HTTPS - HSTS

Π. Αγγελάτος, Δ. Ζήνδρος

Μία μικρη ιστορία

1. Η Alice πάει σε μία καφετέρια
2. Συνδέεται στο public Wifi
3. Συνδέεται στο online banking της
4. ?!?!?
5. Χάνει όλα της τα λεφτά

Το πρόβλημα του HTTP

ΟΛΑ τα δεδομένα στέλνονται
χωρίς κρυπτογράφηση στο δίκτυο

Ένας τρίτος μπορεί να:

- Δει πού μπαίνουμε
- Δει τις σελίδες που βλέπουμε
- Πάρει τους κωδικούς μας
- Αλλάξει αυτό που βλέπουμε

Wireshark Demo

HTTPS

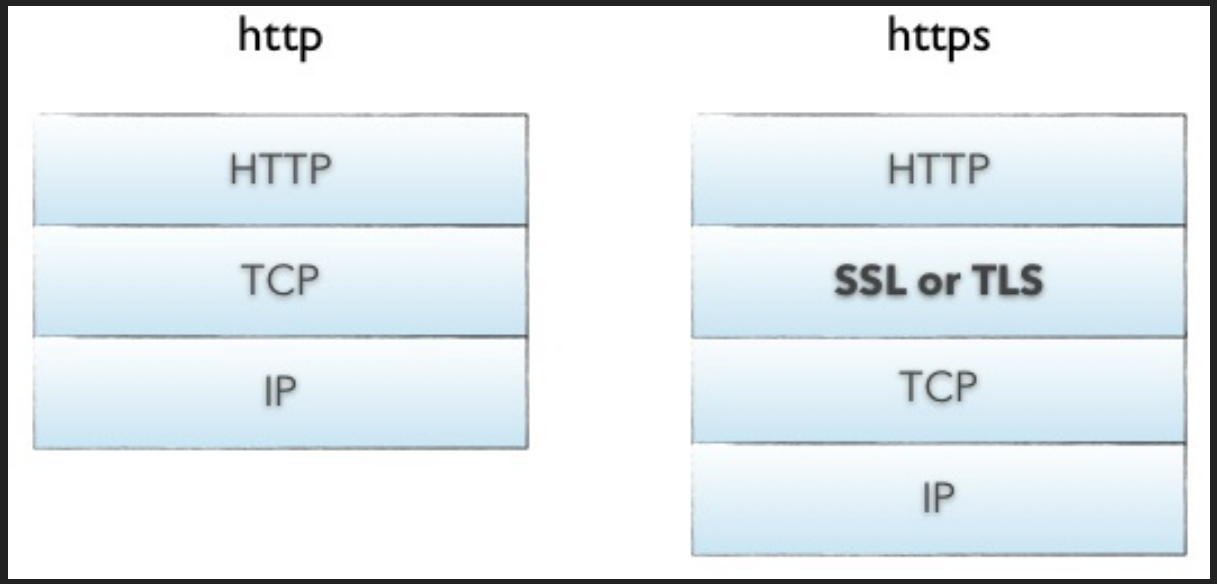
Σημαίνει HTTP Secure

Είναι συνδυασμός του SSL/TLS με το απλό HTTP

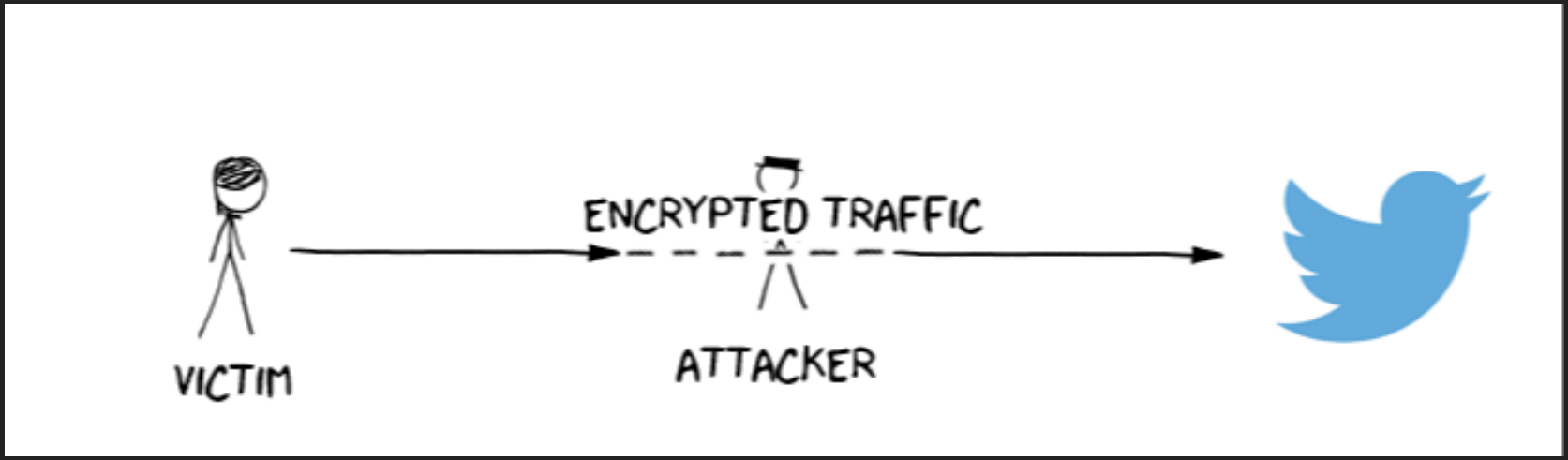
Η σύνδεση γίνεται στην πόρτα 443

Κάποιος που βλέπει το δίκτυο δεν μπορεί
να μάθει τι δεδομένα ανταλλάσσονται

Network Stack



Wireshark demo



Τι προσφέρει το HTTPS

- Confidentiality
- Integrity
- Authenticity

Μειονεκτήματα

- Αυξημένο latency της πρώτης σύνδεσης
- Αυξημένες ανάγκες επεξεργαστικής ισχύος
- Κοστίζει


but what about performance??
OPTIMIZE ELSWHERE!

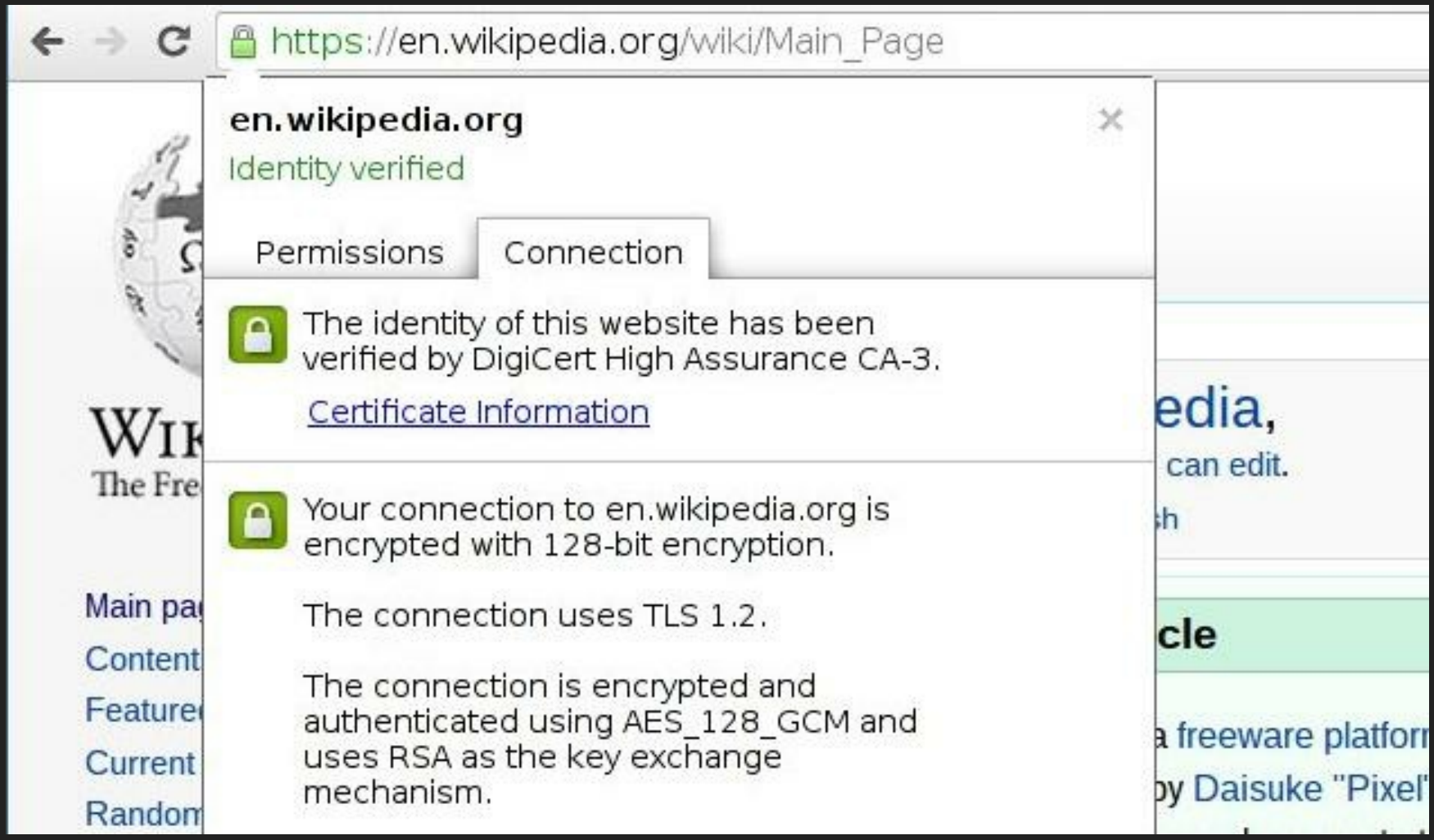
Πιστοποιητικά

Το HTTPS βασίζεται σε πιστοποιητικά

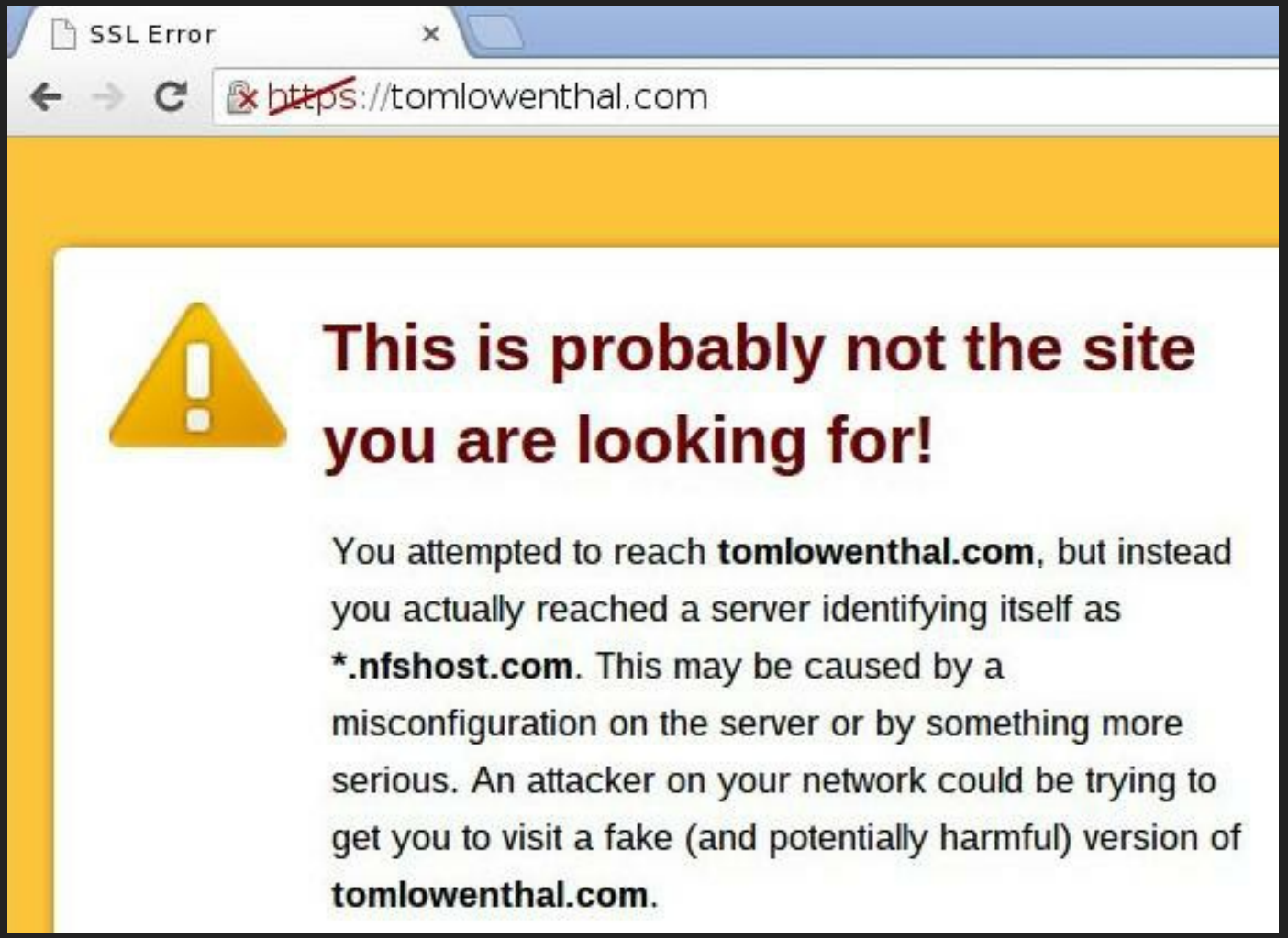
Ένα πιστοποιητικό είναι ένα public key
με κάποια μετα-δεδομένα

Ο καθένας μπορεί να φτιάξει ένα

Έγκυρο πιστοποιητικό



Άκυρο πιστοποιητικό



Πιστοποιητικά

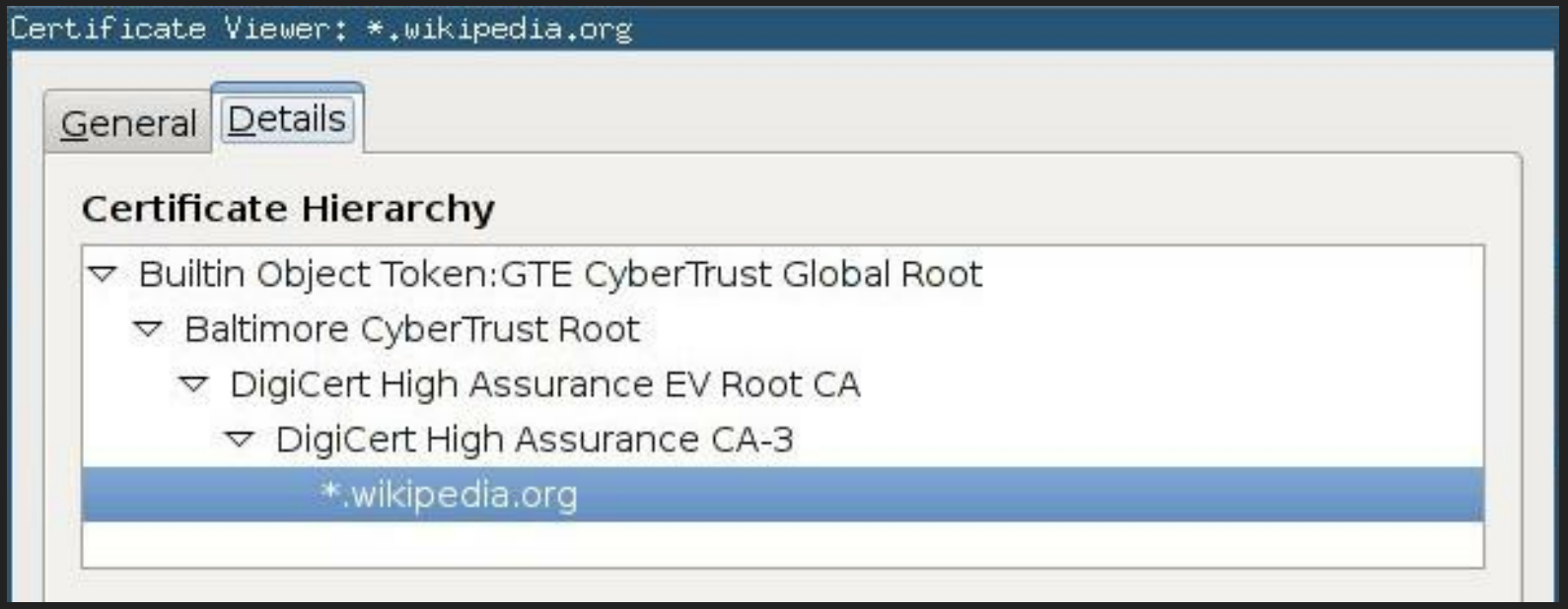
-----BEGIN CERTIFICATE-----
MIIFJDCCBAygAwIBAgIDD4mWMA0GCSqGSIb3DQEBC
wUAMD
MRcwFQYDVQQKEw5HZW9UcnVzdCwgSW5jLjEUMBIG
A1UEAx
HhcNMTMxMjA4MjE0NjI5WhcNMTQxMjExMjExMDI0Wj
CBuT
[....]
5sEK+OxRs8JMijqK5mkO8D/Sqv6iY+TsogPtLVGwbR9d
vW
Ro7JExGV0OE5WOKm2gTDNb88p6d/mVoG9jHLR84Bo
1eW4N
HMXuINIAfZLdEyk5785t9gmEjvIp/4+w
-----END CERTIFICATE-----

Περιεχόμενα πιστοποιητικού

- Common name (*.wikipedia.org)
- Organization (Wikimedia Foundation, Inc.)
- Country (US)
- State (California)
- City/Locality (San Francisco)
- Public key

Πως εμπιστευόμαστε ένα πιστοποιητικό;

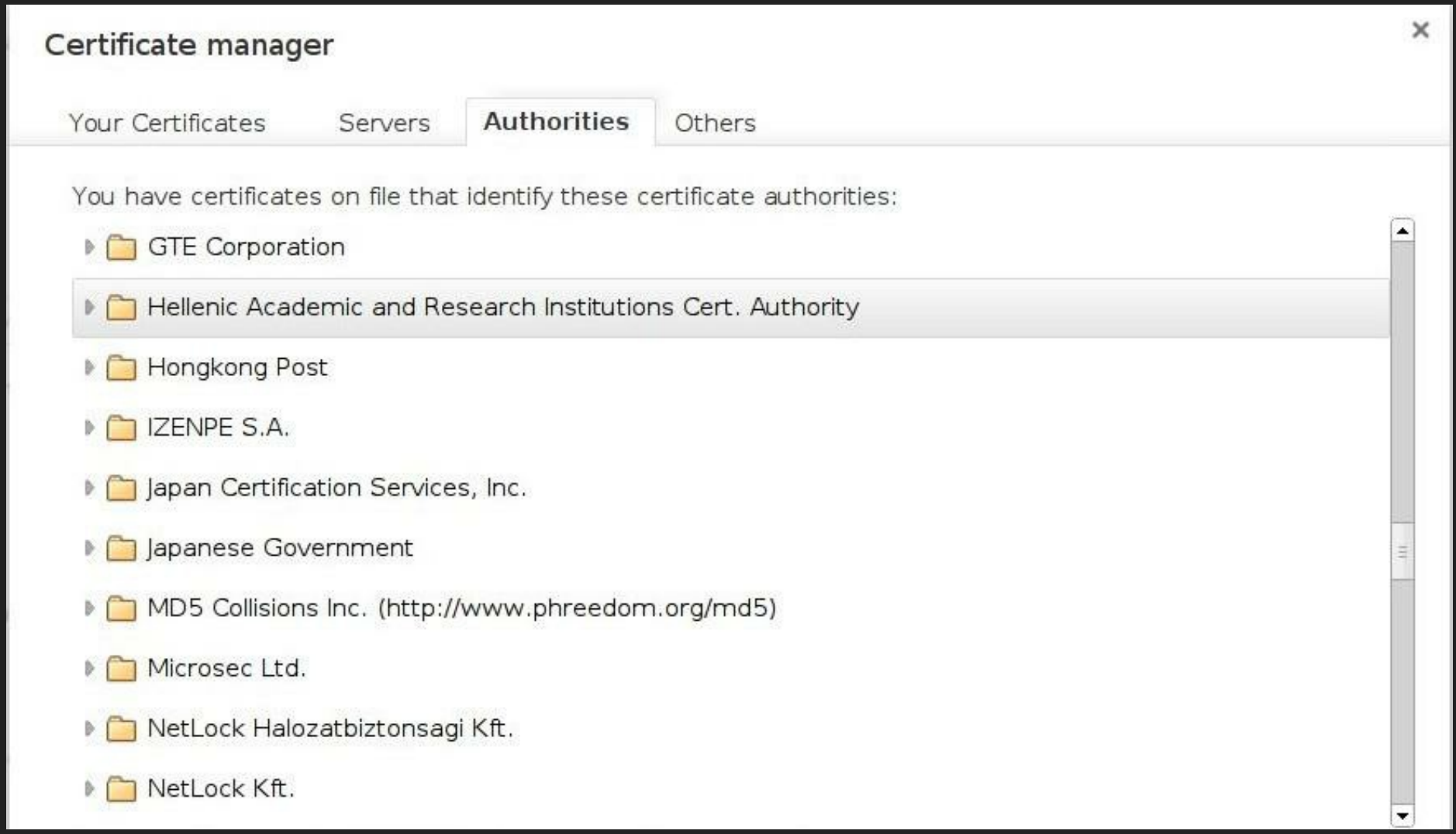
Ένα πιστοποιητικό μπορεί να είναι υπογεγραμμένο από ένα άλλο πιστοποιητικό



Αρχές πιστοποιητικών

Πιστοποιητικά που προϋπάρχουν σε εφαρμογές (Chrome, Firefox) ή σε λειτουργικά συστήματα (Linux, Windows)

Εμπιστευόμαστε αυτά και τα πιστοποιητικά που υπογράφουν!


Certificate manager
Your Certificates
Servers
Authorities
Others
You have certificates on file that identify these certificate authorities:
GTE Corporation
Hellenic Academic and Research Institutions Cert. Authority
Hongkong Post
IZENPE S.A.
Japan Certification Services, Inc.
Japanese Government
MD5 Collisions Inc. (http://www.phreedom.org/md5)
Microsec Ltd.
NetLock Halozatbiztonsagi Kft.
NetLock Kft.

Πρόβλημα

Πολλά websites ξεκινούν με HTTP και κάνουν upgrade σε HTTPS

Ένας active MitM μπορεί να αποτρέψει το upgrade

Πολλοί μέθοδοι

- ARP Poisoning
- DNS Spoofing

DNS Spoofing Demo

HSTS

HTTP Strict Transport Security

HSTS

Είναι ένα HTTP Header

```
Strict-Transport-Security: max-age=9001
```

Browser Support

- Chrome 4+
- Firefox 4+
- Opera 12+
- Safari (OS X Mavericks)

HSTS

```
Strict-Transport-Security: max-age=9001
```

Όλες οι συνδέσεις στο συγκεκριμένο domain
θα είναι HTTPS για 9001 δευτερόλεπτα

Μέχρι να υιοθετηθεί το HSTS...

HTTPS Everywhere browser extension

Από το EFF και το Tor project

Κατεβάστε το και εγκαταστήστε το

Ερωτήσεις;