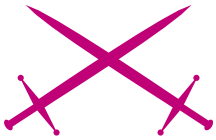

Sicurezza delle soluzioni VoIP enterprise

Marco Misitano, Antonio Mauro

Grado di difficoltà

Se correttamente implementata su una rete con un buon livello di sicurezza, una soluzione IPT può essere sicura quanto una soluzione di telefonia tradizionale.

Consapevolmente o meno, tutti siamo utilizzatori della Voice over IP (VoIP). Molteplici sono i motivi per cui la Voce su IP (VoIP) attira sempre più utilizzatori, ed altrettante sono le implicazioni di sicurezza da conoscere.

Differenza fra VoIP e IPT

Con l'acronimo VoIP – che sta per Voice over IP - s'intende la tecnica con la quale il suono della voce viene campionato ed inoltrato su una rete a pacchetto. In questo ambito rientrano tutti i protocolli di segnalazione, di trasporto della voce, del campionamento, codifica e successiva decodifica. Con il termine Telefonia su IP – occasionalmente abbreviato con l'acronimo IPT - s'intende invece una soluzione che, basandosi sulle tecnologie che fanno capo alla VoIP, permette di telefonare. Una soluzione di Telefonia su IP è comprensiva dei terminali (telefoni), server di gestione delle chiamate (*call manager*) e gateway verso la rete telefonica tradizionale.

Di quale ambito ci occupiamo

Sono diversi gli ambiti che la telefonia su IP può avere. La soluzione può essere implementata aziendalmente in un singolo ufficio come anche in diversi uffici distanti fra loro. Può anche essere utilizzata da utenti singoli attraverso internet tramite servizi gratuiti o a pagamento. Parlando di VoIP e di telefonia su IP s'intende che il protocollo IP è usato come base di trasporto; questo non per forza vuol dire che si utilizza internet. L'ambito preso in considerazione è prevalentemente quello aziendale, e molti degli scenari analizzati si riferiscono ad una rete locale, anche se molte considerazioni sono di carattere generale.

Rete telefonica tradizionale

Nella telefonia tradizionale, il terminale di sinistra è collegato al centralino A, il quale

Dall'articolo imparerai...

- Principi di funzionamento della VoIP,
- Considerazioni sulle tecniche di attacco,
- Linee guida di design.

Cosa dovresti sapere...

- Principi di funzionamento delle reti,
- Modello ISO/OSI,
- Principi di IDS/IPS e tecniche di attacco.

è collegato alla rete telefonica. Lo stesso accade per il terminale di destra con il centralino B. Al momento in cui il telefono di sinistra alza la cornetta il centralino A gli farà avere il segnale di libero. Si stabilisce in questo caso il segmento 1 della chiamata. Componendo un numero, il centralino A si farà carico di instradare la telefonata sulla rete telefonica individuando il centralino B, al quale è collegato il telefono di destra. Si stabilisce in questo modo il segmento 2 della telefonata. Il centralino B farà suonare il telefono di destra ed al momento in cui verrà sollevata la cornetta sarà stabilito anche il segmento 3 della chiamata ed i tre segmenti saranno a questo punto messi in comunicazione. Lo stesso accade al telefono di sinistra e quello di destra. È da notare che il centralino A non ha nessuna conoscenza dei telefoni gestiti dal B, e viceversa.

Analogia con le reti a pacchetto

Mantenendo il principio di funzionamento appena descritto per la telefonia tradizionale, immaginiamo di sostituire i centralini con dei dispositivi di instradamento del traffico come i router, e la nuvola della rete telefonica con una rete IP, ecco spiegato a grandi linee il funzionamento di una soluzione di telefonia su IP.

I benefici principali che rendono questa soluzione sempre più popolare sono legati all'immediato risparmio. In una rete IP non c'è il vincolo del costo a tempo e questo rende le chiamate più economiche. Allo stesso tempo, in un'azienda, il fatto di non dover avere due reti fisiche separate, quella IP e quella telefonica incide positivamente sui costi. Sullo stesso cavo – quello della rete IP – è possibile far transitare anche voce oltre che dati, con una buona economia anche operazionale.

Più da vicino

Descritta l'idea ed in linee generali i principi di funzionamento di una soluzione aziendale di IPT, analizziamo più in dettaglio sia i moduli che costituiscono una soluzione IPT, sia le fasi di costruzione di una telefonata IP.

Al momento in cui il telefono si accende si è nella fase di booting (1) in cui il telefono individua il server delle configurazioni, che gli fornirà una configurazione (2) ed eventualmente anche un'immagine del software. Dopodiché

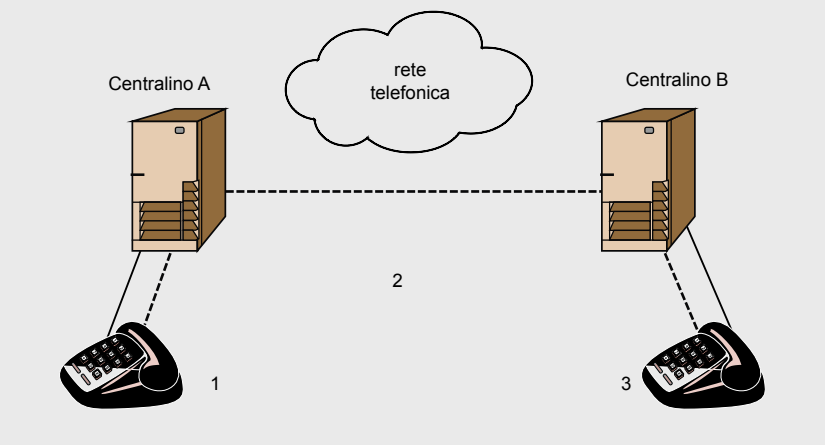

Figura 1: *Principi di funzionamento della rete telefonica tradizionale*

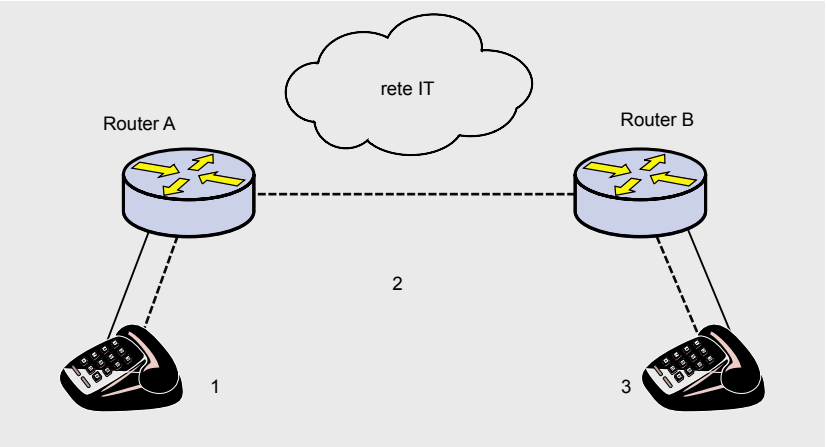

Figura 2: *Analogia con le reti a pacchetto*

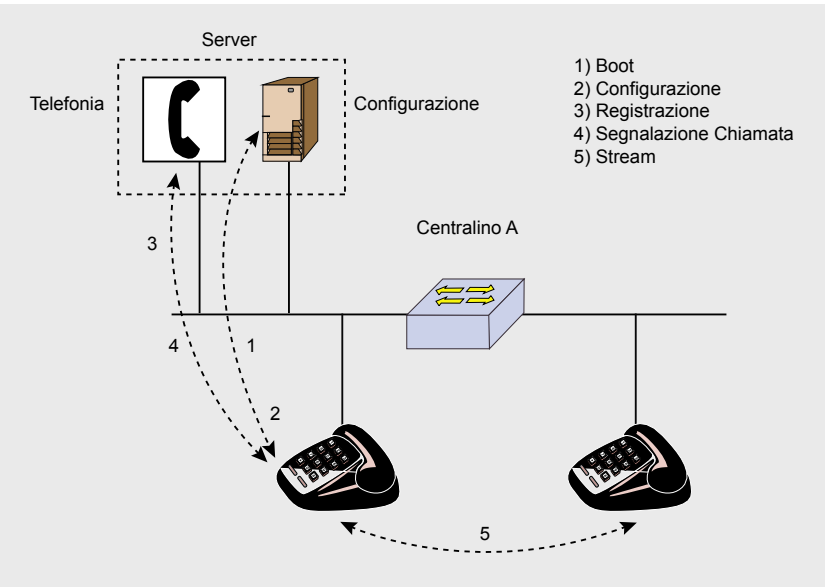

Figura 3: *Dettaglio della costruzione di una chiamata Voip*

il telefono effettuerà la propria registrazione (3) verso il server della telefonia. Il server di telefonia e quello delle configurazioni possono anche essere la stessa macchina. A questo punto il telefono è pronto per essere usato. Dal momento in cui si solleva la cornetta (4) e si compone il numero, il server di telefonia negozia l'instradamento verso il terminale richiesto. I telefoni (in basso nel diagramma) saranno informati su come stabilire (5) il flusso della telefonata direttamente fra loro.

La fase di Booting

Al telefono (a sinistra) è assegnata una VLAN, fatto questo invia una richiesta DHCP, che passa attraverso le fasi di *discover, offer, request,* e *configuration*. Alla fine del processo DHCP il telefono avrá indirizzo IP ed altri dati relativi alla sua configurazione IP, compreso l'indirizzo IP del server a cui richiedere la configurazione. La fase di DHCP Discover è un broadcast.

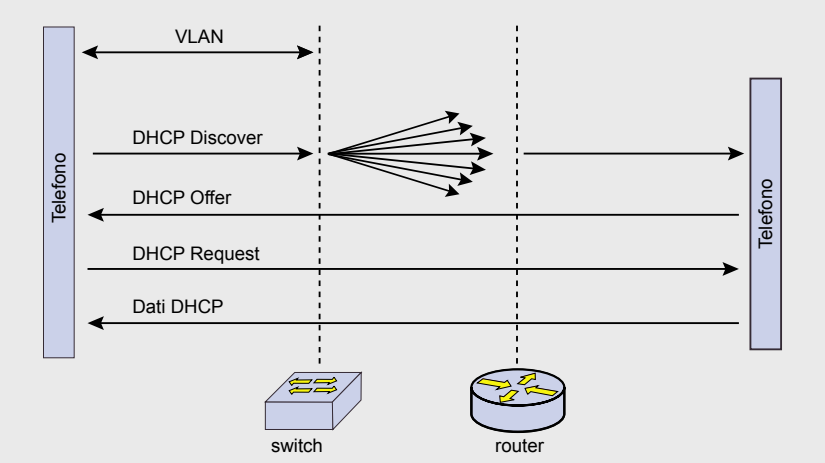

Figura 4: *Dettaglio della fase di boot*

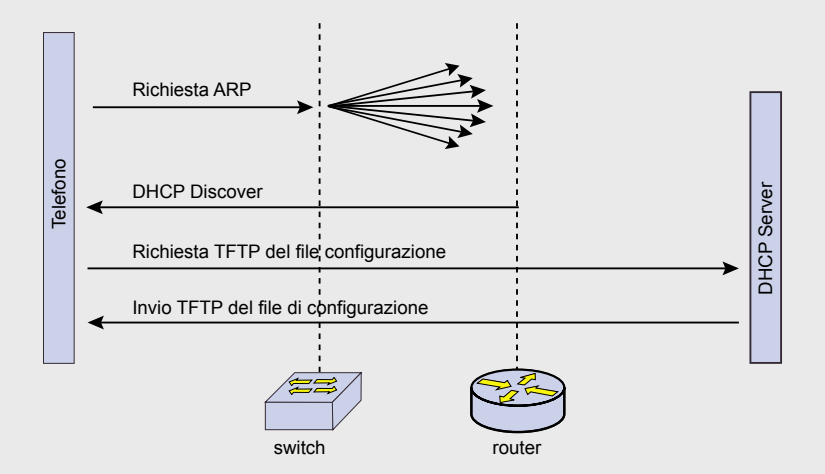

Figura 5: *Dettaglio della fase di configurazione*

Figura 6: *Dettaglio della fase di segnalazione*

La fase di configurazione

Il telefono si rivolge dunque al server di configurazione ed utilizza TFTP (*Trivial File Transfer Protocol*) per richiedere la propria configurazione, che gli è inviata dal configuration server. Per l'individuazione del configuration server, di cui il telefono ha l'indirizzo IP e non il MAC address di livello 2, ci sarà un altro broadcast.

La fase di segnalazione

Questa fase avviene fra il telefono ed il server di telefonia. In questo momento avviene la registrazione del telefono alla fine della quale il server di telefonia è a conoscenza che il telefono è operativo. Nel momento in cui sul telefono è sollevata la cornetta, il server invia il segnale di libero, come anche il segnale del telefono remoto che squilla durante una chiamata. In questa fase la comunicazione fra il telefono ed il server può utilizzare il protocollo SIP e l'ascolto/invio di dati avviene su porte UDP dinamicamente stabilite.

La fase di conversazione

Questa fase avviene fra telefono e telefono. Dal telefono di sinistra viene fatto un ARP Discovery per individuare il MAC address dell'altro telefono. Lo stesso avviene anche dall'altro telefono. A questo punto entrambi i telefoni si scambiano dati, per dirlo precisamente, la voce campionata viene scambiata con il protocollo RTP (*Realtime Transport Protocol*). Questa comunicazione avviene su porte UDP dinamicamente stabilite.

Potenziali Vulnerabilità

La voce su IP eredita il modello di rischio di una rete IP in quanto tutti

i servizi VoIP la utilizzano come trasporto. Un buon livello di protezione sulla rete garantirà un buon livello di protezione anche sui servizi voce. I seguenti sottoparagrafi evidenzieranno quali possono essere le criticità e quali contromisure possono essere adottate. Volontariamente non si farà riferimento a strumenti specifici di attacco.

La tipologia degli attacchi può essere riassunta in 3 grandi categorie: attacchi mirati alla *Confidenzialità* dei dati (*impersonation, interception attacks*), quelli mirati all'*Integrità* dei dati (*impersonation, interception attacks*) ed attacchi mirati alla *Disponibilità* dei servizi (*floods, malicious packets*).

Gli attacchi possono essere effettuati a diversi livelli della pila ISO/OSI (dal livello fisico (L1) a quello applicativo (L7), ne descriveremo alcuni con particolare riferimento agli accessi fisici ed ai layer 2 e 3 del modello ISO/OSI.

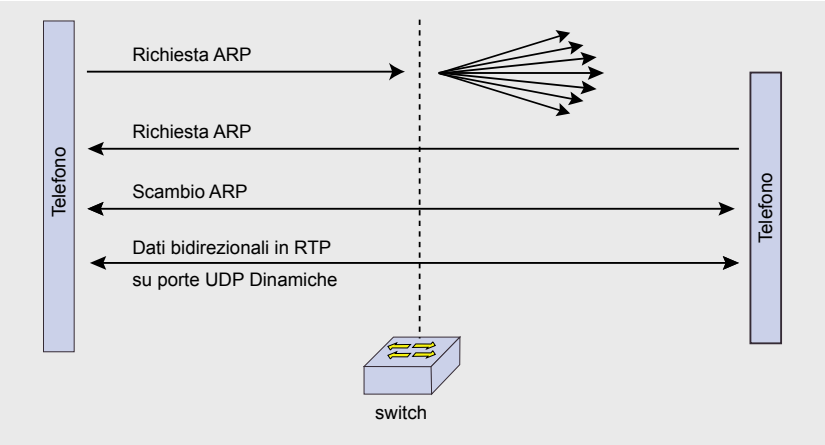

Figura 7: *Dettaglio della fase di conversazione*

Attacchi e contromisure sugli accessi fisici

Oltre alle normali regole di sicurezza, è importante prestare attenzione ai vari livelli di accesso fisico ai terminali. Un buon design prevede che l'accesso fisico al telefono sia consentito solo al personale autorizzato, in tal modo si possono evitare alcuni attacchi tipo spoofing come ad esempio: leggere nome ed interno del possessore del telefono, vedere le chiamate perse, ascoltare la casella vocale ed

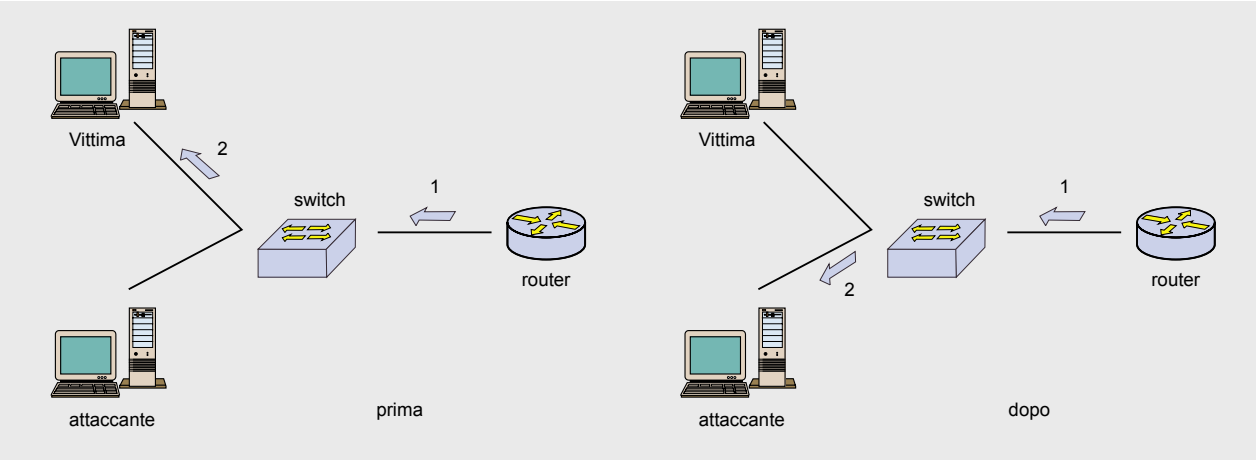

Figura 8: *Rappresentazione MAC Address spoofing*

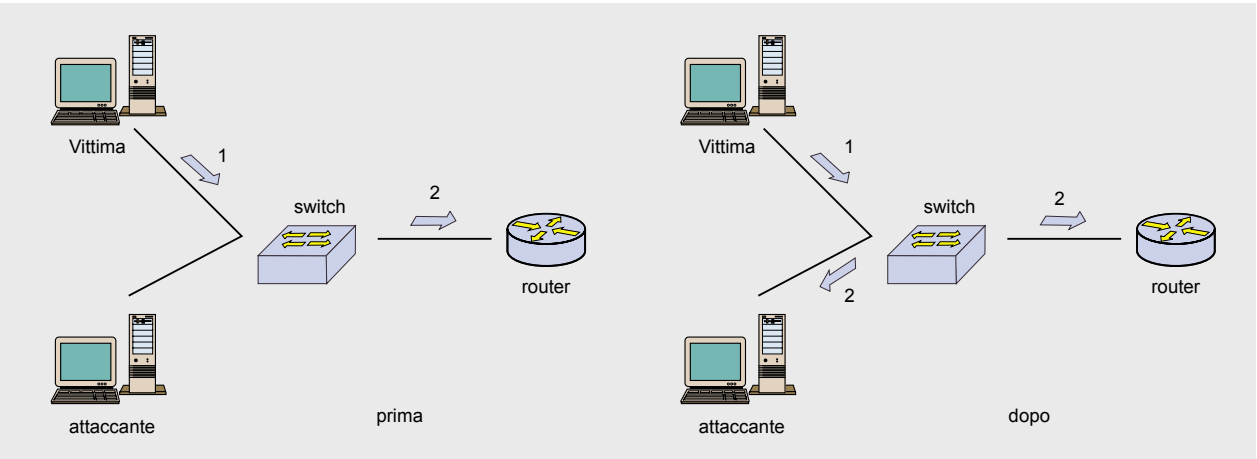

Figura 9: *Rappresentazione CAM Table Overflow*

evitare che siano effettuate chiamate non autorizzare o illegali.

La sicurezza *fisica* fa parte del concetto generico di sicurezza. Gli accessi privilegiati e controllati sono necessari per prevenire quanto in precedenza descritto. Per evitare che l'attaccante riesca ad utilizzare il telefono e le sue applicazioni senza le dovute autorizzazioni, si possono utlizzare delle regole di autenticazione sia del dispositivo stesso sia dell'utente, utilizzando ad esempio una username e password o delle chiavi di cifratura.

Il livello di protezione fisica di un telefono dipende generalemente da due fattori: il primo di solito chiamato *diritto del telefono*; ad esempio un telefono che si trova in un'area di passaggio, essendo alla portata di tutti avrà delle regole diverse rispetto ad un telefono situato all'interno degli uffici. Il secondo di solito chiamato *autorizzazioni degli utenti*, in altre parole gli utenti che si trovano negli uffici avranno dei privilegi legati alle proprie utenze, generalmente username e password, mentre i telefoni delle zone comuni non saranno soggetti ad autenticazione.

Attacchi e contromisure sull'infrastruttura di rete

Il Media Access Control (MAC) *flooding* è un attacco che tenta di inondare la memoria interna degli switch con un gran numero di indirizzi MAC falsificati, questo può avvenire perché gli switch apprendono gli indirizzi MAC dagli host che generano traffico su un segmento di rete. Se la quantità di MAC falsi è di grandi dimensioni, è possibile riempire la memoria dello switch facendo in modo che esso smetta di funzionare, in alcuni casi lo switch si comporterà come uno hub.

Il MAC *spoofing* tenta di falsificare un indirizzo MAC sorgente conosciuto o autenticato per tentare di ottenere maggiori privilegi di accesso alla rete. Questo tipo di attacco può di conseguenza portare a creare degli attacchi denominati *Denial of Service* (DoS) inviando una grande quantità di Address Resolution Protocol (ARP) Reply a host bersaglio. (vedi figura 8).

La *Content Addressable Memory* (CAM) table è una risorsa di memoria che contiene tutti i MAC Address dei terminali conosciuti. Per quanto grande possa essere questa tabella è pur sempre di una grandezza finita. La vulnerabilità è dovuta al riempimento dello spazio disponibile in memoria. Nel caso in cui esso dovesse terminare, ad esempio a causa di un gran numero di pacchetti aventi indirizzo MAC mittente fasullo, e quindi non ancora presente all'interno della CAM, lo switch cercherà di memorizzarli tutti (*CAM Flooding o CAM Table Overflow - vedi figura 9*).

In questa situazione lo switch si comporta come se fosse un hub, ovvero inviando i pacchetti su tutte le porte. Per prevenire questa e le altre situazioni descritte è opportuno configurare la *port security* in modo che ogni porta accetti un numero finito di MAC address (in genere due o tre). Gli scenari descritti saranno correttamente mitigati da questa contromisura. *L'IP spoofing* è uno degli attacchi più comuni, e consiste nel falsificare l'indirizzo IP uno host (A) in modo da farlo sembrare un'altro (B) e superare in questo modo la difesa basata sul controllo dell'indirizzo IP sorgente.

Il principale tipo di filtraggio usato per garantire la sicurezza delle connessioni è basato sulla rilevazione dell'indirizzo IP degli host tenendo in considerazione, oltre all'indirizzo IP destinazione anche quello sorgente.

L'attacco *DHCP Starvation*, può essere generato da richieste DHCP

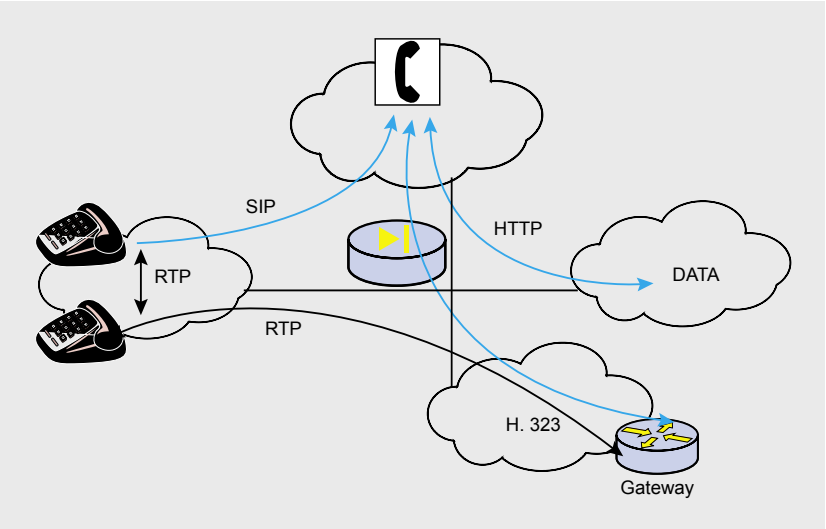

Figura 10: *Esempio di traffico filtrato da un firewall*

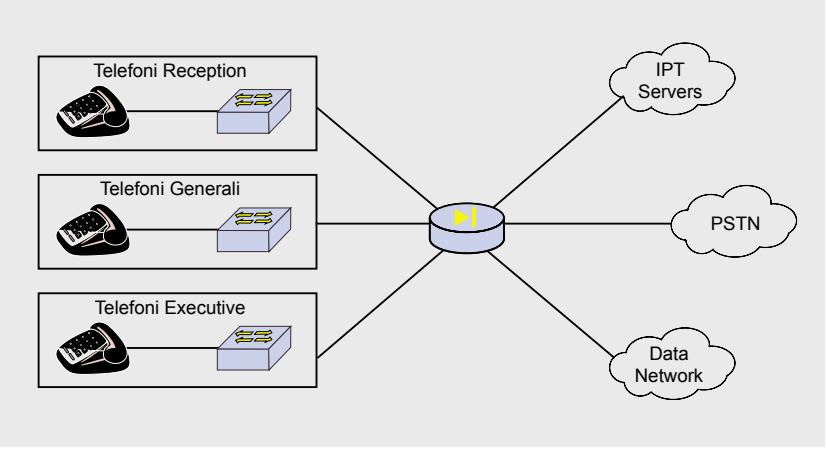

Figura 11: *Esempio di separazione*

con indirizzo MAC Address falso in modo da acquisire tutti gli indirizzi IP ancora non assegnati agli host, fatto ciò, l'attaccante potrebbe fingersi DHCP server ed inviare agli host dei parametri contraffatti, come ad esempio IP e default gateway o DNS.

Un'utile contromisura a questo tipo di attacco può essere l'utilizzo di sistemi di *Network Intrusion Detection / Protection*, usare indirizzi IP statici o limitare il numero di MAC address sulle porte dello switch come descritto nel paragrafo precedente.

Tutti gli attacchi che abbiamo appena descritto mirano a compromettere i terminali. Se analizziamo attentamente quanto descritto finora, molti degli attacchi possono essere mitigati con semplici accortezze di configurazione e con strumenti di controllo della rete come ad esempio i sistemi di Network Intrusion Detection / Protection. Non è da dimenticare comunque che un livello di sicurezza accettabile prevede l'autenticazione dei terminali tramite nome utente e password, ed eventualmente autenticazione forte con chiavi di cifratura. Non per ultimo rimangono da adottare delle politiche di qualità del servizio che ci verranno in aiuto nel caso in cui la quantità di traffico generato dagli attaccanti superi quella standard richiesta a garantire sempre un ottimo servizio VoIP.

I firewall di una rete hanno il compito di analizzare tutto il traffico in transito. Come approfondiremo in seguito, è opportuno avere delle separazioni tra la rete dati e quella voce. In un ambiente VoIP, tutto il traffico di segnalazione e quello RTP dovrà attraversare il firewall in modo da garantirne l'integrità delle comunicazioni.

Per quanto riguarda la riservatezza delle comunicazioni è possibile cifrare il traffico tra i due terminali in modo ottenere un elevato livello di sicurezza ed evitare qualsiasi alterazione della comunicazione (vedi figura 10) .

Creare delle separazioni

Un buon design prevede la separazione del traffico voce da quello dati. È buona regola dividere in VLAN (*Virtual Local Area Network*) le varie zone di accesso ai dispositivi. Questa separazione permette di avere diversi livelli di accesso e di conseguenza di privilegio. La figura sottostante illustra un esempio di configurazione (vedi figura 11).

Attacchi sui Sistemi ed Applicazioni

I sistemi che sono composti da sistemi operativi ed applicazioni, possono essere soggetti ad attacchi da parte di codice pericoloso, comunemente conosciuto come *Malware*.

Esistono vari tipi di Malware tra cui i *Virus* che sono delle parti di codice infetto con la caratteristica di replicarsi, Worm che sono in grado di modificare il sistema operativo e replicarsi in rete saturando le risorse di questa ultima, ed i *Trojan* parti di codice dannoso che vengono eseguite in modo non visibile dall'utente, spesso mascherate all'interno di software apparentemente innocuo.

Per quanto riguarda le contromisure da adottare per questa tipologia di attacchi, si possono consigliare, oltre al frequente aggiornamento delle versioni software per impedire che l'attaccante sfrutti eventuali difetti di programmazione, anche la disabilitazione dei servizi non utilizzati e l'utilizzo di chiavi di accesso ai servizi (*username/password, autenticazione forte, chiavi digitali, ecc...*) oltre agli strumenti di monitoraggio e prevenzione quali sistemi *Intrusion Detection / Protection* .

Conclusioni

Le tecnologie VoIP destinate alle aziende, sono una flessibile soluzione di telefonia che permette di contenere la spesa del tradizionale traffico telefonico. Adottando le opportune politiche di sicurezza, si potranno ottenere ottimi risultati. In fin dei conti una rete IP offre molti più ambiti dove implementare sicurezza rispetto ad una rete tradizionale telefonica. ●

In Rete

- NIST: Security Consideration for Voice Over IP systems: *www.nist.gov,*
- Voice Over IP Security Alliance: *www.voipsa.org.*

Cenni sugli autori

Marco Misitano, CISSP, CISA, CISM si occupa di sicurezza informatica da oltre dieci anni. Nel breve passato si è occupato in particolare della sicurezza delle soluzioni di voce su IP, di wireless security e di tecnologie di Admission Control. Nel 2005 è fra i soci fondatori di AIPSI, Associazione Italiana Professionisti Sicurezza Informatica, capitolo Italiano di ISSA (*Information Systems Security Association*), ed in questa associazione è parte del consiglio direttivo con la qualifica di Communication Officer. Collabora attivamente con altri enti quali ISACA, (ISC)², AIEA e CLUSIT. Misitano è lo specialista di Sicurezza Informatica per Cisco in Italia.

In quest'articolo Marco Misitano ha curato la parte iniziale dei principi di funzionamento delle soluzioni di telefonia IP. Può essere raggiunto all'email marco@misitano.com.

Antonio Mauro, Security Consultant, si occupa di sicurezza informatica da 5 anni. La sue competenze in campo informatico e delle telecomunicazioni sono frutto di esperienze maturate all'interno di importanti aziende multinazionali. È socio di AIPSI – *Associazione Italiana Professionisti Sicurezza Informatica*, capitolo Italiano di ISSA (*Information Systems Security Association*), del CLUSIT – *Associazione Italiana Professionisti per la Sicurezza Informatica* e collabora con l'ICAA – *International Crime Analysis Association.* Attualmente Mauro lavora in Cisco Systems.

Antonio Mauro ha curato la seconda parte dell'articolo.