Πανεπιστήμιο Κύπρου – Τμήμα Πληροφορικής
(Εαρινό Εξάμηνο 2010-2011)

ΕΠΛ 674: Ασφάλεια Συστημάτων και Δικτύων

Εργαστήριο 6 – Λύσεις

Ασφαλής Επικοινωνία με SSL – Client side

[1] Ανοίξτε το cmd στα Windows και πληκτρολογείστε την εντολή:
openssl s_client -connect www.pki.auth.gr:443

Με την εντολή αυτή θα συνδεθείτε με την χρήση SSL στο site www.pki.auth.gr και θα εμφανιστούν πληροφορίες σχετικά με τα στοιχεία του εξυπηρέτη (Ctrl+C για έξοδο).

a. Το πιστοποιητικό που βλέπετε σε ποιον ανήκει;
Είναι πιστοποιητικό εξυπηρέτη (Server certificate).

b. Ποια είναι η έκδοση του SSL που χρησιμοποιείται για την σύνδεση;
SSLv3

c. Ποιο είναι το υποκείμενο (subject) του πιστοποιητικού (CN);
CN=www.pki.auth.gr/emailAddress=uadmin@ccf.auth.gr

d. Ποιος είναι ο εκδότης (issuer) του πιστοποιητικού (CN);
CN=AUTH Network Operations Center Certification Authority R3/emailAddress=pkiadmin@ccf.auth.gr

e. Ποιο είναι το μέγεθος του κλειδιού που χρησιμοποιείται;
1024 bits (Server public key is 1024 bit)

Με την παράμετρο **–msg** μπορείτε να δείτε τα μηνύματα τα οποία ανταλλάσσονται. Επειδή η έξοδος του προγράμματος είναι πολύ μεγάλη σε μέγεθος χρησιμοποιείστε στο τέλος της παρακάτω εντολής τη σύνταξη **|more** ώστε να την δείτε σε σελίδες (πλήκτρο space για συνέχεια):
openssl s_client –msg -connect www.pki.auth.gr:443 | more

f. Ποια μηνύματα στέλνει ο εξυπηρέτης;
ServerHello, Certificate, ServerKeyExchange, ServerHelloDone, ChangeCipherSpec, Finished

g. Ποια μηνύματα στέλνει ο εξυπηρετούμενος;
ClientHello, ClientKeyExchange, ChangeCipherSpec, Finished

h. Τα στοιχεία του πιστοποιητικού του εξυπηρέτη (υποκείμενο, εκδότης, μέγεθος κλειδιού) έχουν αλλάξει;
Όχι

i. Τα στοιχεία της SSL συνόδου(Session-ID, Master-Key) έχουν αλλάξει;
Ναι

[2] Ανοίξτε το Mozilla Firefox και επισκεφθείτε τη σελίδα https://www.cacert.org. Το https://www.cacert.org χρησιμοποιεί ένα **μη έμπιστο ψηφιακό πιστοποιητικό**. Προσθέσετε μια εξαίρεση κάνοντας λήψη πιστοποιητικού και επιλέγοντας να μη γίνει μόνιμη αποθήκευση αυτής της εξαίρεσης. Όταν προβληθεί η σελίδα, στη γραμμή διεύθυνσης πριν από το url θα δείτε με **μπλε** χρώμα πληροφορίες για τη σύνδεσή σας σε σχέση με το πιστοποιητικό εξυπηρέτη. Από την προβολή πιστοποιητικού βρείτε:

j. Ποιος είναι ο εκδότης του πιστοποιητικού;
CA Cert Signing Authority

k. Πότε εκδόθηκε και πότε λήγει το πιστοποιητικό;
14/5/2010 - 13/5/2012

Επισκεφθείτε τη σελίδα https://www.amazon.co.uk. Το https://www.amazon.co.uk χρησιμοποιεί ένα **έμπιστο ψηφιακό πιστοποιητικό**. Και πάλι όταν προβληθεί η σελίδα, στη γραμμή διεύθυνσης πριν από το url θα δείτε με **μπλε** χρώμα πληροφορίες για τη σύνδεσή σας σε σχέση με το πιστοποιητικό εξυπηρέτη. Από την προβολή πιστοποιητικού βρείτε:

l. Ποιος είναι ο εκδότης του πιστοποιητικού;
VeriSign Class 3 Secure Server CA - G2

m. Πότε εκδόθηκε και πότε λήγει το πιστοποιητικό;
8/10/2010 - 8/10/2013

Επισκεφθείτε τη σελίδα https://www.winbank.gr. Το https://www.winbank.gr όχι μόνο χρησιμοποιεί ένα **έμπιστο ψηφιακό πιστοποιητικό** αλλά επιπλέον ένα πιστοποιητικό με χαρακτηρισμό ***extended validation***, το οποίο σημαίνει ότι η Αρχή Πιστοποίησης έχει επιβεβαιώσει σε φυσικό επίπεδο ότι το ψηφιακό πιστοποιητικό αντιστοιχεί στον οργανισμό ο οποίος περιγράφεται μέσα στο Υποκείμενο (subject). Όταν προβληθεί η σελίδα, στη γραμμή διεύθυνσης πριν από το url θα δείτε με **πράσινο** χρώμα πληροφορίες για τη σύνδεσή σας σε σχέση με το πιστοποιητικό εξυπηρέτη. Από την προβολή πιστοποιητικού βρείτε:

n. Ποιος είναι ο εκδότης του πιστοποιητικού; Συγκρίνετέ τον με αυτόν του https://www.amazon.co.uk.
VeriSign Class 3 Extended Validation SSL SGC CA. Πρόκειται για πιστοποιητικό τύπου Extended Validation το οποίο σημαίνει ότι η αρχή έκδοσης του πιστοποιητικού έχει επισκεφθεί από κοντά και επιβεβαίωσε τον οργανισμό στο όνομα του οποίου εξέδωσε το πιστοποιητικό.

o. Πότε εκδόθηκε και πότε λήγει το πιστοποιητικό;
24/3/2009 - 24/5/2011

p. Ποιο είναι το υποκείμενο (subject) του πιστοποιητικού;
PIRAEUS BANK S.A.
ATHENS
ATTICA, GR

Ασφαλής Επικοινωνία με SSL – Server side

[3] Για την υποστήριξη SSL στην Υπηρεσία Web, δηλαδή στο πρωτόκολλο HTTP, είναι απαραίτητη η κατάλληλη ρύθμιση του εξυπηρέτη π.χ. Apache. Σε αυτή τη σελίδα (http://www.apache-ssl.org/httpd.conf.example) θα βρείτε ένα παράδειγμα του αρχείου **httpd-ssl.conf** το οποίο περιέχει εντολές διαμόρφωσης (configuration) για τη δημιουργία ενός ασφαλούς Host σε έναν Apache Web Server (σύνδεση με χρήση **HTTPS**). Ανοίξτε το παραπάνω αρχείο και εντοπίστε:

q. Την εντολή με την οποία ορίζεται η θύρα στην οποία ο εξυπηρέτης δέχεται HTTPS συνδέσεις (port).
Listen 443

r. Την εντολή με την οποία ορίζεται το πιστοποιητικό του εξυπηρέτη.
SSLCertificateFile /www/certs/ssl.fictional.co.cert

s. Την εντολή με την οποία ορίζεται το ιδιωτικό κλειδί του εξυπηρέτη.
SSLCertificateKeyFile /www/certs/ssl.fictional.co.key

t. Την εντολή με την οποία ορίζεται το αρχείο καταγραφής σφαλμάτων (log file).
ErrorLog /www/hosts/ssl.fictional.co/logs/error.log

u. Την εντολή με την οποία ορίζεται το αρχείο καταγραφής προσβάσεων (log file).
TransferLog /www/hosts/ssl.fictional.co/logs/access.log