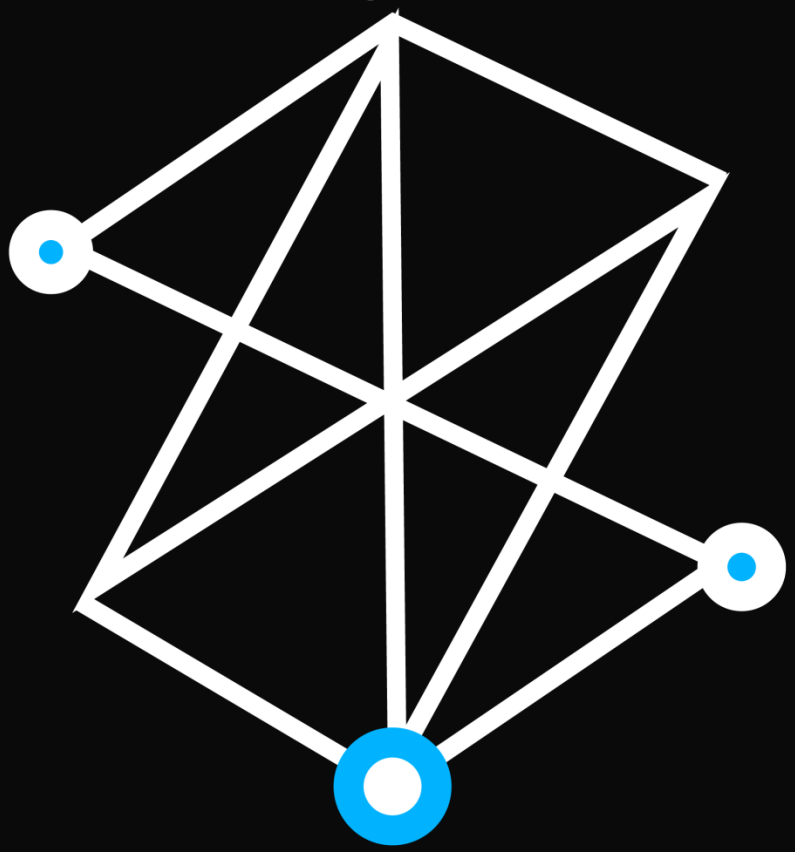
PKI – Παρόν και μέλλον



Παπίτσης Δημήτρης
Senior Premier Field Engineer
Microsoft Hellas

Public Key Infrastructure (PKI)

Ο συνδυασμός λογισμικού, τεχνολογιών κρυπτογράφησης, διαδικασιών και υπηρεσιών που καθιστούν ασφαλείς τις ηλεκτρονικές επικοινωνίες & συναλλαγές.

Αρχή πιστοποίησης

Ανακληθέντα πιστοποιητικά

Πιστοποιητικά

Εφαρμογές χρήσης PKI

«Χρόνια» προβλήματα του PKI

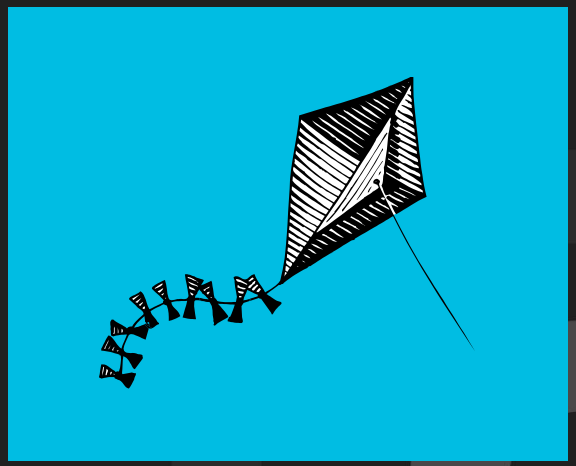
- Αδύναμοι αλγόριθμοι hashing (πχ, MD5)
  - Rogue CAs
- Παλαιό πρότυπο για CAs (X.509)
  - Μη ύπαρξη delegation, exploits
- Κανένας ευρέως αποδεκτός οργανισμός ελέγχου
  - CAs που καταλήγουν ξέφραγα αμπέλια
- Ανάκληση πιστοποιητικών (certificate revocation)
  - Μη αποτελεσματικές διαδικασίες
- Ενδοεταιρικά Certification Authorities (certificate revocation)
  - Προβλήματα trust, διαχείρισης

Πρότυπο για PKI – 1ο θέμα

- X.509, η βάση για το PKI - από το 1988! Τρέχουσα Ver. 3 από το 1996
- Η ασφάλειά του βασίζεται στην ποιότητα του client κώδικα που κάνει τον έλεγχο!
- Δεν υφίσταται η έννοια του delegation (περιορισμού έκδοσης πιστοποιητικών από intermediate CAs βάσει namespace ή/και attributes)

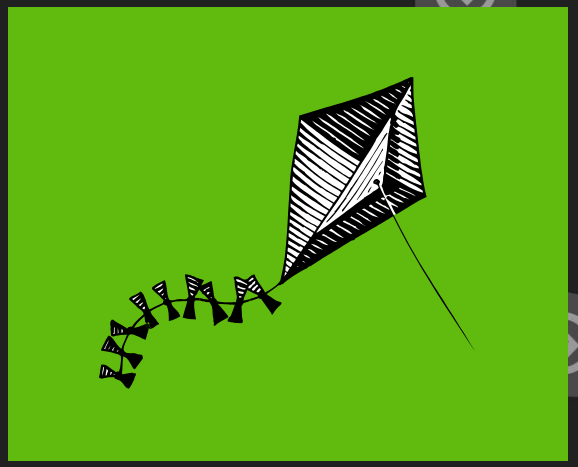
Έλλειψη ελέγχου – 2ο θέμα

- Προβληματική μεθοδολογία αυτόματου revocation των trusted root CA
- Κανένας κεντρικός έλεγχος των trusted root CAs
- Κάποια CAs επιτρέπουν έκδοση πιστοποιητικών χωρίς CRLs
- Ανάγκη εμπιστοσύνης intermediate CAs



Η περίπτωση της Diginotar

- Trusted root CA, χειριζόταν intermediate CA για την Ολλανδική κυβέρνηση
- Το 2011 έγινε παράνομη έκδοση πιστοποιητικού "*.google.com" χωρίς να το αντιληφθεί κανείς
  - Δεν είχε συστήματα ελέγχου έκδοσης παράνομων πιστοποιητικών
  - Δεν είχε δικλείδες ασφαλείας στη χρήση servers (AV...)
  - Δεν είχε κανένα σύστημα audit - logging
- Το πιστοποιητικό χρησιμοποιήθηκε στο Ιράν για man-in-the-middle attack σε όποιον χρησιμοποιούσε υπηρεσίες της Google
- Το CA certificate αφαιρέθηκε από όλους τους browsers αργότερα με update



Ανάκληση πιστοποιητικών – 3ο θέμα

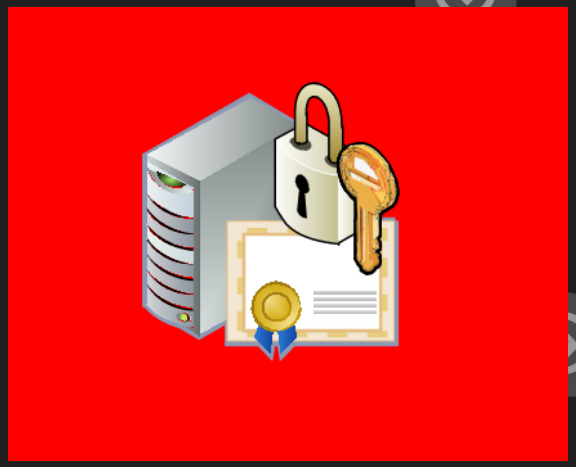
- CRL: Certificate Revocation List (RFC 3280)
  - Εκδίδεται από το CA και είναι διαθέσιμη με HTTP (συνήθως), LDAP κα.
  - Περιέχει τα serial number(s) των revoked certificate(s).
- Πολλά τα προβλήματα
  - Προαιρετικός έλεγχος (client-side)
  - Μεγάλος χρόνος επικοινωνίας με CRL
  - Κίνδυνος μη διαθεσιμότητας λόγω DDoS
  - Rogue CRLs (προαιρετική υπογραφή)
  - Κίνδυνος λανθασμένων revocations

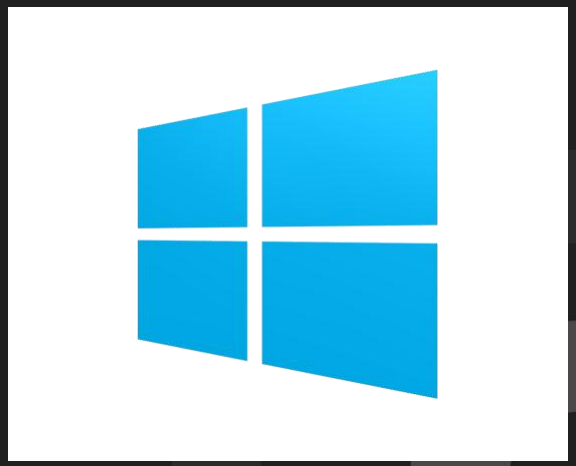
Ο Chrome «παρατά» το μοντέλο CRL/OCSP

- Η πρόταση/λύση της Google αντί για CRLs:
  - Τα CA θα στέλνουν στην Google τα revoked certificates
    - Ποιος θα κρίνει ποια;
  - Η λίστα θα γίνεται update για τον browser και θα αποστέλλεται
    - Κάθε πότε; Ποιοι θα είναι μέσα στη λίστα;
    - Πολλοί οργανισμοί απενεργοποιούν τα automatic updates (όχι τα CRL/OCSP requests)

Ενδοεταιρικά CAs – 4ο θέμα

- Windows Server, EJBCA κλπ.
  - Εύκολα στην εγκατάσταση και τη διαχείριση
  - Πολύ μικρό κόστος υλοποίησης
- Όμως:
  - Συνήθως με έλλειμα ασφάλειας
  - Δεν υπάρχει lifecycle management
  - Απαιτεί δομές και επιπλέον διαχειριστικό κόστος για υψηλή διαθεσιμότητα





Άρα …πεθαίνει το PKI?

Λύσεις για τη νέα εποχή

- Αδύνατοι αλγόριθμοι hashing (πχ, MD5)
  - Καινούργιοι αλγόριθμοι (SHA-256 κλπ.), υποστήριξη clients (OS, browser, custom-made apps)
- Παλαιό πρότυπο για CAs (X.509)
  - Συνεχίζουμε ως έχουμε
- Κανένας ευρέως αποδεκτός οργανισμός ελέγχου
  - Δυστυχώς (ή ευτυχώς;) καμία ενέργεια ακόμα…
- Ανάκληση πιστοποιητικών (certificate revocation)
  - Συνδυασμός updates/CRLs/OCSPs
- Ενδοεταιρικά Certification Authorities (certificate revocation)
  - Cloud CAs, IT Ops