Ασφάλεια Δικτύων Υπολογιστών & Τεχνολογίες Προστασίας της Ιδιωτικότητας

Αναφορά Εργασίας “SIPKAP”

Αυλακιώτης Χρήστος – 321|2012015
Τρίτσης Νίκος – 321|2011162

Πίνακας περιεχομένων

1 Εισαγωγή

Σε αυτή την εργασία ασχοληθήκαμε με την χρήση των του πρωτόκολλου συμφωνίας κλειδιών (που υλοποιήσαμε στην πρώτη εργασία του μαθήματος "MULTI-KAP") προκειμένου να εξασφαλισθεί η εμπιστευτικότητα των μηνυμάτων του πρωτοκόλλου SIP, μεταξύ τεσσάρων (ή και περισσοτέρων) οντοτήτων (Bob, ProxyA, ProxyB, Alice). Το πρωτόκολλο Session Initiation Protocol (SIP) χρησιμοποιείται για την εγκαθίδρυση, τροποποίηση και τερματισμό μιας VoIP επικοινωνίας. Το SIP βασίζεται στο μοντέλο πελάτη εξυπηρετητή (client-server model), είναι text-based, και μοιάζει με το πρωτόκολλα μεταφοράς υπερ-κειμένων (HTTP) και μεταφοράς ταχυδρομείου (SMTP). Το SIP υλοποιεί στην ουσία ένα σύνολο βημάτων, τα οποία έχουν ως στόχο να μετατρέψουν την client-server επικοινωνία μεταξύ των 2 χρηστών σε peer-to-peer. Μετά την εδραίωση της peer-to-peer επικοινωνίας, επιλαμβάνεται το RTP πρωτόκολλο, το οποίο αναλαμβάνει να μεταφέρει τα πολυμεσικά δεδομένα. Στην υλοποίηση μας δεν έχουμε υλοποιήσει VoIP επί της ουσίας, αλλά μια ασφαλή εφαρμογή ανταλλαγής μηνυμάτων βασισμένη πάνω στο πρωτόκολλο SIP που δεν χρησιμοποιεί όμως το πρωτόκολλο RTP για την μεταφορά και τη διαχείριση των δεδομένων καθώς τα δεδομένα της υλοποίησης μας δεν είναι πολυμεσικού περιεχομένου.

2 Σχετικά με την υλοποίηση

2.1 Key Agreement Protocol

Στην προηγούμενη εργασία ασχοληθήκαμε με την υλοποίηση τριών πρωτοκόλλων, συμφωνίας κοινού κλειδιού. Για την συμφωνία κλειδιών μεταξύ των οντοτήτων αυτής της εργασίας, χρησιμοποιήσαμε το πιο ασφαλές από αυτά, το "Station-to-Station Elliptic Curve Daffier Hellman". Σε αυτή την υλοποίηση φτιάξαμε την κλάση STSKAP η όποια περιέχει μεθόδους για τα διαφορά στάδια της συμφωνίας κοινού κλειδιού. Η μέθοδος doAgreement παίρνει ως παράμετρο το ObjectInputStream και ObjectOutputStream της οντότητας και τον ρόλο του ο οποίος είναι είτε REFERRER είτε REFEREE και εκτελεί όλη την ακολουθία των βημάτων του πρωτοκόλλου. Το συμφωνηθέν κλειδί κάθε σύνδεσης διατηρείται και χρησιμοποιείται για την κρυπτογράφηση των πακέτων μέχρι αυτή να κλείσει.

2.2 Δίκτυο Ανωνυμοποίησης

Για την διατήρηση της ανωνυμίας των χρηστών, κάναμε χρήση του δικτυού Tor, καθώς πέρσι είχαμε εκπονήσει σε σχετική υλοποίηση με χρήση του δικτυού I2P και θέλαμε να δούμε και την υλοποίηση των Tor Sockets σε java. Για τον σκοπό αυτό κάναμε χρήση βιβλιοθήκης T0rlib4j που είναι μια βιβλιοθήκη Java ανοιχτού κώδικα, για διαχείριση του Tor την οποία και παραμετροποιήσαμε ώστε να ξεφορτωθούμε τα log που εμφάνιζε στο output.

2.3 Πρωτόκολλο RTP

Η υλοποίηση μας αφορά το υπόβαθρο μιας ανώνυμης VoIP υπηρεσίας (χρήση του πρωτοκόλλου SIP), στο οποίο βασίσαμε μιας ασφαλή εφαρμογή ανώνυμης ανταλλαγής μηνυμάτων. Κανονικά, στο content των πακέτων του SIP περιέχονται και οι παράμετροι για το πρωτόκολλο RTP για τη μεταφορά πολυμεσικών δεδομένων κάτι που δε περικλείεται στη παρούσα υλοποίηση.

2.4 Απλότητα

Αρχικά πήγαμε να κάνουμε implement τον SIPListener του JAIN API. Ωστόσο είδαμε πως για κάτι τέτοιο θα χρειαζόταν να υλοποιήσουμε ολόκληρη την επικοινωνία μεταξύ των οντοτήτων με το πρωτόκολλο SIP. Αντιθέτως στην υλοποίηση μας αρκεστήκαμε στο απλό σενάριο όπου αρχικά ο Bob κάνει register στον ProxyB και έπειτα λαμβάνει ένα INVITE για έναρξη κλήσης από την Alice η όποια είναι συνδεδεμένη με τον ProxyA. Έτσι για να μειωθεί και η πολυπλοκότητα του κώδικα που είχαμε να αναπτύξουμε λέγω του επιβαρυμένου προγράμματος και μειωμένου μας χρόνου αρκεστήκαμε σε αυτό το απλό σενάριο όπου δεν υπάρχουν λάθη ή σφάλματα συνεπώς δεν παρέχονται false responses (πχ άμα ο Bob δώσει λάθος κωδικό κατά το REGISTER ή άμα αρνηθεί την έναρξη της κλήσης με την Alice). Όμως για να είμαστε σίγουροι ότι είναι έγκυρο το κομμάτι της υλοποίησης μας, ακολουθήσαμε τα πρότυπα που περιγράφουν την πορεία ανταλλαγής μηνυμάτων στα Sessions του S.IP. Η βασική μας καθοδήγηση ήταν τα SIP: Session Initiation Protocol (RFC 3261), SIP Basic Call Flow Examples (RFC 3665) και Hitchhiker's Guide to SIP (RFC 5411).

2.5 Λεπτομέρειες.

Στο απλό μας παράδειγμα δεν υπάρχει ανάγκη για την υλοποίηση Registrar και Location Service. Ο ρόλος των δυο οντοτήτων συμπεριλαμβάνεται στη λειτουργιά του ο Proxy. Αυτό που κάναμε έξτρα είναι ένας Server που λειτουργεί με RMI και διαβάζει τους κωδικούς των χρηστών από μια βάση και υπολογίζει και επιστρέφει την σύνοψη τους στον Proxy. Έπειτα σκεφτήκαμε πως και αυτό ήταν άσκοπο και ίσως καλύτερα να χαμε κάνει αντ'αυτού το Location Service με τον ίδιο τρόπο άλλα ήταν πλέον αργά. Επίσης ο κωδικός που πρέπει να δώσει ο χρηστής για την εξουσιοδότηση του, επιστρέφεται από μια μια μέθοδο που είναι στον Client ανάλογα αν ο πελάτης είναι ο Bob ή η Alice. Τέλος στα πακέτα SIP παραλείψαμε την προσθήκη των πεδίων header: Contact, Route και Record-Route που περιγράφονται στο RFC για λογούς λιτότητας.

Για τον έλεγχο της υλοποίησης παρέχονται δυο Main κλάσεις, η SimpleRun και η SimpleRunTor. Η δεύτερη με χρήση του δικτυού του Tor για ανωνυμία των Clients. Σημειώνεται ότι η εκτέλεση της άνωθεν διαρκεί τουλάχιστον 2:30 λεπτά.

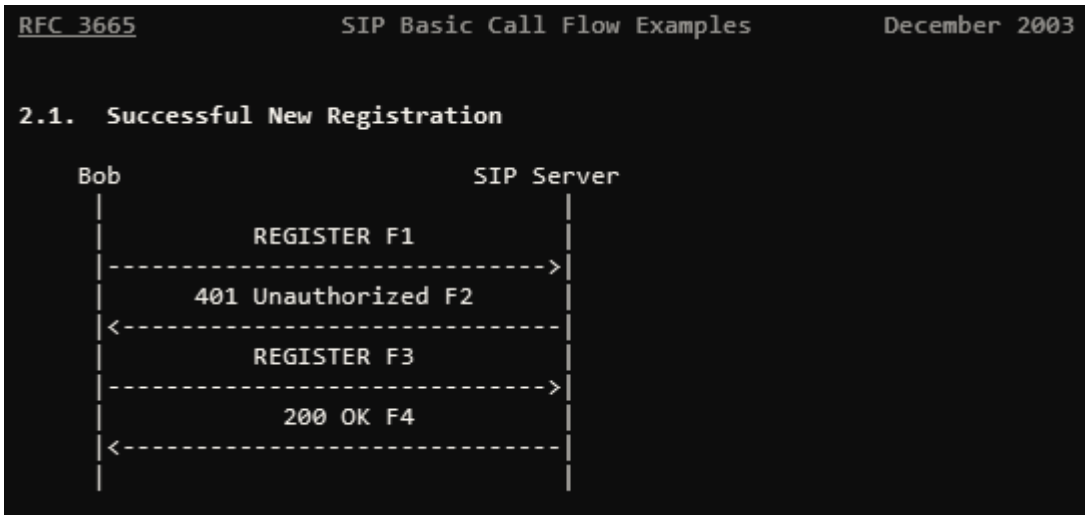
3 Οθόνες Εκτέλεσης

Ακολουθούν στιγμιότυπα από την εκτέλεση της SimpleRunTor, συνοδευόμενα από τα αντίστοιχο Call Flow που υποδεικνυει το RFC 3665 όπου εμφανίζονται όλα τα (αποκρυπτογραφημένα) SIP πακέτα που ανταλλάσσονται μεταξύ των οντοτήτων καθώς και ενημερώσεις για την ορθή εκτέλεση όλων τα βημάτων των πρωτοκόλλων συμφωνίας κλειδιού. Τα οποία μπορείτε να επιβεβαιώσετε και από τον κώδικα στα σημεία όπου και αυτά τυπώνονται.

3.1 Εκκίνηση εξυπηρετητών και σύνδεση των χρηστών:

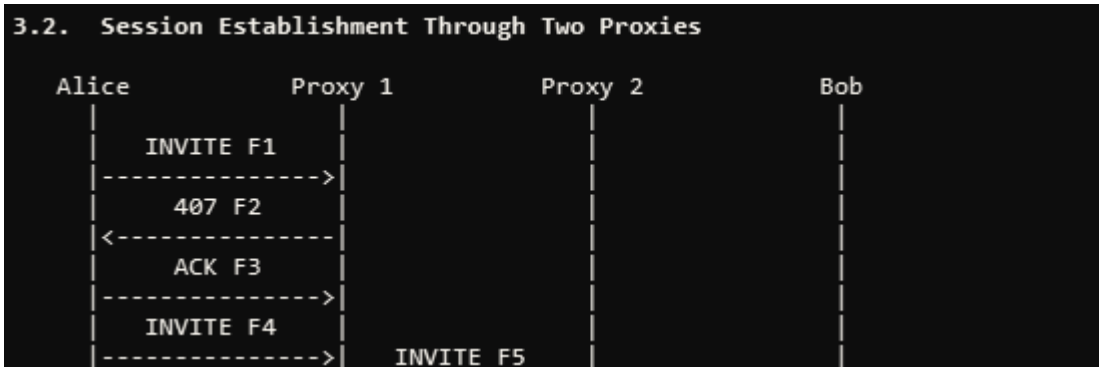
```
run:
[11:17:48] Started server at: 127.0.0.1:7060.
[11:17:48] Hidden Service Binds to: eeguphpmatkrgsxd.onion:5060.

[11:17:59] Started server at: 127.0.0.1:7061.
[11:17:59] Hidden Service Binds to: s4d4d7bk7xgemt3i.onion:5060.


[11:18:28] Proxy at: /127.0.0.1:7060/eeguphpmatkrgsxd.onion:5060 accepted connection from: 127.0.0.1:1306
[11:18:29] Client's DiffieHellman Key Agreement initialized
[11:18:29] Client sent DiffieHellman Public Key to Client
[11:18:30] Received Proxy's DiffieHellman Public Key
[11:18:31] Proxy's DiffieHellman Key Agreement initialized
[11:18:31] Proxy generated Common Secret Key and Signature
[11:18:32] Proxy sent Common Secret Key and Signature to Proxy
[11:18:32] Client received Client's DiffieHellman Public Key and Signature
[11:18:33] Client generated Common Secret Key and Signature
[11:18:33] Client's Protocol Session Authenticated
[11:18:33] Client sent Common Secret Key and Signature to Client
[11:18:34] Proxy received Client's DiffieHellman Public Key and Signature
[11:18:34] Proxy generated Common Secret Key and Signature
[11:18:34] Proxy's Protocol Session Authenticated
[11:18:34] Client's Station-to-Station Key Agreement Finished
[11:18:35] Proxy's Station-to-Station Key Agreement Finished
[11:18:35] Connection thread: 76b6a5d86d4a is running.


[11:18:58] Proxy at: /127.0.0.1:7061/s4d4d7bk7xgemt3i.onion:5060 accepted connection from: 127.0.0.1:1321
[11:18:59] Client's DiffieHellman Key Agreement initialized
[11:18:59] Client sent DiffieHellman Public Key to Client
[11:19:00] Received Proxy's DiffieHellman Public Key
[11:19:00] Proxy's DiffieHellman Key Agreement initialized
[11:19:01] Proxy generated Common Secret Key and Signature
[11:19:01] Proxy sent Common Secret Key and Signature to Proxy
[11:19:01] Client received Client's DiffieHellman Public Key and Signature
[11:19:02] Client generated Common Secret Key and Signature
[11:19:02] Client's Protocol Session Authenticated
[11:19:02] Client sent Common Secret Key and Signature to Client
[11:19:03] Proxy received Client's DiffieHellman Public Key and Signature
[11:19:04] Proxy generated Common Secret Key and Signature
[11:19:04] Proxy's Protocol Session Authenticated
[11:19:04] Client's Station-to-Station Key Agreement Finished
[11:19:05] Proxy's Station-to-Station Key Agreement Finished
```

3.2 Εγγραφή του Bob σε ProxyB:



```
----------BOB REGISTRATION----------
------------------------------------------
[11:19:05] Connection thread: 6828c8da6e6d is running.


[11:19:06] Proxy at: /127.0.0.1:7061/s4d4d7bk7xgemt3i.onion:5060 Received an Encrypted SIP Packet from: 127.0.0.1:1321
[11:19:06] Decrypted with the Common Secret Key:

REGISTER sip:bob@s4d4d7bk7xgemt3i.onion SIP/2.0
Via: SIP/2.0/TCP bob@s4d4d7bk7xgemt3i.onion;branch=f561c24d
Max-Forwards: 70
From: Bob <sip:bob@s4d4d7bk7xgemt3i.onion>;tag=059a7cb2
To: Bob <sip:bob@s4d4d7bk7xgemt3i.onion>
Call-ID: ac943b2493af@s4d4d7bk7xgemt3i.onion
CSeq: 1 REGISTER
Content-Length: 0

[11:19:06] Client at: /127.0.0.1:1319 Received an Encrypted SIP Packet from Proxy at: /127.0.0.1:1316
[11:19:06] Decrypted with the Common Secret Key:

sip:bob@s4d4d7bk7xgemt3i.onion SIP/2.0 407 Proxy Authentication Required
Via: SIP/2.0/TCP bob@s4d4d7bk7xgemt3i.onion;branch=f561c24d;received=127.0.0.1
From: Bob <sip:bob@s4d4d7bk7xgemt3i.onion>
To: Bob <sip:bob@s4d4d7bk7xgemt3i.onion>
Call-ID: ac943b2493af@s4d4d7bk7xgemt3i.onion
CSeq: 1 REGISTER
Content-Length: 0
Proxy-Authenticate: Digest
        realm="s4d4d7bk7xgemt3i.onion",
        qop="auth",
        nonce="vAGj4jlIlQv9wdeNnL3+OQ==",
        algorithm="MD5"

[11:19:06] Proxy at: /127.0.0.1:7061/s4d4d7bk7xgemt3i.onion:5060 Received an Encrypted SIP Packet from: 127.0.0.1:1321
[11:19:06] Decrypted with the Common Secret Key:

REGISTER sip:bob@s4d4d7bk7xgemt3i.onion SIP/2.0
Via: SIP/2.0/TCP s4d4d7bk7xgemt3i.onion:5060;branch=f561c24d
Max-Forwards: 70
From: Bob <sip:bob@s4d4d7bk7xgemt3i.onion>
To: Bob <sip:bob@s4d4d7bk7xgemt3i.onion>
Call-ID: ac943b2493af@s4d4d7bk7xgemt3i.onion
CSeq: 2 REGISTER
Content-Length: 0
Proxy-Authorization: Digest
        username="bob",
        realm="s4d4d7bk7xgemt3i.onion",
        nonce="vAGj4jlIlQv9wdeNnL3+OQ==",
        cnonce="7mA6GndJTv4="
        responce="mOqSTBbhp7T9AbDRTZCz1Q=="

[11:19:07] Client at: /127.0.0.1:1319 Received an Encrypted SIP Packet from Proxy at: /127.0.0.1:1316
[11:19:07] Decrypted with the Common Secret Key:

sip:bob@s4d4d7bk7xgemt3i.onion SIP/2.0 200 OK
Via: SIP/2.0/TCP s4d4d7bk7xgemt3i.onion:5060;branch=f561c24d;received=127.0.0.1
From: Bob <sip:bob@s4d4d7bk7xgemt3i.onion>
To: Bob <sip:bob@s4d4d7bk7xgemt3i.onion>
Call-ID: ac943b2493af@s4d4d7bk7xgemt3i.onion
CSeq: 2 REGISTER
Content-Length: 0
```

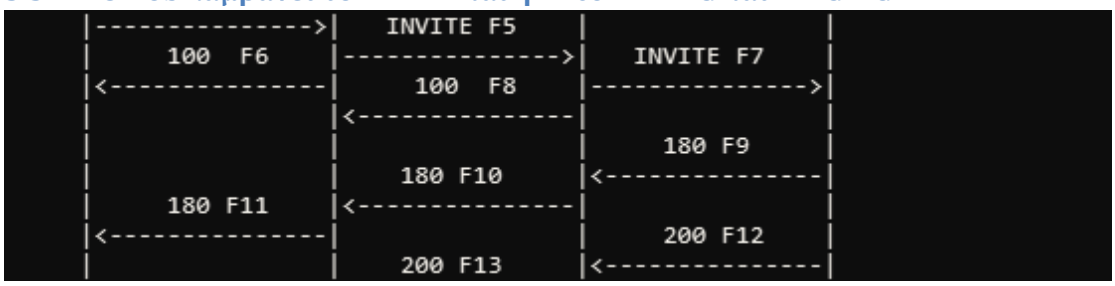
3.3 Αποστολή πρόσκλησης σε κλήση από την Alice στον Bob:



3.3.1 Αποστολή και αυθεντικοποίηση του INVITE από Alice:

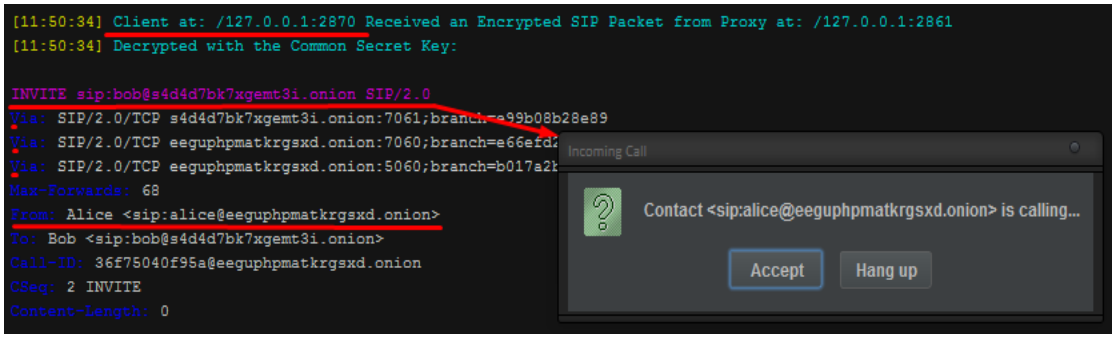
```
--------------ALICE INVITE BOB--------------
--------------------------------------------

[11:19:11] Proxy at: /127.0.0.1:7060/eeguphpmatkrgsxd.onion:5060 Received an Encrypted SIP Packet from: 127.0.0.1:1306
[11:19:11] Decrypted with the Common Secret Key:

INVITE sip:bob@s4d4d7bk7xgemt3i.onion SIP/2.0
Via: SIP/2.0/TCP eeguphpmatkrgsxd.onion:5060;branch=9228d569
Max-Forwards: 70
From: Alice <sip:alice@eeguphpmatkrgsxd.onion>;tag=7c9dd734
To: Bob <sip:bob@s4d4d7bk7xgemt3i.onion>
Call-ID: eba86371113a@eeguphpmatkrgsxd.onion
CSeq: 1 INVITE
Content-Length: 0

[11:19:12] Client at: /127.0.0.1:1303 Received an Encrypted SIP Packet from Proxy at: /127.0.0.1:1301
[11:19:12] Decrypted with the Common Secret Key:

sip:bob@s4d4d7bk7xgemt3i.onion SIP/2.0 407 Proxy Authentication Required
Via: SIP/2.0/TCP eeguphpmatkrgsxd.onion:5060;branch=9228d569;received=127.0.0.1
From: Alice <sip:alice@eeguphpmatkrgsxd.onion>
To: Bob <sip:bob@s4d4d7bk7xgemt3i.onion>
Call-ID: eba86371113a@eeguphpmatkrgsxd.onion
CSeq: 1 INVITE
Content-Length: 0
Proxy-Authenticate: Digest
        realm="eeguphpmatkrgsxd.onion",
        qop="auth",
        nonce="X/mISg7J/9iFKP+rX4xNOA==",
        algorithm="MD5"

[11:19:12] Proxy at: /127.0.0.1:7060/eeguphpmatkrgsxd.onion:5060 Received an Encrypted SIP Packet from: 127.0.0.1:1306
[11:19:12] Decrypted with the Common Secret Key:

ACK sip:bob@s4d4d7bk7xgemt3i.onion SIP/2.0
Via: SIP/2.0/TCP eeguphpmatkrgsxd.onion:5060;branch=9228d569
Max-Forwards: 70
From: Alice <sip:alice@eeguphpmatkrgsxd.onion>
To: Bob <sip:bob@s4d4d7bk7xgemt3i.onion>
Call-ID: eba86371113a@eeguphpmatkrgsxd.onion
CSeq: 1 ACK
Content-Length: 0

[11:19:12] Proxy at: /127.0.0.1:7060/eeguphpmatkrgsxd.onion:5060 Received an Encrypted SIP Packet from: 127.0.0.1:1306
[11:19:12] Decrypted with the Common Secret Key:

INVITE sip:bob@s4d4d7bk7xgemt3i.onion SIP/2.0
Via: SIP/2.0/TCP eeguphpmatkrgsxd.onion:5060;branch=9228d569
Max-Forwards: 70
From: Alice <sip:alice@eeguphpmatkrgsxd.onion>
To: Bob <sip:bob@s4d4d7bk7xgemt3i.onion>
Call-ID: eba86371113a@eeguphpmatkrgsxd.onion
CSeq: 2 INVITE
Content-Length: 0
Proxy-Authorization: Digest
        username="alice",
        realm="eeguphpmatkrgsxd.onion",
        nonce="X/mISg7J/9iFKP+rX4xNOA==",
        cnonce="7eByckEHj4Q="
        responce="QzqJrWAS4yVuM7ZEouk34Q=="
```

3.3.2 Ο Bob λαμβάνει το INVITE και η Alice TRYING και RINGING:

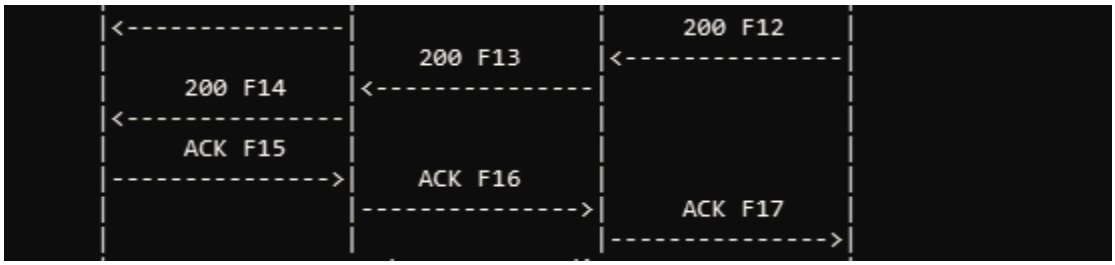


```
INVITE sip:bob@s4d4d7bk7xgemt3i.onion SIP/2.0
Via: SIP/2.0/TCP s4d4d7bk7xgemt3i.onion:7061;branch=8c97f73fe292
Via: SIP/2.0/TCP eeguphpmatkrgsxd.onion:7060;branch=76b6a5d86d4a;received=eeguphpmatkrgsxd.onion
Via: SIP/2.0/TCP eeguphpmatkrgsxd.onion:5060;branch=9228d569;received=127.0.0.1
Max-Forwards: 68
From: Alice <sip:alice@eeguphpmatkrgsxd.onion>
To: Bob <sip:bob@s4d4d7bk7xgemt3i.onion>
Call-ID: eba86371113a@eeguphpmatkrgsxd.onion
CSeq: 2 INVITE
Content-Length: 0

[11:19:37] Proxy at: /127.0.0.1:7061/s4d4d7bk7xgemt3i.onion:5060 Received an Encrypted SIP Packet from: 127.0.0.1:1321
[11:19:37] Decrypted with the Common Secret Key:

sip:bob@s4d4d7bk7xgemt3i.onion SIP/2.0 180 Ringing
Via: SIP/2.0/TCP s4d4d7bk7xgemt3i.onion:7061;branch=8c97f73fe292;received=/127.0.0.1
Via: SIP/2.0/TCP eeguphpmatkrgsxd.onion:7060;branch=76b6a5d86d4a;received=eeguphpmatkrgsxd.onion
Via: SIP/2.0/TCP eeguphpmatkrgsxd.onion:5060;branch=9228d569;received=127.0.0.1
From: Alice <sip:alice@eeguphpmatkrgsxd.onion>
To: Bob <sip:bob@s4d4d7bk7xgemt3i.onion>
Call-ID: eba86371113a@eeguphpmatkrgsxd.onion
CSeq: 2 INVITE
Content-Length: 0

[11:19:38] Proxy at: /127.0.0.1:7060/eeguphpmatkrgsxd.onion:5060 Received an Encrypted SIP Packet from: 127.0.0.1:1332
[11:19:38] Decrypted with the Common Secret Key:

sip:bob@s4d4d7bk7xgemt3i.onion SIP/2.0 180 Ringing
Via: SIP/2.0/TCP eeguphpmatkrgsxd.onion:7060;branch=76b6a5d86d4a;received=eeguphpmatkrgsxd.onion
Via: SIP/2.0/TCP eeguphpmatkrgsxd.onion:5060;branch=9228d569;received=127.0.0.1
From: Alice <sip:alice@eeguphpmatkrgsxd.onion>
To: Bob <sip:bob@s4d4d7bk7xgemt3i.onion>
Call-ID: eba86371113a@eeguphpmatkrgsxd.onion
CSeq: 2 INVITE
Content-Length: 0

[11:19:38] Client at: /127.0.0.1:1303 Received an Encrypted SIP Packet from Proxy at: /127.0.0.1:1301
[11:19:38] Decrypted with the Common Secret Key:

sip:bob@s4d4d7bk7xgemt3i.onion SIP/2.0 180 Ringing
Via: SIP/2.0/TCP eeguphpmatkrgsxd.onion:5060;branch=9228d569;received=127.0.0.1
From: Alice <sip:alice@eeguphpmatkrgsxd.onion>
To: Bob <sip:bob@s4d4d7bk7xgemt3i.onion>
Call-ID: eba86371113a@eeguphpmatkrgsxd.onion
CSeq: 2 INVITE
Content-Length: 0

[11:19:46] Proxy at: /127.0.0.1:7061/s4d4d7bk7xgemt3i.onion:5060 Received an Encrypted SIP Packet from: 127.0.0.1:1321
[11:19:46] Decrypted with the Common Secret Key:

sip:bob@s4d4d7bk7xgemt3i.onion SIP/2.0 200 OK
Via: SIP/2.0/TCP s4d4d7bk7xgemt3i.onion:7061;branch=8c97f73fe292;received=/127.0.0.1
Via: SIP/2.0/TCP eeguphpmatkrgsxd.onion:7060;branch=76b6a5d86d4a;received=eeguphpmatkrgsxd.onion
Via: SIP/2.0/TCP eeguphpmatkrgsxd.onion:5060;branch=9228d569;received=127.0.0.1
From: Alice <sip:alice@eeguphpmatkrgsxd.onion>
To: Bob <sip:bob@s4d4d7bk7xgemt3i.onion>
Call-ID: eba86371113a@eeguphpmatkrgsxd.onion
CSeq: 2 INVITE
Content-Length: 0
```

3.3.2.1 *Ο Bob κάνει αποδοχή της κλήσης:*



3.3.3 Η Alice λαμβάνει OK και ο Bob λαμβάνει ACK:




```
sip:bob@s4d4d7bk7xgemt3i.onion SIP/2.0 200 OK
Via: SIP/2.0/TCP eeguphpmatkrgsxd.onion:7060;branch=76b6a5d86d4a;received=eeguphpmatkrgsxd.onion
Via: SIP/2.0/TCP eeguphpmatkrgsxd.onion:5060;branch=9228d569;received=127.0.0.1
From: Alice <sip:alice@eeguphpmatkrgsxd.onion>
To: Bob <sip:bob@s4d4d7bk7xgemt3i.onion>
Call-ID: eba86371113a@eeguphpmatkrgsxd.onion
CSeq: 2 INVITE
Content-Length: 0

[11:19:46] Client at: /127.0.0.1:1303 Received an Encrypted SIP Packet from Proxy at: /127.0.0.1:1301
[11:19:46] Decrypted with the Common Secret Key:

sip:bob@s4d4d7bk7xgemt3i.onion SIP/2.0 200 OK
Via: SIP/2.0/TCP eeguphpmatkrgsxd.onion:5060;branch=9228d569;received=127.0.0.1
From: Alice <sip:alice@eeguphpmatkrgsxd.onion>
To: Bob <sip:bob@s4d4d7bk7xgemt3i.onion>
Call-ID: eba86371113a@eeguphpmatkrgsxd.onion
CSeq: 2 INVITE
Content-Length: 0

[11:19:47] Proxy at: /127.0.0.1:7060/eeguphpmatkrgsxd.onion:5060 Received an Encrypted SIP Packet from: 127.0.0.1:1306
[11:19:47] Decrypted with the Common Secret Key:

ACK sip:bob@s4d4d7bk7xgemt3i.onion SIP/2.0
Via: SIP/2.0/TCP eeguphpmatkrgsxd.onion:5060;branch=9228d569
Max-Forwards: 70
From: Alice <sip:alice@eeguphpmatkrgsxd.onion>
To: Bob <sip:bob@s4d4d7bk7xgemt3i.onion>
Call-ID: eba86371113a@eeguphpmatkrgsxd.onion
CSeq: 1 ACK
Content-Length: 0

[11:19:47] Proxy at: /127.0.0.1:7061/s4d4d7bk7xgemt3i.onion:5060 Received an Encrypted SIP Packet from: 127.0.0.1:1336
[11:19:47] Decrypted with the Common Secret Key:

ACK sip:bob@s4d4d7bk7xgemt3i.onion SIP/2.0
Via: SIP/2.0/TCP eeguphpmatkrgsxd.onion:7060;branch=76b6a5d86d4a
Via: SIP/2.0/TCP eeguphpmatkrgsxd.onion:5060;branch=9228d569;received=127.0.0.1
Max-Forwards: 69
From: Alice <sip:alice@eeguphpmatkrgsxd.onion>
To: Bob <sip:bob@s4d4d7bk7xgemt3i.onion>
Call-ID: eba86371113a@eeguphpmatkrgsxd.onion
CSeq: 1 ACK
Content-Length: 0

[11:19:47] Client at: /127.0.0.1:1319 Received an Encrypted SIP Packet from Proxy at: /127.0.0.1:1316
[11:19:47] Decrypted with the Common Secret Key:

ACK sip:bob@s4d4d7bk7xgemt3i.onion SIP/2.0
Via: SIP/2.0/TCP s4d4d7bk7xgemt3i.onion:7061;branch=8c97f73fe292
Via: SIP/2.0/TCP eeguphpmatkrgsxd.onion:7060;branch=76b6a5d86d4a;received=eeguphpmatkrgsxd.onion
Via: SIP/2.0/TCP eeguphpmatkrgsxd.onion:5060;branch=9228d569;received=127.0.0.1
Max-Forwards: 68
From: Alice <sip:alice@eeguphpmatkrgsxd.onion>
To: Bob <sip:bob@s4d4d7bk7xgemt3i.onion>
Call-ID: eba86371113a@eeguphpmatkrgsxd.onion
CSeq: 1 ACK
Content-Length: 0
BUILD STOPPED (total time: 2 minutes 23 seconds)
```