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

2η Εργαστηριακή Άσκηση

Οκτώβριος 2016

ΑΣΚΗΣΗ 2

TrackMeIfYouCanChat: Υλοποίηση εφαρμογής ανταλλαγής μηνυμάτων μέσω κρυπτογραφημένων και ανώνυμων καναλιών

Περιγραφή

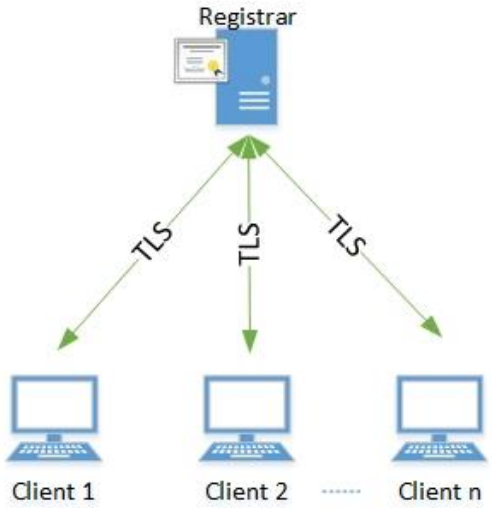
Στη 2η εργαστηριακή άσκηση καλείστε να υλοποιήσετε ένα ChatRoom το οποίο διασφαλίζει την ανωνυμία των συμμετεχόντων. Πιο συγκεκριμένα, η προστασία της ανωνυμίας θα εξασφαλίζεται κάνοντας χρήση του δικτύου ανωνυμίας I2P, ενώ οι συμμετέχοντες θα μπορούν να επικοινωνούν είτε ένας προς έναν (Unicast channel) είτε πολλοί προς πολλούς (Multicast Channel). Η υποδομή του ChatRoom υποστηρίζεται από ένα Registrar Server που διατηρεί ένα αρχείο με τους διαθέσιμους χρήστες.

Registrar

Ο Registrar διατηρεί μία λίστα με όλους τους Clients της υποδομής. Οποισδήποτε client επιθυμεί να συμμετάσχει στο ChatRoom, αρχικά πρέπει να επικοινωνήσει με τον server γνωστοποιώντας του ένα ψευδώνυμο και το προορισμό του Client μέσα στο δίκτυο ανωνυμίας I2P <Nickname, I2P_Destination>. Στη συνέχεια, ο server ανταποκρίνεται αποστέλλοντας τη λίστα με όλους τους διαθέσιμους χρήστες στο ChatRoom. Σε επόμενο στάδιο ο Client μπορεί να επιλέξει από τη λίστα και να επικοινωνήσει με ένα άλλο χρήστη ή να ξεκινήσει μία ομαδική συνομιλία.

Ανά τακτά χρονικά διαστήματα (έστω 2 mins) οι Clients στέλνουν ένα μήνυμα heartbeat στο server για να επιβεβαιώσουν στην παρουσία τους στο ChatRoom. Αν ο server δεν λάβει heartbeat από κάποιον client τον διαγράφει από τη λίστα του. Σε κάθε heartbeat που στέλνει ο client, ο server απαντάει με τη λίστα συνδεδεμένων χρηστών, σε περίπτωση που υπάρχει κάποια αλλαγή σε σχέση με αυτή που στάλθηκε στο προηγούμενο heartbeat.

Η επικοινωνία μεταξύ Clients-Server διασφαλίζεται μέσω το πρωτοκόλλου TLS. Για το σκοπό αυτό καλείστε να κάνετε χρήση των κατάλληλων κλάσεων του Java API για τη δημιουργία SSLSockets. Ο server έχει στη κατοχή του ένα αυτο-υπογεγραμμένο (self-signed) ψηφιακό πιστοποιητικό στο πρότυπο X.509. Το πιστοποιητικό θα πρέπει να περιέχει ανάμεσα στις διάφορες άλλες πληροφορίες τους αριθμούς μητρώου της ομάδας εργασίας, π.χ. icsd12001_icsd12002_icsd12003.



Clients

Οι Clients αποτελούν ουσιαστικά τους χρήστες που συνομιλούν στο ChatRoom. Κάθε Client πρέπει να συνδεθεί στο δίκτυο I2P για να του αποδοθεί ένας I2P_Destination, τον οποίο στη συνέχεια θα αποστείλει στον Registrar όπως περιεγράφηκε παραπάνω.

Αφού ο Client λάβει τη λίστα με τους χρήστες μπορεί:

1. Να εκκινήσει μία συνομιλία με ένα χρήστη (Unicast mode).
2. Να επιλέξει μία ομάδα χρηστών για ομαδική συνομιλία (Multicast mode).

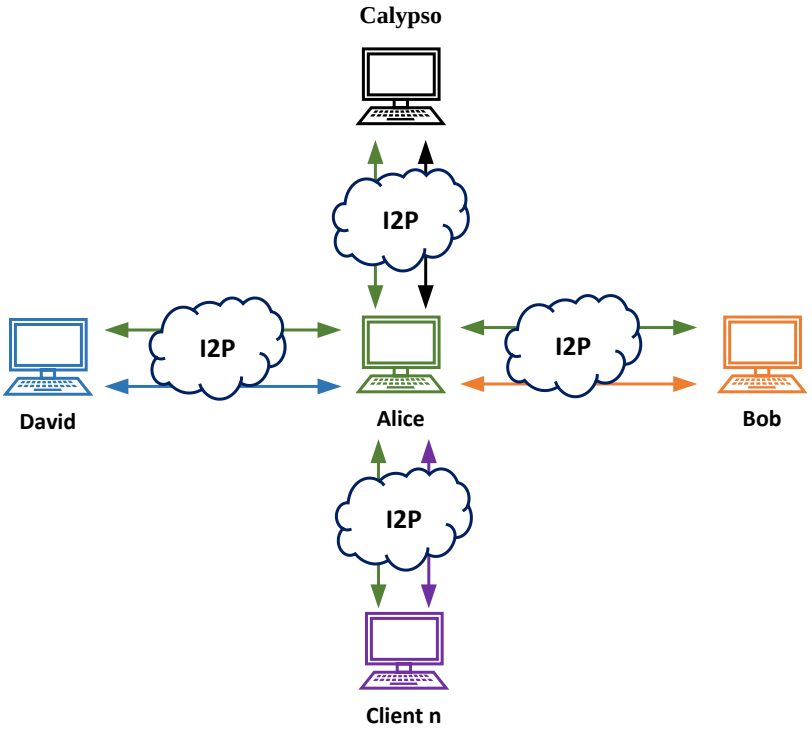
Η επικοινωνία μεταξύ των Clients είναι αμφίδρομη, δηλαδή κάθε Client πρέπει να λειτουργεί και ως Client και Server συγχρόνως για να μπορεί να στέλνει και να λαμβάνει μηνύματα ανά πάσα στιγμή.

1. Unicast mode

Έστω ότι η Alice (A) επιθυμεί να μιλήσει στο Bob (B). Ο B ακούει σε ένα I2P_destination. Η A επικοινωνεί με τον B στο I2P_destination του αποστέλλοντας ένα μήνυμα για τη δημιουργία μίας συνεδρίας (session). Αν ο B αποδεχτεί το αίτημα της A, τότε αποστέλλει ένα μήνυμα επιβεβαίωσης στην A, η οποία απαντάει με το δικό της I2P_destination. Ο B συνδέεται με τη σειρά του στην A και με αυτόν τον τρόπο ξεκινάει μία αμφίδρομη επικοινωνία μεταξύ A και B.

2. Multicast mode

Έστω ότι η Alice επιθυμεί να μιλήσει με τους Bob (B), Calypso (C) και David (D). Η A αποστέλλει στους υπόλοιπους ένα μήνυμα πρόσκλησης σε μία ομαδική συνομιλία. Όσοι το αποδεχτούν θα εισέλθουν σε μία ομαδική συνομιλία όπου όλα τα μηνύματα θα προωθούνται σε όλους τους συμμετέχοντες μέσω του Client που εκκίνησε τη συνομιλία (A στη προκειμένη περίπτωση). Για το σκοπό αυτό, ο A θα πρέπει να είναι σε θέση διαχειριστεί πολλές συνδέσεις.



Στην πλευρά του Client καλείστε να δημιουργήσετε γραφική διεπαφή (GUI) που να υποστηρίζει τις λειτουργίες που περιεγράφηκαν προηγουμένως. Για την υλοποίηση του GUI μπορείτε να κάνετε χρήση έτοιμων εργαλείων που προσφέρονται από τα προγράμματα ανάπτυξης. Στη πλευρά του Registrar Server δεν απαιτείται η υλοποίηση γραφικής διεπαφής.

Για να επιβεβαιώσετε την ορθή λειτουργία του TLS πρωτοκόλλου και την προστασία του καναλιού επικοινωνίας Client-Registrar θα πρέπει να κάνετε χρήση κάποιου εργαλείου σύλληψης πακέτων (sniffers), όπως το Wireshark, tcpdump κ.α. και να επιβεβαιώσετε πως οι 2 οντότητες επικοινωνούν μέσω ενός κρυπτογραφημένου καναλιού. Για να αποδείξετε την ορθή λειτουργία της υλοποίησης σας θα πρέπει να δοκιμάσετε τη σύλληψη πακέτων όταν χρησιμοποιείτε απλά sockets και να συγκρίνετε τις δύο περιπτώσεις.

Ερωτήσεις (10%)

Ποια θα είναι η διαφορά αν τα TLS τούνελ αντικατασταθούν με IPSec σε ESP+transport mode;

Bonus: Υλοποιήστε το multicast mode με επικοινωνία P2P. Δηλαδή κάθε Client θα πρέπει να είναι συνδεδεμένος με όλους τους συμμετέχοντες στη συνομιλία. (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.
[7] Ανάλυση των αποτελεσμάτων χρήσης του εργαλείου σύλληψης πακέτων (sniffer) και ενδεικτικά στιγμιότυπα εκτέλεσης (screenshots). Επεξήγηση των φίλτρων που χρησιμοποιήθηκαν.

Η εργασία πρέπει να παραδοθεί μέχρι τις **27/11** 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.

Για την υλοποίηση της επικοινωνίας μεταξύ Registrar-Clients θα πρέπει να χρησιμοποιήσετε κατάλληλες κλάσεις από το Java API για τη δημιουργία SLL Sockets. Για τη δημιουργία του πιστοποιητικού του Register χρησιμοποιείστε το εργαλείο openssl.

Η υλοποίηση θα βασίζεται σε 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.

Συμπληρωματική Βιβλιογραφία

[1] I2P Project – The invisible internet project, https://geti2p.net/
[2] Openssl - Cryptography and SSL/TLS Toolkit, https://www.openssl.org/
[3] Διαφάνειες Μαθήματος