Πανεπιστήμιο Πελοποννήσου

Τμήμα Επιστήμης και Τεχνολογίας Τηλεπικοινωνιών

Διαχείριση και Ασφάλεια Δικτύων – 2011

2η Σειρά Ασκήσεων

Προθεσμία παράδοσης: η ημέρα της εξέτασης (ή και λίγο αργότερα).

Τρόπος παράδοσης: αποστολή με e-mail στη διεύθυνση **gelioud@ieee.org**.

Οι ασκήσεις θα παραδοθούν είτε ατομικά είτε σε ομάδες των δύο ατόμων.

Σημείωση: Βασικός σκοπός των παρακάτω ασκήσεων είναι να αντιμετωπίσετε τα υποκείμενα θέματα μέσω της διερεύνησης των σχετικών τεχνολογιών. Ακόμα και εάν δεν καταφέρετε να επιλύσετε πλήρως τις ασκήσεις, μη διστάσετε να παραδώσετε σύντομη αναφορά που να περιγράφει τον τρόπο που δουλέψατε, τα προβλήματα που αντιμετωπίσατε, κλπ.

Για τη διευκόλυνσή σας, θα βρείτε ικανοποιητική τεκμηρίωση των εργαλείων OpenSSL εδώ: http://www.openssl.org/docs/apps/openssl.html.

Άσκηση 1

Χρησιμοποιώντας τα εργαλεία του OpenSSL, δημιουργήστε τη δική σας Αρχή Πιστοποίησης. Θα πρέπει να χρησιμοποιηθεί αλγόριθμος κρυπτογράφησης RSA με κλειδί μήκους 2048 bits και αλγόριθμος κατακερματισμού SHA1. Αναφορικά με τα πεδία Country, Organization, κλπ., χρησιμοποιήστε "ρεαλιστικές" τιμές (Greece, University of Peloponnese, …).

Παραδοτέα:

- Η σειρά των εντολών που χρησιμοποιήσατε.
- Το δημόσιο πιστοποιητικό X.509 της Αρχής Πιστοποίησης.

Άσκηση 2

Δημιουργήστε ζεύγος κλειδιών RSA και χρησιμοποιήστε την Αρχή Πιστοποίησης της Άσκησης 1 προκειμένου να εκδώσετε το αντίστοιχο ψηφιακό πιστοποιητικό X.509.

Παραδοτέα:

- Η σειρά των εντολών που χρησιμοποιήσατε.
- Το ψηφιακό πιστοποιητικό που δημιουργήθηκε, καθώς και το ιδιωτικό κλειδί.

Άσκηση 3

Θεωρήστε κάποιο αρχείο κειμένου με "λογικό" μέγεθος, όπως το http://www.ietf.org/rfc/rfc791.txt. Πραγματοποιήστε ψηφιακή υπογραφή του αρχείου χρησιμοποιώντας τα αποτελέσματα της Άσκησης 2.

Παραδοτέα:

- Η σειρά των εντολών που χρησιμοποιήσατε.
- Τα δύο αρχεία (αρχικό και ψηφιακά υπογεγραμμένο).