστικά Σφάλματα Πρωτοκόλλων

- Ένα πρωτόκολλο προσφέρει υποστήριξη τόσο στην επικοινωνία όσο και στην επεξεργασία των δεδομένων
  - Οπότε επιτρέπει την εξασφάλιση μιας ασφαλούς οικολογίας υπολογισμών στην ακμή του δικτύου
  - Όμως, τα περισσότερα πρωτόκολλα που χρησιμοποιούνται σε αυτό το είδος υπολογισμού δεν έχουν σχεδιαστεί με γνώμονα την ασφάλεια αλλά εστιάζουν στην εμπειρία χρήστη και την ωφέλεια
  - Επομένως, γίνονται εύκολα εκμεταλλεύσιμα από επιτιθέμενους που μπορούν να διενεργήσουν διάφορα είδη επιθέσεων
    - DDoS για τον περιορισμό της διαθεσιμότητας ή το κλείσιμο των συσκευών/εξυπηρετητών ακμής
    - Πλήρης έλεγχος συσκευών/εξυπηρετητών ακμής

Σφάλματα στο Επίπεδο Υλοποίησης

- Ακόμα και αν ένα πρωτόκολλο μπορεί μαθηματικά να αποδεικνύεται ασφαλές, η υλοποίησή του μπορεί να είναι λανθασμένη
- Κοινά λάθη:
  - Παρεξήγηση των θεμελιώσεων σχετικών με το πρωτόκολλο (protocol foundations)
  - Εισαγωγή προσαρμοστικών ασυνεπειών (adaptivity inconsistencies) κατά την μετανάστευση του πρωτοκόλλου σε πλατφόρμες υπολογισμού στις ακμές του δικτύου
- Αποτέλεσμα:
  - Παράκαμψη των χαρακτηριστικών ασφάλειας που ένα πρωτόκολλο υποτίθεται προσφέρει

Τρωτότητες στο Επίπεδο Κώδικα

- Εν γένει, ένας κώδικας είναι μια υλοποίηση απαιτούμενης λειτουργικότητας με συνήθεις ατέλειες
  - Προγραμματιστικά σφάλματα
  - Τρωτότητες ασφάλειας (πχ. μη έλεγχος δεδομένων)
- Τα προβλήματα αυτά οδηγούν σε τερματισμό προγράμματος ή διαβρώσεις της κύριας μνήμης ή εξασθένιση της ακεραιότητας των δεδομένων
  - Παραδείγματα: υπερχείλιση στοίβας/σωρού, χρήση εκκρεμούς δείκτη (dangling pointer)
- Επιπλέον, ένας επιτιθέμενος μπορεί να τα εκμεταλλευτεί για να πάρει τον έλεγχο μιας συσκευής/εξυπηρετητή (πχ. μέσω έκχυσης κακόβουλου κώδικα σε περίπτωση υπερχείλισης στοίβας)

Συσχετίσεις Δεδομένων

- Τα παραγόμενα δεδομένα, εκτός από ότι είναι μεγάλα, θα πρέπει να προστατευτούν, ιδιαίτερα τα ευαίσθητα ή προσωπικά
- Ακόμη και αν υπάρχει διαχωρισμός των δεδομένων και καλύτερο επίπεδο προστασίας των ευαίσθητων δεδομένων, υπάρχει πάντοτε ο κίνδυνος
  - Είτε κρυμμένων συσχετίσεων μεταξύ ευαίσθητων και μη δεδομένων
  - Είτε λανθασμένης απάλειψης των συσχετίσεων αυτών
- Επομένως, ο επιτιθέμενος μπορεί είτε να ανακαλύψει συσχετίσεις ώστε να εξάγει τα ευαίσθητα δεδομένα (πχ. μέσω πλευρικών καναλιών) ή ακόμη και να τα πειράξει (πχ. μέσω έκχυσης κακών δεδομένων)

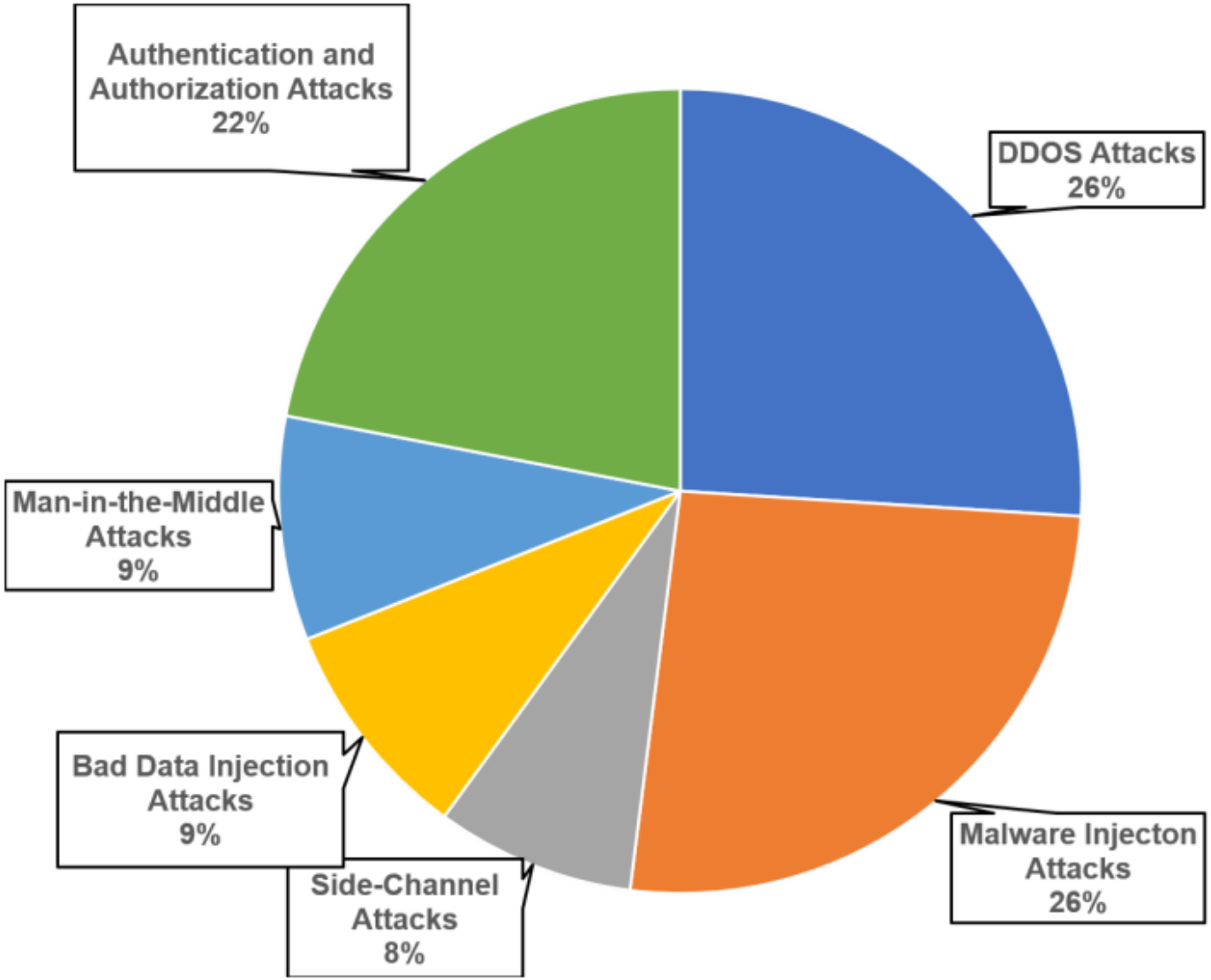
Έλλειψη Εκλεπτυσμένου Ελέγχου Πρόσβασης

- Τα τρέχοντα συστήματα edge computing είτε εφαρμόζουν μη εκλεπτυσμένο έλεγχο πρόσβασης είτε κανέναν έλεγχο πρόσβασης
- Όμως, όπως αναλύθηκε πριν, ο εκλεπτυσμένος έλεγχος πρόσβασης είναι μια αναγκαιότητα λόγω της μεγάλης κατανομής του συστήματος, της ύπαρξης μυριάδων συσκευών & χρηστών καθώς και της εν γένει πολυπλοκότητας του περιβάλλοντος χρήσης (context of use)
- Καθώς αυξάνει η επιφάνεια των τρωτοτήτων, η έλλειψη ενός τέτοιου μηχανισμού ασφάλειας διευκολύνει την διενέργεια και επιτυχία επιθέσεων, όπως ενδιάμεσου & εξουσιοδότησης

Επιθέσεις

- Έχουν δραστική αύξηση πρόσφατα
- Μόνο το 2017 πραγματοποιήθηκαν 159.700 επιθέσεις σε υποδομές υπολογισμού στις ακμές του δικτύου
- Όλες οι επιθέσεις εμπίπτουν σε 6 κατηγορίες:
  - Κατανεμημένης άρνησης υπηρεσίας (DDoS)
  - Πλευρικού καναλιού (side-channel)
  - Έκχυσης κακόβουλου λογισμικού (malware injection)
  - Ταυτοποίησης και εξουσιοδότησης (authentication & authorization)
  - Ενδιάμεσου (man-in-the-middle – MitM)
  - Κακών δεδομένων (bad data)

Κατανομή Επιθέσεων



Πηγή: [1]

Παραδείγματα Επιθέσεων

- Ο ιός Mirai μόλυνε 65.000 IoT συσκευές λόγω τρωτοτήτων ταυτοποίησης
- Οι συσκευές έγιναν botnets για την διενέργεια DDoS επιθέσεων εναντίον εξυπηρετητών δικτύου
- Αυτό οδήγησε σε κλείσιμο 178.000 τομέων

Παραδείγματα Επιθέσεων

- Παρόμοιοι ιοί με τον Mirai, όπως οι IoTReaper & Hajime, μόλυναν 378 εκατομ. IoT συσκευές το 2017 και έχουν χρησιμοποιηθεί για την διενέργεια DDoS επιθέσεων

Αντίκτυπο Επιθέσεων

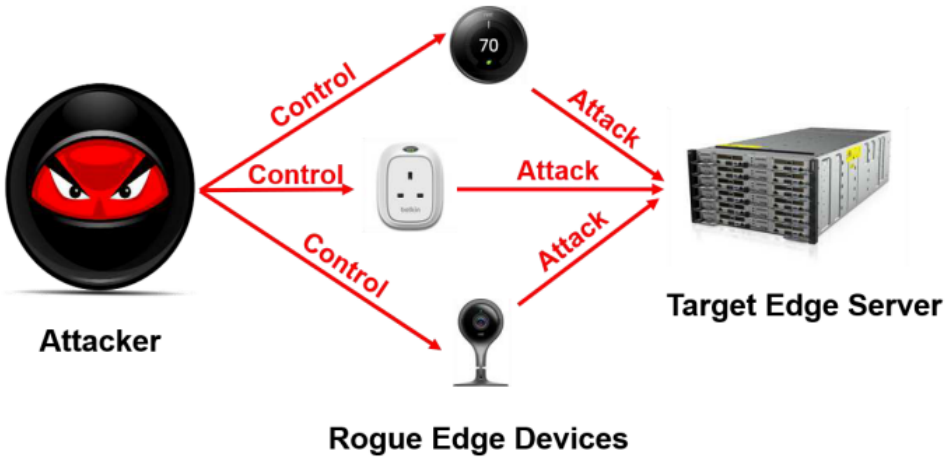
- 100 εκατ. δολάρια μέχρι τον Σεπτέμβριο του 2018
- Αλλά οι ζημιές υπολογίζονται πως είναι ακόμη περισσότερες από τις αναφερόμενες

Είδη Επιθέσεων – DDoS

- *Σκοπός*: περιορισμός διαθεσιμότητας υπηρεσίας & παρεμπόδιση εξυπηρέτησης νόμιμων/έγκυρων χρηστών
- Οι εξυπηρετητές ακμής είναι πιο τρωτοί από τους εξυπηρετητές νέφους διότι δεν έχουν την απαραίτητη ισχύ να διατηρούν ισχυρά συστήματα προστασίας
- Οι υπηρεσίες που προσφέρουν σε τελικές συσκευές ενδέχεται να είναι λανθασμένες ως προς την διαμόρφωση ασφάλειάς τους λόγω της περιορισμένης ισχύς του υλικού (hardware) τους και το ετερογενές υλικολογισμικό (firmware) τους

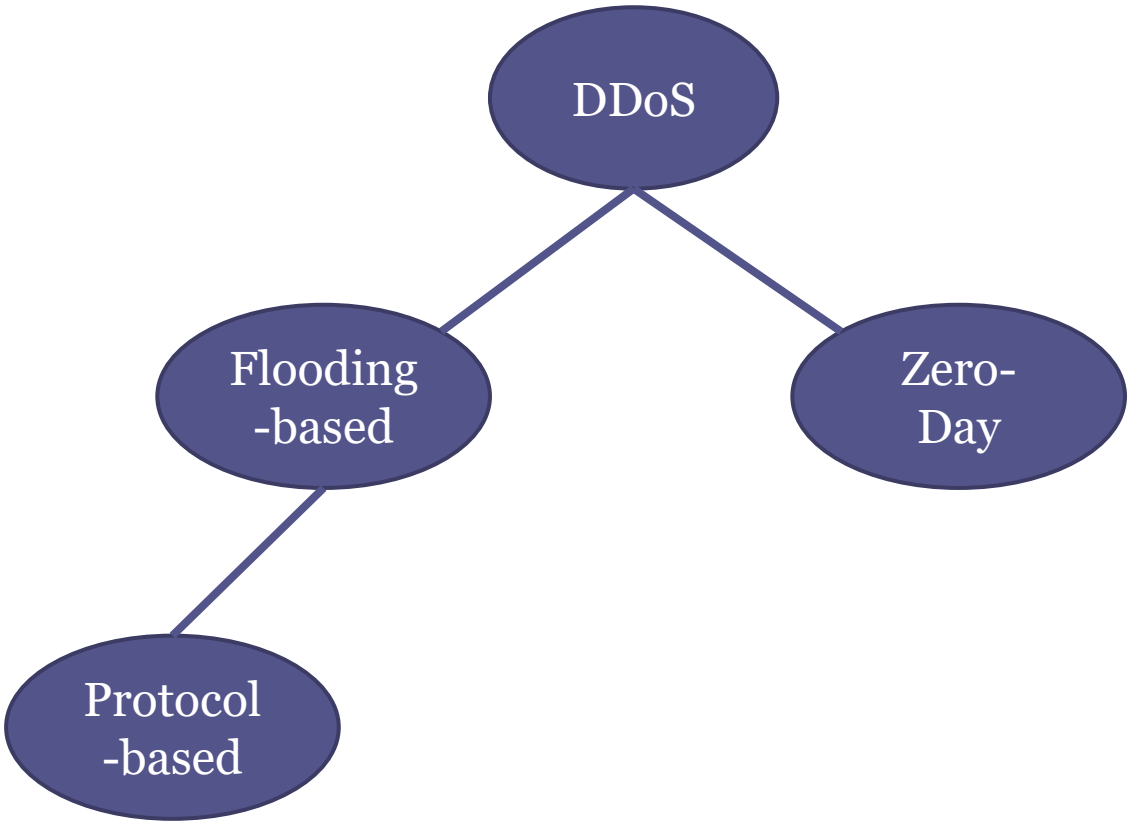
Είδη Επιθέσεων – DDoS

- Μια τέτοια επίθεση συνήθως αρχίζει με κακόβουλες συσκευές ακμής που επιτίθενται σε άλλες για να πάρουν τον έλεγχό τους
- Μόλις δημιουργηθεί ένα botnet από συσκευές ακμής, πραγματοποιείται η επίθεση DDoS που στοχεύει σε κάποιον εξυπηρετητή ακμής



Πηγή: [1]

Είδη Επιθέσεων DDoS



Είδη Επιθέσεων - DDoS

- Μπορούν να ταξινομηθούν σε
  - *επιθέσεις πλημμυρίσματος (flooding-based attacks)*
    - οφείλονται σε σφάλματα πρωτοκόλλου
  - *επιθέσεις μηδενικής ημέρας (zero-day attacks)*
    - οφείλονται σε σφάλματα κώδικα

Επιθέσεις Πλημμυρίσματος

- Στοχεύουν να κατακλείσουν έναν εξυπηρετητή με ένα μεγάλο αριθμό από δύσμορφα ή κακόβουλα πακέτα δικτύου
- Ταξινομούνται συνήθως ανάλογα με το είδος του πρωτοκόλλου που χρησιμοποιείται:
  - UDP, ICMP, TCP/SYN, HTTP
  - Περιλαμβάνουν τις ping-of-death & Slowloris

HTTP Επιθέσεις Πλημμυρίσματος

- Είναι 2 ειδών:
  - Η κλασική HTTP επίθεση αφορά την αποστολή ενός μεγάλου όγκου από αιτήσεις HTTP (με οποιοδήποτε HTTP verb ή συνδυασμό τους) σε έναν εξυπηρετητή ακμής ώστε να τον «γονατίσει»
  - Η Slowloris επίθεση αφορά την δημιουργία πολλαπλών συνδέσεων HTTP με τον εξυπηρετητή θύμα όπου αποστέλλεται μόνο πληροφορία κεφαλίδας και όχι το σώμα της αίτησης
    - Ο εξυπηρετητής διατηρεί την κάθε σύνδεση σε ξεχωριστή διαδικασία μέχρι ο συνολικός αριθμός των συνδέσεων να φθάσει το άνω όριο (maximum connection pool size)
      - το γεγονός αυτό οδηγεί στο κλείσιμό του (shut down)

Μηδενικής Μέρας DDoS Επίθεση

- Αποτελεί πιο προηγμένο είδος επίθεσης και ποιο δύσκολο στην υλοποίηση
- Θα πρέπει να ανιχνευθεί από τον επιτιθέμενο πρώτα μια άγνωστη τρωτότητα για την οποία δεν έχει αναπτυχθεί μηχανισμός αντιμετώπισης
- Έπειτα, σχεδιάζεται και υλοποιείται η επίθεση ώστε να περιορίσει την διαθεσιμότητα του εξυπηρετητή στο ελάχιστο
- Παράδειγμα:
  - Η τρωτότητα CVE-2010-3972 οδηγούσε σε υπερχείλιση στοίβας στον IIS 7.0 & 7.5 οδηγώντας στην παύση του

Είδη Επιθέσεων – Επίθεση Πλευρικού Καναλιού

- Είδος επίθεσης όπου εκμαιεύεται έξτρα πληροφορία με βάση τον καθιερωμένο τρόπο που υλοποιείται / λειτουργεί ένας αλγόριθμος ή ένα σύστημα σε αντίθεση με σφάλματα στην σχεδίαση ή υλοποίησή του
  - Παραδείγματα πληροφορίας:
    - Χρονισμού, κατανάλωσης ενέργειας, ήχου, ευαίσθητων δεδομένων
- Η βασική αρχή είναι πως οι φυσικές επιδράσεις που προκαλούνται από την λειτουργία ενός κρυπτοσυστήματος (πλευρικά) μπορεί να παρέχουν χρήσιμη έξτρα πληροφορία για μυστικά στο σύστημα, όπως το κρυπτογραφικό κλειδί, μερική κατάσταση συστήματος, ολόκληροι ή μερικοί κωδικοί, κα.

Είδη Επιθέσεων Πλευρικού Καναλιού

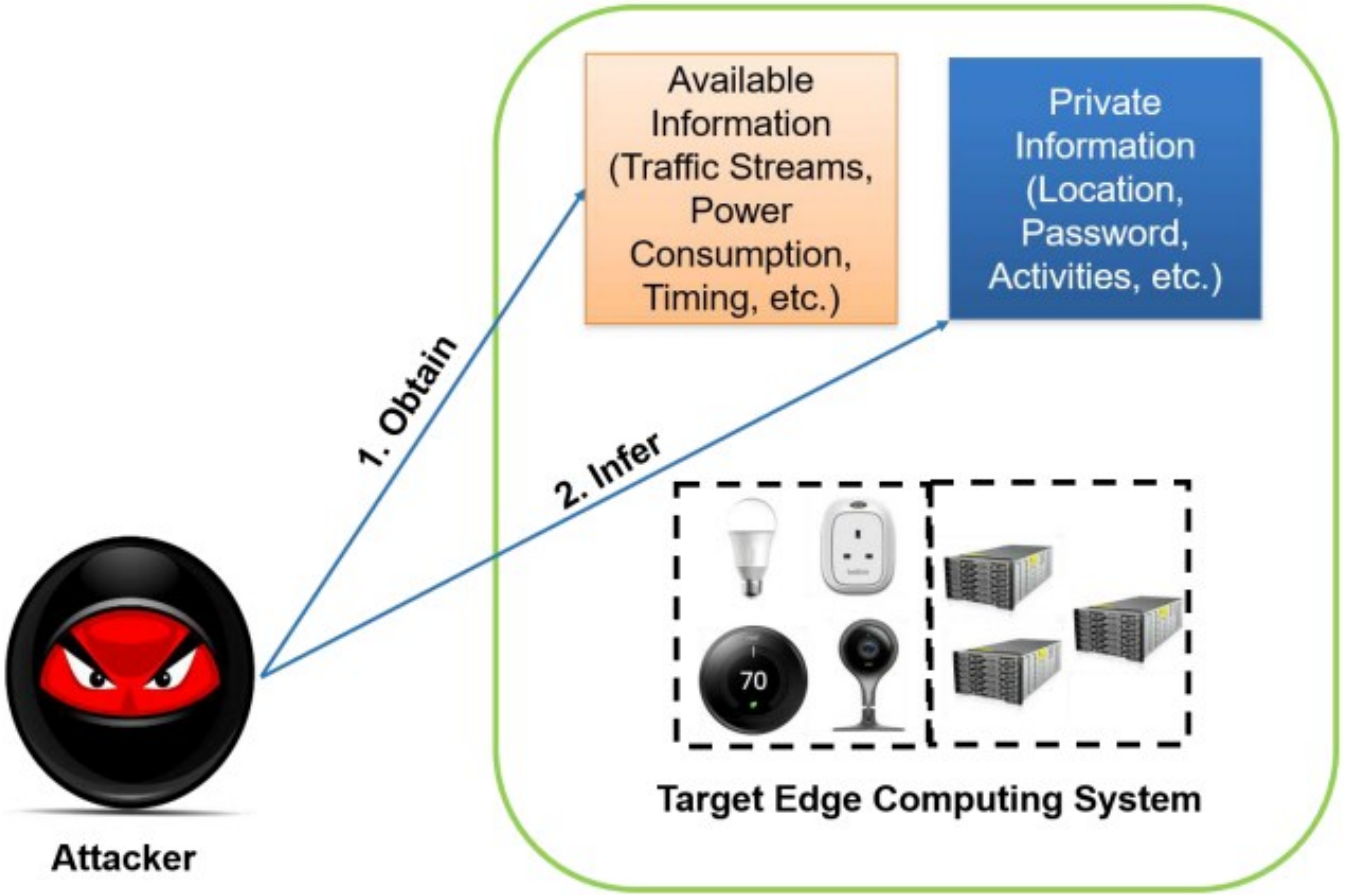
- Κρυφής μνήμης (cache attack)
  - πρόσβαση στην κρυφή μνήμη του θύματος σε ένα διαμοιραζόμενο φυσικό σύστημα
- Χρονισμού (timing attack)
  - Βασιζόμενη σε πόσο χρόνο παίρνει ένας υπολογισμός
- Παρακολούθησης ισχύς (power-monitoring attack)
  - Χρήση διαφοροποιούμενης κατανάλωσης ενέργειας από το υλικό κατά τον υπολογισμό
- Ηλεκτρομαγνητική (electromagnetic attack)
  - Βασιζόμενη στην διαρροή ηλεκτρομαγνητικής ακτινοβολίας που μπορεί να αποκαλύψει κείμενο (κωδικού) και άλλες πληροφορίες
  - Οπότε, οι μετρήσεις χρησιμοποιούνται για την εξαγωγή κρυπτογραφικών κλειδιών με βάση τεχνικές παρόμοιες με την ανάλυση ισχύος ή για την διενέργεια μη κρυπτογραφικών επιθέσεων

Είδη Επιθέσεων Πλευρικού Καναλιού

- Ακουστικής κρυπτανάλυσης (acoustic cryptanalysis)
  - Βασίζονται στον ήχο που παράγεται κατά την διάρκεια υπολογισμού
- Διαφορικής ανάλυσης σφαλμάτων (differential fault analysis)
  - Ανακάλυψη μυστικών μέσω εισαγωγής σφαλμάτων σε έναν υπολογισμό
- Διατήρησης δεδομένων (data remanence)
  - Διάβασμα ευαίσθητων δεδομένων που κανονικά έχουν διαγραφεί
- Λίστας επίτρεψης (Allowlist)
  - Βασίζεται στην διαφοροποίηση της συμπεριφοράς μιας συσκευής όταν επικοινωνεί με άλλες συσκευές που είτε βρίσκονται ή όχι στην λίστα επίτρεψης
  - Μπορεί να χρησιμοποιηθεί για την καταγραφή διευθύνσεων MAC στο πρωτόκολλο Bluetooth
- Οπτική (optical)
  - Μυστικά και ευαίσθητα δεδομένα μπορούν να αναγνωστούν μέσω οπτικής καταγραφής χρησιμοποιώντας κάμερες ή άλλες συσκευές με υψηλή ανάλυση

Επίθεση Πλευρικού Καναλιού

- Λόγω της φύσης της, μπορεί να πραγματοποιηθεί σε οποιοδήποτε μέρος ενός edge computing συστήματος
- Τρόπος επίθεσης
  - Ο επιτιθέμενος συνεχώς λαμβάνει πληροφορίες πλευρικού καναλιού από την στοχευμένη υποδομή edge computing και την διοχετεύει σε αλγορίθμους ή μοντέλα μηχανικής μάθησης για την παραγωγή της επιθυμητής ευαίσθητης πληροφορίας

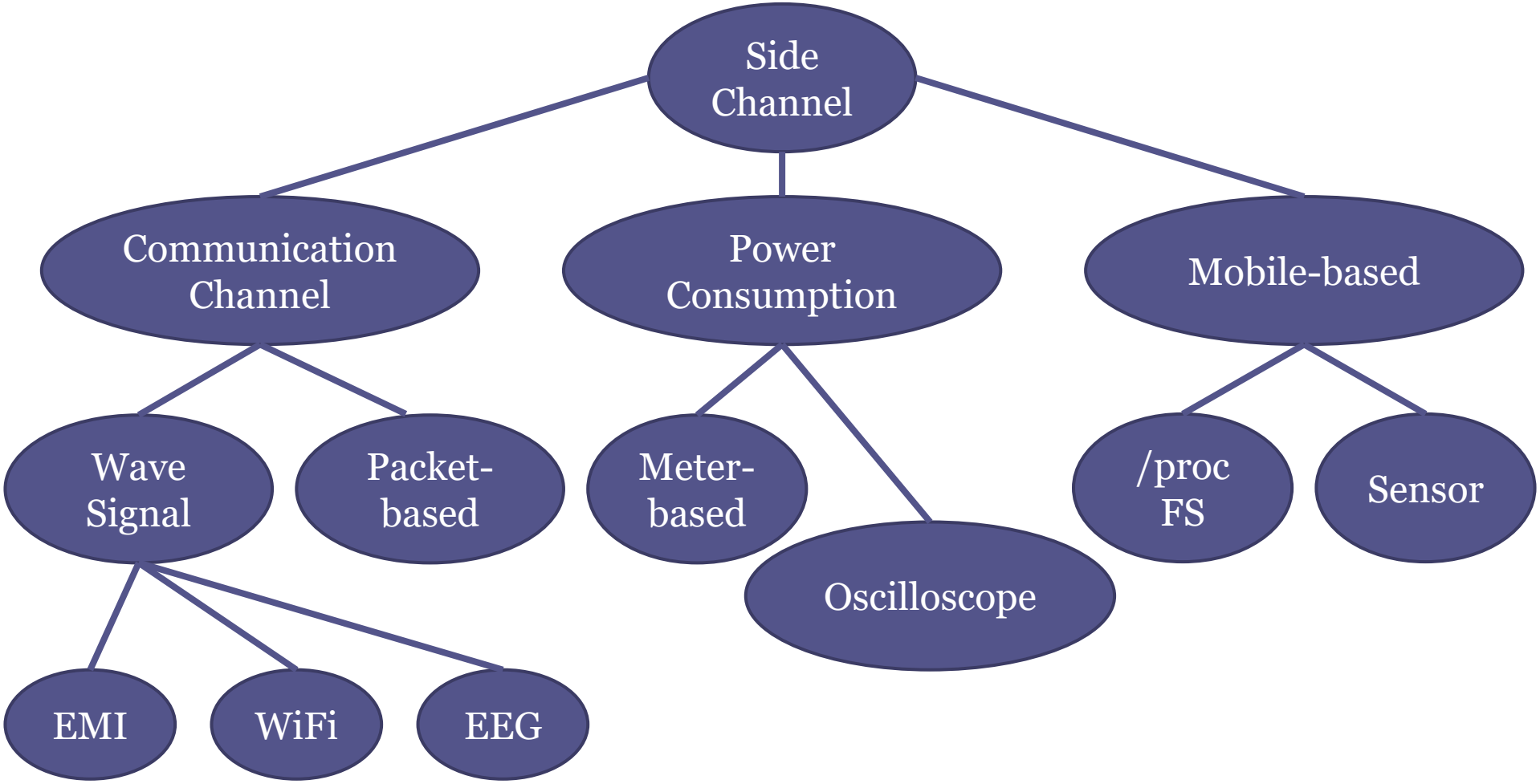

Available Information (Traffic Streams, Power Consumption, Timing, etc.)
Private Information (Location, Password, Activities, etc.)
1. Obtain
2. Infer
70
Attacker
Target Edge Computing System

Πηγή: [1]

Επίθεση Πλευρικού Καναλιού

- Τα πιο δημοφιλή είδη επιθέσεων πλευρικού καναλιού στο edge computing βασίζονται σε επικοινωνιακά σήματα, την κατανάλωση ηλεκτρικής ενέργειας και στο σύστημα αρχείων /proc ή σε αισθητήρες σε κινητά

Επιθέσεις Πλευρικού Καναλιού



Πλευρική Επίθεση Καναλιού Επικοινωνίας

- Σε αυτό το είδος επίθεσης πλευρικού καναλιού, ο επιτιθέμενος παρακολουθεί την κίνηση που πραγματοποιείται σε ένα κανάλι επικοινωνίας που συνδέει 2 κόμβους ακμής
- Ο επιτιθέμενος δεν χρειάζεται να αντιστοιχεί σε μια συσκευή ή εξυπηρετητή ακμής
- Η επίθεση αυτή έχει 2 υπο-είδη
  - Εκμετάλλευσης ροής πακέτων (packet streams)
  - Εκμετάλλευσης σημάτων κύματος (wave signals)

Εκμετάλλευσης Ροής Πακέτων

- Παρατηρήθηκε πως το διαφορετικό σχήμα κωδικών στα πρωτόκολλα H.264 & MPEG-4 για την μείωση του χρονικού πλεονασμού (temporal redundancy) μπορεί να οδηγήσει σε απώλεια ιδιωτικότητας κατά την οικιακή επιτήρηση (home surveillance)
  - Ειδικότερα απλοί αλγόριθμοι μηχανικής μάθησης (πχ. k-NN) μπορούν να χρησιμοποιηθούν για την εξαγωγή των 4 βασικών καθημερινών δραστηριοτήτων ενός ατόμου (ρουχισμός, φτιάξιμο μαλλιών, φαγητό & μετακίνηση)

Εκμετάλλευσης Ροής Πακέτων

- Ένα άλλο παράδειγμα αφορά την χρήση του δικτύου βαθιάς μάθησης Long Short-Term Memory (LSTM) για την ανίχνευση της ύπαρξης ασύρματων καμερών και την εξαγωγή της ανθρώπινης παρουσίας σε ένα σπίτι
- Σε ένα τελευταίο παράδειγμα, υπάρχει η τρωτότητα καναλιού χρονισμού σε πολλούς ασύρματους δρομολογητές, οι οποίοι απαντούν με διαφορετικά χρονικά κενά σε διαφορετικά TCP πακέτα. Με αυτό τον τρόπο, ο επιτιθέμενος μπορεί εύκολα να εξάγει το σωστό αριθμό πακέτου TCP και να επιτελέσει επιθέσεις έκχυσης πακέτων TCP εκτός μονοπατιού (off-path TCP packet injection attacks)

Εκμετάλλευσης Σημάτων Κύματος

- Βασίζεται στην ηλεκτρομαγνητική παρεμβολή (electromagnetic interference – EMI), WiFi κύματα & κυματοειδή δεδομένα ανθρώπινου εγκεφάλου
- Παραδείγματα ηλεκτρομαγνητικής παρεμβολής
  - Εξαγωγή περιεχομένου βίντεο που παίζεται σε μοντέρνες τηλεοράσεις μέσω των διακριτών EMI υπογραφών
  - Χειρισμός σημάτων εισόδου & εξόδου από μια IoT συσκευή διαίσθησης (IoT sensing device) από το φυσικό επίπεδο ώστε να παρακάμψει τους παραδοσιακούς μηχανισμούς ελέγχου ακεραιότητας

Εκμετάλλευσης Σημάτων Κύματος

- Παράδειγμα χρήσης WiFi κυμάτων
  - Εκμετάλλευση πληροφορίας κατάστασης καναλιού για την εξαγωγή εισόδου κωδικού (password) από ένα θύμα με βάση τις κινήσεις των δακτύλων του
- Παράδειγμα κυματοειδών δεδομένων εγκεφάλου
  - Η σύλληψη EEG δεδομένων με την χρήση αλγορίθμων μηχανικής μάθησης μπορεί να οδηγήσει στην εξαγωγή τραπεζικών πληροφοριών, πληροφοριών γέννησης και τοποθεσίας για το θύμα με περισσότερη ακρίβεια σε σχέση με μια επίθεση τυχαίας εικασίας (random guess attack) καθώς και τις δραστηριότητές του σε εκλεπτυσμένο επίπεδο

Πλευρική Επίθεση Καναλιού Κατανάλωσης Ενέργειας

- Η κατανάλωση ενέργειας είναι ένας δείκτης της ηλεκτρικής χρήσης ενός συστήματος
- Φέρει πληροφορία σχετιζόμενη είτε με την συσκευή που καταναλώνει ενέργεια (διότι κάθε συσκευή έχει το δικό της ενεργειακό προφίλ) είτε με την ένταση των υπολογισμών σε μια υπολογιστική εργασία
- Οι επιθέσεις πάνω σε αυτήν εστιάζουν στο να την συσχετίσουν με ευαίσθητη πληροφορία
- Οι επιθέσεις αυτές μπορούν να ταξινομηθούν ανάλογα με το μέσο μέτρησης, δηλ. είτε μετρητές είτε παλμογράφους

Επιθέσεις με βάση τον Μετρητή

- Τρόποι εκμετάλλευσης
  - Οι έξυπνοι μετρητές μετρούν επακριβώς την κατανάλωση ενέργειας σε ένα νοικοκυριό
    - Οπότε μπορούν να χρησιμοποιηθούν για την εξαγωγή δραστηριοτήτων του νοικοκυριού (μαγείρεμα, πλύσιμο, κλπ.)
  - Η παρακολούθηση της πρίζας ρεύματος μιας συσκευής ακμής μπορεί να οδηγήσει στην εξαγωγή της ιστοσελίδας που η συσκευή επισκέπτεται
    - Ενδιαφέρον: μπορεί να οδηγήσει και σε ανίχνευση κακόβουλου λογισμικού που εκτελείται σε μια συσκευή

Επιθέσεις με βάση τον Παλμογράφο

- Σε μοντέρνες ενσωματωμένες συσκευές, ένα τσιπ μπορεί να εκτελεί περίπλοκους κρυπτογραφικούς αλγορίθμους με βάση ένα μυστικό κλειδί που έχει ενσωματωθεί σε αυτό
- Η κατανάλωση ενέργειας σε μια τέτοια συσκευή που μετριέται από παλμογράφο μπορεί να οδηγήσει σε ανακάλυψη του κλειδιού
  - Παράδειγμα: περίπτωση μυστικού κλειδιού για τον αλγόριθμο κρυπτογράφησης AES-CCM
- Όμως, σε αντίθεση με τις επιθέσεις με βάση τον μετρητή, ο επιτιθέμενος θα πρέπει να έχει είτε φυσική πρόσβαση στην συσκευή είτε απομακρυσμένη μέσω κάποιας κακόβουλης εφαρμογής
  - Επομένως, η επίθεση αυτή είναι δύσκολη στην υλοποίηση

Επιθέσεις Πλευρικού Καναλιού σε Κινητά

- Τα κινητά έχουν πιο προηγμένα ΛΣ και παρέχουν πιο πλούσια πληροφορία συστήματος
- Επομένως, έχουν πιο μεγάλη επιφάνεια τρωτοτήτων σε σχέση με άλλες συσκευές IoT
- Οι επιθέσεις πλευρικού καναλιού στα κινητά εστιάζουν είτε στο σύστημα αρχείων /proc είτε σε ενσωματωμένους αισθητήρες

Επιθέσεις στο Σύστημα Αρχείων

- Το σύστημα αρχείων /proc δημιουργείται από το κέλυφος αλλά μπορεί να αναγνωστεί από εφαρμογές και διαδικασίες στο επίπεδο του χρήστη
- Εμπεριέχει πληροφορίες συστήματος, όπως δεδομένα δικτύωσης & διακοπών (interrupt)
- Τρόποι επίθεσης:
  - Επιτέλεση UI phishing ώστε ένα θύμα να ξεγελαστεί και να κάνει ανεπιθύμητες αιτήσεις σε εξυπηρετητές ακμής χρησιμοποιώντας δεδομένα μνήμης στο /proc
  - Εξαγωγή ευαίσθητης πληροφορίας από το κινητό μέσω πληροφορίας διακοπών στο /proc, όπως το μοτίβο κλειδώματος (pattern lock) και το UI που εκτελείται στο προσκήνιο
  - Χρήση πληροφορίας tcp_snd, tcp_rcv, & BSSID στο /proc για την εξαγωγή ευαίσθητης πληροφορίας, όπως κατάσταση υγείας, τοποθεσία και ταυτότητα κοινωνικού δικτύου
- Προϋπόθεση: θα πρέπει να υπάρχει πρόσβαση στο κινητό πχ. μέσω κακόβουλης εφαρμογής

Επιθέσεις σε Αισθητήρες Κινητού

- Τρόποι επίθεσης:
  - Ανάλυση ακουστικών ήχων από το πάτημα των πλήκτρων του κινητού για την εξαγωγή των κουμπιών που πατήθηκαν
  - Εξαγωγή πλήκτρων που πατήθηκαν σε οθόνη αφής μέσω της χρήσης δεδομένων από το επιταχυνσιόμετρο (accelerometer) και το γυροσκόπιο (gyroscope)
    - Εναλλακτικά, χρήση βίντεο από την κάμερα που επιβλέπει τις κινήσεις των ματιών του χρήστη

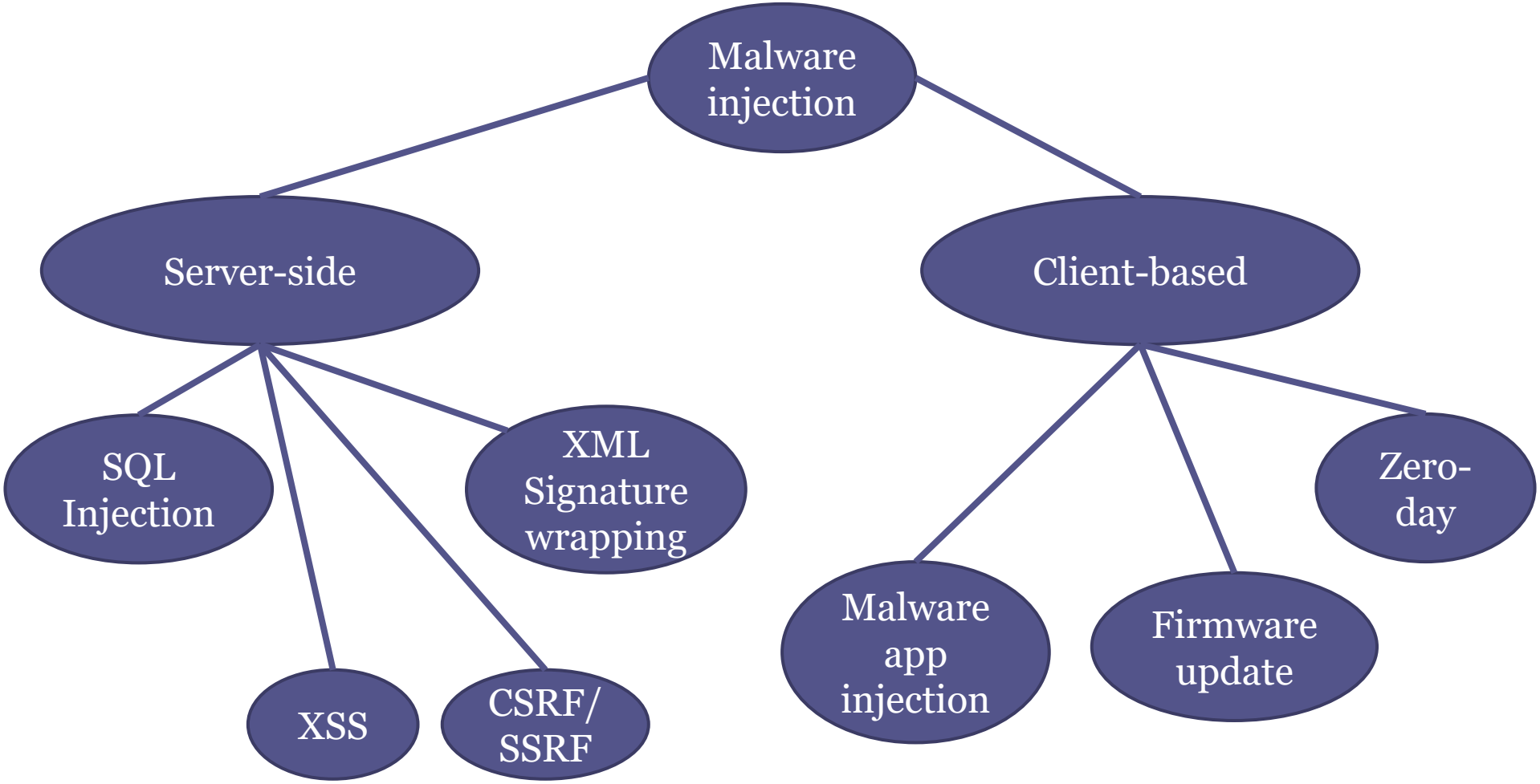
Είδη Επιθέσεων – Επίθεση Έκχυσης Κακόβουλου Λογισμικού

- Αν και αυτό το είδος επίθεσης είναι από τα πιο επικίνδυνα, μια συσκευή/εξυπηρετητής ακμής δεν μπορεί να προστατευθεί από αυτό λόγω χρήσης αδύναμων μηχανισμών προστασίας
- Οι επιθέσεις αυτού του είδους χωρίζονται ανάλογα με το είδος του στόχου θύματος σε:
  - *Εκχύσεις στην πλευρά του εξυπηρετητή (ακμής) (server-side injections)*
  - *Εκχύσεις στην πλευρά της συσκευής (ακμής) (device-side injections)*


Edge Servers
Attacker
Edge Devices
Inject
Malware
Inject
Malware
70

Πηγή: [1]

Επιθέσεις Έκχυσης Κακόβουλου Κώδικα



Εκχύσεις στην Πλευρά του Εξυπηρετητή

- Διακρίνονται σε 4 είδη
  - Εκχύσεις SQL (SQL injections)
  - Εκχύσεις XSS (Cross-Site Scripting)
  - Εκχύσεις CSRF/SSRF (Cross-Site Request Forgery / Service-Side Request Forgery)
  - Περιτύλιξη υπογραφής XML (XML signature wrapping)

Εκχύσεις SQL

- Εστιάζουν στην άντληση ή και τροποποίηση/διαγραφή ευαίσθητης πληροφορίας
- Η πληροφορία εντοπίζεται σε υποκείμενη βάση δεδομένων (σε σχέση με τον εξυπηρετητή)
- Βασίζεται στο γεγονός πως σε περιπτώσεις αποστολής δεδομένων φόρμας ή δεδομένων παραμέτρων επερώτησης είναι δυνατή η χρήση χαρακτήρων διαφυγής
  - Αυτό έχει ως αποτέλεσμα να εμπλουτίζεται η αντίστοιχη επερώτηση SQL του εξυπηρετητή προς την βάση δεδομένων με σκοπό την έκθεση/τροποποίηση των δεδομένων (πχ. χρηστών)
- Εκτός από το «πείραγμα» των ευαίσθητων δεδομένων, είναι δυνατή και η έκχυση κακόβουλου script

Εκχύσεις XSS

- Θεωρείται επίθεση στην πλευρά του πελάτη όπου ο επιτιθέμενος εκχύνει κακόβουλο κώδικα (πχ. σε Javascript) σε εμπιστευμένες ιστοσελίδες που έπειτα μπορεί να εκτελεστεί αυτόματα από τον πελάτη (όταν επισκέπτεται τις ιστοσελίδες αυτές)
- Σε περιβάλλον edge computing ο εξυπηρετητής μπορεί να παίξει τον ρόλο ενός πελάτη όταν επισκέπτεται ή προσπελαύνει τις υπηρεσίες που παρέχονται από άλλους εξυπηρετητές ακμής ή νέφους

Εκχύσεις CSRF/SSRF

- Κατά μια επίθεση CSRF ο επιτιθέμενος προσποιείται έναν νόμιμο χρήστη (πχ. έναν εξυπηρετητή ακμής) και αιτεί μέσω εφαρμογών ιστού την εκτέλεση ενεργειών που είναι εις βάρος του θύματος/χρήστη (συνήθως τύπου τροποποίησης καταστάσεων)
- Σε μια επίθεση SSRF ένας εξυπηρετητής ακμής «εκβιάζεται» να διαβάσει ή να τροποποιήσει εσωτερικούς πόρους μέσω χειρισμού URL που ο εξυπηρετητής αυτός πρέπει να επισκεφθεί ή να στείλει δεδομένα σε αυτό
  - Οι εσωτερικοί πόροι μπορεί να είναι προφανώς και άλλοι εξυπηρετητές ακμής με τους οποίους μπορεί να συνεργάζεται
- Η κύρια αιτία και για τα δύο είδη επιθέσεων είναι η μη εκλεπτυσμένη σχεδίαση του μηχανισμού επικύρωσης (verification mechanism) που μπορεί εύκολα να «σπάσει»

Περιτύλιξη Υπογραφής XML

- Η επίθεση αυτή σχετίζεται με την χρήση του πρωτοκόλλου SOAP (ειδικό για την επικοινωνία με καταστατικές υπηρεσίες ιστού)
- Σε αυτή την επίθεση
  - ο επιτιθέμενος πρώτα συλλαμβάνει ένα νόμιμο XML μήνυμα, δημιουργεί μια νέα ετικέτα σε αυτό και τοποθετεί ένα αντίγραφο του αρχικού περιεχομένου μέσα στην ετικέτα αυτή
  - ο επιτιθέμενος έπειτα αντικαθιστά τις αρχικές τιμές με κακόβουλους κώδικες στο αρχικό μήνυμα και συνδυάζει το τροποποιημένο αρχικό μήνυμα με την νέα ετικέτα τοποθετώντας την ετικέτα αυτή πριν τις (κανονικές) ετικέτες του αρχικού μηνύματος
  - Μόλις ο εξυπηρετητής ακμής λάβει το μήνυμα, θα το επικυρώσει
    - Αυτό θα επιτύχει διότι ο επιτιθέμενος δεν διέγραψε τις αρχικές τιμές αλλά τις έβαλε σε ένα περιτύλιγμα νέας ετικέτας
  - Τέλος, ο εξυπηρετητής θα εκτελέσει τον κακόβουλο κώδικα που έχει εκχυθεί στο μήνυμα

Εκχύσεις στην Πλευρά του Πελάτη

- Διάφορες μέθοδοι για την έκχυση κακόβουλου κώδικα σε IoT συσκευές υπάρχουν διότι οι IoT συσκευές είναι αρκετά ετερογενής τόσο στο υλικό όσο και στο υλικολογισμικό
- Η πιο κοινή προσέγγιση επίθεσης για την απομακρυσμένη έκχυση του κακόβουλου κώδικα σχετίζεται με την εκμετάλλευση τρωτοτήτων μηδενικής ημέρας που μπορούν να οδηγήσουν στην απομακρυσμένη εκτέλεση κώδικα (remote code execution – RCE) ή την έκχυση εντολών
  - Παράδειγμα:
    - Ο ιός IoTReaper μόλυνε εκατομμύρια IoT συσκευές μέσω του διαδικτύου και του WiFi εκμεταλλευόμενος 30 τρωτότητες RCE σε 9 διαφορετικά είδη συσκευών, από δικτυακούς δρομολογητές μέχρι IP κάμερες

Εκχύσεις στην Πλευρά του Πελάτη

- Μια άλλη προσέγγιση βασίζεται στον εντοπισμό έλλειψης ελέγχου (πχ. επικύρωσης υπογραφών) ή προστασίας κατά την ανανέωση υλικολογισμικού οδηγώντας σε επιθέσεις τροποποίησης υλικολογισμικού
  - Παραδείγματα:
    - Το πρωτόκολλο HP-RFU επιτρέπει έναν επιτιθέμενο να τροποποιήσει οποιοδήποτε προεγκατεστημένο υλικολογισμικό σε έναν εκτυπωτή
    - Το ίδιο μπορεί να γίνει για Smart Nest θερμοστάτες ή ποντίκια Logitech G600 μέσω της χρήσης USB συνδέσεων ή της δικτύωσης
    - Εν γένει, αυτό μπορεί να υποστηριχθεί σε οποιαδήποτε συσκευή όταν χρησιμοποιείται το πρωτόκολλο Zigbee Light Link

Εκχύσεις στην Πλευρά του Πελάτη

- Μια άλλη προσέγγιση, αν και πιο δύσκολη, είναι η έκχυση κακόβουλου κώδικα με ικανότητας πρόσβασης κατά μήκος (εφαρμογών) σε κινητές συσκευές
  - Η δυσκολία έγκειται στο γεγονός πως τα ΛΣ έχουν μηχανισμούς απομόνωσης εφαρμογών
- Παραδείγματα επιθέσεων:
  - Εκμετάλλευσης της δομής επιπέδου ΛΣ Android Task Structure (ATM) για την έκχυση κακόβουλου UI σε εφαρμογές ενός κινητού
- Οι επιθέσεις αυτές δεν έχουν σοβαρό αντίκτυπο διότι εκμεταλλεύονται επίσημα APIs & δομές

Εκχύσεις στην Πλευρά του Πελάτη

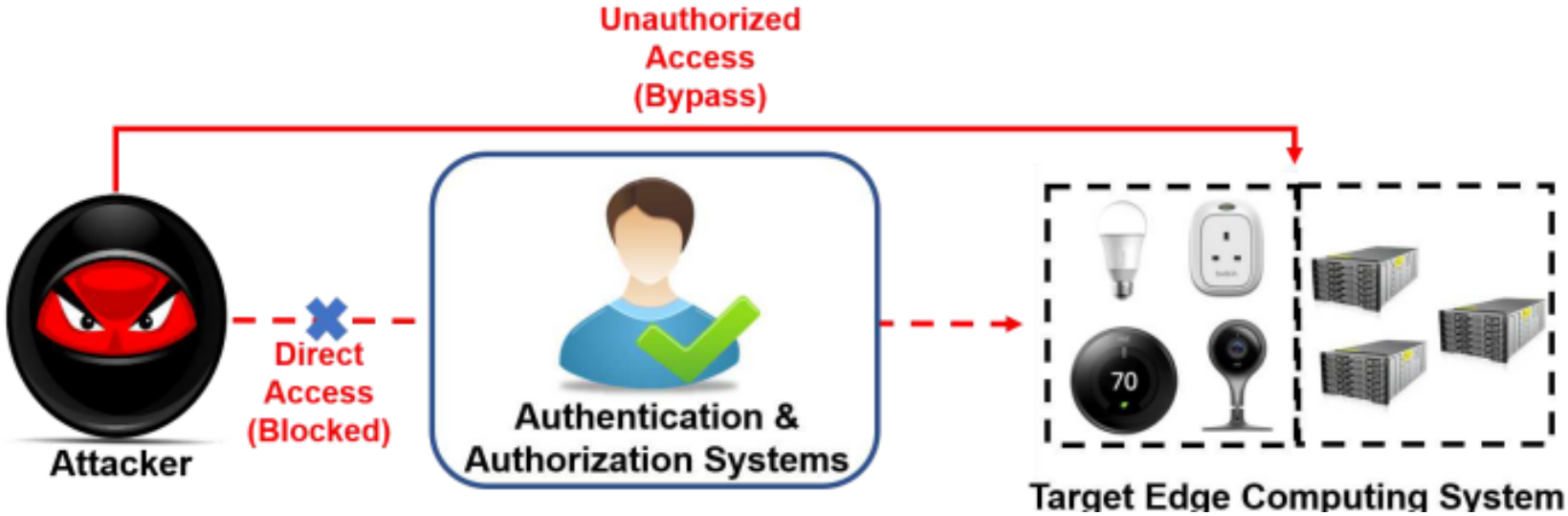
- Μια παραλλαγή της προηγούμενης προσέγγισης για να παρακάμψει το προαναφερόμενο μειονέκτημα είναι η χρήση κακόβουλων βιβλιοθηκών που είναι πιο ισχυρές και λιγότερο πιθανό να ανιχνευθούν
  - Οι βιβλιοθήκες αυτές μπορεί να δημιουργούν ανοικτές πόρτες (backdoor) για την έκχυση κακόβουλου κώδικα
  - 6,84% των εφαρμογών Android & 2,94% των εφαρμογών iOS χρησιμοποιούν τέτοιες βιβλιοθήκες
- Σε κάθε περίπτωση, θα πρέπει το θύμα να ξεγελαστεί και να εγκαταστήσει την κακόβουλη εφαρμογή του επιτιθέμενου στο κινητό του
  - Αυτό μπορεί να γίνει μέσω ενός App Store ή επίθεσης κοινωνικής μηχανικής (πχ. με το άνοιγμα κακόβουλου URL)

Είδη Επιθέσεων – Επίθεση Ταυτοποίησης & Εξουσιοδότησης

- Η ταυτοποίηση συνήθως πραγματοποιείται μεταξύ συσκευών και εξυπηρετητών ακμής
  - Σε ορισμένες περιπτώσεις, πραγματοποιείται μεταξύ συσκευών ακμής ή μεταξύ εξυπηρετητών ακμής με ένα αποκεντρωμένο τρόπο
- Η εξουσιοδότηση αφορά την απονομή αδειών από έναν εξυπηρετητή ακμής σε μια συσκευή ακμής ή τις εφαρμογές της
  - Όμως, είναι δυνατή η απονομή αδειών από συσκευές/εφαρμογές σε άλλες συσκευές/εφαρμογές σε σενάρια τύπου εναύσματος-δράσης (trigger-action) (πχ. σε ένα σύστημα αυτοματοποίησης οικίας)

Είδη Επιθέσεων – Επίθεση Ταυτοποίησης & Εξουσιοδότησης

- Όταν ένας επιτιθέμενος πρόκειται να προσπελάσει άμεσα προστατευμένους εξυπηρετητές ή συσκευές ακμής, θα μπλοκαριστεί από το σύστημα ταυτοποίησης
- Επομένως, ο επιτιθέμενος θα αναζητήσει μεθόδους για να παρακάμψει την διαδικασία ταυτοποίησης

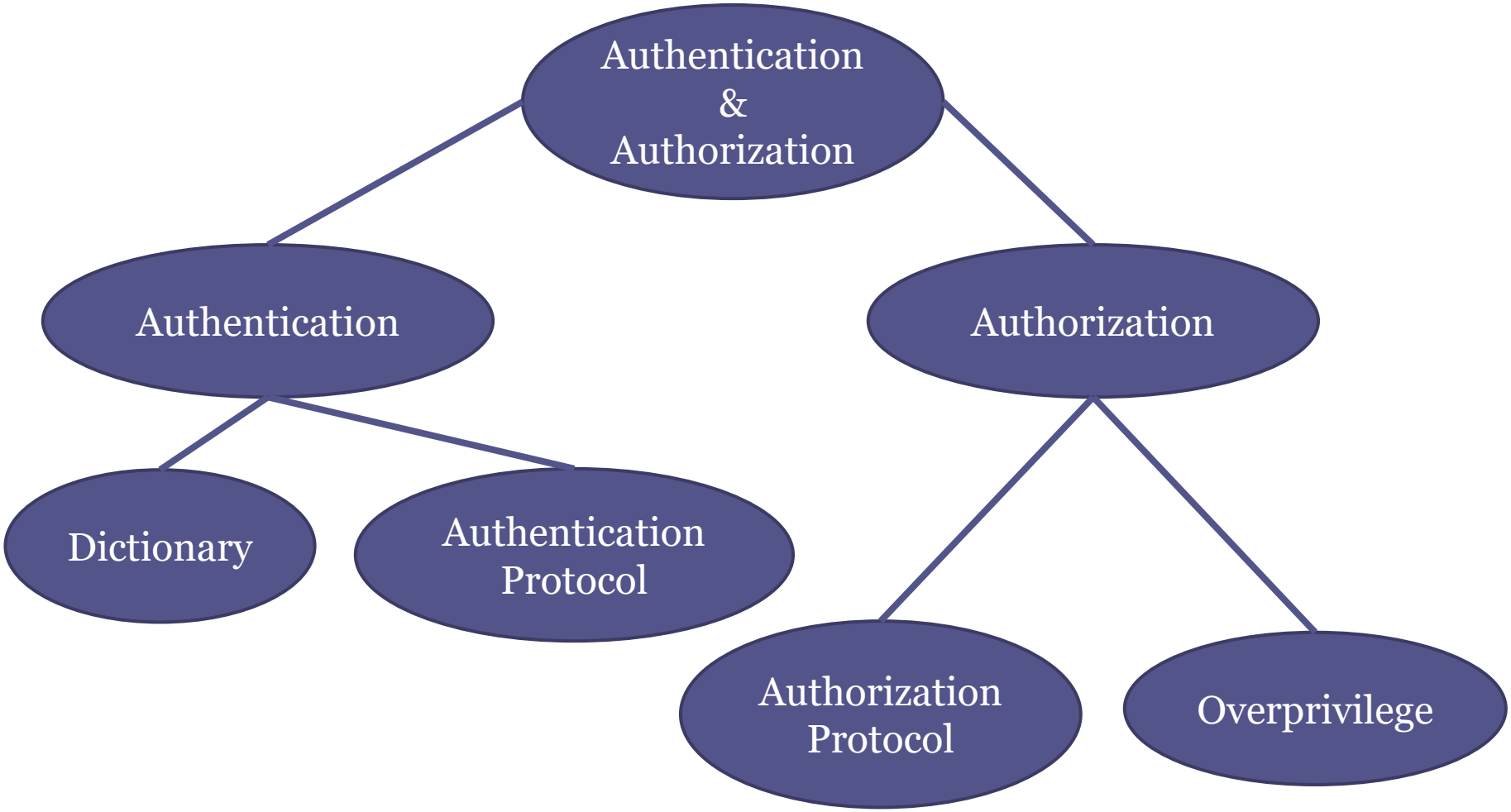

Unauthorized
Access
(Bypass)
Attacker
Direct
Access
(Blocked)
Authentication &
Authorization Systems
70
Target Edge Computing System

Πηγή: [1]

Είδη Επιθέσεων - Επίθεση Ταυτοποίησης & Εξουσιοδότησης

- Οι επιθέσεις αυτού του τύπου χωρίζονται σε
  - Ταυτοποίησης
    - Επιθέσεις λεξικού (dictionary attacks)
    - Επιθέσεις εκμετάλλευσης τρωτοτήτων σε πρωτόκολλα ταυτοποίησης
  - Εξουσιοδότησης
    - Επιθέσεις εκμετάλλευσης τρωτοτήτων σε πρωτόκολλα εξουσιοδότησης
    - Υπερπρονομιούχες επιθέσεις (overprivilege attacks)

Επιθέσεις Αυθεντικοποίησης & Εξουσιοδότησης



Επιθέσεις Λεξικού

- Ονομάζονται και επιθέσεις brute-force
- Ο επιτιθέμενος χρησιμοποιεί συχνούς/κοινούς κωδικούς από ένα λεξικό για να «σπάσει» την ταυτοποίηση
- Οι επιθέσεις αυτές απαιτούν πολλούς πόρους και έχουν μικρό ποσοστό επιτυχίας
- Επίσης, απαιτούν την χρήση διαφορετικών τεχνικών για το «σπάσιμο» διαφορετικών μηχανισμών και πρωτοκόλλων ταυτοποίησης

Επιθέσεις Λεξικού

- Παραδείγματα:
  - Διενέργεια offline επίθεσης στο πρωτόκολλο S-3PAKE που χρησιμοποιείται μερικές φορές από το Bluetooth όταν εγκαθιδρυθεί το αρχικό κλειδί συνόδου
  - Διενέργεια παράλληλης online επίθεσης στο πρωτόκολλο WPA2-PSK σε WiFi δίκτυα
  - Στην περίπτωση χρήσης βιομετρικών χαρακτηριστικών, είναι δυνατή η δημιουργία ενός συνθετικού αποτυπώματος που ταιριάζει με πολλά στοχευμένα δακτυλικά αποτυπώματα

Επιθέσεις στο Πρωτόκολλο Ταυτοποίησης

- Οι επιθέσεις αυτές προσπαθούν να εκμεταλλευτούν τρωτότητες που σχετίζονται με σφάλματα σχεδίασης των πρωτοκόλλων ταυτοποίησης
- Παραδείγματα:
  - Η τρωτότητα αδύναμης δέσμευσης (weak binding) στο WPA πρωτόκολλο επιτρέπει την διενέργεια επίθεσης τύπου stealthy evil twin attack
  - Στην έκδοση 2 του πρωτοκόλλου αυτού είναι δυνατή η επαναχρησιμοποίηση nonce ώστε να πραγματοποιηθεί επαναπομπή, αποκρυπτογράφηση και πλαστογράφηση μηνυμάτων ταυτοποίησης
  - Επιθέσεις σύγκρουσης μεταγραφής (transcript collision) στο TLS μπορούν να οδηγήσουν σε επιθέσεις υποβάθμισης και πλαστοπροσωπίας (impersonation)
  - Τρωτότητα επαναχρησιμοποίησης κλειδιών (key reuse) σε υπηρεσίες ταυτοποίησης 4 παρόχων νέφους/ακμών που οδηγεί σε επίθεση πλαστοπροσωπίας εξυπηρετητή ή συσκευής

Επιθέσεις στο Πρωτόκολλο Ταυτοποίησης

- Έχει αποδειχθεί πως τρωτότητες υπάρχουν και σε πρωτόκολλα ταυτοποίησης σε 4G ή 5G δίκτυα
- Οι επιθέσεις αυτές μπορούν να πετύχουν:
  - Άρνηση υπηρεσίας σε νόμιμους χρήστες
  - Αποκάλυψη μη κρυπτογραφημένων ευαίσθητων δεδομένων
  - Πλαστοπροσωπία της τοποθεσίας ενός χρήστη
  - Εντοπισμό τοποθεσίας χρήστη

Επιθέσεις στο Πρωτόκολλο Εξουσιοδότησης

- Εκμεταλλεύονται σφάλματα στην σχεδίαση ή λογική των πρωτοκόλλων εξουσιοδότησης για να επιχειρήσουν μη εξουσιοδοτημένες δράσεις σε ευαίσθητους πόρους ή να εκτελέσουν προνομιούχες δράσεις
- Το πρωτόκολλο OAuth χρησιμοποιείται ευρέως αλλά έχουν εντοπιστεί αδυναμίες και για τις 2 εκδόσεις του

Επιθέσεις στο Πρωτόκολλο Εξουσιοδότησης

- Η έκδοση 1.0 του OAuth έχει «σπάσει» και είναι τρωτή σε επιθέσεις στερέωσης (fixation attacks)
  - Στις επιθέσεις αυτές πρέπει ο επιτιθέμενος να παρέχει ένα νόμιμο αναγνωριστικό συνόδου και να αναγκάσει τον φυλλομετρητή του χρήστη να το χρησιμοποιήσει για να ταυτοποιήσει τον χρήστη. Εφόσον η ταυτοποίηση επιτύχει, ο επιτιθέμενος πειρατεύει την σύνοδο του χρήστη με την αντίστοιχη εφαρμογή
- Η έκδοση 2.0 φαίνεται άτρωτη αλλά έχει κάποιες κακές υλοποιήσεις
  - 59.7% των κινητών εφαρμογών χρησιμοποιούν λανθασμένη υλοποίηση του OAuth
  - 96 πωλητές relaying party έχουν σύστημα με τρωτό χαρακτηριστικό OAuth SSO που επιτρέπει σε επιτιθέμενο να προσπελάσει την ιδιωτική πληροφορία του θύματος χωρίς κάποια εξουσιοδότηση

Υπερπρονομιούχες Επιθέσεις

- Τα τυπικά συστήματα εξουσιοδότησης παρουσιάζουν υπερπρονομιούχα ζητήματα
  - Η πλατφόρμα έξυπνης οικίας SmartThings παρουσιάζει τέτοιες τρωτότητες επιτρέποντας σε κακόβουλες εφαρμογές να αλλάξουν τον κωδικό πόρτας ή να ενεργοποιήσουν τον συναγερμό φωτιάς
  - Όλα τα τρέχοντα προϊόντα έξυπνου κλειδώματος είναι τρωτά στο να επιτρέπουν είτε σε έναν επιτιθέμενο να αποφύγει ένα μηχανισμό ανάκλησης συσκευής (device revocation) είτε σε μια εφαρμογή/πρωτόκολλο έξυπνου κλειδώματος να ξεκλειδώσει ανεπιθύμητα την πόρτα ενός χρήστη
  - Το 1/3 των εφαρμογών Android παρουσιάζουν υπερπρονομιούχες τρωτότητες

Αντίμετρα για Επιθέσεις DDoS

DDoS Category	Security Measure
Flooding-based	Detection & filtering based on packets
	Statistics-based detection & filtering
Zero-day	Memory issues detection in programs
	Protection (network – firewalls, memory isolation)

Αντίμετρα για Επιθέσεις DDoS

- Αντιμετώπιση επιθέσεων πλημμυρίσματος
  - Ανίχνευση & φιλτράρισμα με βάση τα πακέτα
    - Σε πλαίσια ελέγχου συμφόρησης (congestion control frameworks)
    - Τρόποι ανίχνευσης
      - Με βάση το αναγνωριστικό του πακέτου – το πακέτο αντιστοιχεί στο ίδιο μονοπάτι
      - Με βάση eigenvalue σύνολα που σχηματίζονται από νόμιμες IP διευθύνσεις
  - Ανίχνευση & φιλτράρισμα με βάση την στατιστική
    - Τρόποι ανίχνευσης
      - Με βάση την εντροπία πακέτων
      - Με βάση την χρήση αλγορίθμων μηχανικής μάθησης

Αντίμετρα για Επιθέσεις DDoS

- Αντιμετώπιση επιθέσεων μηδενικής ημέρας
  - Ανίχνευση προβλημάτων μνήμης σε ένα πρόγραμμα μέσω
    - Μηχανισμών ανίχνευσης μολυσμένου δείκτη και ECC-μνήμης
      - Απαιτούν την ύπαρξη πηγαίου κώδικα που δεν είναι διαθέσιμος για συσκευές ακμής
    - Ανάλυσης μνήμης πάνω στο υλικολογισμικό με την χρήση αλγορίθμων μηχανικής μάθησης
      - Αλλά το υλικολογισμικό δεν είναι πάντοτε διαθέσιμο
  - Προστασία από επιθέσεις:
    - Ενότητα επέκτασης για την απομόνωση μνήμης σε διαδικασίες ώστε να αντιμετωπισθούν επιθέσεις διαφθοράς μνήμης
    - Δημιουργία IoT τειχών προστασίας μέσω SDN (Software-Defined Networking) για την μείωση των επιφανειών τρωτοτήτων για μια εκτεθειμένη συσκευή ακμής
    - Εφαρμογή ελαφριών μηχανισμών απομόνωσης σε δρομολογητές πρόσβασης πριν ένα IoT botnet προσπελάσει μια συσκευή ακμής

Αντίμετρα για Επιθέσεις Πλευρικού Καναλιού

Basic Direction	Security Measure
Privacy Protection	k-anonymity
	l-diversity
	t-closeness
	Differential privacy
Channel Access Restriction	Channel obfuscation at code-level
	Hardware-based isolation technologies (e.g., SGX)

Αντίμετρα για Επιθέσεις Πλευρικού Καναλιού

- Η αντιμετώπιση των επιθέσεων αυτών μπορεί να πάρει 2 κατευθύνσεις
  - Περιορισμός πρόσβασης σε πληροφορία πλευρικού καναλιού
  - Προστασία ευαίσθητων δεδομένων από επιθέσεις εξαγωγής/συσχέτισης (inference attacks)
    - Τεχνικές προστασίας της ιδιωτικότητας (δείτε επόμενη διάλεξη)
      - k-ανωνυμία
      - l-ποικιλομορφία
      - t-εγγύτητα
      - διαφορική ιδιωτικότητα

Περιορισμός Πρόσβασης Πληροφορίας Πλευρικού Καναλιού

- Τεχνικές συσκότισης (obfuscation) πλευρικού καναλιού στο επίπεδο πηγαίου κώδικα
  - Από πλευρικές επιθέσεις ροής ελέγχου
  - Από πλευρικές επιθέσεις κρυφής μνήμης
- Χρήση του SGX, ενός υλικού που ενισχύεται από την τεχνολογία TrustZone, το οποίο αποτρέπει την μη εξουσιοδοτημένη πρόσβαση σε πλευρικά κανάλια μέσω μηχανισμών απομόνωσης

Αντίμετρα για Επιθέσεις Έκχυσης Κακόβουλου Κώδικα στην Πλευρά του Εξυπηρετητή

Attack Type	Security Measure
SQL Injection	Code analysis
	Prevention techniques
	Machine-learning based malware detection
XSS	Client-side fixed rules set
	Instruction-set randomization
	Context-aware data sanitization
	XSS vulnerability detection based on machine learning
CSRF	Secret token usage
	“Referer” header check + “origin” header sending
SSRF	Credential embedding in requests
	Static WAF approach extension
XML signature wrapping	Schema hardening
	Side-channel based detection mechanism
	Positional tokens usage

Αντίμετρα για Επιθέσεις Έκχυσης Κακόβουλου Κώδικα στην Πλευρά της Συσκευής

Device Type	Security Measure
IoT	Automatic binary structure randomization
	Software symbiotic methods
	Blockchain-based firmware update
	Memory protection module for privacy protection
Mobile	Static code analysis for malware API usage detection
	Vulnerability & malware behaviour detection in libraries
	Task structure-based malware injection prevention

Αντίμετρα για Επιθέσεις Έκχυσης Κακόβουλου Κώδικα

- Για την αντιμετώπιση εκχύσεων στην πλευρά του εξυπηρετητή υιοθετούνται προσεγγίσεις ανίχνευσης-φιλτραρίσματος
- Για την αντιμετώπιση εκχύσεων στην πλευρά της συσκευής υιοθετείται η ανάλυση στο επίπεδο του κώδικα για την ανίχνευση κακόβουλης συμπεριφοράς και ο εκλεπτυσμένος έλεγχος πρόσβασης

Αντιμετώπιση Έκχυσης στην Πλευρά του Εξυπηρετητή

- Αντιμετώπιση SQL εκχύσεων
  - Τεχνικές που εστιάζουν στην ανίχνευση ελέγχοντας τον κώδικα με διάφορα σχήματα
    - Στατική ανάλυση
    - Δυναμική αποσφαλμάτωση
    - Δοκιμή μαύρου κουτιού
    - Ανάλυση taint-based
  - Τεχνικές αποτροπής
    - Εγκαθίδρυση ενός φίλτρου πληρεξουσίου (proxy filter)
    - Τυχαιοποίηση συνόλου οδηγιών (instruction-set randomization)
    - Παραμετροποιήσιμες επερωτήσεις (parameterized queries)
  - Εντοπισμός τρωτοτήτων μέσω μηχανικής μάθησης

Αντιμετώπιση Έκχυσης στην Πλευρά του Εξυπηρετητή

- Αντιμετώπιση XSS εκχύσεων
  - Χρήση χειρωνακτικών κανόνων στην πλευρά του πελάτη για την εμπόδιση εκτέλεσης κακόβουλου κώδικα XSS
  - Τυχαιοποίηση συνόλου οδηγιών του XSS κώδικα ώστε να γίνει ακίνδυνος
  - Καθαρισμός με επίγνωση περιβάλλοντος των δεδομένων
  - Τεχνικές μηχανικής μάθησης για την ανίχνευση XSS τρωτοτήτων

Αντιμετώπιση Έκχυσης στην Πλευρά του Εξυπηρετητή

- Αντιμετώπιση CSRF εκχύσεων
  - Χρήση μυστικών tokens
  - Έλεγχος κεφαλίδας referer + αποστολή κεφαλίδας origin από τον πελάτη
- Αντιμετώπιση SSRF εκχύσεων
  - Μηχανισμός προστασίας ιδιωτικότητας μέσω της ενσωμάτωσης των διαπιστευτηρίων των πελατών στις αιτήσεις
  - Επέκταση της στατικής WAF προσέγγισης για την αντιμετώπιση SSRF επιθέσεων

Αντιμετώπιση Έκχυσης στην Πλευρά του Εξυπηρετητή

- Αντιμετώπιση περιτύλιξης XML υπογραφής
  - Προσέγγιση σκλήρυνσης σχήματος
  - Μηχανισμός ανίχνευσης με βάση πλευρικό κανάλι μέσω αρίθμησης της συχνότητας κάθε κόμβου σε μια αιτούμενη υπηρεσία
  - Χρήση tokens θέσεως (positional tokens)

Αντιμετώπιση Έκχυσης στην Πλευρά του Πελάτη

- Για IoT συσκευές:
  - Autotomic Binary Structure Randomization (ABSR): λαμβάνει εκτελέσιμο ή υλικολογισμικό ως είσοδο και παράγει ως έξοδο μια εκδοχή του εκτελέσιμου με μείωση του μη χρησιμοποιούμενου κώδικα για την ελαχιστοποίηση της επιφάνειας επίθεσης
  - Μέθοδος συμβιοτικού λογισμικού (software symbiotic method) που εκχύνει λειτουργικότητα ανίχνευσης τρωτοτήτων στο δυαδικό υλικολογισμικό υπαρχόντων IoT συσκευών για την αποτροπή κακόβουλων τροποποιήσεων
  - Κρυπτογραφική προσέγγιση με βάση blockchain για την ασφαλή ανανέωση υλικολογισμικού για IoT συσκευές
  - Απομόνωση ευαίσθητων δεδομένων και κώδικα από τα μη ευαίσθητα μέσω μονάδας προστασίας μνήμης για την παρεμπόδιση επιθέσεων τροποποίησης υλικολογισμικού

Αντιμετώπιση Έκχυσης στην Πλευρά του Πελάτη

- Για κινητές συσκευές:
  - Στατική ανάλυση για τον εντοπισμό πιθανών κακόβουλων χρήσεων επικίνδυνων Android APIs
  - Τεχνική ανίχνευσης βιβλιοθήκης που αντιστέκεται σε κοινές μεθόδους συσκότισης κώδικα και μπορεί να ανιχνεύσει τρωτότητες ασφάλειας & κακόβουλες συμπεριφορές σε βιβλιοθήκες Android
  - Task Interface Checker για την απαλοιφή έκχυσης κακόβουλου κώδικα μέσω της χρήσης της Δομής Λειτουργιών Android (Android Task Structure)

Αντίμετρα για Επιθέσεις Ταυτοποίησης & Εξουσιοδότησης

Attack Type	Security Measure
Dictionary Attacks	Extra authentication level
	Extending existing or proposing new authentication protocols
Authentication Protocol Attacks	Empowering existing authentication protocols
	Protecting cryptographic implementation
	Extending existing or proposing new 4G/5G protocols
	Applying scalable & secure authentication architectures
Authorisation Protocol Attacks	Static code analysis for detecting protocol implementation vulnerabilities
	Application-based framework development for confronting OAuth API abuse
	Implementing OAuth protocol for HTTP/CoAP services

Αντίμετρα για Υπερπρονομιούχες Επιθέσεις

Device Type	Security Measure
IoT	NLP method for inconsistency discovery between IoT apps and their descriptions
	Taint-based analysis for detecting and preventing sensitive information leakage from IoT apps
	Information detection technique for leakage monitoring from overprivileged apps
	Model-based checking for automatic detection of overprivileged apps
	Comparing the app behaviour context with historical knowledge for detecting possible suspicious inconsistencies
	Environmental situation oracles for IoT access control enforcement based on situational environments
Mobile	Semantic permission generator for Android based on app description
	System-level sandbox for code requesting sensitive rights so as to isolate it for further analysis
	Prohibiting overprivileged apps from rights abuse over sensors based on 3 machine learning models
	Combining graph abstraction and reasoning algorithms for detecting overprivileged Android app components

Αντίμετρα για Επιθέσεις Ταυτοποίησης & Εξουσιοδότησης

- Η αντιμετώπιση επιθέσεων λεξικού εστιάζει στην προσθήκη ενός ισχυρότερου επιπέδου ταυτοποίησης ή την σκλήρυνση της διαδικασίας επικύρωσης κωδικών
- Η αντιμετώπιση των άλλων 3 ειδών επιθέσεων εστιάζει στην φιλοσοφία της ενδυνάμωσης των τρεχόντων πρωτοκόλλων (ταυτοποίησης/εξουσιοδότησης) ή την επιτέλεση ανάλυσης στο επίπεδο κώδικα

Αντιμετώπιση Επιθέσεων Λεξικού

- Η απλή χρήση ισχυρότερων/μεγαλύτερων κωδικών δεν επιλύει το πρόβλημα για 3 κύριους λόγους
  - Επίβαρο υπολογισμού για ισχυρούς κωδικούς για συσκευές με περιορισμένες υπολογιστικές δυνατότητες
  - Υψηλός φόρτος αποθήκευσης λόγω μεγάλου όγκου συνδρομητών στην υποδομή edge computing
  - Η αποθήκευση διαπιστευτηρίων σε IoT συσκευές είναι εύθραυστη και τρωτή στην διαρροή κωδικών

Αντιμετώπιση Επιθέσεων Λεξικού

- Χρήση έξτρα επιπέδου ταυτοποίησης
  - Αποτυπώματα, ταυτοποίηση προσώπου, κώδικας ταυτοποίησης με SMS, γραφικά κείμενα, κα.
  - Αλλά απαιτείται συνήθως αλληλεπίδραση με τον χρήστη ενώ πρέπει να υπάρχει αυτοματοποίηση
- Επέκταση υπαρχόντων ή εισαγωγή νέων πρωτοκόλλων ταυτοποίησης
  - Balloon αλγόριθμος κατακερματισμού κωδικών με βάση συναρτήσεις τύπου memory-hard για την αύξηση του κόστους διενέργειας offline επιθέσεων λεξικού
  - Device-Enhanced Password-Authenticated Key Exchange (DEPAKE) πρωτόκολλο για την αντιμετώπιση τόσο online όσο και offline επιθέσεων χωρίς την ανάγκη PKI υποδομής

Αντιμετώπιση Επιθέσεων στο Πρωτόκολλο Ταυτοποίησης

- Ενδυνάμωση του πρωτοκόλλου
  - Υλοποίηση αναμείκτη (jammer) σημάτων και έκχυση ασύρματων πακέτων για την απαγόρευση επιθέσεων brute-force που στοχεύουν στην αποκρυπτογράφηση της WPA κίνησης
  - Εφαρμογή κρυπτογραφίας δημόσιου κλειδιού στην διαδικασία ανταλλαγής κλειδιών στο WPA
- Προστασία των κρυπτογραφικών υλοποιήσεων
  - Μηχανισμός επικύρωσης μαύρου κουτιού για την αποτροπή πιθανών πλαστοπροσωπιών ονομάτων ξενιστών
  - Συμβολική εκτέλεση για την ανίχνευση αν η TLS 1.3 υλοποίηση είναι τρωτή σε διάφορες γνωστές επιθέσεις που υπάρχουν στην έκδοση 1.2 του TLS

Αντιμετώπιση Επιθέσεων στο Πρωτόκολλο Ταυτοποίησης

- Για 4G/5G πρωτόκολλα:
  - Λύση 3 βημάτων για την αποφυγή άρνησης υπηρεσίας σε νόμιμους χρήστες: (α) προσθήκη λεπτού επιπέδου για την μεταφορά σημάτων, (β) αποσύνδεση (decoupling) τομέων στο επίπεδο 4G Radio και (γ) συντονισμός παρόμοιων συναρτήσεων σε διαφορετικά συστήματα
  - Θεωρητικό πρωτόκολλο για ταχεία ταυτοποίηση σε ετερογενή δίκτυα 5G μέσω SDN
  - Ελαφριά, κλιμακώσιμη και ασφαλής αρχιτεκτονική ταυτοποίησης κατά μήκος επιπέδων για το 5G με την χρήση RF αποτυπωμάτων ως κομμάτι πειστηρίου για την αντιμετώπιση επιθέσεων πλαστοπροσωπίας
  - Κρυπτογραφικά ασφαλές και υπηρεσιο-κεντρικό πρωτόκολλο ταυτοποίησης για το 5G με χρήση τεμαχισμού δικτύου (network slicing)

Αντιμετώπιση Επιθέσεων στο Πρωτόκολλο Εξουσιοδότησης

- Αντιμετώπιση εσφαλμένων υλοποιήσεων OAuth
  - Στατική ανάλυση κώδικα για τον έλεγχο και επιδιόρθωση των τρωτοτήτων υλοποίησης του OAuth σε 3 παρόχους (Google, Facebook & Sina)
  - Ανάπτυξη βασιζομένου σε εφαρμογές πλαισίου τύπου OAuth Manager για την αποτροπή καταχρήσεων των OAuth APIs
  - Υλοποίηση OAuth πρωτοκόλλου ειδικά για HTTP/CoAP υπηρεσίες για την υποστήριξη εξουσιοδότησης σε IoT εφαρμογές

Αντιμετώπιση Υπερπρονομιούχων Επιθέσεων

- NLP μέθοδος για τον έλεγχο ασυνεπειών μεταξύ IoT εφαρμογών (apps) και των περιγραφών τους για την ανίχνευση υπερπρονομιούχων εκμεταλλεύσεων
- Ανάλυση taint-based για την ανίχνευση και αποτροπή διαρροής ευαίσθητης πληροφορίας λόγω υπερπρονομιούχας σχεδίασης των IoT εφαρμογών
- Τεχνική ανίχνευσης (ευαίσθητης) πληροφορίας για την παρακολούθηση διαρροής από υπερπρονομιούχες εφαρμογές
- Λύση με βάση τον έλεγχο των μοντέλων για την αυτόματη ανίχνευση υπερπρονομιούχων εφαρμογών
- Σύγκριση των περιβαλλόντων (context) των συμπεριφορών (εφαρμογών) με ιστορική γνώση για τον εντοπισμό πιθανών ύποπτων ασυνεπειών
- Μαντεία περιβαλλοντικής κατάστασης (environmental situation oracles – ESOs) για την επιβολή ελέγχου πρόσβασης στο IoT μέσω καταστατικών περιβαλλόντων (situational environments)

Αντιμετώπιση Υπερπρονομιούχων Επιθέσεων

- Για κινητά
  - Γεννήτρια σημασιολογικών αδειών για Android που διερμηνεύει την (ειλικρινή) περιγραφή μιας εφαρμογής ώστε να αποδίδει τα σωστά δικαιώματα σε αυτήν
  - Αμμοκιβώτιο (sandbox) επιπέδου συστήματος για τοποθέτηση κώδικα που αιτεί ευαίσθητα δικαιώματα ώστε να απομονωθεί για περαιτέρω ανάλυση χωρίς να αποδοθούν σε αυτόν κατά λάθος προνομιούχα δικαιώματα
  - 6thSense – μηχανισμός για την απαγόρευση της κατάχρησης δικαιωμάτων προς αισθητήρες από υπερπρονομιούχες εφαρμογές με χρήση 3 αλγορίθμων μηχανικής μάθησης
  - Τεχνική εντοπισμού υπερπρονομιούχων συστατικών Android εφαρμογής με βάση αλγόριθμο αφαίρεσης γράφων και αλγόριθμο συλλογιστικής (reasoning)

Προκλήσεις

- Έλλειψη Εφαρμογής Ασφάλειας από την Σχεδίαση
- Ανικανότητα Μετανάστευσης Πλαισίων Ασφάλειας
- Κατακερματισμένος & Μη Εκλεπτυσμένος Έλεγχος Πρόσβασης
- Απομονωμένοι & Παθητικοί Μηχανισμοί Ασφάλειας

Έλλειψη Εφαρμογής Ασφάλειας από την Σχεδίαση

- Τρέχουσα εστίαση στην απόδοση αντί για την ασφάλεια κατά την σχεδίαση της αρχιτεκτονικής (εφαρμογών) edge computing
  - Εκθέτει τις υποδομές edge computing σε ποιο ευρείς επιφάνειες τρωτοτήτων

Ανικανότητα Μετανάστευσης Πλαισίων Ασφάλειας

- Τα πλαίσια ασφάλειας για υπολογιστικά συστήματα γενικού σκοπού παρέχουν ισχυρές εγγυήσεις ασφάλειας
- Όμως, δεν μπορούν να μεταναστεύσουν σε συστήματα edge computing για διάφορους λόγους όπως μικρότερη επεξεργαστική ισχύ, διαφορετικά ΛΣ & λογισμικό, διαφορετικές τοπολογίες δικτύωσης & ετερόκλητα πρωτόκολλα
- Ακόμη και αν σχεδιαστεί ένα πλαίσιο ασφάλειας για μια εφαρμογή edge computing δεν θα μπορεί να μεταναστεύσει απευθείας σε άλλα σενάρια/εφαρμογές για πολλούς λόγους, όπως ετερογένεια των συσκευών ακμής και πρωτοκόλλων επικοινωνίας

Κατακερματισμένος & Μη Εκλεπτυσμένος Έλεγχος Πρόσβασης

- Είναι κατακερματισμένος διότι διαφορετικά σενάρια edge computing μπορεί να υιοθετήσουν διαφορετικά μοντέλα ελέγχου πρόσβασης που ενδέχεται να σχεδιαστούν με τελείως διαφορετικούς τρόπους σε σχέση με τον διαχωρισμό, την απόδοση και την πρόσβαση στα δικαιώματα
  - Αυτό εμποδίζει την ανάπτυξη ενός ενιαίου και διαχειρίσιμου πλαισίου για έλεγχο πρόσβασης σε συστήματα edge computing
- Τα τρέχοντα μοντέλα ελέγχου πρόσβασης στο edge computing είναι μη εκλεπτυσμένα λόγω της πολυπλοκότητας της εκλέπτυνσης δικαιωμάτων και της μη διεξοδικής έρευνας στο πεδίο αυτό για την ανακάλυψη κατάλληλων λύσεων

Απομονωμένοι & Παθητικοί Μηχανισμοί Ασφάλειας

- Είναι απομονωμένοι διότι κάθε μηχανισμός άμυνας είναι αποτελεσματικός για μια ή μερικές μόνο επιθέσεις και καθόλου αποτελεσματικός για τις άλλες
- Είναι παθητικοί διότι οι περισσότερες λύσεις άμυνας εκτελούνται με προκαθορισμένους κανόνες και δεν έχουν την δυνατότητα επιτέλεσης αυτόνομων και ενεργών δράσεων άμυνας
  - Αυτό οδηγεί σε μια άκαμπτη και προκαθορισμένη επιφάνεια άμυνας που αναγκάζει τις περισσότερες λύσεις άμυνας να υιοθετήσουν την φιλοσοφία «ανίχνευσε και μετά επιδιόρθωσε» (“detect then patch”), η οποία είναι αποτελεσματική μετά την πραγματοποίηση των επιθέσεων που ανιχνεύονται

Μελλοντική Έρευνα

- 3 Γενικές κατευθύνσεις
  - Επινόηση ισχυρότερων λύσεων άμυνας για την αντιμετώπιση διαφορετικών επιθέσεων
  - Πρόταση νέων αρχιτεκτονικών που ενσωματώνουν μηχανισμούς ασφάλειας για την προστασία ολόκληρου του συστήματος με έναν ενιαίο τρόπο
  - Ευρεία υιοθέτηση και ανασκόπηση της φιλοσοφίας σχεδίασης με γνώμονα την ασφάλεια (security-by-design)

Μελλοντική Έρευνα

- Υλοποίηση ασφαλούς πλαισίου κατά μήκος 3 επιπέδων
  - Επίπεδο εξωτερικού, εκλεπτυσμένου ελέγχου πρόσβασης
  - Μεσαίο επίπεδο λειτουργίας ασφάλειας
  - Εσωτερικό επίπεδο ΛΣ που είναι απομονωμένο με βάση το υλικό

Εξωτερικό Επίπεδο

- Κατάλληλη σχεδίαση και αυστηρή εφαρμογή μοντέλου πρόσβασης που στηρίζεται σε τουλάχιστον 5 συστατικά πληροφορίας: ποιος, πότε, που, τι και πως
- Αποτέλεσμα
  - Μετρίαση επιθέσεων λόγω σφαλμάτων στα επίπεδα πρωτοκόλλου ή υλοποίησης
    - Οι επιθέσεις αυτές ουσιαστικά εμπίπτουν στις περισσότερες κατηγορίες

Μεσαίο Επίπεδο

- Υλοποίηση ισχυρών μηχανισμών ασφάλειας
  - Υιοθέτηση SDN για το φιλτράρισμα κακόβουλης κίνησης με βάση τα πακέτα
  - Υιοθέτηση NFV (Network Function Virtualization) (Εικονικοποίηση Λειτουργιών Δικτύου) μαζί με περισσότερο προηγμένους αλγορίθμους βαθιάς μάθησης για την ανίχνευση κακόβουλων συμπεριφορών με ένα αυτόνομο και αυτό-εξελισσόμενο τρόπο
- Αποτέλεσμα:
  - Αντιμετώπιση επιθέσεων με βάση
    - τα πακέτα (πχ. DDoS)
    - τα συσχετιζόμενα δεδομένα (απαιτεί ανίχνευση βασιζόμενη στην μάθηση)
    - αδύναμους ελέγχους πρόσβασης

Εσωτερικό Επίπεδο

- Σχεδίαση ΛΣ ενισχυμένο με απομόνωση με βάση το υλικό στο επίπεδο των συσκευών ακμής
  - Απομόνωση του κελύφους και όλων των ευαίσθητων δεδομένων της συσκευής σε διαφορετικούς ασφαλείς χώρους μέσω απομόνωσης με βάση το υλικό ώστε να είναι άνοσα από σφάλματα λογισμικού
- Αποτέλεσμα
  - Μετρίαση επιθέσεων που προκαλούνται από τρωτότητες μηδενικής ημέρας που οδηγούν σε επιθέσεις DDoS & έκχυσης κακόβουλου λογισμικού

Βιβλιογραφία

1. Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu and W. Lv, "Edge Computing Security: State of the Art and Challenges," in *Proceedings of the IEEE*, vol. 107, no. 8, pp. 1608-1631, Aug. 2019, doi: 10.1109/JPROC.2019.2918437