La Sicurezza nella comunicazione VoIP

Giuseppe Tetti

SIP e Sicurezza

- **Sicurezza : Autenticazione, Riservatezza, Integrità** ..
- Attacchi informatici tipici che possono provocare disservizio e frode
  - *Registration Hijacking*
  - *Impersonating a Server*
  - *Tampering with Message Bodies*
  - *Tearing Down Sessions*
  - *Denial of Service*
- Il protocollo SIP mette a disposizione due meccanismi per aumentare il livello di sicurezza:
  - **Meccanismi di autenticazione** del client verso il server;
  - **Riservatezza e integrità dei messaggi** scambiati tra gli elementi di rete (cifratura della segnalazione tramite *TLS – Transport Layer Security*);

Problematiche di sicurezza

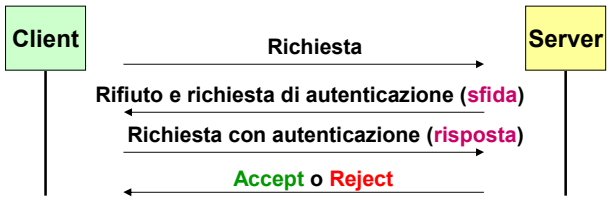
- Le problematiche di sicurezza legate ad una infrastruttura VOIP non coinvolgono solo i livelli più bassi della pila ISO/OSI ma anche il livello applicativo.
- A livello applicativo i problemi che si possono avere sono molto più preoccupanti data la complessità dei sistemi utilizzati, infatti più un sistema è complesso e più facile risulta la probabilità che il codice e gli applicativi contengano errori nei protocolli, nella loro implementazione, nella interazione e nella realizzazione pratica dei programmi.
- Considerando che il VoIP è una tecnologia nuova, la possibilità che nel prossimo futuro possa venire soggetta a problemi di sicurezza a livello applicativo è molto probabile.
- ***Occorre pensare ad un telefono IP come ad un usuale PC, aspettarsi che possa essere soggetto ad attacchi, a virus, worm ecc., ovvero dover intervenire velocemente con la applicazione di patch di sicurezza.***
- A differenza di un telefono tradizionale, un telefono IP è in pratica un'appliance con il proprio Sistema Operativo e i propri applicativi, e come tale deve essere considerato. Questo richiede anche che l'infrastruttura di rete sia progettata tenendo conto di questi fattori, e che l'infrastruttura di gestione sia in grado di intervenire in maniera proattiva e sempre meno reattiva.

VoIP – Best Practice

- Per la protezione delle infrastrutture VOIP si potrebbe pensare ad utilizzare le medesime tecniche e tecnologie impiegate per proteggere una struttura basata su IP ovvero i Firewall e le tecniche crittografiche
- Purtroppo per le caratteristiche intrinseche del VOIP l'applicazione di queste tecnologie non sempre ottiene l'effetto voluto, ritardi nella trasmissione voce, impossibilità di raggiungere o garantire i servizi più banali sono solo alcuni dei problemi che si possono avere.
- Ai fini della sicurezza vengono indicate alcune pratiche di sicurezza da adottare:
  - **separare il traffico voce su IP dal traffico dati** laddove possibile (ad esempio isolando i PBX IP e i server VOIP su VLAN dedicate) facendo suo di server DHCP separati
  - **Fare uso di switch in luogo di hub** per usufruire di funzionalità più elevate nonché di caratteristiche di sicurezza intrinseche.
  - **Accertarsi che tutti gli apparecchi telefonici siano dotati di password** di accesso e che le password non siano quelle fornite dalla fabbrica (o di default).
  - **Fare uso di Firewall progettati per il traffico VOIP**, i filtri stateful possono tracciare lo stato delle connessioni respingendo i pacchetti che non fanno parte della chiamata originaria
  - **Utilizzare tecniche di cifratura** della comunicazione all'esterno della rete aziendale come all'interno tenendo in considerazione aspetti indotti dall'uso di tali tecnologie di protezione e prevenendo con una opportuna progettazione i possibili disagi
  - Utilizzare tecniche di cifratura IPSEC o Secure Shell per tutta la gestione remota, se possibile sarebbe opportuno evitare la gestione remota e realizzare l'accesso all'IP PBX da un sistema trusted.

Autenticazione

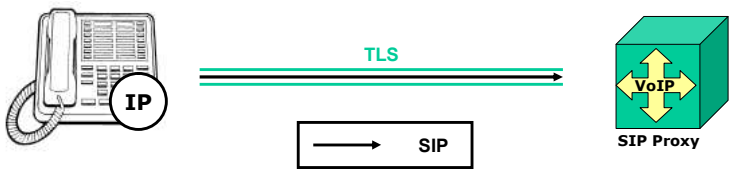
- L'autenticazione **consente ad un Server di verificare l'autenticità di un Client** che sottopone una certa richiesta di servizio.
- In SIP (RFC 3261) si utilizza il "***Digest Authentication Scheme***";



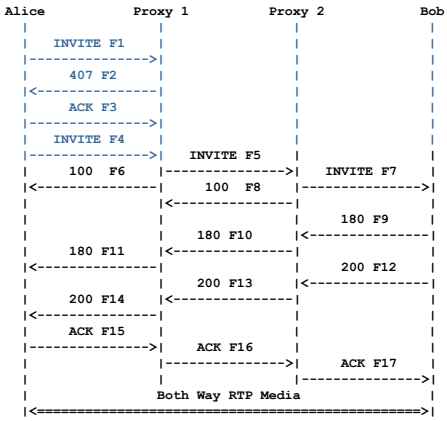
- SIP utilizza meccanismi di autenticazione basati sul paradigma *challenge-response* : il Server "sfida" il Client a "dimostrare" la propria *identità*
- Se il Client vince la sfida la richiesta di servizio viene portata avanti dal Server, in caso contrario il Server rilascia la transazione.
- Le *response* utilizzate per richiedere l'autenticazione sono:
  - Risposta "**401 – Unauthorized** " per i Server di tipo UA
  - Risposta "**407 – Proxy authentication required**" per i server di tipo Proxy

Cifratura dei messaggi

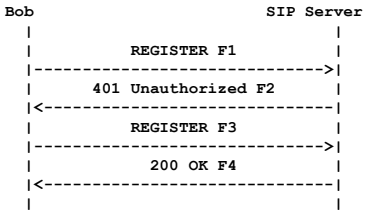
- Per garantire la riservatezza e l'integrità della segnalazione scambiata tra UA il protocollo SIP si appoggia ad altri strumenti:
  - **TLS (Transaction Layer Security) – RFC 2246**
    - Derivato da SSL 3.0, è un protocollo di livello 5 (*Session Layer*) in grado di garantire:
      - **Confidenzialità** dei messaggi (cifratura simmetrica con chiave segreta DES, 3DES e scambio del segreto con Diffie-Helman o RSA);
      - **Autenticazione** (opzionale con utilizzo di Certificati);
      - **Integrità** (con funzioni di hash MD5 e SHA-1)
    - *Richiede un trasporto TCP*
  - **IPSEC (IP Security)**
    - Framework in grado di gestire tecniche e protocolli in grado di garantire alti livelli di sicurezza su reti IP;
    - Offre anche meccanismo di gestione delle chiavi (Internet Key Exhange);
    - Implementazione a maggior impatto in rete;



Autenticazione

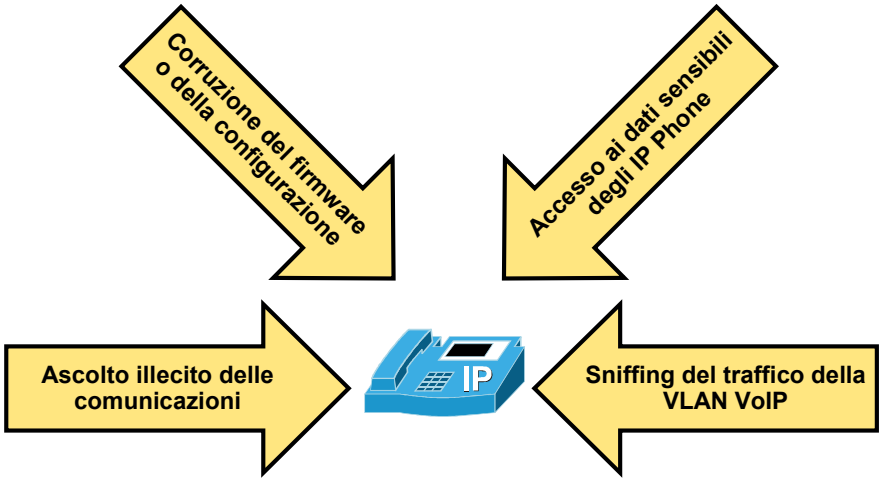


Autenticazione in chiamata

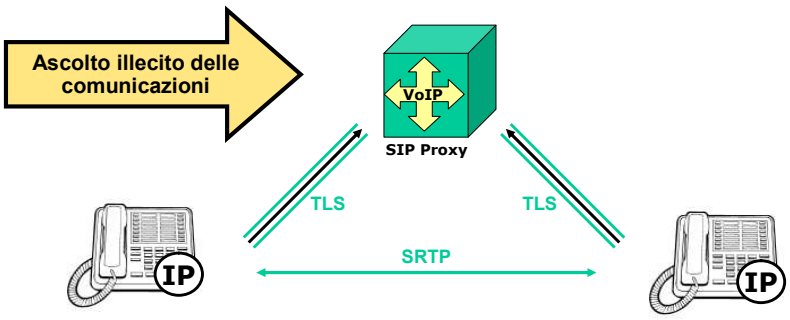


Autenticazione in registrazione

Minacce tipiche

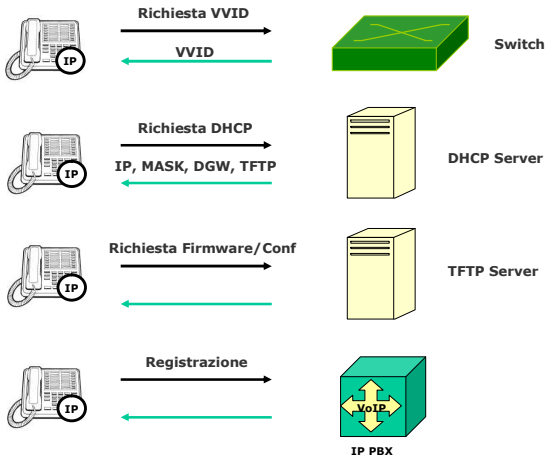


Secure Media Transfer

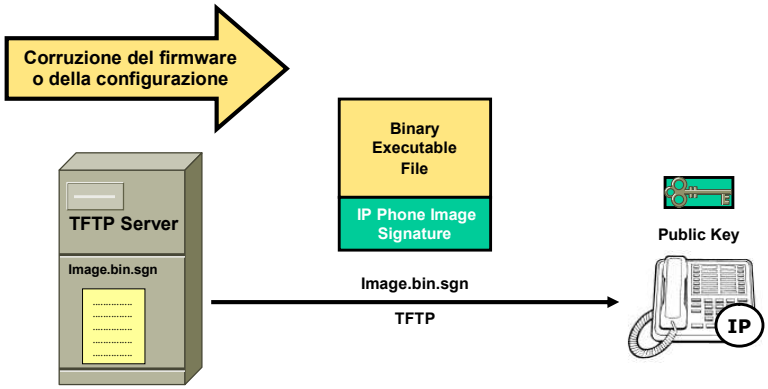


I pacchetti RTP sono cifrati utilizzando lo standard RFC 3711 (**Secure RTP**)

Accesso in rete di un IP-Phone

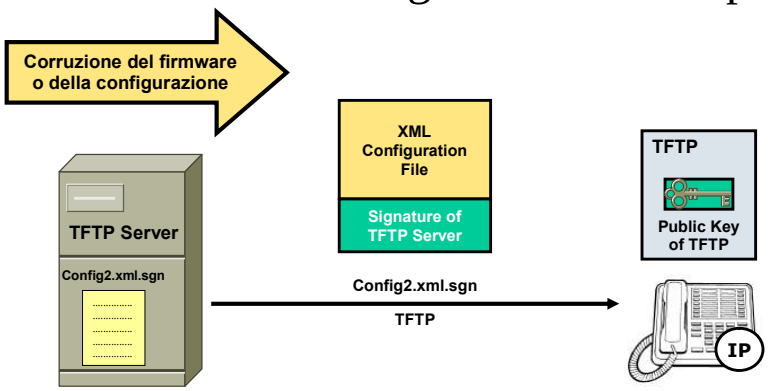


IP Phone Image Checkup



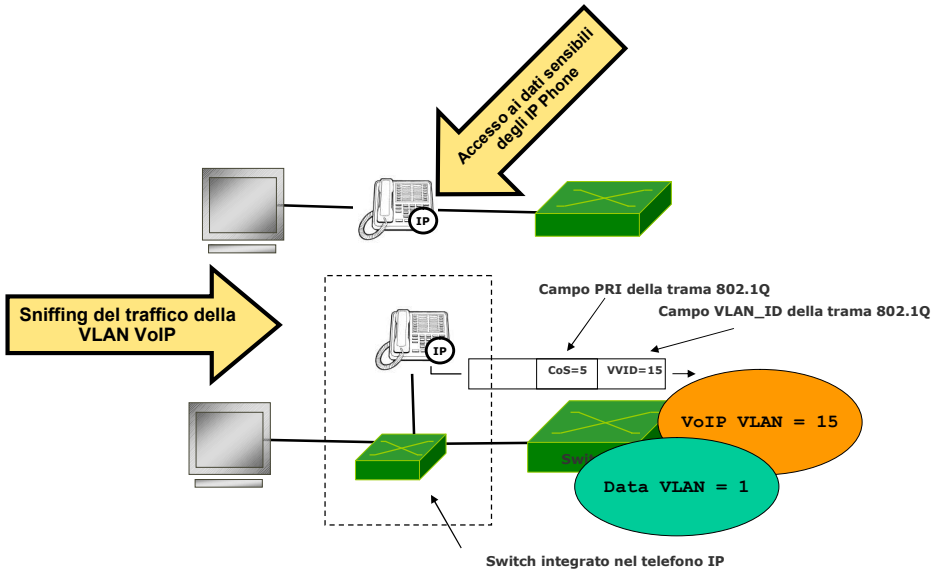
– I file contenenti il firmware dei telefoni posseggono una firma digitale ottenuta utilizzando la chiave privata del costruttore
– Il telefono IP verifica la firma utilizzando la chiave pubblica del costruttore.

IP Phone Configuration Checkup

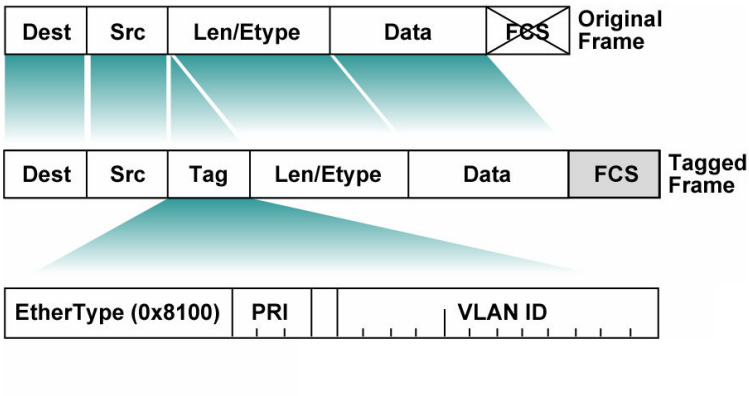


– I file di configurazione vengono firmati dal server TFTP
– Prima di utilizzare la configurazione i telefoni IP verificano la validità della firma.

Accesso in rete di un IP-Phone

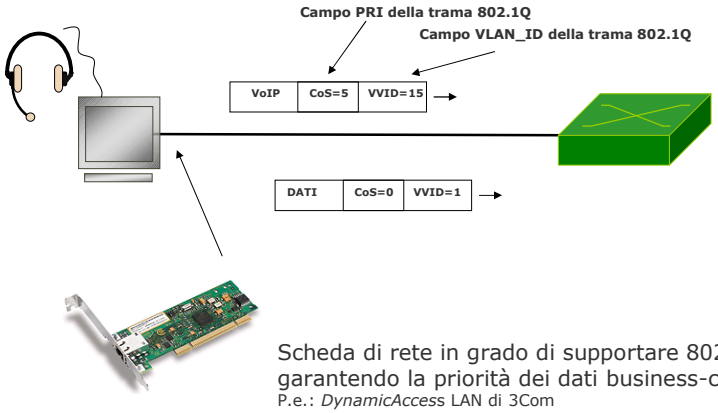


IEEE 802.1Q



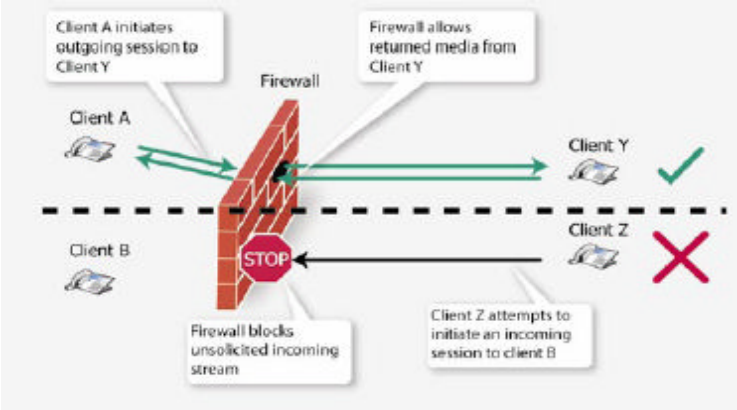
– Le frame sono etichettate con l'identificativo numerico della VLAN di appartenenza.

Accesso in rete di un Soft-Phone

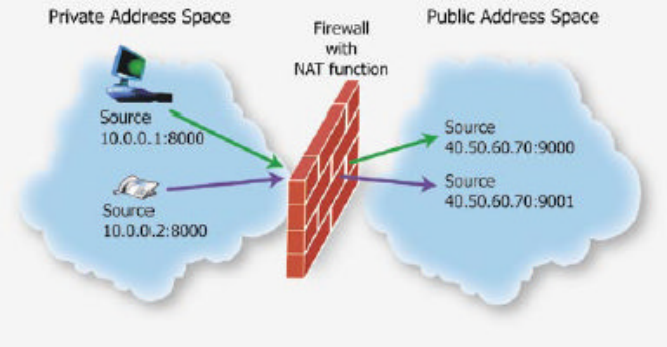


Scheda di rete in grado di supportare 802.1p/Q garantendo la priorità dei dati business-critical.
P.e.: *DynamicAccess* LAN di 3Com

Il problema del Firewall

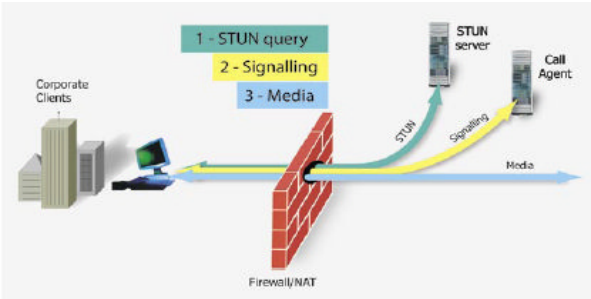


NAT Traversal

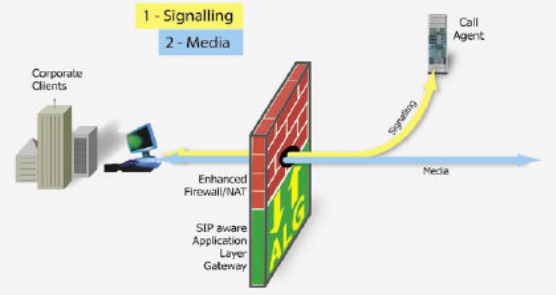


- STUN
- TURN
- Universal P&P
- ALG
- Tunnel
- Configurazioni Manuali

STUN

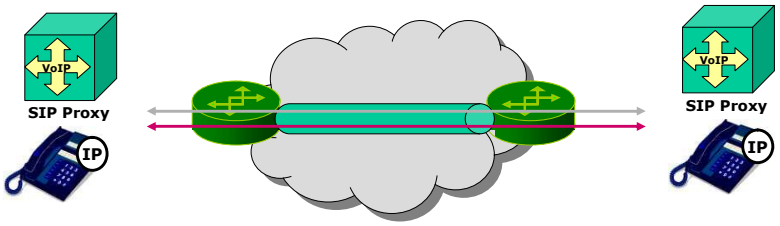


Application Level Gateway



Tracciato

Tunnel



Segnalazione

Streaming RTP

Tunnel: GRE, IPSec

Link Utili

- **VoIP Security Alliance (http://www.voipsa.org)**
- Security Focus (http://www.securityfocus.com/)
- SANS Instituite (http://www.sans.org/)
- http://sicurezza.html.it/
- http://www.blogvoip.it/
- http://www.hackingvoip.com/sec_tools.html

VoIP Sniffing Tools

- AuthTool - Tool that attempts to determine the password of a user by analyzing SIP traffic.
- Cain & Abel - Multi-purpose tool with the capability to reconstruct RTP media calls.
- Etherpeek - general purpose VoIP and general ethernet sniffer.
- NetDude - A framework for inspection, analysis and manipulation of tcpdump trace files.
- Oreka - Oreka is a modular and cross-platform system for recording and retrieval of audio streams.
- PSIPDump - psipdump is a tool for dumping SIP sessions (+RTP traffic, if available) from pcap to disk in a fashion similar to "tcpdump -w".
- SIPomatic - SIP listener that's part of LinPhone
- SIPv6 Analyzer - An Analyzer for SIP and IPv6.
- VoiPong - VoIPong is a utility which detects all Voice Over IP calls on a pipeline, and for those which are G711 encoded, dumps actual conversation to separate wave files. It supports SIP, H323, Cisco's Skinny Client Protocol, RTP and RTCP.
- VoIPong ISO Bootable - Bootable "Live-CD" disc version of VoIPong.
- VOMIT - The vomit utility converts a Cisco IP phone conversation into a wave file that can be played with ordinary sound players.
- Wireshark - Formerly Ethereal, the premier multi-platform network traffic analyzer.
- WIST - Web Interface for SIP Trace - a PHP Web Interface that permits you to connect on a remote host/port and capture/filter a SIP dialog

VoIP Scanning and Enumeration Tools

- enumIAX - An IAX2 (Asterisk) login enumerator using REGREQ messages.
- iWar - IAX2 protocol Wardialer
- Nessus - The premier free network vulnerability scanner.
- nmap - the premier open source network port scanner.
- SIP Forum Test Framework (SFTF) - The SIP Forum Test Framework (SFTF) was created to allow SIP device vendors to test their devices for common errors.
- SIP-Scan - A fast SIP network scanner
- SIPcrack - SIPcrack is a SIP protocol login cracker. It contains 2 programs, SIPdump to sniff SIP logins over the network and SIPcrack to bruteforce the passwords of the sniffed login.
- SIPSCAN - SIPSCAN is a SIP username enumerator that uses INVITE, REGISTER, and OPTIONS methods.
- SiVuS - A SIP Vulnerability Scanner.
- SMAP - SIP Stack Fingerprinting Scanner
- VLANping - VLANPing is a network pinging utility that can work with a VLAN tag.
- VoIPAudit - VoIP specific scanning and vulnerability scanner.

VoIP Packet Creation and Flooding Tools

- IAXFlooder - A packet flooder that creates IAX packets.
- INVITE Flooder - Send a flurry of SIP INVITE messages to a phone or proxy.
- kphone-ddos - Using KPhone for flooding attacks with spoofed SIP packets
- RTP Flooder - Creates "well formed" RTP Packets that can flood a phone or proxy.
- Scapy - Scapy is a powerful interactive packet manipulation program. It can easily handle most classical tasks like scanning, tracerouting, probing, unit tests, attacks or network discovery.
- Seagull - a multi-protocol traffic generator especially targeted towards IMS.
- SIPBomber - SIPBomber is sip-protocol testing tool for Linux.
- SIPNess - SIPness Messenger is a SIP testing tool which is used for testing SIP applications.
- SIPp - SIPp is a free Open Source test tool / traffic generator for the SIP protocol.
- SIPsak - SIP swiss army knife.

VoIP Fuzzing Tools

- Asteroid - this is a set of malformed SIP methods (INVITE, CANCEL, BYE, etc.) that can be crafted to send to any phone or proxy.
- Codenomicon VoIP Fuzzers - Commercial versions of the free PROTOS toolset
- Fuzzy Packet - Fuzzy packet is a tool to manipulate messages through the injection, capturing, receiving or sending of packets generated over a network. Can fuzz RTP and includes built-in ARP poisoner.
- Mu Security VoIP Fuzzing Platform - Fuzzing platform handling SIP, H.323 and MGCP protocols.
- ohrwurm - ohrwurm is a small and simple RTP fuzzer.
- PROTOS H.323 Fuzzer - a java tool that sends a set of malformed H.323 messages designed by the University of OULU in Finland.
- PROTOS SIP Fuzzer - a java tool that sends a set of malformed SIP messages designed by the University of OULU in Finland.
- SIP Forum Test Framework (SFTF) - SFTF was created to allow SIP device vendors to test their devices for common errors. And as a result of these tests improve the interoperability of the devices on the market in general.
- Sip-Proxy - Acts as a proxy between a VoIP UserAgent and a VoIP PBX. Exchanged SIP messages pass through the application and can be recorded, manipulated, or fuzzed.
- Spirent ThreatEx - a commercial protocol fuzzer and ribustness tester.

VoIP Signaling Manipulation Tools

- BYE Teardown - This tool attempts to disconnect an active VoIP conversation by spoofing the SIP BYE message from the receiving party.
- Check Sync Phone Rebooter - Transmits a special NOTIFY SIP message which will reboot certain phones.
- RedirectPoison - this tool works in a SIP signaling environment, to monitor for an INVITE request and respond with a SIP redirect response, causing the issuing system to direct a new INVITE to another location.
- Registration Adder - this tool attempts to bind another SIP address to the target, effectively making a phone call ring in two places (the legitimate user's desk and the attacker's)
- Registration Eraser - this tool will effectively cause a denial of service by sending a spoofed SIP REGISTER message to convince the proxy that a phone/user is unavailable.
- Registration Hijacker - this tool tries to spoof SIP REGISTER messages in order to cause all incoming calls to be rerouted to the attacker.
- SIP-Kill - Sniff for SIP-INVITEs and tear down the call.
- SIP-Proxy-Kill - Tears down a SIP-Session at the last proxy before the opposite endpoint in the signaling path.
- SIP-RedirectRTP - Manipulate SDP headers so that RTP packets are redirected to an RTP-proxy.
- SipRogue - a multifunctional SIP proxy that can be inserted between two talking parties

VoIP Media Manipulation Tools

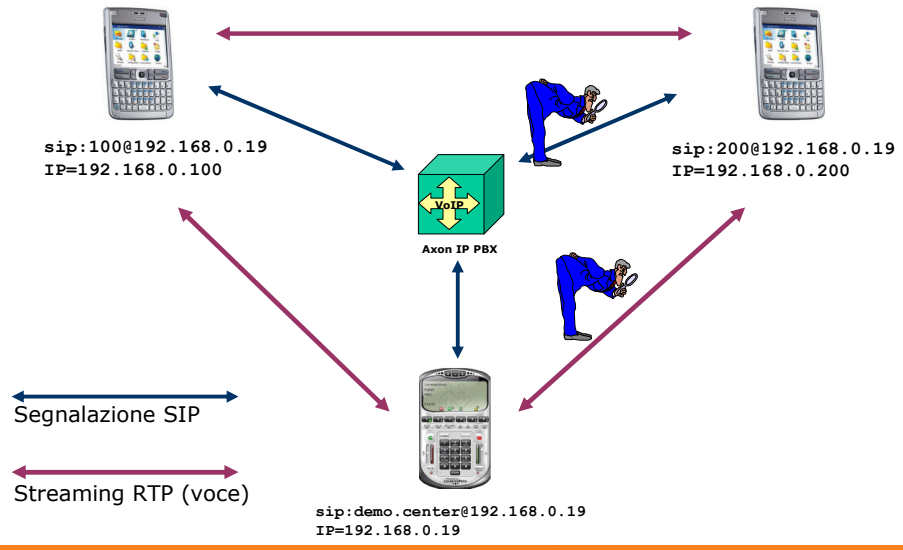
- RTP InsertSound - this tool takes the contents of a .wav or tcpdump format file and inserts the sound into an active conversation.
- RTP MixSound - this tool takes the contents of a .wav or tcpdump format file and mixes the sound into an active conversation.
- RTPProxy - Wait for incoming RTP packets and send them to wanted (signaled by a tiny protocol) destination.

- Altro
  - Yersinia (http://sourceforge.net/projects/yersinia)

Simulazioni di attacchi

- Intercettazione di una chiamata con cattura del traffico vocale e successiva riproduzione.
- Scanning di una rete VoIP e analisi dei rischi.
- Attacchi DoS con messaggi SIP pirata:
  - REGISTER
  - INVITE
  - BYE
- Strumenti utilizzati:
  - Ethereal, Wireshark, Cain
  - SiVus

Nostro obiettivo



Grazie per la cortese attenzione

giuseppe.tetti@ncp-italy.com

NCP
Networking Competence Provider
IL VALORE DELLA CONOSCENZA.