VoIP (in)security: strumenti Open Source per il Security Assessment

Alessio L.R. Pennasilico, Marco Misitano & Elisa Bortolani

04 Ottobre 2006

Come dimostrano i fatti di cronaca, i rischi di subire un attacco alla propria infrastruttura VoIP sono reali. Il paper descrive e analizza alcuni dei più efficaci strumenti open source a disposizione tanto dell'amministratore di sistema, interessato a mettere alla prova la sicurezza delle proprie infrastrutture, quanto dell'*attacker*. Vengono riportati infine alcuni consigli su come proteggere la propria rete da tali rischi.

Introduzione

Recenti statistiche[1] stimano che, già a partire dal 2007, il 75% dei servizi voce mondiali si avvarrà del *VoIP* (*Voice over IP*) e che, dal 2008, il 44% delle linee telefoniche aziendali si baserà su Internet. Queste e altre numerose indagini rilevano che tale sistema sta conquistando il mercato tanto in ambito business quanto nel privato. Diversi sono i motivi alla base dell'enorme successo. Se questa tecnologia, infatti, spesso risulta economicamente vantaggiosa, ancora più spesso si dimostra estremamente efficace. Grazie al VoIP, infatti, molte aziende possono gestire in modo flessibile le proprie risorse, accentrandole o decentrandole a seconda delle necessità aziendali, ma soprattutto usufruendo di servizi innovativi, altrimenti estremamente costosi.

Come per ogni progetto, è tuttavia indispensabile un'iniziale analisi del rischio corretta e proattiva, che permetta di evitare sorprese durante le successive fasi di implementazione e di utilizzo. Uno dei più comuni errori che si compiono in questa fase è proprio il fatto di minimizzare le problematiche relative alla sicurezza. Solitamente, i responsabili IT non si pre-occupano dei rischi legati alla telefonia, ritenendola esente da rischi o assimilandola alla telefonia tradizionale. Quest'ultima, in effetti, si è basata fino ad oggi su tecnologie, sistemi e protocolli completamente proprietari e quasi sempre non intercomunicanti. Per accedere a

[1] Cfr: Frost & Sullivan, 2006; Gartner Inc., 03.04.2005; Synergy Research, 17.08.2004

questo tipo di reti erano infatti necessarie costose connessioni dedicate o strumenti specifici altrettanto costosi.

Tuttavia, molti sono gli esempi di vulnerabilità pubblicate da *phreakers* e da esperti di sicurezza della rete telefonica. Il più famoso tra essi, John Draper, meglio conosciuto come Captain Crunch, piegava al suo volere, tra gli altri, il sistema telefonico di AT&T. Il fischietto-giocattolo dei suoi cereali preferiti, infatti, emetteva un tono a 2600 Hz, frequenza che la centrale telefonica interpretava come un comando. Tale espediente gli consentiva di effettuare lunghe e costose chiamate a prezzi irrisori.

Se già i sistemi telefonici tradizionali, quindi, sono vulnerabili ad una discreta quantità di attacchi, il VoIP moltiplica tali rischi per quelli normalmente legati alle reti IP[2]. Oggi, infatti, tutti i sistemi sono tra loro interconnessi, parlano un linguaggio comune, documentato e conosciuto, e il mezzo per accedere a questi sistemi, spesso, è una banale connessione ad Internet.

Già da tempo è possibile leggere su Internet segnalazioni di attacchi mirati alle infrastrutture VoIP e frodi compiute ai danni dei *carrier*. Vale la pena di citare, in proposito, il caso eclatante[3] di Edwin Andreas Pena, il ventitreenne di Miami che, assoldato un criminale informatico per compromettere la sicurezza delle reti di diversi *VoIP Service Provider*, in sei mesi ha rivenduto sottoscosto dieci milioni di minuti di telefonate, guadagnando un milione di dollari.

Anche la legge, talvolta, peggiora la situazione, imponendo vincoli che abbassano sensibilmente la sicurezza dell'infrastruttura. Ne è un esempio *CALEA* (*Communications Assistance for Law Enforcement Act*), legge statunitense vigente dal 1994[4], che sancisce l'obbligo per ogni operatore telefonico di garantire all'autorità giudiziaria la possibilità di intercettare qualsiasi tipo di chiamata che attraversi il sistema. Recenti proposte prevedono di estendere tale legge alle comunicazioni VoIP. Molte nazioni, però, tra cui anche Stati Uniti e Francia, concludevano, più di dieci anni fa, che indebolire la sicurezza di Internet nella speranza di poter occasionalmente aiutare le forze dell'ordine, fosse un pessimo compromesso[5]. Il fatto di estendere CALEA al VoIP, perciò, sarebbe un passo pericoloso per la sicurezza dell'intero sistema (cfr. Bellovin et al., 2006). Ad esempio di ciò riportiamo il caso di *Vodafone Grecia*[6] che, per aderire alle norme vigenti, installò presso la propria rete degli strumenti che mettessero in grado la magistratura di poter effettuare

[2] New Technology, New Threats, *Communications News*, June 2005, 46, (2).
[3] Per consultare il rapporto dell'FBI: http://www.usdoj.gov/usao/nj/press/files/pdffiles/penacomplaint.pdf; http://www.usdoj.gov/usao/pae/News/Pr/2005/feb/Moore.pdf
[4] In: http://www.askcalea.net/calea.html
[5] E un gran numero di organizzazioni, non da ultimi il Dipartimento della Difesa e il Dipartimento di Giustizia degli Stati Uniti (Bellovin, Blaze, Landau, 2005) si sono scoperti vulnerabili
[6] In *Greek Wiretapping Scandal*, http://www.schneier.com/blog/archives/2006/06/greek_wiretappi_1.html

intercettazioni telefoniche a seguito di un mandato. Tali strumenti, però, furono utilizzati illegalmente dalla criminalità organizzata che, per mesi, intercettò qualsiasi conversazione transitasse sul sistema, in particolare quelle di politici e magistrati.

A fronte di tali considerazioni, ogni analisi tesa a valutare sensatamente i rischi legati ad un'infrastruttura VoIP, deve tener conto di eventuali attacchi *DoS* (*Denial of Service*), intercettazioni, furti di identità, frodi, *SPIT* (*SPam over Internet Telephony*) e *vishing*[7] (Tanner, 2005; Materna, 2006).

Con l'esplosione del VoIP, perciò, stiamo assistendo alla nascita di un enorme numero di progetti, la cui *mission* consiste nello sviluppo di strumenti per il *security assessment*, specifici per il VoIP. Molti di questi *tool* sono *open source*, disponibili su Internet e gratuiti. Tali programmi, chiaramente, sono di per se stessi neutri e, al di là delle intenzioni originarie dell'autore, possono essere utilizzati indistintamente, e in base ai propri scopi, da consulenti che testano la rete dei propri clienti, amministratori di sistema che mettono alla prova periodicamente la sicurezza della propria infrastruttura, criminali interessati ad introdursi in un sistema.

Tutti gli accorgimenti in merito all'*hardening* della rete VoIP sono e devono essere a carico del fornitore di servizio. È il carrier che deve proteggere i diritti dei propri utenti, mentre l'azienda deve occuparsi di quelli dei propri dipendenti. Infatti, tutti gli strumenti necessari per rendere sicura l'infrastruttura VoIP possono essere implementati esclusivamente da chi gestisce il servizio e non da chi ne usufruisce. L'utente finale, perciò, non può fare nulla in prima persona per proteggersi, ma deve passivamente adeguarsi alle caratteristiche del servizio offerto.

Caratteristiche di una chiamata VoIP

Analizziamo ora, in maniera sintetica, il funzionamento di un telefono per capire dove potenzialmente si annidano i rischi di un eventuale attacco.

Appena un telefono viene acceso invia sulla rete un *broadcast* necessario ad individuare il *server DHCP* (*Dynamic Host Configuration Protocol*), ovvero il server che fornisce in modo automatico l'indirizzo a tutti i *device* di quella rete. Il server DHCP risponde al telefono assegnando non solo i parametri di rete

[7] Con il termine *vishing*, derivante dalla contrazione di *VoIP* e *phishing*, ci si riferisce ad un attacco finalizzato ad ottenere dati personali (password, numeri di carte di credito, numeri di conto bancario, ecc.) di un ignaro utente per un uso illecito. Il malintenzionato, cioè, attiva un sistema automatico di chiamata per contattare potenziali vittime alle quali, al momento della risposta, una voce registrata comunica l'esistenza di problemi al proprio conto corrente, per risolvere i quali l'utente deve chiamare un certo numero. Tale numero, però, appartiene al truffatore che può così impossessarsi dei dati.

corretti (indirizzo IP, *subnet mask, default gateway*, ecc.), ma anche l'indirizzo del server *TFTP* (*Trivial File Transfer Protocol*) che contiene gli eventuali aggiornamenti per il sistema operativo del telefono e la sua configurazione (opzione 150 delle *DHCP options*). La comunicazione con il TFTP server avviene esclusivamente in *UDP* (*User Datagram Protocol*), quindi senza alcun meccanismo di affidabilità. Ottenute le informazioni necessarie dal TFTP server, se configurato per farlo, il telefono si autentica sul proprio server VoIP, comunicando numero di telefono e password. Da questo momento, server e telefono si scambieranno tutte le informazioni necessarie alla gestione delle chiamate (ID chiamante, ID chiamato, eventuali deviazioni, trasferimenti, fine conversazione, ecc.). Questo flusso di informazioni prende il nome di *signaling*.

Al momento di una nuova chiamata, terminata la fase iniziale di signaling, si instaura un flusso di dati trasportati, sempre in UDP, dal protocollo *RTP* (*Real-time Transport Protocol*). Tale flusso di traffico, a seconda delle configurazioni, avviene tra ogni telefono e il proprio server oppure direttamente tra i telefoni coinvolti nella conversazione.

Security Assessment Tools

A chiunque abbia un minimo di esperienza o conoscenza degli attacchi perpetrabili ad una rete IP, il sistema appena descritto risulterà estremamente vulnerabile ad un gran numero di attacchi.

È possibile, ad esempio, sostituire l'autentico server DHCP con uno funzionale all'attacco che fornisce i parametri da noi decisi, a patto di far giungere al telefono la nostra risposta prima di quella del vero server DHCP. Così facendo è possibile imporre al device di scaricare un sistema operativo modificato ad hoc dal server TFTP dell'attaccante, nonché imporre al telefono una configurazione creata appositamente per perpetrare l'attacco (ad esempio, fornendo l'indirizzo IP di un server VoIP installato di proposito e configurato in modo funzionale all'attacco).

Potremmo anche decidere di ignorare la fase relativa al DHCP e, attraverso *l'ARP Spoofing*, dirottare sul nostro server TFTP il traffico destinato a server TFTP dell'organizzazione vittima. Questi tipi di attacco si gestiscono, anche su reti *switchate*, con estrema facilità grazie a strumenti come *Ettercap*[8]. Ettercap, la *suite* più famosa al mondo per gestire attacchi di tipo *MITM* (*Man In The Middle*), è un programma multipiattaforma che permette di intercettare il traffico, decodificarlo e generarne *ad hoc* per inquinare la *cache arp* o la *cache DNS*. Ettercap prevede inoltre la possibilità di inserirsi all'interno di una

[8] http://ettercap.sourceforge.net/

conversazione già stabilita e, non soltanto di osservarne il contenuto, ma anche di modificarlo in tempo reale. Per garantire l'efficacia di questi attacchi è previsto anche un modulo per diversi attacchi di tipo DoS, ad esempio il *flooding*, necessario per "zittire" il server che vogliamo impersonare.

Esistono inoltre un'enorme quantità di *sniffer* in grado di interpretare i protocolli VoIP, ad esempio per intercettare il nome utente e la password che il telefono comunica al server durante l'autenticazione. Tra questi segnaliamo *Wireshark*[9], ritenuto ad oggi uno dei più potenti *network sniffer* disponibili sul mercato. In questo contesto sono da segnalare inoltre progetti come *Vomit*[10]. Tale programma legge il *dump* del traffico di rete, in formato *tcpdump*[11], creato da uno sniffer ed ottiene un file audio con la registrazione della conversazione telefonica intercettata. Vomit, uno dei primi progetti di questo tipo, può decodificare qualsiasi conversazione avvenuta con protocollo *MGCP* (*Media Gateway Control Protocol*) con *Codek G. 711*. In brevissimo tempo, sono apparsi programmi più complessi orientati a svolgere le stesse funzioni. Ad esempio *Oreka*[12], che permette di decodificare il traffico VoIP di diversi protocolli, spesso anche di formati proprietari, e di archiviare le registrazioni in un database consultabile via web. Se Oreka si limita ad intercettare il traffico, *Scapy*[13] permette di capire quanto fragile sia l'infrastruttura se non adeguatamente protetta. Scapy, infatti, permette non soltanto di osservare un flusso di traffico VoIP, ma anche di interagire con esso, modificandolo in tempo reale e forgiandolo secondo necessità. Sua peculiarità è, da una parte, la modularità ma, dall'altra, la sua mancanza *by design* di vincoli formali durante l'operazione di *forging* nella generazione del traffico. Questo permette, quindi, tanto di combinare tra loro tecniche note, quanto di creare attacchi del tutto inusuali. Si pensi, nel primo caso, alla combinazione di *VLAN hopping* con l'*ARP Cache Poisoning*, mentre, nel secondo caso, all'incapsulamento dei *frame 802.1q* all'interno di un pacchetto TCP. Una delle *best practice* per rendere più sicura un'infrastruttura *voice*, infatti, è la segmentazione logica delle diverse reti secondo caratteristiche che rendano le *Virtual LAN* (*VLAN*) omogenee. Questo impedisce, ad esempio ad un eventuale *attacker*, che si trovi sulla VLAN a cui appartengono i PC, di poter interagire con i telefoni che stanno nella propria VLAN. La tecnica di VLAN hopping prevede di poter generare traffico in una VLAN diversa da quella di appartenenza, inficiando quindi questo meccanismo di protezione.

---

[9] http://wireshark.org/

[10] *Vomit*, acronimo di *voice over misconfigured internet telephones* è stato insignito del *Compendium Award for Worst Product Name of the Day*. In: http://vomit.xtdnet.nl

[11] Formato conosciuto e gestito ad esempio da *Wireshark*.

[12] http://oreka.sourceforge.net/

[13] http://freshmeat.net/projects/scapy/

Oltre agli amministratori di sistema, che vogliono rendersi conto della robustezza delle misure di sicurezza adottate per proteggere il traffico voce, esiste un'altra categoria di persone, i ricercatori, gli hacker, che si occupano di rendere più sicura questa tecnologia. Poter capire quanti e quali *device VoIP* sono collegati ad Internet ci permette di comprendere meglio il fenomeno. Analizzare l'implementazione dei diversi standard VoIP, fatta dai diversi produttori, permette di trovare errori di implementazione e aiutare il *vendor* a migliorare il proprio prodotto.

Per condurre analisi di questo tipo è necessario appoggiarsi a strumenti che permettano di interfacciarsi in modo *nativo* ai device da testare. Tra questi possiamo citare *SIPsak*[14], il coltellino svizzero del VoIP Admin, che permette di simulare il traffico di *signaling* e/o di inviare pacchetti con un contenuto creato ad hoc. Strumenti come questo sono molto utili in contesti quali il *debug* mentre, per un'efficace analisi dei difetti di implementazione, si utilizzano i cosiddetti *fuzzer*. Tra i *VoIP fuzzer*, citiamo *Ohrwurm*[15] che, stando alle parole dell'autore, è stato scritto in un pomeriggio e testato su qualche decina di telefoni. Nessuno dei quali ha passato il test.

Conclusioni

Tutti gli strumenti illustrati mettono in evidenza i rischi ai quali il VoIP espone. Ogni amministratore di sistema, che si curi della sicurezza della propria infrastruttura VoIP, dovrebbe scaricarli, installarli e utilizzarli per testare a quali tipi di attacco è vulnerabile il suo sistema.

Le contromisure, per quanto non possano eliminare completamente i rischi, di certo li mitigano in modo soddisfacente. La divisione in VLAN del traffico voce e del traffico dati, ad esempio, contrasta gli attacchi *MITM e* minimizza attacchi di tipo *flooding* o *spoofing* provenienti dalla rete dati. Inoltre, l'adozione di *switch* che prevedano meccanismi di protezione da questi tipi di attacchi è altresì consigliata. Una corretta configurazione del *Quality of Service* (QoS) permette di aumentare la disponibilità della nostra infrastruttura e di minimizzare ulteriormente attacchi di tipo flooding. Risultano inoltre indispensabili meccanismi di *AAA* (*Authentication, Authorization, Accounting*) adeguatamente pianificati ed implementati. Per quanto non ci soffermeremo, non possiamo però tralasciare l'indiscutibile necessità di implementare meccanismi di *encryption*, tanto del traffico di signaling quanto dei flussi RTP.

[14] *SIPsak* è acronimo di *SIP swiss army knife*. In: http://sipsak.org/
[15] http://www.first.org/newsroom/globalsecurity/46271.html

Bibliografia

Bellovin, S., Blaze, M., Brickell, E., et al. (2006). Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, in: http://www.itaa.org/news/docs/CALEAVOIPreport.pdf

Bellovin, S., Blaze, M., & Landau, S. (2005) The Real National-Security Needs for VoIP, *Inside Risks*, 180, CACM 48, Nov 2005, p.120.

Materna, B. (2006). Proactive Security for VoIP Networks. *Information Systems Security*, May 2006, 15 (2), pp. 16-21.

Tanner, J.C. (2005). The perils of VoIP. *Telecom Asia*, Sept. 2005, 26-29.