ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
Διδάσκων: Επίκουρος Καθηγητής Γεώργιος Καμπουράκης
Εργαστηριακοί Συνεργάτες: Δημήτρης Παπαμαρτζιβάνος (ΥΔ), Αλέξανδρος Φακής (ΥΔ)

Ασφάλεια Δικτύων Υπολογιστών

και Τεχνολογίες Προστασίας της Ιδιωτικότητας

1η Εργαστηριακή Άσκηση

Οκτώβριος 2016

ΑΣΚΗΣΗ 1

I2PAKA: Πρωτόκολλο αυθεντικοποίησης και συμφωνίας κλειδιού με αξιοποίηση του δικτύου ανωνυμίας I2P

Περιγραφή

Στην 1η εργαστηριακή άσκηση καλείστε να υλοποιήσετε ένα πρωτόκολλο αυθεντικοποίησης και συμφωνίας κλειδιού (Authentication and Key Agreement (AKA)) μεταξύ δύο οντοτήτων, όπου τα μηνύματα του πρωτοκόλλου θα ανταλλάσσονται μέσω του δικτύου I2P [2]. Σκοπός της εργασίας είναι να εξοικειωθείτε με τη φιλοσοφία των πρωτοκόλλων αυθεντικοποίησης και να έρθετε σε επαφή με τα δίκτυα ανωνυμίας (Anonymity Networks).

Πιο συγκεκριμένα, απώτερος στόχος ενός πρωτοκόλλου AKA είναι η δημιουργία ενός συμμετρικού κλειδιού κρυπτογράφησης, το οποίο σε επόμενο στάδιο μπορεί να χρησιμοποιηθεί για τη διασφάλιση της εμπιστευτικότητας της επικοινωνίας των συμβαλλόμενων μερών. Η διαδικασία αυθεντικοποίησης βασίζεται σε ψηφιακά πιστοποιητικά (Digital Certificates) που βρίσκονται στην κατοχή είτε της μίας οντότητας της επικοινωνίας (μονομερής αυθεντικοποίηση) είτε και των δύο (αμοιβαία αυθεντικοποίηση). Το πρωτόκολλο AKA λαμβάνει χώρα στην αρχή κάθε επικοινωνίας και ως εκ' τούτου είναι απαραίτητη η διασφάλιση της λειτουργίας του για την αποτροπή επιθέσεων όπως spoofing και security downgrade attacks, αλλά και για την εξασφάλιση της επικαιρότητας της συνόδου.

Δίκτυα ανωνυμίας ονομάζονται τα δίκτυα που στοχεύουν στην απόκρυψη της ταυτότητας των χρηστών. Πρόκειται για δίκτυα που απαρτίζονται από μεγάλο αριθμό εθελοντών χρηστών και με την χρήση κατάλληλων κρυπτογραφικών τεχνικών και τεχνικών δρομολόγησης πακέτων καθιστούν ιδιαίτερα δύσκολη την αποκάλυψη της ταυτότητας των χρηστών από διάφορες αρχές επιτήρησης. Τα δημοφιλέστερα δίκτυα ανωνυμίας είναι τα TOR [1], I2P [2] και Freenet [3].

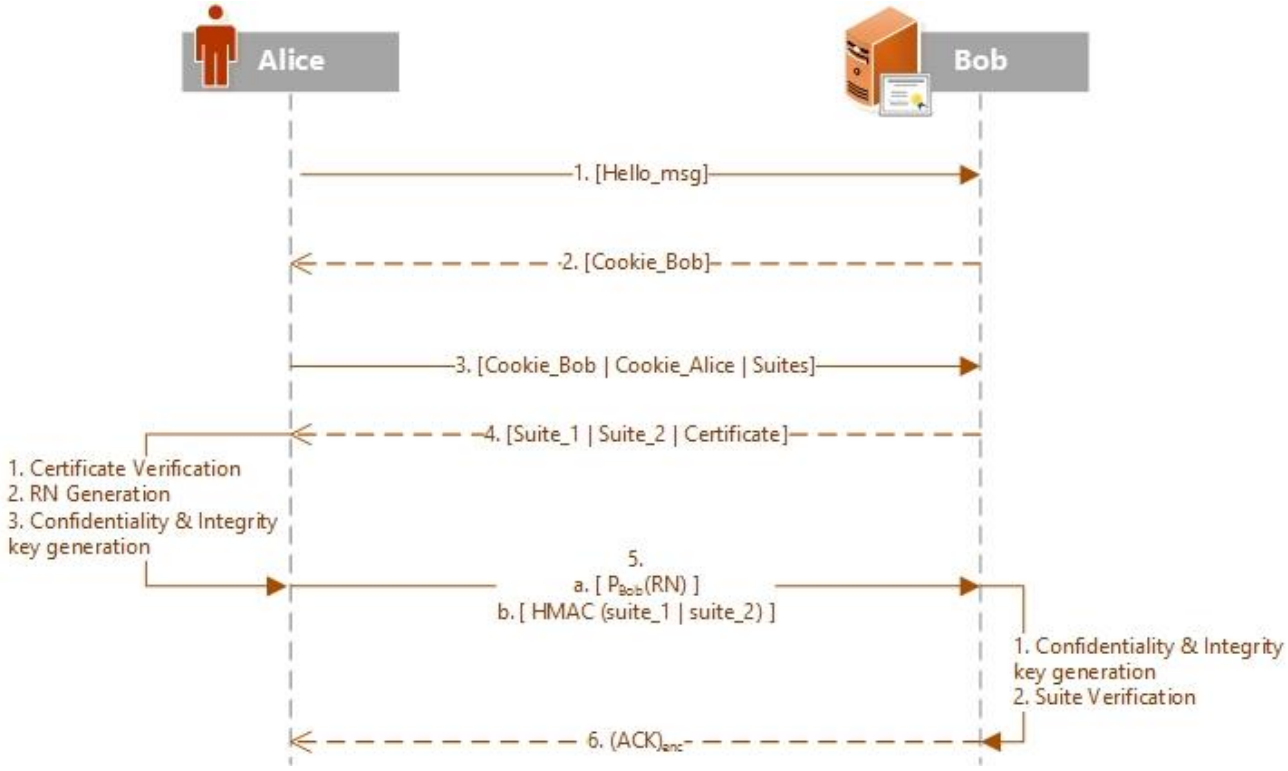
Σκοπός της εργασίας είναι η σύνδεση των δύο παραπάνω τεχνικών ανωνυμίας και αυθεντικοποίησης για την υλοποίηση ενός μηχανισμού για τη δημιουργία ενός συμμετρικού κρυπτογραφικού κλειδιού μέσω του δικτύου I2P.

Πρωτόκολλο αυθεντικοποίησης και δημιουργίας κλειδιού (AKA) – 80%

Τα βήματα του AKA πρωτόκολλου που καλείστε να υλοποιήσετε παρουσιάζονται στο παρακάτω σχήμα. Η Alice (πελάτης) και ο Bob (εξυπηρετητής) ανταλλάσσουν κατάλληλα μηνύματα για την δημιουργία ενός συμμετρικού κρυπτογραφικού κλειδιού μήκους 128bits. Ο Bob έχει στην κατοχή του ένα αυθυπόγραφο ψηφιακό πιστοποιητικό (self-signed certificate) στο πρότυπο X.509, που χρησιμοποιείται για την επιβεβαίωση της ταυτότητας του από τους πελάτες (μονομερής αυθεντικοποίηση). Η Alice ξεκινάει την ανταλλαγή μηνυμάτων αποστέλλοντας ένα μήνυμα χαιρετισμού στο Bob (βήμα 1). Στη συνέχεια, ο Bob απαντάει με ένα Cookie. Το Cookie είναι μία τυχαία συμβολοσειρά 64 bits (βήμα 2). Η Alice δημιουργεί το δικό της Cookie και το αποστέλλει στον Bob μαζί με το Cookie που έλαβε από αυτόν στον βήμα 2 προσθέτοντας και τις κρυπτογραφικές σουίτες που μπορεί να υποστηρίξει (βήμα 3). Η Alice θα πρέπει να υποστηρίζει τουλάχιστον 2 αλγορίθμους συμμετρικής κρυπτογράφησης και τουλάχιστον 2 αλγορίθμους για τη διασφάλιση της ακεραιότητας. Τους αλγορίθμους θα τους επιλέξετε εσείς. Στη συνέχεια (βήμα 4) ο Bob απαντάει

στην Alice αποστέλλοντας τις σουίτες που επέλεξε (1 για ακεραιότητα και 1 για εμπιστευτικότητα) μαζί με το ψηφιακό πιστοποιητικό του. Αφού η Alice επιβεβαιώσει την εγκυρότητα του πιστοποιητικού συνεχίζει με τη δημιουργία ενός τυχαίου αλφαριθμητικού RN μήκους 128 bits ή σε αντίθετη περίπτωση διακόπτει την επικοινωνία με τον Bob. Αν δεν υπάρξει πρόβλημα κατά την επιβεβαίωση της ταυτότητας του Bob, η Alice παράγει την σύνοψη του αλφαριθμητικού (cookie_Bob | Cookie_Alice | RN) χρησιμοποιώντας τον αλγόριθμο SHA-256. Στη συνέχεια η Alice «κόβει» τη σύνοψη σε δύο τμήματα και δημιουργεί 2 κρυπτογραφικά κλειδιά 128 bits όπου το ένα χρησιμοποιείται για την διασφάλιση της εμπιστευτικότητας των μηνυμάτων και το δεύτερο για την διασφάλιση της ακεραιότητας. Στη συνέχεια, αποστέλλει στο Bob το τυχαίο αλφαριθμητικό RN κρυπτογραφημένο με το δημόσιο κλειδί του παραλήπτη (Βήμα 5α) καθώς επίσης και τη σύνοψη που προέκυψε από το HMAC [5] των κρυπτογραφικών σουιτών (Βήμα 5β). Ο Bob στη συνέχεια ακολουθεί την ίδια διαδικασία που ακολούθησε και η Alice για να δημιουργήσει και αυτός στην πλευρά του τα 2 κλειδιά καθώς επιβεβαιώνει την ορθή επιλογή των κρυπτογραφικών σουιτών από την πλευρά της Alice. Τέλος, ο Bob απαντάει με ένα συμμετρικά κρυπτογραφημένο μήνυμα επιβεβαίωσης στην Alice (Βήμα 6).

Σημείωση: Για την δημιουργία των πιστοποιητικών κάντε χρήση του εργαλείου openssl [4]. Υποθέστε ότι το πιστοποιητικό ακολουθεί το RFC5636 [6]. Πρόκειται δηλαδή για ένα "Traceable Anonymous Certificate" που περιέχει ένα ψευδώνυμο και όχι την πραγματική ταυτότητα του κατόχου του. Το πιστοποιητικό θα πρέπει να περιέχει ανάμεσα στις διάφορες πληροφορίες τους αριθμούς μητρώου της ομάδας εργασίας, π.χ. icsd12001_icsd12002_icsd12003. Οι 4 σουίτες (αλγόριθμοι) κρυπτογράφησης και κατακερματισμού που υποστηρίζονται από την Alice είναι στην ευχέρειά σας.



I2P

Το AKA πρωτόκολλο που περιγράψαμε στην προηγούμενη ενότητα καλείστε να το προωθήσετε μέσω του δικτύου ανωνυμίας I2P. Για το σκοπό αυτό θα πρέπει να δημιουργήσετε μία απλή

επικοινωνία τύπου Client-Server μέσα στο δίκτυο I2P εκμεταλλευόμενοι το Streaming library API και τους σχετικούς οδηγούς που παρέχονται στον ιστότοπο του δικτύου [2].

Η υλοποίηση του server σας πρέπει να επιτρέπει την σύνδεση πολλαπλών πελατών μέσω Java sockets που χρησιμοποιούν ObjectStreams. Για το σκοπό αυτό καλείστε να υλοποιήσετε σχετικές κλάσεις για την αναπαράσταση των μηνυμάτων το πρωτοκόλλου που ανταλλάσσονται μεταξύ του Client και του Server.

Ερωτήσεις (20%)

1. Το AKA πρωτόκολλο εξασφαλίζει από επιθέσεις τύπου spoofing και security downgrade; Αν ναι, με ποιόν τρόπο; Αν όχι, πως θα μπορούσαν να αποφευχθούν τέτοιου είδους επιθέσεις; Αναπτύξτε με συντομία.
2. Το πρωτόκολλο εξασφαλίζει την επικαιρότητα (freshness) της συνόδου; Αν ναι, με ποιόν τρόπο; Αν όχι, πως μπορεί να εξασφαλιστεί αυτή η ιδιότητα;
3. Μπορείτε να βελτιώσετε τη λειτουργία του πρωτοκόλλου; Ποια θεωρείτε ότι είναι τα αδύναμα χαρακτηριστικά του και τι θα προτείνατε για τη βελτίωση του;
4. Μελετήστε τη λειτουργία του δικτύου ανωνυμίας I2P και του δικτύου ανωνυμίας TOR. Ποιες διαφορές παρουσιάζουν; Ποιο είναι ασφαλέστερο και γιατί;

Bonus: Η αντικατάσταση του I2P με το δίκτυο ανωνυμίας Tor με χρήση της βιβλιοθήκης SilverTunnel-NG [7] ως επιπλέον υλοποίηση θα επιβραβευτεί με +1 μονάδα.

Παραδοτέα

Καθ' όλη τη διάρκεια εκπόνησης της εργασίας θα πρέπει να χρησιμοποιείτε την πλατφόρμα Gitlab για το διαμοιρασμό του πηγαίου κώδικα μεταξύ των μελών κάθε ομάδας και τον έλεγχο της πορείας της εργασίας σας από τους διδάσκοντες. Κατά την παράδοση όλος ο πηγαίος κώδικας (εκτός από το eclass) θα πρέπει να έχει αναρτηθεί και στο Gitlab σύμφωνα με τις οδηγίες που σας δόθηκαν στο εργαστήριο.

Η **αναφορά** σας ΠΡΕΠΕΙ να περιέχει τα ακόλουθα:

[1] Εκτελέσιμα προγράμματα με τα σχετικά σχόλια (project Netbeans κτλ).
[2] Τεκμηρίωση προγραμμάτων και επεξήγηση τυχόν δικών σας παραδοχών.
[3] Στιγμιότυπα εκτέλεσης προγράμματος (screenshots).
[4] Περιγραφή και τρόπος δημιουργίας πιστοποιητικών.
[5] Ψηφιακά Πιστοποιητικά.
[6] Απαντήσεις στις ερωτήσεις της εργασίας.

Η εργασία πρέπει να παραδοθεί μέχρι τις **30/10** μέσω της πλατφόρμας ηλεκτρονικής μάθησης **e-class**. Το τελικό παραδοτέο πρέπει να είναι αρχείο .zip (ή .rar) με όνομα:

ΑριθμόςΜητρώου1_ΑριθμόςΜητρώου2_ΑριθμόςΜητρώου3_Lab01.zip
(π.χ. icsd12001_icsd12002_icsd12003_Lab01.zip), του κάθε μέλους της ομάδας.

Τεχνικό παράρτημα

Για την υλοποίηση του I2P Client-Server θα πρέπει να εγκαταστήσετε και να ενεργοποιήσετε το I2P στον υπολογιστή σας. Οι απαραίτητες βιβλιοθήκες θα είναι διαθέσιμες στα σχετικά αρχεία

εγκατάστασης του I2P στον υπολογιστή σας. Οι βιβλιοθήκες έχουν δοκιμαστεί από τους διδάσκοντες στις εκδόσεις JDK 1.7 και 1.8.

Συμπληρωματική Βιβλιογραφία

[1] The Tor Project – Anonymity Online, https://www.torproject.org/
[2] I2P Project – The invisible internet project, https://geti2p.net/
[3] Freenet Project – P2P platform for censorship-resistant communication and publishing https://freenetproject.org/
[4] Openssl - Cryptography and SSL/TLS Toolkit, https://www.openssl.org/
[5] HMAC – Hash-based message authentication code, https://en.wikipedia.org/wiki/Hash-based_message_authentication_code
[6] RFC 5636 - Traceable Anonymous Certificate, https://tools.ietf.org/html/rfc5636
[7] SilverTunnel-NG -Java library for easy accessing Tor network, https://sourceforge.net/projects/silvertunnel-ng/
[7] Διαφάνειες Μαθήματος