University of the Aegean

Dept. of I&C Systems Engineering

Ασφάλεια Δικτύων Υπολογιστών και Τεχνολογίες Προστασίας της Ιδιωτικότητας

Μαίρη Πλεξίδα – icsd11138
Γιώργος Λέρτας – icsd11084
Κλιάρης Βαγγέλης – icsd11066

2η Εργαστηριακή άσκηση

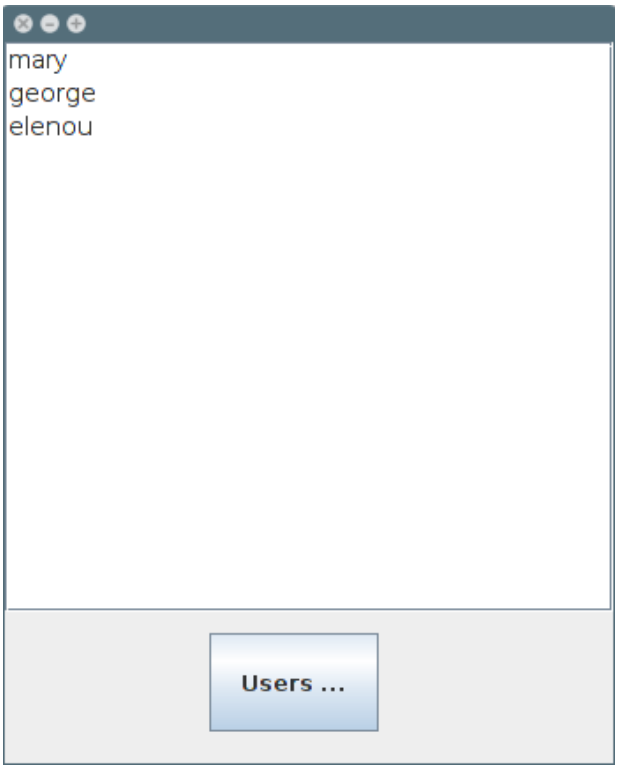
Περιγραφή

Σε αυτήν την εργασία υλοποιήσαμε 1 Registrar και ένα client. Ο Client συνδέετε στο I2P από το οποίο παίρνει ip. Ο registrar κρατάει μια λίστα η οποία ανανεώνεται δυναμικά με όλους τους χρήστες που συνδέονται και εγγράφονται σε αυτόν.

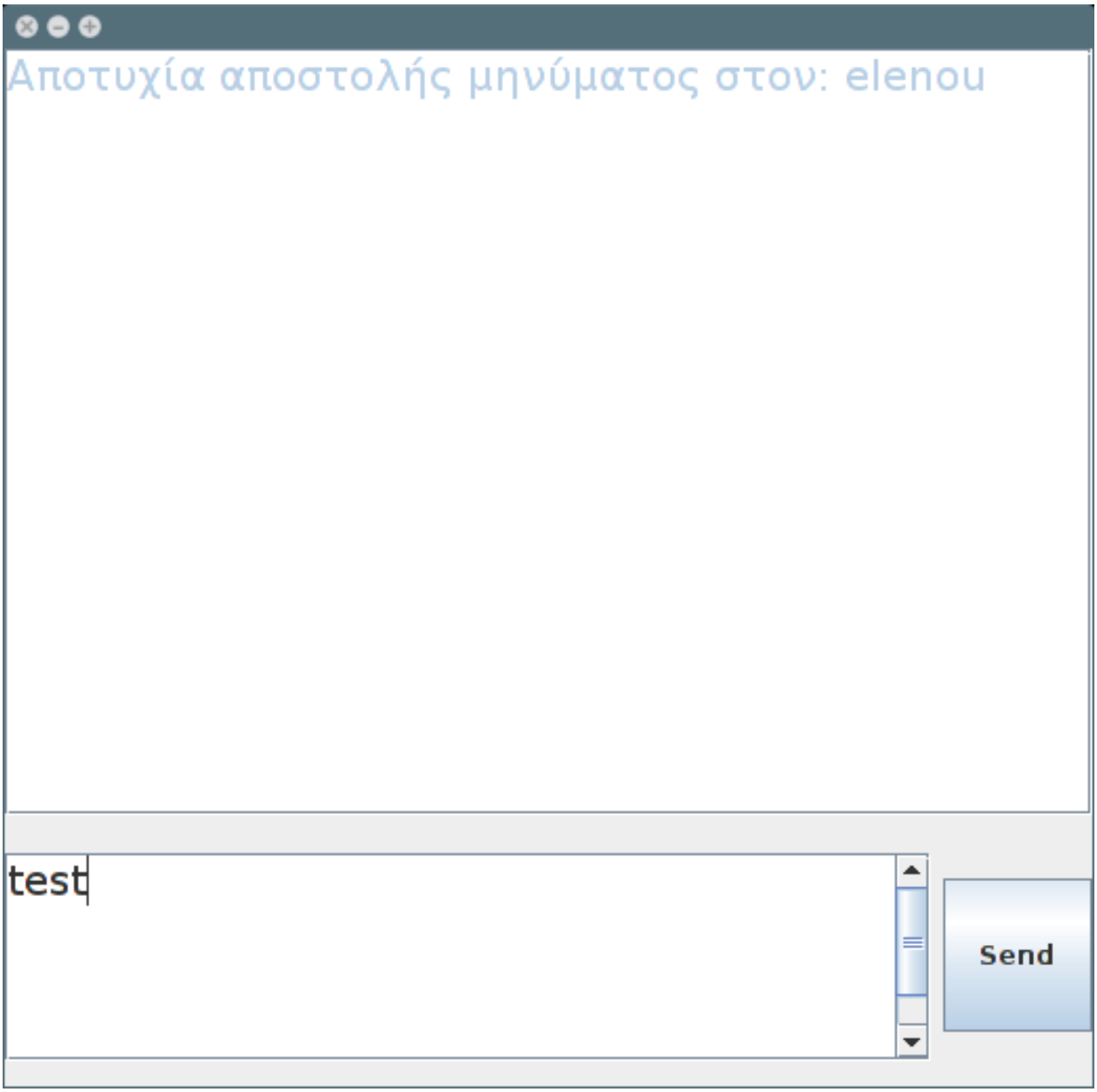
Η σύνδεση registrar και client γίνεται με την χρήση ενός secure SSL socket το οποίο χρησιμοποιεί TLS 1.2 αυστηρά! Μόλις ο client συνδεθεί στον registrar του αποστέλλει το username και την I2P διεύθυνση του. Ο registrar αναλαμβάνει να προωθήσει την λίστα με τους συνδεμένους χρήστες σε όλους τους υπόλοιπους χρήστες. Αν κάποιος χρήστης αποσυνδεθεί τότε ο registrar αυτόματα αναλαμβάνει να στείλει την ανανεωμένη λίστα χρηστών. Για να ξέρει ο registrar αν ο client είναι online χρησιμοποιεί την λογική του heartbeat και αποστέλλει ανά 1 δευτερόλεπτο ένα μήνυμα στον client και ελέγχει αν αυτό έφτασα. Αν όχι τότε θεωρεί πως το socket έκλεισε.

Στην συνέχεια ο client μπορεί να επιλέξει από την λίστα με τους συνδεμένους χρήστες με ποίον/ποίους θα συνομιλήσει. Συνεπώς δημιουργεί ένα server ο οποίος ακούει μέσα στο i2p και στέλνει κατάλληλο μήνυμα στους υπόλοιπους χρήστες να συνδεθούν στο δωμάτιο για να συνομιλήσουν. Αυτό το δωμάτιο είναι πίσω από το i2p και όλοι οι χρήστες-πελάτες εκτός από τον χρήστη-διακομιστή δεν ξέρουν τις διευθύνσεις i2p των υπολοίπων χρηστών-πελατών τουλάχιστον στην υποδομή του δωματίου καθώς μπορούμε να θεωρήσουμε πως τις ξέρουν αφού όλοι μοιράζονται την ίδια λίστα [username,i2p] από τον registrar.

Παραπάνω βλέπουμε τα logs ένος client και παρακάτω το γραφικό κομμάτι.



Παραπάνω βλέπουμε τον registrar



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

Οι διαφορές των 2 πρωτοκόλλων είναι:

- Στο TLS/SSL tunnel οι δυο χρήστες μπορούν να επικοινωνήσουν από οποιο δήποτε δίκτυο μεταξύ τους, ενώ στο i2p πρέπει να είναι και οι δυο μέσα στο i2p onion δίκτυο για να επικοινωνήσουν.

- Το TLS/SSL εφαρμόζεται στο επίπεδο μεταφοράς, ενώ το IPSEC πιο χαμηλά στο επίπεδο δικτύου.
- Το TLS/SSL χρειάζεται stateful connection(TCP), ενώ το IPSEC μπορεί να εφαρμοστεί και σε UDP.
- Στο TLS/SSL γίνεται κρυπτογράφηση ολόκληρου του μηνύματος-πακέτου, ενώ στο IPSEC γίνεται κρυπτογράφηση του περιεχόμενου που βρίσκεται στο πεδίο content, ενώ το P headers είναι ορατό.
- Τέλος το TLS/SSL χρησιμοποιεί την πολιτική ***MAC-then-Encrypt*** η οποία θεωρείται λιγότερο ασφαλή από την ***Encrypt-then-MAC*** που χρησιμοποιεί το IPSEC.

Βιβλιογραφία

- https://geti2p.net/el/get-involved/develop/applications
- http://stilius.net/java/java_ssl.php