ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ

ΤΜΗΜΑ ΕΠΙΣΤΗΜΗΣ ΥΠΟΛΟΓΙΣΤΩΝ

ΠΑΡΟΥΣΙΑΣΗ / ΕΞΕΤΑΣΗ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Δέγκλερη Ειρήνη - Αικατερίνη
Μεταπτυχιακή Φοιτήτρια

Τμήμα Επιστήμης Υπολογιστών, Πανεπιστήμιο Κρήτης
Επόπτης Μεταπτ. Εργασίας: Καθηγητής Ε. Μαρκάτος

Τετάρτη, 21/02/2018, 16:00
Αίθουσα Κ206,Τμήμα Επιστήμης Υπολογιστών, Πανεπιστήμιο Κρήτης

" Μελέτη των ψηφιακών πιστοποιητικών πρωτοκόλλου SSL και του μοντέλου ανάκλησής τους"

ΠΕΡΙΛΗΨΗ

Η διαθέσιμη πληροφορία στο διαδίκτυο έχει αυξηθεί με τεράστιους ρυθμούς τόσο σε όγκο όσο και σε πολυπλοκότητα και η τάση αυτή προβλέπεται να συνεχιστεί. Επιπρόσθετα τα διαμοιραζόμενα δεδομένα αφορούν ευαίσθητες πληροφορίες και ως αποτέλεσμα η διασφάλιση τους είναι απαραίτητη. Στο βασικό πρωτόκολλο μεταφοράς υπερκειμένου Hypertext Transfer Protocol (HTTP) η πληροφορία είναι σε μορφή απλού κειμένου κατά την ανταλλαγή μηνυμάτων, με αποτέλεσμα οποιοσδήποτε να μπορεί να την υποκλέψει. Επίσης, πολλαπλές μελέτες έχουν δείξει την ευκολία μίας επίθεσης για τον έλεγχο μιας συνεδρίας HTTP. Οι παραπάνω λόγοι εντείνουν την ανάγκη για την ύπαρξη κρυπτογραφημένης επικοινωνίας από την πηγή στον προορισμό (E2EE: End-to-End Encryption), όχι μόνο σε ιστοσελίδες στις οποίες πραγματοποιούνται οικονομικές συναλλαγές, αλλά καθολικά. Το πρωτόκολλο HTTPS (HTTP over SSL) αναπτύσσεται για να καλύπτει τις προαναφερθείσες ανάγκες και πλέον το 2017 έχει φτάσει στο σημείο που γίνεται κανόνας και όχι η εξαίρεση.

Ένα ψηφιακό πιστοποιητικό πρωτοκόλλου Secure Sockets Layer (SSL) / Transport Layer Security (TLS) βασίζεται στην κρυπτογραφία δημοσίου κλειδιού Public Key Infrastructure (PKI), ώστε να συνδέσει ένα κρυπτογραφικό κλειδί με την οντότητα που διασφαλίζεται Εκδίδεται από κάποια αρχή πιστοποίησης - Certification Authority (CA), που θεωρείται «έμπιστο τρίτο μέρος», η οποία πραγματοποιεί μία διαδικασία επικύρωσης. Επιπρόσθετα, έχει μία προδιαγεγραμμένη περίοδο ισχύος, με συγκεκριμένη αρχή και τέλος κατά την οποία θεωρείται έγκυρο, εκτός και αν ανακληθεί. Τέλος, για να την εξακρίβωση της γνησιότητας τους οι πληροφορίες αυτές υπογράφονται με έναν κρυπτογραφικό αλγόριθμο, το αποτέλεσμα του οποίου υπολογίζεται από το πρόγραμμα περιήγησης.

Η μεταπτυχιακή αυτή διατριβή, έχει ως σκοπό της τη διερεύνηση του οικοσυστήματος των ψηφιακών πιστοποιητικών πρωτοκόλλου SSL, αναλύοντας τις βασικές τους συνιστώσες και επιχειρώντας να αναδείξει συσχετισμούς και τάσεις που συνδέονται με αυτά, ώστε ο αναγνώστης να αποκτήσει μία συνολική εικόνα της υιοθέτησης τους. Στη συνέχεια, παρουσιάζονται ενδιαφέρουσες περιπτώσεις που προκύπτουν από τα δεδομένα και συζητούνται σε βάθος πιθανές συσχετίσεις τους με ιστοσελίδες με μεγάλη επισκεψιμότητα. Επιπλέον, ελέγχεται η υπόθεση μας ότι οι ιστοσελίδες αυτές εφαρμόζουν συστηματικότερα τις βέλτιστες πρακτικές ασφάλειας. Για την ανάλυση αυτή χρησιμοποιούνται τα δημοσίως διαθέσιμα σύνολα δεδομένων του Certificate Transparency, το οποίο στοχεύει στην διαφάνεια της εξάπλωσης των ψηφιακών πιστοποιητικών καθώς και του Alexa που διατηρεί τη σειρά κατάταξης ιστοσελίδων βάσει της επισκεψιμότητας τους και των στατιστικών για κυβερνοεπιθέσεις, από το Hackmaggedon.

Κατόπιν, εξετάζεται το μοντέλο εμπιστοσύνης γύρω από τις διάφορες πτυχές των ψηφιακών πιστοποιητικών πρωτοκόλλου SSL. Ορμώμενοι από γνωστές αδυναμίες του πρωτοκόλλου SSL και του διαδόχου του TLS, αναφερόμαστε σε περιπτώσεις όπου τα ψηφιακά πιστοποιητικά έχουν χρησιμοποιηθεί για να καλύψουν κακόβουλη συμπεριφορά. Συμπληρωματικά αναφερόμαστε σε περιπτώσεις όπου οι αρχές πιστοποίησης φαίνονται ανεπαρκείς στη διαδικασία της επικύρωσης των οντοτήτων για τις οποίες εγγυώνται Στη συνέχεια, γίνεται ιδιαίτερη μνεία στους μηχανισμούς ανάκλησης των πιστοποιητικών, υπογραμμίζοντας τη σημασία τους δείχνοντας συσχετίσεις και στατιστικά γύρω από αυτούς και αναφέροντας γνωστές επιθέσεις που οφείλονται στην αμέλεια της σωστής εφαρμογής του ελέγχου των μηχανισμών αυτών. Καθώς το φαινόμενο αυτό συνδέεται άμεσα με τις αδυναμίες των υπαρχουσών λύσεων για τον έλεγχο της κατάστασης ισχύος ή την ανάκληση των πιστοποιητικών, συγκρίνουμε τα πιο διαδεδομένα πρωτόκολλα και κάποιες πολλά υποσχόμενες, πρόσφατα προταθείσες λύσεις.

Σαν προοίμιο μελλοντικής ενασχόλησης και έρευνας, συλλογιζόμαστε εάν η υποδομή του δημόσιου κλειδιού X.509 είναι ικανή να υποστηρίξει το εξαιρετικά μεγάλου μεγέθους δίκτυο των διασυνδεδεμένων συσκευών που απαρτίζουν το “Διαδίκτυο των Πραγμάτων” - Internet of Things (IoT), το οποίο αποτελείται από ενσωματωμένες συσκευές με περιορισμένες υπολογιστικές δυνατότητες. Έχοντας ως έναυσμα την φύση αυτών των συσκευών συζητάμε λιγότερο απαιτητικά πρωτόκολλα, καθώς το πρωτόκολλο SSL/TLS έχει αποδειχθεί επαχθές στην παραδοσιακή του μορφή και προτείνουμε παραλλαγές γνωστών πρωτοκόλλων που μπορούν να προσαρμοστούν στην αρχιτεκτονική τους.

Συνοψίζοντας, στην πτυχιακή αυτή εργασία αναλύεται η εξάπλωση των ψηφιακών πιστοποιητικών δημοσίου κλειδιού και πως αυτή συσχετίζεται με την επισκεψιμότητα των ιστοσελίδων και πως επηρεάζεται από κυβερνοεπιθέσεις και γνωστοποιήσεις γνωστών αδυναμιών του πρωτοκόλλου. Δίνεται επίσης έμφαση στους μηχανισμούς ελέγχου ανάκλησης των πιστοποιητικών και των αδυναμιών που έχουν σημειωθεί σε αυτούς και αναλύονται προτεινόμενες λύσεις σε αυτές. Εν κατακλείδι καθώς οι συσκευές του IoT είναι ήδη αρκετά διαδεδομένες χωρίς να έχουν τις απαραίτητες προϋποθέσεις για την διασφάλιση της ασφαλούς επικοινωνίας, αναφερόμαστε στα βασικά προβλήματά τους και τις λύσεις που μπορούν να προσφέρουν τα ψηφιακά πιστοποιητικά, με σκοπό να προετοιμαστεί το έδαφος για μελλοντικές εργασίες.

Degkleri Eirini- Aikaterini
M.Sc. Thesis

Computer Science Department
University of Crete
Master's Thesis Supervisor: Professor Evangelos Markatos

Wednesday, 21/02/2018, 16:00
Room K206, Computer Science Dept., University of Crete

“Study of the SSL certificates and their revocation model”

ABSTRACT

The information shared over the Internet today is enormous, very personal and thus it must be secured. Several studies have pointed out the simplicity of HTTP session hijacking

attacks and this stresses the fact that encrypted end to end communication is not a necessity only for websites with economic transactions. HTTP over SSL (HTTPS) is evolving and in 2017 it has reached the point where it is becoming the norm rather than the exception. TLS protocol, the successor of SSL, has room for improvement and so do the SSL/TLS certificates, which are used to secure and authenticate trusted entities.

An SSL or PKIX certificate binds a cryptographic key to a certain subject. It has a predefined validity period, during which it is considered trusted unless it is revoked. To attest its validity it is issued by a Certification Authority (CA), which is a trusted third party. One certificate may secure one or many entities, under a validation process which is performed by the CA. Moreover, to sign this information, the issuer uses a signature algorithm, that is computed by the browser.

This thesis is a measurement study that aims to shed light on the ecosystem of SSL certificates so that the reader can have an overall perspective on how they are adopted. Initially we analyze their basic components and attempt to indicate correlations and trends, and consequently, we discuss interesting cases within the data and possible correlations of certificates with high traffic sites' maintenance and with known attacks. To this end, Certificate Transparency's public data set, along with Alexa's top sites and Hackmaggedon statistics on cyber attacks are used.

Additionally, the trust model around different aspects of the SSL certificates is closely examined. First, after reviewing known weaknesses, we explore cases where certificates were used as a mean to conceal rogue behavior and last we show where certification authorities fail to correctly validate secured entities. Furthermore, this study focuses on revocation to measure the trends around it and emphasizes the importance of revocation, by demonstrating known cases of attacks, which were due to the negligence of status checking. Additionally, since the main reason that revocation checking mechanisms fail is due to the related protocols applied, we take a step further to analyze and compare existing solutions and newly introduced promising protocols.

As a prime to future work, we contemplate whether the PKIX infrastructure is suitable to support the vast network of the Internet of Things, which is comprised of embedded devices with limited computational capabilities. SSL/TLS protocol proves to be burdensome in its traditional state, so we discuss less demanding protocols and variations tailored to their infrastructure.