ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Ασφάλεια Πληροφοριακών Συστημάτων

Εργαστήριο 3 (Υποδομές Δημόσιου Κλειδιού)
Παράδειγμα πιστοποίησης web server με openssl

Τμήμα Πληροφορικής
Πανεπιστήμιο Πειραιώς

Επ.Καθηγητής Π. Κοτζανικολάου

OpenSSL

- Ευρέως διαδεδομένη εφαρμογή ελεύθερου λογισμικού για την υλοποίηση των πρωτοκόλλων SSL/TLS.
- Λειτουργεί σε κάθε μεγάλη πλατφόρμα
  - Unix / Linux (συνήθως pre-compiled packets)
  - Windows (http://www.openssl.org/related/binaries.html)
- Πληροφορίες
  - http://www.openssl.org/
  - http://www.openssl.org/docs/ (documentation)
  - http://www.openssl.org/docs/apps/openssl.html (περιγραφή εντολών OpenSSL)

Εγκατάσταση σε Windows …

- Εγκατάσταση της κατάλληλης έκδοσης από το σύνδεσμο http://slproweb.com/products/Win32OpenSSL.html
- Πιθανώς να χρειαστεί κάποια επιπλέον βιβλιοθήκη Visual C++ Redistributables.
- Θα την βρείτε στον ίδιο σύνδεσμο.
- Εγκατάσταση του OpenSSL στη διαδρομή C:\OpenSSL

…Εγκατάσταση σε Windows

- Τοποθέτηση του φακέλου openssl/bin στος μεταβλητές περιβάλλοντος του συστήματος
  - Computer → δεξί κλίκ → Ιδιότητες →Advanced Settings →Advanced System Settings
  - Στην καρτέλα Advanced → Environment Variables →Path → Edit
  - Προσθήκη του path C:\OpenSSL\bin

Επεκτάσεις αρχείων openssl

- KEY: περιέχει το ιδιωτικό κλειδί (απαιτείται προστασία του αρχείου)
- CSR (Certificate Signing Request): αίτημα προς την Α.Π. για την υπογραφή ενός πιστοποιητικού (χρήστη, server κτλ)
- CRT: Περιέχει ένα πιστοποιητικό και διανέμεται ελεύθερα σε όλους
- PEM: Αρχείο που περιέχει και το ιδιωτικο κλειδί και το Πιστοποιητικό (είναι απαραίτητο σε ορισμένους server). Απαιτείται προστασία του αρχείου
- CRL (Certificate Revokation List): Λίστα Ανάκλησης Πιστοποιητικών η οποία περιλαμβάνει όσα πιστοποιητικά είχε εκδώσει στο παρελθόν η Α.Π. αλλά δεν τα θεωρεί πλέον αξιόπιστα.

Δημιουργία καταλόγου για την Α.Π.

- Αντιγραφή/αποσυμπίεση βοηθητικού αρχείο lab.zip
  - Linux: Δημιουργήστε στο home folder σας τον φάκελο ~/demo/CA/lab
  - Windows: στον φάκελο C:\OpenSSL\lab
  - Επεξήγηση βοηθητικών αρχείων/φακέλων του lab
    - lab – βασικός κατάλογος για την δοκιμαστική Α.Π.
    - lab/certs – περιέχει τα πιστοποιητικά που έχει εκδώσει η Α.Π.
    - lab/crl – Λίστα ανάκλησης πιστοποιητικών
    - lab/newcerts – νέα πιστοποιητικά
    - lab/private – ιδιωτικά κλειδιά για την Α.Π.
    - lab/public – δημόσια κλειδιά
    - lab/req – αιτήματα πιστοποιητικών προς υπογραφή (csr)
    - lab/CAcnf.txt – αρχείο διαμόρφωσης λειτουργίας Α.Π.
    - lab/usercnf.txt – αρχείο διαμόρφωσης για έκδοση πιστοποιητικών χρήστη

Χρήση OpenSSL

- Δημιουργία πιστοποιητικών X.509
- Δημιουργία αιτημάτων πιστοποίησης
- Πιστοποίηση κλειδιών χρηστών
- Δημιουργία παραμέτρων κλειδιών για RSA, DSA
- Δημιουργία λιστών ανάκλησης πιστοποιητικών (CRLs)
- Υπολογισμός αποτελεσμάτων συναρτήσεων κατακερματισμού
- Κρυπτογράφηση - αποκρυπτογράφηση

Χρήση OpenSSL

- Μορφή εντολών OpenSSL

  openssl command [command_opts] [command_args]

- Εκτέλεση των παρακάτω εντολών από τη γραμμή εντολών, μέσα από τον φάκελο lab

(1) Δημιουργία κλειδιού και αυτο-υπογεγραμμένου πιστοποιητικού της Α.Π.

- Δημιουργία ιδιωτικού κλειδιού και αυτό-υπογεγραμμένου πιστοποιητικού για Α.Π. με RSA και sha1
  - **openssl req -new -x509 -keyout private/CAkey.pem -out certs/CAcert.pem -days 365 -config CAcnf.txt -sha1**
- Επισκόπηση πιστοποιητικού
  - **openssl x509 -in certs/CAcert.pem -text**
- Επισκόπηση ιδιωτικού κλειδιού
  - **openssl rsa -in private/CAkey.pem -text**

(2) Δημιουργία κλειδιού /πιστοποιητικού για server

- Δημιουργία αίτησης πιστοποίησης προς την Α.Π.
  - **openssl req -new -config CAcnf.txt -nodes -keyout private/serverKey.pem -out req/server.csr -days 365 -md5**
    - "-nodes": δεν θα κρυπτογραφηθεί το ιδιωτικό κλειδί. Απαραίτητο σε ορισμένους server. Απαιτείται όμως προστασία των δικαιωμάτων πρόσβασης
- Επισκόπηση ιδιωτικού κλειδιού server
  - **openssl rsa -in private/serverKey.pem -text**
- Υπογραφή αίτησης από την Α.Π.
  - **openssl ca -config CAcnf.txt -policy policy_anything -cert certs/CAcert.pem -keyfile private/CAkey.pem -out certs/serverCert.pem -infiles req/server.csr**
- Επισκόπηση πιστοποιητικού του server
  - **openssl x509 -subject -issuer -enddate -noout –in ./certs/serverCert.pem**

(3) Εγκατάσταση πιστοποιητικού στον server
(a) σε περιβάλλον Windows, xampp

- Αντιγραφή του serverKey.key στον φάκελο:
  - **C:/xampp/apache/conf/ssl.key/serverKey.key**
- Αντιγραφή του serverCert.pem:
  - **C:/xampp/apache/conf/ssl.crt/serverCert.pem**

Δημιουργία φακέλων για ασφαλείς και μη ασφαλείς σελίδες στον server

- Δημιουργία φακέλων secure και plain στον φάκελο htdocs του xampp
- Παραμετροποίηση σελίδων για https (θύρα 443):
  - Στο αρχείο apache/conf/extra/httpd-ssl.conf αλλάζουμε το DocumentRoot "C:/xampp/htdocs/" σε DocumentRoot "C:/xampp/htdocs/**secure".**
- Παραμετροποίηση σελίδων για http (θύρα 80):
  - Στο αρχείο apache/conf/httpd.conf αλλάζουμε το DocumentRoot "C:/xampp/htdocs/" σε DocumentRoot "C:/xampp/htdocs/**plain".**

(3) Εγκατάσταση πιστοποιητικού στον server (β) σε περιβάλλον Linux, apache)

Εκκίνηση server, δοκιμή https πρόσβασης

Ενεργοποίηση ssl mod σε apache web server και προβολή πιστοποιητικού

Εγκατάσταση και δοκιμή πιστοποιητικού

Εκκίνηση server, δοκιμή https πρόσβασης

Περιγραφή	**Ενέργειες**
Δοκιμή http στο localhost	`http://localhost`
Εκκίνηση apache2	`service apache2 start και επαναδοκιμή`
Δοκιμή http στο localhost	`http://localhost`
Δοκιμή https	`https://localhost`

Ενεργοποίηση ssl mod και προβολή πιστοποιητικού

Περιγραφή	**Ενέργειες**
Επισκόπηση /etc/apache2	(mods available, mods enabled sites available, sites enabled)
Ενεργοποίηση ssl	a2enmod ssl service apache2 restart a2ensite default-ssl Service apache2 reload
Δοκιμή https	https://localhost
Προβολή του πιστοποιητικού	(δημιουργία προσωρινής εξαίρεσης και προβολή πιστοποιητικού)
Επισκόπηση /etc/ssl	(ssl/certs, ssl/private)

Εγκατάσταση και δοκιμή πιστοποιητικού

Περιγραφή	**Ενέργειες**
Επεξεργασία αρχείου διαμόρφωση site	`Επεξεργασία αρχείου /etc/apache2/sites-available/default-ssl`

Προσθήκη κλειδιού και πιστοποιητικού	`SSLCertificateFile /etc/apache2/mySSLKeys/serverCert.pem`
	
	`SSLCertificateKeyFile /etc/apache2/mySSLKeys/serverKey.key`

Επανεκκίνηση apache	`service apache2 restart`
Δοκιμή και επισκόπηση πιστοποιητικού	

Άλλα Παραδείγματα:
Δημιουργία DSA κλειδιών και πιστοποιητικού χρήστη …

- Δημιουργία παραμέτρων DSA
  - **openssl dsaparam –out dsaparam.txt –genkey 1024**
- Δημιουργία ιδιωτικού κλειδιού DSA και αυτό-υπογεγγραμένου πιστοποιητικού χρήστη
  - **openssl req -new -x509 -keyout private/userprivatekey.pem -out certs/userselfcert.pem -days 365 -newkey dsa:dsaparam.txt -config usercnf.txt -sha1**

…Δημιουργία DSA κλειδιών και πιστοποιητικού χρήστη

- Δημιουργία αίτησης πιστοποιητικού προς υπογραφή από την Α.Π.
  - **openssl x509 -x509toreq -in certs/userselfcert.pem –signkey private/userprivatekey.pem -out usercertreq.pem**
- Δημιουργία πιστοποιητικού χρήστη και υπογραφή του από την Α.Π.
  - **openssl ca -config usercnf.txt -policy policy_anything –out certs/usersignedcert.pem -infiles usercertreq.pem**
- Λήψη δημοσίου κλειδιού χρήστη από το ιδιωτικό
  - **openssl dsa -in private/userprivatekey.pem -pubout –out public/userpublickey.pem**

Άλλα Παραδείγματα:
Δημιουργία /επαλήθευση ψηφιακής υπογραφής DSA

- Δημιουργία ψηφιακής υπογραφής με DSS1 και DSA
  - **openssl dgst -dss1 -sign private/userprivatekey.pem –out DSAsignature.bin plain.txt**
- Επαλήθευση ψηφιακής υπογραφής με DSS1 και DSA
  - **openssl dgst -dss1 -verify userpublickey.pem –signature DSAsignature.bin plain.txt**

Άλλα Παραδείγματα: Λίστες ανάκλησης πιστοποιητικών

- Δημιουργία λίστας ανάκλησης πιστοποιητικών (χωρίς να έχουν ανακληθεί πιστοποιητικά)
  - **openssl ca -gencrl -out crl/crl1.pem -config CAcnf.txt**
- Επισκόπηση της λίστας
  - **openssl crl -in crl/crl1.pem -text**
- Ανάκληση πιστοποιητικού
  - **openssl ca -gencrl -revoke certs/usersignedcert.crt -config CAcnf.txt**
- Μετατροπή της λίστας σε DER μορφή
  - **openssl crl -in crl/crl1.pem -outform DER -out crl/crl1.crl**

Βιβλιογραφία

1. Δ. Πολέμη, Χ. Δημητριάδης, Σ. Παπαστεργίου, Α. Καλιαντζόγλου, Εργαστηριακά θέματα ασφάλειας, 2006.
2. Openssl. http://openssl.org