

Esercitazione 3

Cattura e analisi di pacchetti SIP

Tecnologie e Servizi di Rete

1 Introduzione

Scopo dell'esercitazione e' analizzare il processo di registrazione SIP e analizzare una sessione multimediale tra due utenti.

L'esercitazione richiede:

- due PC dotati di sistema operativo Windows XP SP1 o superiore
- il software **X-Lite** installato su detti PC scaricabile da:

<http://www.counterpath.com/x-lite.html>

- Due account SIP ottenibili presso iptel.org. Per ciascun account seguire la procedura guidata riportata qui:

<http://serweb.iptel.org/user/reg/>

- un analizzatore di rete installato sul PC in uso

E' possibile utilizzare un altro S.O. e/o un altro client SIP, ma e' responsabilita' dell'utente documentarsi su come configurare il proprio client/S.O. per svolgere questa esercitazione.

Sui PC del LABINF e su parte dei PC del LADISPE il software **X-Lite** e' gia' installato correttamente.

2 Configurazione dello User Agent SIP

1. Installate lo User Agent SIP **X-lite**
2. Create un account SIP presso il servizio [iptel](http://iptel.org)

<http://serweb.iptel.org/user/reg/>

Al termine della procedura di creazione comparira' una pagina web indicante la vostra URI SIP nella forma **sip:<nome utente>@iptel.org**. Presso la casella di posta che avete inserito durante il processo di registrazione riceverete una mail con tutte le informazioni sul vostro nuovo account SIP.

3. Avviate ora il software **X-lite**. Posizionate il puntatore del mouse su **X-lite** e premete il tasto destro. Selezionate ora la voce **SIP Account Settings...** Si aprirà ora la finestra **SIP Accounts**: premete il pulsante **Add...** In riferimento alla finestra che si aprirà:
 - (a) Nella casella **Display name** inserite il nome che volete sia associato al vostro account (mettete quello che preferite)
 - (b) Nella casella **username** inserite il vostro username sip: se la URI che avete ricevuto e' per esempio **sip:torrero@iptel.org** inserite solo **torrero** (**sip:** e **@iptel.org** non servono)
 - (c) Nella casella **password** inserite la password del vostro utente
 - (d) Lasciate vuota la casella **Authorization user name**
 - (e) Nella casella **domain** inserite **iptel.org**
 - (f) Assicuratevi che la voce **Register with domain and receive incoming calls** sia selezionata (ci deve essere la **v** e dovrebbe esserci di default)
 - (g) Nella voce **Send Outbound via:** selezionate **domain** (dovrebbe essere già' selezionato)
 - (h) Nella sezione **voice mail** disabilitate **check for voice mail**
 - (i) Premete **Ok** e la finestra si chiuderà'. A questo punto appena premerete **Close** nella finestra **SIP Accounts** partirà' la procedura di registrazione presso il dominio **iptel.org**.
4. Ora chiudete l'applicazione **X-lite** e subito dopo avviate l'analizzatore di rete. Selezionate l'interfaccia corretta e preparatevi ad effettuare la cattura
5. Iniziate la cattura e poi avviate **X-lite**: dovrete poter catturare la sessione di registrazione
6. Se la cattura della fase di registrazione SIP avviene con successo, salvate la cattura e iniziate i preparativi per la cattura della chiamata SIP. A questo scopo dovete creare un secondo account SIP su **iptel.org** ripetendo la procedura illustrata al punto 3. E' necessario anche un secondo pc con installato **X-lite**. Se lo desiderate potete accordarvi con i membri di un altro gruppo e provare ad instaurare una chiamata con loro. In questo caso ciascun gruppo dovrà' effettuare la cattura dal proprio PC e inviare separatamente la propria cattura attraverso il form preposto allo scopo.
7. A questo punto avviate l'analizzatore di rete, iniziate la chiamata e catturate il traffico generato: per chiamare un utente e' sufficiente digitare dall'interfaccia di **X-lite** l'URI completa dell'utente che si desidera contattare (nella forma **sip:<nome_utente>@iptel.org**).
8. Completate entrambe le catture potete iniziare a rispondere ai quesiti riportati nel seguito

TSR Lab3: Domande e Risposte

1. Indicare il gruppo di appartenenza.

user_106

2.1 Analisi della fase di registrazione

2. Riportare i dati principali della connessione (URI dell'utente che si registra, l'indirizzo IP dell'UA che si registra, dominio SIP e indirizzo IP del proxy)

URI: sip:alessandroavila@iptel.org

IP: 130.192.31.206

DOMINIO SIP: iptel.org

INDIRIZZO IP PROXY: 213.192.59.75

3. Elencare i messaggi SIP scambiati durante la fase di registrazione (richieste e risposte, escludendo eventuali pacchetti SIP non necessari alla registrazione stessa)

SOURCE	DESTINATION	PROT	INFO
130.192.31.206	213.192.59.75	SIP	Request: REGISTER sip:iptel.org
213.192.59.75	130.192.31.206	SIP	Status: 401 Unauthorized (0 bindings)
130.192.31.206	213.192.59.75	SIP	Request: REGISTER sip:iptel.org
213.192.59.75	130.192.31.206	SIP	Status: 200 OK (1 bindings)
130.192.31.206	213.192.59.75	SIP	Request: REGISTER sip:iptel.org
213.192.59.75	130.192.31.206	SIP	Status: 200 OK (0 bindings)
130.192.31.206	213.192.59.75	SIP	Request: REGISTER sip:iptel.org
213.192.59.75	130.192.31.206	SIP	Status: 200 OK (1 bindings)

4. Commentare brevemente ciascun messaggio elencato descrivendone il significato e illustrandone i campi più significativi dei relativi header SIP nel contesto della registrazione

Lo UA invia una richiesta di registrazione al server sip (213.192.59.75)
Metodo: REGISTER sip:iptel.org SIP/2.0
I principali campi dell' header sono:
To/From: contengono l'URI da registrare (sip:alessandroavila@iptel.org)
Contact: contiene le informazioni da utilizzare per il dialogo diretto UA-UA
Call-ID: identificatore univoco di registrazione
(MDdiMjRiOWI3MWUwY2U2MjRkZTFiZmVmZTQxOTAwYzY)
CSeq: numero di sequenza e metodo richiesto (1 REGISTER); poichè sip può usare UDP, i numeri di sequenza mettono in correlazione le risposte con le relative richieste.
Abbiamo, inoltre, il periodo di validità della registrazione (3600 s --> 1h) e la sequenza di comandi interpretabili dallo UA in questione (INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO)

Il server risponde con un messaggio di errore (401 Unauthorized) poiché richiede l'autenticazione.

I principali campi dell' header contengono gli stessi valori del messaggio precedente, eccetto che per il campo WWW-Authenticate, che indica il realm (iptel.org) e la stringa usata come sfida per l'autenticazione (nonce="TSrh7k0q4eQ3HIJ1WX52hzbXWmnRpTkk")

Lo UA risponde alla sfida con un altro messaggio di REGISTER contenente le informazioni per l'autenticazione (è infatti presente il campo 'Authorization'):

Lo schema di autenticazione: si tratta di un message digest.

Lo username e il realm presso cui lo UA si autentica (coincide con quello presente nel messaggio di errore precedente)

Infine, la stringa da codificare fornita dal server SIP (nonce), la stringa codificata (response="32ad66311522c04779e885c7b5a0ac20") e l'algoritmo di codifica adottato (in questo caso MD5)

Il server SIP risponde quindi con un messaggio di avvenuta autenticazione (200 OK).

Infine, altre due richieste di registrazione, a cui fanno seguito le relative risposte.

2.2 Analisi della fase di chiamata

5. Riportare i dati principali della connessione (URI degli utenti coinvolti nella chiamata, dominio SIP di entrambi gli utenti, ecc)

URI chiamante: sip:alessandroavila@iptel.org
URI chiamato: sip:nicola.domingo@iptel.org
Domino: iptel.org in entrambi i casi.

6. Riportare una lista di tutti i messaggi SIP scambiati durante l'instaurazione della sessione (possibilmente rappresentandoli graficamente attraverso un trapezioide SIP, ricordandosi di includere richieste e risposte)

Vedi ultima pagina.

7. Specificare se e' abilitato o meno il `record routing`. Nel caso lo sia, in quale messaggio tra quelli che avete catturato compare il relativo header? Chi lo inserisce e perche'?

Il `record routing` è abilitato.
Il relativo header compare per la prima volta nell'INVITE che riceve il chiamato (130.192.31.206 nel nostro caso) e viene inserito dal proxy SIP.
Così facendo impone il passaggio dei messaggi SIP attraverso di lui.
La prima volta che il chiamante (130.192.31.200) trova tale header è invece nel primo RINGING che riceve.

8. Descrivere brevemente il significato dei principali messaggi SIP scambiati nel contesto della chiamata illustrando brevemente anche i campi più significativi degli stessi

Il primo INVITE indica la richiesta di inizio di una comunicazione.
In tale pacchetto, nel campo "To" troviamo l'URI del destinatario (sip:alessandroavila@iptel.org) e nel campo "From" l'URI del mittente (nicola.domingo@iptel.org); tali campi non vengono invertiti nel corso della comunicazione.
Il campo "Contact" informa, invece, quale indirizzo e numero di porta deve usare l'altro UA nella comunicazione diretta (sip:nicola.domingo@130.192.31.220:1719).
Il campo ALLOW indica, invece, i comandi che l'UA supporta.
Il server SIP a questo primo INVITE risponde con un 407 Proxy Authentication Required, in quanto l'utente deve identificarsi, e indica anche il nonce di sfida.
Lo UA chiamante dopo aver inviato un ACK (necessari in quanto SIP non deve necessariamente eseguito su TCP), invia un secondo INVITE (con numero di sequenza 2) in cui riporta il response al nonce.
Questi quindi riceve prima un 100 TRYING ad indicare che il server SIP sta processando la sua richiesta e poi un 180 RINGING, ad indicare che la richiesta è andata a buon fine e che adesso si attende che lo UA destinatario accetti la chiamata.
Quando ciò avviene, si riceve un 200 OK e viene inviato un ACK. Il messaggio di BYE indica che la chiamata dall'altro capo, è stata chiusa e viene inviato un 200 OK.
Questi pacchetti, inoltre, presentano il campo RECORD-ROUTE: ciò indica che tutti i pacchetti della connessione, eccetto quelli dati contenente messaggi e campioni vocali, debbono passare attraverso il Proxy SIP.

213.192.59.75

SIP Proxy/SIP Server

130.192.31.220

User Agent



130.192.31.206

User Agent

