Sicurezza del Voice over IP

Giuseppe Paternò
Gennaio 2005

In questi mesi stiamo assistendo allo sviluppo della telefonia su IP, detta Voice over IP (VoIP). Questa tecnologia permette di convergere la telefonia su una rete dati IP esistente, consentendo l'abbassamento dei costi delle telefonate tra sedi remote, i costi di interurbane (detto *toll-bypass*), di mantenimento di due infrastrutture (fonia/dati) e di cablaggio. Oltre a tanti vantaggi si pone come sempre il problema della sicurezza, tema che, a mio avviso, non sempre viene affrontato nella giusta maniera da i produttori. Quali sono i problemi e come si fa quindi a proteggere la propria infrastruttura di voce su IP ?

Prima di affrontare l'argomento sicurezza, ripassiamo brevemente insieme quali sono le componenti di una infrastruttura e gli standard esistenti. Gli elementi funzionali dell'infrastruttura sono sostanzialmente tre, anche se per ognuna delle funzioni possono esserci piu' sistemi per ridondanza o per complessita' dell'infrastruttura in essere.

- **Call Processors/Controllers**. E' un software presente su di un sistema (proprietario o un sistema Unix/Windows) che si occupa di fare il setup e il monitor delle chiamante. Mantiene inoltre il piano di numerazione, o "dial plan", effettua traslazioni della numerazione (es: un numero fittizio di help desk), e si occupa –piu' in generale- della segnalazione tra i terminali e i media/signaling gateway. In certi casi viene anche chiamato softswitch, call manager o gatekeeper (a secondo delle implementazioni o dei prodotti)
- **Media/Signaling Gateway**. In generale, i gateway si occupano di interfacciarsi verso la rete telefonica "tradizionale", convertendo il segnale analogico in digitale o trasformando il segnale digitale (ISDN o trunk E1) in fonia su IP. Solitamente il Media Gateway (MG) e il Signaling Gateway (SG) risiedono sulla stessa macchina, tuttavia svolgono due compiti diversi. Il primo si occupa di traslare (attraverso CODEC) il segnale vocale proveniente dalla rete telefonica PSTN in codifica digitale compatibile con il terminale remoto IP, ad esempio tra il PCM (Pulse Code Modulation) della rete PSTN e il codec G.723 presente sul telefono VoIP. Il Signaling Gateway si occupa di traslare la segnalazione telefonica proveniente dalla rete PSTN nella segnalazione compatibile con il proprio Call Processor (es: H.323 o SIP). Personalmente ho avuto difficolta' a capire il concetto di *segnalazione*: ho sempre pensato che agganciare/sganciare la cornetta e che il numero di telefono viaggiasse "in band", senza pensare che potesse "prendere altre strade". In realta' queste operazioni, al di la' della linea di casa, viaggiano in un canale separato, il canale di segnalazione appunto.
- **User Terminal (or Subscriber Terminal)**. Il vero e proprio telefono con il quale l'utente interagisce. Un telefono IP puo' essere di due tipi, ovvero hardware o software (softphone), quest'ultimo si installa come una normale applicazione PC.

Queste funzionalita' si traducono poi in implementazioni, alcune di esse diventate standard. Esistono tre standard principali, ovvero *H.323*, il *Session Initiation Protocol (SIP)* ed il *Media Gateway Control Protocol (MGCP)*. Il MGCP e' poco usato, vediamo pertanto i protocolli H.323. ed il piu' recente SIP.

H.323 e' il piu' usato dei protocolli di telefonia su IP, in quanto e' stato il primo vero protocollo usabile. Standardizzato da ITU (International Telecommunication Union, chi fa gli standard per la telefonia), concettualmente e' di derivazione telefonica ed in particolare prende spunto dal protocollo ISDN. Esistono quattro elementi, il primo e' il *terminale*, che svolge la funzionalita' del telefono utente. Il secondo e' il *gatekeeper*, che svolge la funzoone di Call Processor/Controller; poi il *gateway*, che svolge la funzionalita' di media e signaling gateway e, per ultimo, il *Multipoint Control Unit (MCU)* che permette la funzionalita' di confernza

SIP invece e' piu' recente ed e' invece di derivazione piu' "Internet like", non a caso infatti e' standardizzato da IETF (Intenet Engineering Task Force). Il protocollo e' concettualmente simile ad HTTP e prevede due macro aree: gli *User Agent* ed i *Network Server*. I primi possono dividersi ulteriormente in due, ovvero gli *User Agent Client (UAC)* e gli *User Agent Server (UAS)*. UAC e' usato per iniziare la chiamata, mentre UAS rimane in ascolto per ricevere le chiamate. UAS e UAC tipicamente risiedono nello stesso device, ad esempio un telefono IP. Esistono invece tre tipi di Network Servers, il *Registration Server* e' il piu' importante: mantiene un repository degli utenti locali e della loro posizione (IP address) e si occupa di autorizzare l'accesso del client (registration requests). Il *Proxy Server* funge da proxy per il protocollo SIP, ruotandone la richiesta verso il server di destinazione corretto o verso un altro proxy server. Ad esempio, se si inizia una chiamata vocale, il proxy sever prende l'indirizzo di destinazione (il numero del destinatario) e lo passa al registration server che ha in carico l'utente di destinazione. Quando il registration server ricevera' la richiesta del proxy, girera' la richiesta al terminale finale che squillera'. Solitamente il proxy server viene utilizzato quando le richieste SIP devono attraversare un firewall. Il *Redirect Server* e' simile al proxy server, ma invece di ruotare la richiesta al SIP server di destinazione (come fa il proxy), invia un "redirect" al chiamante: in questo modo sara' il telefono IP chiamante a contattare direttamente il server SIP di destinazione.

Abbiamo detto all'inzio che il l'adozione dl traffico voce su IP e' sostanzialmente dovuto nell'ottica del ridurre i costi della telefonia, convergendo il sistema telefonico nel sistema dati IP. Come per tutti i protocolli IP, anche il VoIP pero' non e' esente dalle vulnerabilita' tipiche di IP, con qualche differenza. Vediamo quali tipi di attacchi sono possibili:

Lo sniffing puo' rivelare importanti informazioni, credenziali dell'utente (username e password) e, di conseguenza, la possibilita' di impersonare qualcun'altro. E' possibile anche carpire preziose informazioni sul proprio sistema VoIP ed eventualmente usarlo come ponte per attaccare altri sistemi. Esistono tool di sniffing che possono decodificare il traffico SIP e H.323, quindi la segnalazione (numeri di telefono, identita', ...), ma anche flussi RTSP (quindi ascoltare le conversazioni).

Denial of Service (DoS). Come per qualsiasi rete IP, anche il VoIP e' suscettibile ad attacchi di tipo DoS, ad esempio mandando pacchetti falsi in rete al fine di saturare le componenti VoIP (Call Processors e Media/Signaling Gateways).

Trafffic Flow Disruption. Un DoS evoluto, mirato a saturare la banda VoIP e quindi non permettere la comunicazione vocale tra gli utenti.

Come possiamo fare quindi per proteggere la nostra nuova infrastruttura di fonia su IP ? Ecco qualche pratico consiglio:

Usate apparati differenti o una VLAN dedicata. E' bene separare fisicamente il traffico voce da quello dati, creando una rete IP dedicata, sia attraverso apparati diversi o attraverso l'uso delle VLAN. Oltre ad avere un vantaggio da un punto di vista della sicurezza, si avra' anche un vantaggio relativo alla riduzione della latenza di rete, in quanto si tratta di una rete separata e nessun altro traffico verra' veicolato sulla VLAN.

Usate indirizzi non ruotati. Sebbene ormai e' abbastanza diffuso l'uso delle reti private, e' bene non usare indirizzi IP pubblici per la propria rete VoIP, ma indirizzi coerenti con l'RFC1918, ovvero le classi 10.0.0.0/8, 172.16.0.0/12 o 192.168.0.0/24. Per i "pochi fortunati" che hanno a disposizione IP pubblici in abbondanza (universita', grosse aziende) e' bene comunque differenziare il traffico IP voce.

Separate il traffico voce da quello dati con un firewall. Spesso e' necessario interconnettere le reti VoIP da quella dati IP, ad esempio per l'amministrazione dei server o, piu' semplicemente, permettere l'aggiornamento dei server VoIP tramite Internet (Windows Update, ...). E' bene pertanto usare un firewall di tipo stateful inspection per separare le due reti, permettendo solo il traffico necessario. Da un punto di vista della sicurezza, il VoIP apre numerose porte rendendo difficile la gestione delle policy (in tabella 1 le porte piu' usate), ma alcuni firewall piu' evoluti permettono di ispezionare i protocolli VoIP e aprire le porte di conseguenza. Alcuni terminali e media gateway, che aprono la connessione voce RTSP, permettono di limitare le porte UDP da aprire: per quanto possibile e' bene usare questa opzione per ottenere un miglior controllo sul firewall e, ovviamente, una migliore configurabilita'.

Table 1 - Porte VoIP

Servizio	Porta
Skinny	TCP 2000-2002
MGCP	UDP 2427
H.323 RAS	TCP 1719
H.323 H.225	TCP 1720
H.323 H.245	TCP 11000-11999
CTIM (CTI Manager)	TCP 8003
CTI/QBE	TCP 2478
SCCP	TCP 3224
SIP	TCP/UDP 5060

Proteggete i telefoni VoIP. Abbiamo accennato in precedenza che esistono due tipi di telefoni VoIP: hardware, ovvero un vero e proprio telefono dotato di scheda di rete, o software, un programma da installare su un PC.

- Se si adotta un telefono software (softphone), e' bene dotare il PC di due schede di rete, una interconnessa sulla rete dati ed una interconnessa alla rete VoIP. Visto che sistema e' potenzialmente vulnerabile, e' importante quindi proteggerlo adeguatamente installando un personal firewall e disablitando il routing tra le interfacce di rete.
- Se si adottano i telefoni IP hardware, e' bene non far visualizzare sul display il proprio IP address o username associato al telefono (per i protocolli che permettono l'autenticazione). Molti telefoni IP hanno anche la possibilita' di collegare un PC con un apposita porta, svolgendo il ruolo di hub. Questi ultimi sono in grado di usare le VLAN, in modo da dividere i dati dalla fonia, assegnando al PC una determinata VLAN. In questo caso e' bene impostare la porta dello switch in modo da propagare solo ed esclusivamente le VLAN del VoIP e quella in cui deve essere interconnesso il PC. Se non ci fosse questa limitazione, un eventuale attaccante potrebbe togliere il telefono hardware e ed inserire un PC (es: Linux) che puo' analizzare le VLAN e inserirsi in una VLAN "interessante", quale ad esempio quella di amministrazione.

Autenticate i client. Alcuni protocolli VoIP, ad esempio il SIP, permette di autenticare tramite username e password il telefono o l'utente. Inoltre e' legare un telefono (o interno) ad un determinato IP o MAC address. Per quanto possibile e' bene usare queste funzionalita: per maggiori informazioni, guardate la documentazione fornita con il vostro call manager/gatekeeper.

Fate l'hardening dei sistemi. Alcuni centralini telefonici hanno apparati hardware dedicati e con un sistema operativo proprietario. Altri pero' sono normali applicativi eseguiti all'interno di un sistema Unix o Windows. In quest'ultimo caso e' bene proteggere i sistemi eseguendo un hardening del sistema e togliendo i servizi non necessari. E' bene trattare un sistema VoIP, sia che si tratti di Call Processors che di Media/Signaling Gateways, come se fosse un sistema sensibile di DMZ

Usate protocolli criptati per il management degli apparati VoIP, ad esempio attraverso SSH o HTTPS. In caso si tratti di protocolli non criptati si potrebbe usare IPSec.

Proteggete le connessioni VoIP sulla WAN. Se non abbiamo linee dedicate verso sedi remote o se abbiamo una interconnessione con altri sistemi VoIP (ad esempio i nostri partner), e' bene usare unaVPN per criptare il traffico voce al fine di salvaguardare la nostra privacy.

Fate cambiare spesso la password della casella vocale. Molti centralini VoIP hanno la funzionalita' di segreteria telefonica. Molto spesso pero' ci si dimentica di cambiare la password di accesso alla propria casella vocale, lasciando la password di default (es: il "classico" 1234). In questo modo chiunque abbia accesso al vostro centralino VoIP e' in grado di ascoltare i messaggi vocali e carpire preziose informazioni relative alla vostra azienda, ad esempio per fare "social engineering".

Proteggete i telefoni Wi-Fi. Si stanno diffondendo i telefoni VoIP che sfruttano la tecnologia wireless 802.11b/g (Wi-Fi). Abbiamo affrontato in passatoi problemi di sicurezza che il Wi-Fi ha intrinsecamente, principalmente dovuti al mezzo trasmissivo (Si consiglia la lettura del libro "Sicurezza nelle Wireless LAN" sul sito *http://www.gpaterno.com*). Una connessione VoIP su Wi-Fi e' ovviamente ancora piu' sensibile. E' bene quindi dedicare una rete Wi-Fi apposita, con un SSID distinto, usando Access Point dedicati oppure utilizzando la possibilita' di gestire piu' SSID, propri di alcuni Access Point (che associano SSID a VLAN). E' necessario impostare comunque la crittografia WEP, filtri MAC e, quando i telefoni VoIP lo permettono, l'autenticazione 802.1x.