Ασφάλεια Δικτύων και Υπηρεσιών

ΧΑΡΟΚΟΠΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ
HAROKOPIO UNIVERSITY

Project 2

Όνομα: **ΑΜ:**

Κωνσταντίνος Κοκκορόγιαννης 20111

Πρώτο μέρος

Εισαγωγή

Το HTTPs (Hypertext Transfer Protocol Secure) μέσω των SSL/TLS πρωτοκόλλων χρησιμοποιεί public key για την κρυπτογράφηση. Απώτερος στόχος είναι να προστατεύονται οι επικοινωνίες που πραγματοποιούνται μέσω των προγραμμάτων περιήγησης στο διαδίκτυο.

Οι servers παρέχουν ένα δημόσιο κλειδί που χρησιμοποιείται για τη δημιουργία κρυπτογραφημένης σύνδεσης, για όλες τις επακόλουθες ανταλλαγές δεδομένων μεταξύ client-server που πραγματοποιούνται κατά την περιήγηση των χρηστών στο διαδίκτυο.

Ωστόσο, η λήψη ενός δημόσιου κλειδιού από μόνη της δεν εγγυάται ότι η εταιρεία, ο οργανισμός ή το άτομο και κατ'επέκταση ο εκάστοτε server με τον οποίο αλληλεπιδρούμε ανήκει πράγματι στα επιθυμητά πρόσωπα-εταιρείες.

Αυτό που παρατηρείται συχνά είναι ότι κακόβουλοι χρήστες (hackers) "παρεμβαίνουν" στα δίκτυα έτσι ώστε να είναι σε θέση να παρέχουν τα δικά τους κλειδιά, διακυβεύοντας έτσι την ασφάλεια των χρηστών σε κάθε επικοινωνία.

Τα προγράμματα περιήγησης το αποτρέπουν με τον έλεγχο ταυτότητας για τους HTTPS servers. Αυτό επιτυγχάνεται με την χρήση πιστοποιητικών, τα οποία είναι ψηφιακά έγγραφα που δεσμεύουν ένα δημόσιο κλειδί σε ένα μεμονωμένο subject.

Η δέσμευση επιβεβαιώνεται με την κατοχή μιας αξιόπιστης Certification Authority (CA), δηλαδή μιας αρχής πιστοποίησης, όπως για παράδειγμα η SSL.com, η οποία συμβάλλει στην επαλήθευση της ταυτότητας των υποψήφιων κατόχων πιστοποιητικών, μέσω αυτοματοποιημένων και μη ελέγχων, σε κατάλληλες βάσεις δεδομένων, προκειμένου να αξιολογήσουν τους υποψήφιους κατόχους πιστοποιητικών.

Να σημειωθεί ότι τα προγράμματα περιήγησης είναι διαμορφωμένα κατά τέτοιο τρόπο, ώστε να έχουν τουλάχιστον 100 πιστοποιητικά από CAs. Οποιοδήποτε δημόσιο κλειδί πιστοποιηθεί από CAs, τότε αυτομάτως γίνεται αποδεκτό από τα προγράμματα περιήγησης.

Η μορφή του X.509

Τα πιστοποιητικά όπως αναφέρθηκε και παραπάνω είναι ουσιαστικά ορισμένα ψηφιακά αρχεία. Αυτό σημαίνει ότι πρέπει να ακολουθούν μια μορφή αρχείου για την αποθήκευση πληροφοριών (π.χ. υπογραφές, κλειδιά, εκδότες κ.λπ.). Επίσης, πρέπει να ανταλλάσσονται με τρόπο που να διασφαλίζει ότι αυτός που παρουσιάζει ένα πιστοποιητικό διαθέτει το ιδιωτικό κλειδί που σχετίζεται με το δημόσιο κλειδί που περιέχεται στο πιστοποιητικό.

Στο σημείο αυτό αξίζει να αναφερθούν ορισμένοι κανόνες για τα ιδιωτικά και τα δημόσια PKIs, καθώς και για το πρότυπα που έχουν επικρατήσει μέχρι σήμερα. Τα private PKI configurations μπορούν να εφαρμόσουν οποιαδήποτε μορφή για τα πιστοποιητικά τους, ενώ τα δημόσια PKIs που θεωρούνται εμπιστευτικά (δηλαδή αυτά που εμπιστεύονται τα προγράμματα περιήγησης), πρέπει να συμμορφώνονται με το πρότυπο RFC 5280.

Το RFC 5280 περιγράφει έναν τυπικό αλγόριθμο που ακολουθούν τα προγράμματα περιήγησης για την επικύρωση του path ενός X.509 πιστοποιητικού. Να σημειωθεί, ότι το RFC 5280 απαιτεί τη χρήση της μορφής X.509 v3. Συνεπώς, παρατηρείται ότι με την πάροδο του χρόνου βγαίνουν συνεχώς νέες εκδόσεις, γεγονός που δείχνει ότι υπήρξαν διάφορες ευπάθειες σε προηγούμενες εκδόσεις, τις οποίες εκμεταλλεύτηκαν κακόβουλοι χρήστες προκειμένου να υποκλέψουν χρήσιμες για εκείνους πληροφορίες.

Επιπλέον, το X.509 v3 περιέχει ορισμένα καινούργια features σε αντίθεση με προηγούμενες εκδόσεις του. Πιο συγκεκριμένα, επιτρέπει στα πιστοποιητικά να περιλαμβάνουν επιπλέον δεδομένα, όπως περιορισμούς χρήσης ή πληροφορίες πολιτικής, ως επεκτάσεις. Τέλος, να σημειωθεί ότι τα προγράμματα περιήγησης μπορούν να αγνοήσουν μη έγκυρες ή μη αναγνωρισμένες επεκτάσεις.

Διαδικασία ελέγχου ενός πιστοποιητικού

Τα προγράμματα περιήγησης πραγματοποιούν iteration για όλα τα πιστοποιητικά με βάση το path τους, ξεκινώντας από το root certificate. Με αυτόν τον τρόπο καταφέρνουν να επικυρώσουν τις βασικές πληροφορίες και τις κρίσιμες επεκτάσεις κάθε πιστοποιητικού. Εάν η διαδικασία ολοκληρωθεί ακόμη και για το τελευταίο πιστοποιητικό του path χωρίς σφάλματα, τότε το path γίνεται αποδεκτό και από εδώ και στο εξής θεωρείται έγκυρο. Ενώ εαν δημιουργηθούν σφάλματα, τότε το path δεν είναι έγκυρο. Επίσης, τα προγράμματα περιήγησης πρέπει πάντα να επαληθεύουν βασικές πληροφορίες πιστοποιητικού, όπως η υπογραφή ή ο εκδότης. Παρακάτω θα παρουσιαστούν ορισμένα από τα βασικά βήματα που απαιτούνται για τον έλεγχο ενός πιστοποιητικού

- **Επαλήθευση της ακεραιότητας**

Η υπογραφή στο πιστοποιητικό μπορεί να επαληθευτεί χρησιμοποιώντας κανονική κρυπτογραφία δημόσιου κλειδιού. Εάν η υπογραφή δεν είναι έγκυρη, τότε το πιστοποιητικό θεωρείται τροποποιημένο μετά την έκδοσή του και συνεπώς απορρίπτεται.

- **Επαλήθευση της εγκυρότητας**

Η περίοδος ισχύος ενός πιστοποιητικού είναι το χρονικό διάστημα κατά το οποίο το CA εγγυάται ότι θα διατηρήσει πληροφορίες σχετικά με την κατάστασή του. Πρέπει να απορρίπτονται τυχόν πιστοποιητικά με περίοδο ισχύος που λήγει πριν ή αρχίζει μετά την ημερομηνία και ώρα του ελέγχου επικύρωσης.

➢ **Επαλήθευση του εκδότη (issuer)**

Τα πιστοποιητικά συνήθως συνδέονται με δύο οντότητες:

1. Ο εκδότης, που είναι η οντότητα που κατέχει το κλειδί υπογραφής και
2. Το θέμα (subject), το οποίο αναφέρεται στον κάτοχο του δημόσιου κλειδιού που επικυρώνει το πιστοποιητικό.

Πρέπει να γίνεται έλεγχος έτσι ώστε να διασφαλίζεται ότι το πεδίο έκδοσης πιστοποιητικού είναι ίδιο με το πεδίο θέματος του προηγούμενου πιστοποιητικού στο path. Για πρόσθετη ασφάλεια, οι περισσότερες εφαρμογές PKI επαληθεύουν επίσης ότι το κλειδί του εκδότη είναι το ίδιο με το κλειδί που υπέγραψε το τρέχον πιστοποιητικό. (Αυτό δεν συμβαίνει για το root certificate)

➢ **΄Ελεγχος της κατάστασης ανάκλησης (revocation status)**

Όταν εκδίδεται πιστοποιητικό, αναμένεται να χρησιμοποιείται για ολόκληρη την περίοδο ισχύος του. Ωστόσο κατά τη διάρκεια αυτή, ενδέχεται να υπάρξουν διάφορες περιστάσεις οι οποίες μπορεί να προκαλέσουν την ακύρωση ενός πιστοποιητικού πριν την προβλεπόμενη ημερομηνία λήξης του. Τέτοιες περιστάσεις μπορεί να περιλαμβάνουν ένα θέμα που αλλάζει στην πορεία το όνομά του ή τον εντοπισμό ενός ύποπτου συμβιβασμού του ιδιωτικού κλειδιού. Σε τέτοιες περιπτώσεις, το CA πρέπει να ανακαλέσει το αντίστοιχο πιστοποιητικό.

➢ **Επεξεργασία κρίσιμων επεκτάσεων**

Όπως αναφέρθηκε και παραπάνω, τα προγράμματα περιήγησης προχωρούν στην επικύρωση όλων των υπόλοιπων επεκτάσεων που το τρέχον πιστοποιητικό χαρακτηρίζει ως κρίσιμες, προτού προχωρήσουν στην επόμενη. Εάν ένα πρόγραμμα περιήγησης φτάσει στο root certificate μιας διαδρομής χωρίς σφάλμα, τότε το path γίνεται αποδεκτό ως έγκυρη. Εάν δημιουργηθούν σφάλματα, το path επισημαίνεται ως μη έγκυρο και δεν δημιουργείται ασφαλής σύνδεση.

Δεύτερο μέρος

Με βάση την θεωρία και την χρήση της Python η οποία παρέχει πληθώρα βοηθητικών βιβλιοθηκών που απλοποιούν πολύ αρκετές λειτουργίες ασφάλειας, δημιουργήθηκε μία εφαρμογή η οποία δέχεται σαν παράμετρο ένα η πολλαπλά domain names και επιστρέφει ένα report για το πιστοποιητικό όπως φαίνεται και στα ακόλουθα παραδείγματα εκτέλεσης.
Στον κώδικα υπάρχουν αναλυτικά σχόλια για όλους τους ελέγχους που πραγματοποιούνται.

Παραδείγματα εκτέλεσης του κώδικα

Για την εκτέλεση χρειάζεται το όνομα του αρχείου και τουλάχιστον ένα argument σαν παράμετρο από το user input (domain name) όπως φαίνεται στην ακόλουθη εικόνα:

```
kostasmac@Kostass-MacBook-Pro project-2 % python verify-certificate.py


Usage:
python verify-certificate.py <domain Name>
EXAMPLE: python verify-certificate.py www.hua.gr
OR with multiple domains: python verify-certificate www.hua.gr www.google.com
```

Στην ακόλουθη εικόνα φαίνεται ένα παράδειγμα εκτέλεσης με παράμετρο το domain name www.google.com :

```
kostasmac@Kostass-MacBook-Pro project-2 % python verify-certificate.py www.google.com
The issuer GTS CA 1O1 for the following domain is trusted:
www.google.com
Success! The host name: www.google.com matches to the common name on the certificate.
Expiry Date: 2021-03-30 Expiry Day: 54
Certificate's version is: 3
kostasmac@Kostass-MacBook-Pro project-2 %
```

Στην ακόλουθη εικόνα φαίνεται ένα παράδειγμα εκτέλεσης με παράμετρο το domain name www.hua.gr :

```
kostasmac@Kostass-MacBook-Pro project-2 % python verify-certificate.py www.hua.gr
The issuer TERENA SSL CA 3 for the following domain is trusted:
*.hua.gr
Success! The host name: www.hua.gr matches to the common name on the certificate.
Expiry Date: 2021-02-22 Expiry Day: 18
Certificate's version is: 3
kostasmac@Kostass-MacBook-Pro project-2 %
```

Στην ακόλουθη εικόνα φαίνεται ένα παράδειγμα εκτέλεσης με πολλαπλές παραμέτρους (π.χ. www.hello.gr , www.facebook.com) :

```
kostasmac@Kostass-MacBook-Pro project-2 % python verify-certificate.py  www.hello.gr www.facebook.com
The issuer for the following domain doesn't belong in trusted issuer's list:
sni.cloudflaressl.com
Warning! The host name: www.hello.gr doesn't match to the common name on the certificate.
Expiry Date: 2021-07-22 Expiry Day: 168
Certificate's version is: 3
The issuer DigiCert SHA2 High Assurance Server CA for the following domain is trusted:
*.facebook.com
Success! The host name: www.facebook.com matches to the common name on the certificate.
Expiry Date: 2021-03-21 Expiry Day: 46
Certificate's version is: 3
kostasmac@Kostass-MacBook-Pro project-2 %
```

Χρήσιμες πηγές για την υλοποίηση

1. https://rambling-ideas.salessandri.name/validating-a-ssl-certificate-in-python/
2. https://github.com/wbond/certvalidator
3. https://stackoverflow.com/questions/1087227/validate-ssl-certificates-with-python
4. https://rambling-ideas.salessandri.name/validating-a-ssl-certificate-in-python/
5. https://access.redhat.com/articles/2039753