

# Forensics VoIP

Corso di Informatica Forense - OIG  
Facoltà di Giurisprudenza  
Università degli studi di Bologna

*dr. Stefano Fratepietro*

*m@il: stefano.fratepietro@unibo.it*

*skype: stefano.fratepietro*



CIRSFID



stevlab.net



## Contenuti

- **Intruduzione alla telefonia VoIP**
- Caratteristiche tecniche
- Sicurezza e VoIP
- Skype vs CIA & FBI
- Futuro del VoIP
- Tool

## Introduzione al VoIP I

“Voice over Internet Protocol” è la tecnologia che rende possibile effettuare una conversazione telefonica sfruttando una connessione internet o un'altra rete dedicata che utilizza il protocollo IP, anziché passare attraverso la normale linea di trasmissione telefonica.

Wikipedia



## Introduzione al VoIP II

Com'è possibile che un computer riesca a fare una telefonata con un normalissimo telefono di “vecchia generazione”?

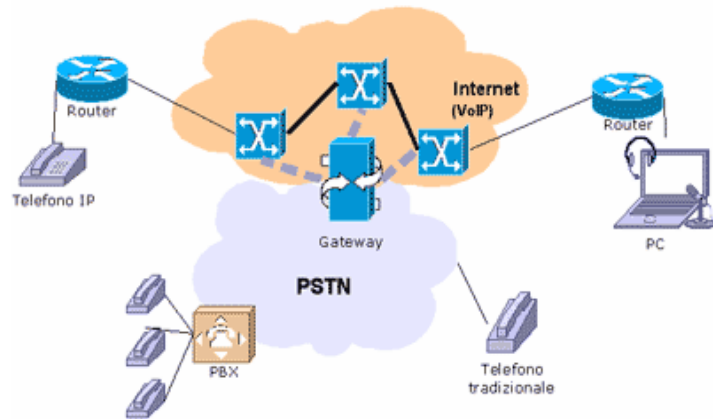
“ Facile! ”

I telefoni che usano le PSTN (Public Switched Telephone Network) sono collegati ai telefoni VoIP tramite veri e propri gateway messi a disposizione dalle compagnie telefoniche che permettono la comunicazione tra le due differenti tipologie di rete.





## Introduzione al VoIP III



## Contenuti

- Intruduzione alla telefonia VoIP
- **Caratteristiche tecniche**
- Sicurezza e VoIP
- Skype vs CIA & FBI
- Futuro del VoIP
- Tool



## Caratteristiche tecniche I

- Ad ogni componente hardware (telefono VoIP o computer) in grado di poter stabilire una connessione VoIP (telefonata) vi è associato un indirizzo IP all'interno della rete (Internet o una qualsiasi altra tipologia di rete che usa l'Internet Protocol)
- I telefoni, avendo un indirizzo IP, vengono considerati veri e propri "embedded computer" connessi alla rete in grado di poter stabilire connessioni al router VoIP.

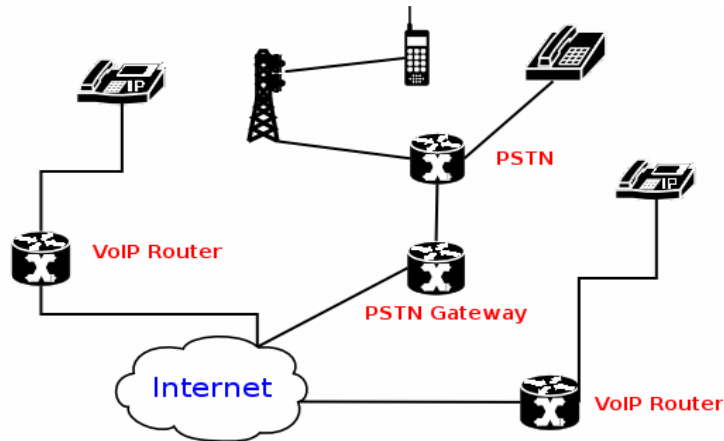


## Caratteristiche tecniche II

- Generalmente la procedura usata per iniziare una sessione VoIP è la seguente:
  - nel momento in cui viene alzata la cornetta il telefono IP (A) effettua il login con il router VoIP (generalmente senza password)
  - il router autentica il telefono (A) e dà il segnale di libero permettendo l'utente di effettuare la telefonata
  - l'utente digita il numero del telefono (B) che si vuole chiamare
  - il router IP instrada la chiamata al telefono (B) iniziando una connessione, (B) squillerà prontamente.



## Caratteristiche tecniche III



## Caratteristiche tecniche IV

- Il trasporto dei pacchetti per la telefonia VoIP necessita due tipologie di protocolli che lavorano in parallelo. Una tipologia cura il trasporto dei pacchetti, l'altra la codifica della segnalazione della conversazione.
- Per la gestione del trasporto dei pacchetti vi è un protocollo standard chiamato RTP (Real time Transport Protocol), per la codifica, invece, le grosse società hanno sviluppato diversi protocolli spesso proprietari e brevettati.



## Caratteristiche tecniche V

Protocolli più diffusi:

- SIP (Session Initiation Protocol) IETF
- SCCP (Skinny Client Control Protocol) Cisco
- H.323 ITU
- H.248 Megaco
- IAX (Inter Asterisk Xchange) Digium
- Per le soluzioni business, SCCP e H.323 risultano i protocolli più usati (i router Cisco System hanno il monopolio sulle vendite nel ramo business enterprise e utilizzano sistemi che sfruttano ambe due i protocolli)

(Esistono altri protocolli non menzionati in questa lista)



## Caratteristiche tecniche VI

**Problema: Diversi protocolli per la VoIP posso dialogare tra di loro direttamente? (ad esempio Skype e Msn)**

**No!** Tutti i protocolli sono stati sviluppati per dialogare solo con se stessi. Per ovviare a questo problema vengono usati dei software di supporto che rendono possibile il dialogo tra essi (Interoperabilità tra protocolli)



## Contenuti

- Intruduzione alla telefonia VoIP
- Caratteristiche tecniche
- **Sicurezza e VoIP**
- Skype vs CIA & FBI
- Futuro del VoIP
- Tool



## Sicurezza e VoIP I

- Ogni apparecchiatura essendo riconosciuta nella rete tramite un indirizzo IP viene considerata come se fosse un normalissimo computer, quindi essa potrebbe essere esposta alle classiche e ormai note tipologie di attacchi informatici:
  - Sniffing
  - Dos
  - Man in the middle
  - Buffer overflow



## Sicurezza e VoIP II

Phreaking: *L'esplorazione del funzionamento dei sistemi telefonici e di quelli ad essi strettamente correlati*

In molti film narranti ipotetiche storie di hacker, il protagonista dimostra com'è facile telefonare senza pagare la telefonata facendo semplicemente ascoltare un suono avente la stessa frequenza del rumore della monetina inserita nell'apparecchio.

**La situazione al giorno d'oggi non è cambiata molto!!!**



## Sicurezza e VoIP III

Alcuni protocolli, ma soprattutto alcune strumentazioni hardware, presentano grosse problematiche di sicurezza.

Nella maggior parte dei casi nelle reti di telefonia VoIP, vengono usati dei gatekeeper Cisco con un sistema per la gestione del traffico e delle tariffazioni dei clienti. Questi router utilizzano sistemi embedded che sfruttano il protocollo h.323

**Come avviene l'autenticazione?**



## Sicurezza e VoIP IV

Il sistema di accounting generalmente prevede un login con userID e password o una qualsiasi altra procedura simile all'inserimento di una parola chiave. **Questo non avviene!**

Nella maggior parte dei casi le funzioni di accounting prevedono solo l'inserimento dell'userID che in quasi tutti i sistemi corrisponde al numero telefonico assegnato a quel determinato doppino. Cosa succede se, conoscendo l'ip del gatekeeper e utilizzando un determinato software che usa il protocollo h.323, apro una sessione dando come login il numero di telefono di "caio" invece del mio?



## Sicurezza e VoIP V

```
steve@osiris:~# ohphone -r -u caio -t -g IPKEEPER NUMERODITELEFONO
Gatekeeper set: nome_del_gatekeeper@IP.DEL.GATE.KEEPER
caio is calling host NUMERODITELEFONO
Command ? 0:07.246 H225CallThread:24f4680 transports.cxx(1023)
TCP Started connection to IPKEEPER:1720
(if=10.xxx.xxx.xx:1062)
Started logical channel: sending G.711-ALaw-64k{sw} <4>
Started logical channel: receiving G.711-ALaw-64k{sw} <4>
Ringing phone for "IPKEEPER"
```



## Sicurezza e VoIP VI

### **FUNZIONA!**

Per ovviare a questo problema alcuni operatori hanno adoperato un sistema di riconoscimento con userID e mac address dell'apparecchio. Soluzione facilmente aggirabile se si adoperava un mac spoofing appropriandosi e fingendosi quel determinato mac address di quel determinato telefono/computer.



## Contenuti

- Intruduzione alla telefonia VoIP
- Caratteristiche tecniche
- Sicurezza e VoIP
- **Skype vs CIA & FBI**
- Futuro del VoIP
- Tool



## Skype vs CIA & FBI

- Skype ed altri software di gestori per la telefonia VoIP non utilizzano nessuno dei protocolli elencati precedentemente, essi utilizzano protocolli proprietari che sfruttando sistemi di criptazione del traffico.  
(Voicepring di Tiscali utilizza h.323)
- Il protocollo Skype è uno dei pochi protocolli sviluppati pensando anche alla sicurezza dei dati durante il transito dei pacchetti nella rete, cosa che molti dei precedenti protocolli non curano.



## Brevi su Skype I

Skype è un software "peer to peer VoIP" sviluppato da KaZaa che permette di effettuare:

- chiamate vocali
- video chiamate
- instant messaging
- trasferimento di file

Tutto questo utilizzando Internet.



## Brevi su Skype II

Caratteristiche principali:

- basato su protocolli proprietari closed source
- chiamate "punto-punto" criptate con SSL
- alto livello di riservatezza e privacy
- alta qualità audio e video
- stabilità e facilità d'uso



## Brevi su Skype III

| Skype contro gli altri  |                                |                           |  |                                     |
|---|--------------------------------|---------------------------|--|-------------------------------------|
|   | skype                          | Net2Phone                 | MSN Messenger, ICQ, AIM, Yahoo Messenger | Altre applicazioni in standard Voip |
| Funziona con qualsiasi configurazione firewall/NAT - nulla da impostare | ✓                              | ✗                         | ✗  | ✗                                   |
| Chiamate illimitate agli utenti della stessa applicazione               | ✓                              | ✗                         | ✓  | A volte                             |
| Qualità audio superiore   | ★★★★★<br>Migliore del telefono | ★<br>Peggior del telefono | ★★★<br>Peggior del telefono              | ★★★<br>Peggior del telefono         |
| Comunicazioni sicure e criptate   | ✓                              | ✗                         | ✗  | ✗                                   |
| 100% gratis   | ✓                              | ✗                         | ✗  | A volte                             |

Schema obsoleto, manca il confronto con le video chiamate e msn di Microsoft ora funziona anche con NAT



## Brevi su Skype IV

Caratteristiche principali del protocollo SSL:

- **Privatezza del Collegamento:** Per assicurare un collegamento sicuro tra due utenti coinvolti in una comunicazione, i dati vengono protetti utilizzando algoritmi di crittografia a chiave simmetrica (DES, RC4)
- **Autenticazione:** L'autenticazione dell'identità nelle connessioni può essere eseguita usando la crittografia a chiave pubblica (RSA, DSS ). In questo modo i client sono sicuri di comunicare con il server corretto, prevenendo eventuali interposizioni. Inoltre è prevista la certificazione sia del server che del client



## Brevi su Skype V

- **Affidabilità:** Il livello di trasporto include un controllo sull'integrità del messaggio basato su un apposito MAC (Message Authentication Code) che utilizza funzioni hash sicure (SHA, MD5). In tal modo è possibile la verifica della non alterazione dei dati spediti tra client e server
- **Efficienza:** Le operazioni di crittografia tendono a essere laboriose per la CPU, particolarmente le operazioni con le chiavi pubbliche. SSL incorpora uno schema di session caching per ridurre il numero di collegamenti che hanno bisogno di essere stabiliti cercando di "alleggerire" il più possibile il traffico sulla rete

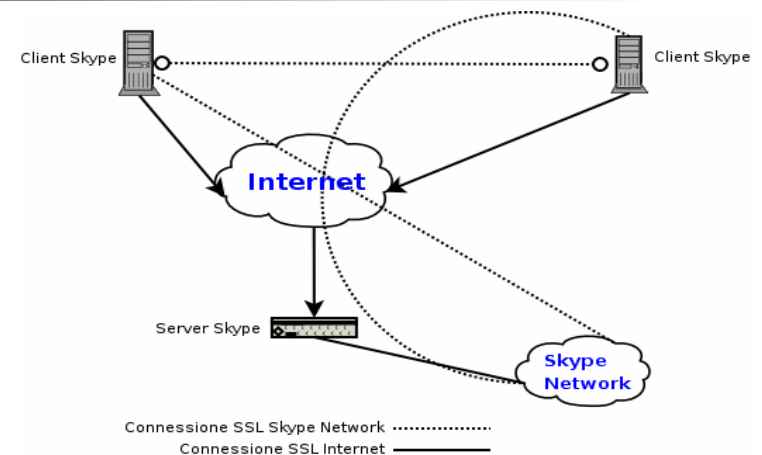


## Skype vs CIA & FBI I

- Le intercettazioni telefoniche per clienti Skype sono attualmente impossibili! Non esiste alcun metodo per "sniffare" una comunicazione che utilizza Skype questo perché il traffico è tutto criptato in SSL, dal login fino all'ultimo bit della conversazione.
- Questo crea grossi problemi ai servizi segreti di tutto il mondo, nel dettaglio CIA ed FBI hanno pubblicamente espresso il disagio, ne ha parlato il sole 24 ore in un articolo del novembre 2005 (*avranno risolto?*)



## Skype vs CIA & FBI II





## Contenuti

- Intruduzione alla telefonia VoIP
- Caratteristiche tecniche
- Sicurezza e VoIP
- Skype vs CIA & FBI
- **Futuro del VoIP**
- Tool



## Futuro del VoIP

- Entro il 2010 il VoIP avrà 100 milioni di utenti
- Microsoft entrerà nel mondo VoIP e si potrà telefonare con Office (già disponibile la prima beta del server)
- Telefonate VoIP anche dai dispositivi mobile grazie al Wi-Fi e gli hot spot
- VoIP sempre più come cellulari ma con servizi aggiuntivi



## Contenuti

- Intruduzione alla telefonia VoIP
- Caratteristiche tecniche
- Sicurezza e VoIP
- Skype vs CIA & FBI
- Futuro del VoIP
- **Tool**



## Tool

- In alcuni casi, l'intercettazione e la registrazione della telefonata può essere possibile anche in situazioni di tipologie di architetture complesse
- Esiste un software per sistemi Linux chiamato "Vomit" (voice over misconfigured internet telephones) il quale, prendendo come input il log dello sniffing creato con Tcpdump, riesce a convertire i dati sniffati in un file wave di ottima qualità audio contenente la conversazione sniffata



## Tool - Vomit

- Funziona SOLO con reti VoIP che utilizzano il protocollo H.323
- Funziona su molti router Cisco che adottano H.323
- i dati passano in chiaro sulla rete, quindi sono soggetti a sniffing



## Tool – Abel&Cain

- è un software che racchiude un insieme di tool di recovery e sniffing che, tra le tante operazioni, riesce a registrare conversazioni in chiaro in una qualsiasi LAN
- A&C incorpora le funzioni di sniffing (tcpdump) e di Vomit in un' unica applicazione



## Bibliografia

- [http://it.wikipedia.org/wiki/Voice\\_over\\_IP](http://it.wikipedia.org/wiki/Voice_over_IP)
- <http://www.openh323.org/>
- <http://www.skype.com>
- <http://www.openssl.org/>
- <http://arxiv.org/pdf/cs.NI/0412017>
- <http://vomit.xtdnet.nl/>
- <http://www.oxid.it/cain.html>

## DOMANDE???

