Χαροκόπειο Πανεπιστήμιο
Τμήμα Πληροφορικής και Τηλεματικής

Ασφάλεια Δικτύων και Υπηρεσιών

Έλεγχος εγκυρότητας πιστοποιητικού

Τσερπέ Παρασκευή

Α.Μ. : 21117

Το **X.509** είναι διεθνές πρότυπο που καθορίζει τον τρόπο λειτουργίας των Υποδομών Δημόσιου Κλειδιού (Public Key Infrastructure, PKI). Το πρότυπο προδιαγράφει τις μορφές διάθεσης της σχετικής πληροφορίας (κλειδιά, πιστοποιητικά, λίστες ανάκλησης) και τους αλγορίθμους επαλήθευσης του κύρους ενός πιστοποιητικού.

Πιστοποιητικά και επαλήθευση

Στο X.509, η Αρχή Πιστοποίησης (Certification Authority, συντομογραφία: CA) εκδίδει ένα πιστοποιητικό το οποίο περιλαμβάνει πληροφορίες για μια οντότητα-υποκείμενο (subject). Το υποκείμενο του πιστοποιητικού μπορεί να είναι ένα όνομα (common name) ή κάποια άλλη οντότητα (alternative name), όπως μια διεύθυνση ηλεκτρονικού ταχυδρομείου, μια IP διεύθυνση ή ένα όνομα DNS. Ένα πιστοποιητικό X.509 περιέχει τις ακόλουθες πληροφορίες:

- Πιστοποιητικό
- Έκδοση X.509 (π.χ. 3)
- Αύξων Αριθμός

- Αλγόριθμος
- Εκδούσα Αρχή Πιστοποίησης
- Περίοδος εγκυρότητας
- Όχι νωρίτερα από
- Όχι αργότερα από
- Υποκείμενο Πληροφορίας δημόσιου κλειδιού υποκειμένου
- Αλγόριθμος δημόσιου κλειδιού
- Τιμή δημόσιου κλειδιού
- Προαιρετικές πληροφορίες
- Επεκτάσεις (extensions)
- Αλγόριθμος υπογραφής πιστοποιητικού
- Υπογραφή πιστοποιητικού

Η Αρχή Πιστοποίησης υπογράφει ψηφιακά τις πληροφορίες του πιστοποιητικού. Έτσι, όποιος διαθέτει το δημόσιο κλειδί της μπορεί να επαληθεύσει την ισχύ των πληροφοριών που φέρει το πιστοποιητικό. Κάθε Αρχή Πιστοποίησης διαθέτει δικό της πιστοποιητικό, υπογεγραμμένο από κάποια άλλη αρχή πιστοποίησης (η οποία είναι γνωστή ως ενδιάμεση αρχή πιστοποίησης, intermediate CA) ή από τον εαυτό της (γνωστή ως αρχική αρχή πιστοποίησης, root CA). Επομένως η επαλήθευση της εγκυρότητας ενός πιστοποιητικού μπορεί να γίνει ακολουθώντας μια αλυσίδα Αρχών Πιστοποίησης μέχρι το φτάσιμο σε μια έμπιστη Αρχή Πιστοποίησης (trusted CA).

Κάθε λειτουργικό σύστημα διανέμεται με έναν κατάλογο έμπιστων αρχικών και ενδιάμεσων Αρχών Πιστοποίησης. Αυτό σημαίνει ότι μπορεί να επαληθεύσει την εγκυρότητα ενός μεγάλου αριθμού πιστοποιητικών.

Βασική επεξεργασία ενός πιστοποιητικού

Το πρώτο βήμα λοιπόν είναι να ανακτήσουμε την αλυσίδα Αρχών πιστοποίησης. Με μία από τις πιθανές μεθόδους (tlsv1.2, tlsv1.1, tlsv1.0, ssl) δημιουργούμε το context φορτώνουμε τον κατάλογο έμπιστων αρχικών και ενδιάμεσων Αρχών Πιστοποίησης, πραγματοποιούμε τη σύνδεση, κάνουμε handshake μέσω της οποίας και λαμβάνουμε όλη την αλυσίδα πιστοποιητικών. Έπειτα θα πρέπει να ελέγξουμε την εγκυρότητα του server certificate(chain[0]) που βρίσκεται την αρχή της αλυσίδας. Η διαδικασία αυτή περιλαμβάνει τα εξής στάδια:

1. Ο client (π.χ. ένας browser) επαληθεύει την περίοδο ισχύος ενός πιστοποιητικού. Πρόκειται στην ουσία για το χρονικό διάστημα κατά το οποίο η CA που υπογράφει, εγγυάται ότι θα διατηρήσει πληροφορίες σχετικά με την κατάστασή του. Απορρίπτονται τυχόν πιστοποιητικά με περίοδο ισχύος που λήγει πριν

(“not_valid_before”) ή ξεκινά μετά (“not_valid_after”) την ημερομηνία του ελέγχου επικύρωσης.

2. Έλεγχος του issuer. Χρήσιμοι ορισμοί αποτελούν
    a. Issuer: μοναδικό όνομα για την CA που εξέδωσε το πιστοποιητικό.
    b. Subject: το όνομα της οντότητας (υπολογιστής, χρήστης, συσκευή δικτύου κ.λπ.) στην οποία η CA εξέδωσε το πιστοποιητικό.

    Σε αυτό το σημείο ελέγχεται αν το common name του πιστοποιητικού περιλαμβάνει τον host του server. Η επαλήθευση εν δυνάμει επεκτείνεται και στα extensions, συγκεκριμένα στα subject alternative names (DNS Name & IP Address).
3. Έλεγχος για το αν πρόκειται για ενα self-singed πιστοποιητικό. Τέτοιου είδους πιστοποιητικά έχουν εκδοθεί από χρήστες για προσωπική χρήση και δεν σχετίζονται με κάποια "έμπιστη" Αρχή έκδοσης πιστοποιητικών (CA).
4. Ο client ελέγχει επίσης το revocation status ενός πιστοποιητικού. Όταν εκδίδεται ένα πιστοποιητικό αναμένεται να είναι σε χρήση για όλη την περίοδο ισχύος του. Υπάρχει όμως περίπτωση να ακυρωθεί ένα πιστοποιητικό πριν τη φυσική του λήξη. Τέτοιες καταστάσεις μπορεί να είναι ότι το subject αλλάζει όνομα, ύποπτη παραβίαση κλειδιού κ.α. Σε περιπτώσεις όπως αυτή, μια CA πρέπει να ανακαλέσει το αντίστοιχο πιστοποιητικό. Οι εκάστοτε clients των χρηστών οφείλουν να ανιχνεύσουν πότε ένα πιστοποιητικό έχει ανακληθεί χρησιμοποιώντας τις αντίστοιχες λίστες ανάκλησης (πρωτόκολλο RFC 5280).

    Λίστες ανάκλησης πιστοποιητικών (CRL): Οι αρχές έκδοσης πιστοποιητικών εκδίδουν περιοδικά μια υπογεγραμμένη, με χρονική σφραγίδα λίστα ανακληθέντων πιστοποιητικών που ονομάζεται λίστα ανάκλησης πιστοποιητικών (CRL). Τα CRL διανέμονται σε δημόσια διαθέσιμα αποθετήρια και οι browsers μπορούν να αποκτήσουν και να συμβουλευτούν το πιο πρόσφατο CRL της CA κατά την επικύρωση ενός πιστοποιητικού.

    Πρωτόκολλο κατάστασης πιστοποιητικού στο διαδίκτυο (OCSP): το OCSP επιτρέπει σε ένα πρόγραμμα περιήγησης να ζητά την κατάσταση ανάκλησης ενός συγκεκριμένου πιστοποιητικού από έναν OCSP server (ονομάζεται επίσης reponder).

Παίρνουμε λοιπόν την απάντηση σε der format, το μετατρέπουμε σε pem και έπειτα σε x.509. και ελέγχουμε αν το certificate status = GOOD. Εφόσον οι παραπάνω έλεγχοι ολοκληρωθούν επιτυχώς, συνεχίζουμε με την επαλήθευση της αλυσίδας των πιστοποιητικών (CA trusted). Συγκεκριμένα, δημιουργούμε ένα X509store που είναι μια κλάση της OpenSSL Python βιβλιοθήκης, και φορτώνουμε τον κατάλογο έμπιστων αρχικών και ενδιάμεσων Αρχών Πιστοποίησης. Εν συντομία, η προηγούμενη διαδικασία διατρέχει την αλυσίδα πιστοποιητικών ελέγχοντας για κάθε πιστοποιητικό ότι ο issuer του, αναπαριστά το γειτονικό πιστοποιητικό. Όταν φτάσει στο τελευταίο πιστοποιητικό της αλυσίδας (root CA certificate) ελέγει ότι βρίσκεται στην λίστα έμπιστων CA του λειτουργικού συστήματος.

Περαιτέρω συνιθησμένοι έλεγχοι των clients κατά την ανάλυση εγκυρότητας ενός πιστοποιητικού

Η μορφή X.509 v3 επιτρέπει σε μια CA να ορίζει περιορισμούς σχετικά με τον τρόπο επικύρωσης και χρήσης κάθε πιστοποιητικού ως κρίσιμες επεκτάσεις. Κάθε πιστοποιητικό στο path μπορεί να επιβάλλει πρόσθετους περιορισμούς στους οποίους πρέπει να υπακούουν όλα τα επόμενα πιστοποιητικά. Οι περιορισμοί αυτοί περιλαμβάνουν:

1. Περιορισμοί ονόματος.
2. Περιορισμοί πολιτικής.
3. Βασικοί περιορισμοί, όπως το μήκος του path.
4. Περιορισμοί στην χρήση κλειδιού.
5. Επεξεργασία κρίσιμων επεκτάσεων.