HACKINBO

IL TELEFONO, LA TUA VOCE

SICUREZZA NELLE RETI VOIP

A cura di
Michele Garribba

SU DI ME

- Ingegnere delle telecomunicazioni, libero professionista
- Mi occupo di reti e sicurezza da 15 anni
- Collaboro con un'azienda di Roma che si occupa di sicurezza e reti principalmente per PA, settore governativo e militare
- Cisco CCIE Collaboration 46804
- Lavoro con soluzioni voip opensource da oltre 10 anni
- Formatore con oltre 10 anni di esperienza in reti e sicurezza

AGENDA

- Introduzione: il mondo VOIP
- Attacchi VOIP
- Frodi nel VOIP
- Contromisure
- ZRTP
- Symbiote
- Conclusioni

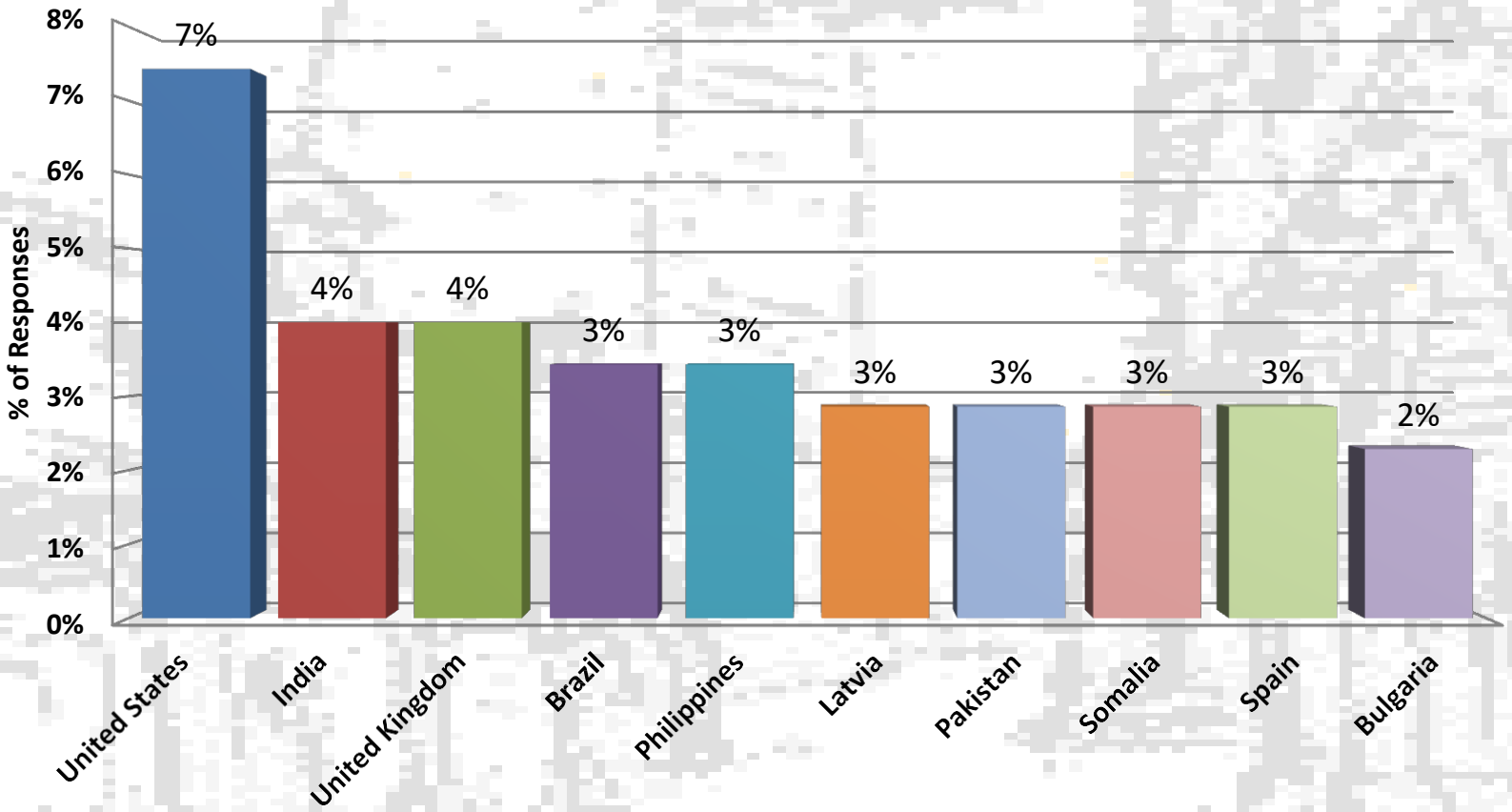
Introduzione

- Il mercato VOIP sta crescendo esponenzialmente grazie anche alla larga diffusione dei sistemi mobili quali smartphone e tablet, le reti IMS, e al concetto della Unified Communication che integra numerosi servizi al VOIP come, IM, caselle vocali, presence, billing, call center e molte altre funzionalità.
- Al pari del mercato crescono gli attacchi e le frodi ai sistemi VOIP
- Il report della CFCA (Communications Fraud Control Association) per il 2013 ha quantificato un giro di affari legato agli attacchi e alle frodi di circa **50 miliardi di $:**

  - 2013 Estimated Global Telecom Revenues: $2.214 Trillion (USD)
  - 2013 Estimated Global Loss: $46.3 Billion (USD), or 2.09%

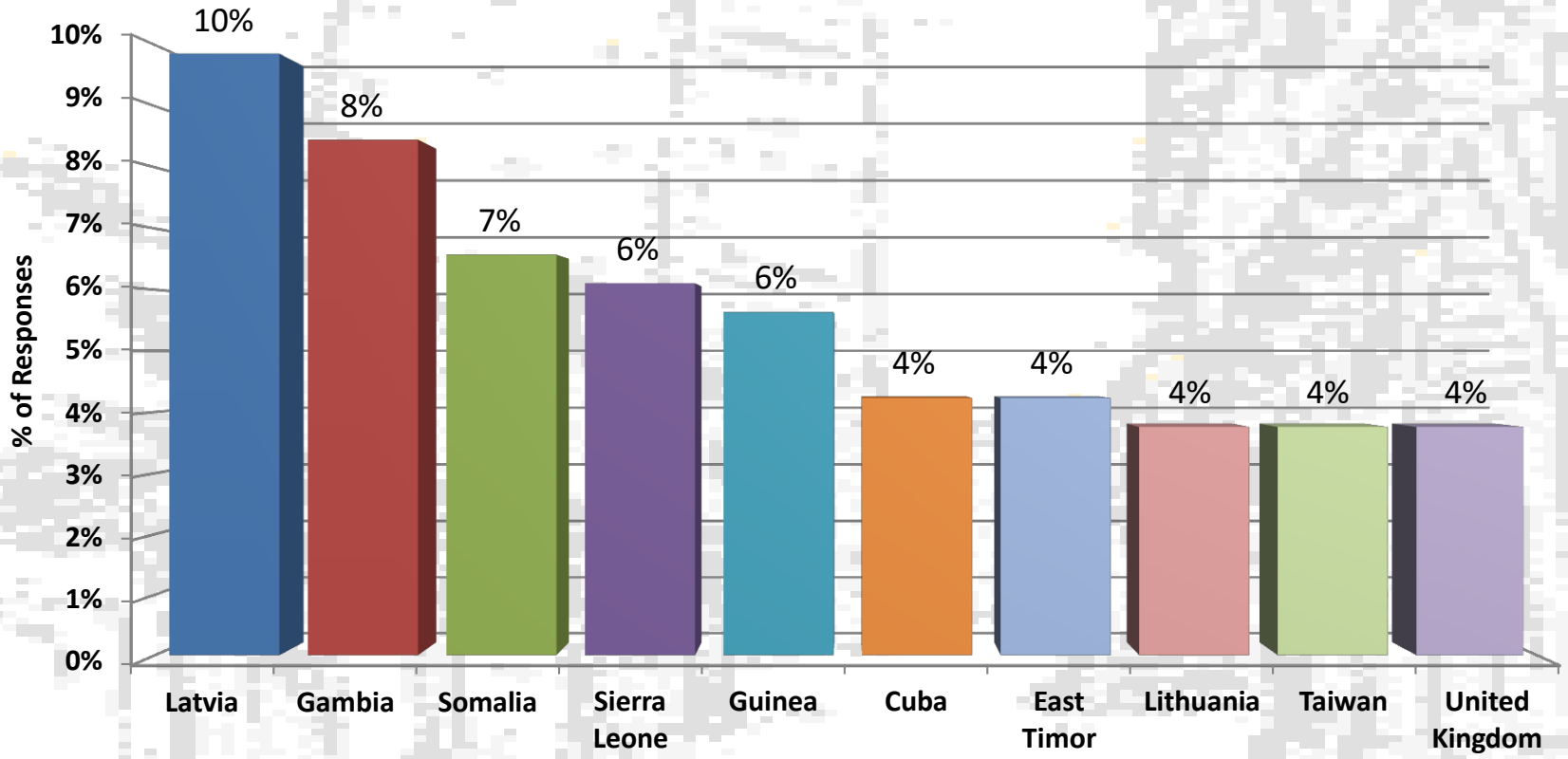
Stati “canaglia”

Top 10 dei Paesi ORIGINE di traffico VOIP Fraudolento :



Stati “vittima”

Top 10 dei Paesi TERMINATORI di traffico fraudolento



Sicurezza nelle reti VoIP

Cosa vogliamo garantire in una rete VOIP ?

1. **Riservatezza** delle comunicazioni
2. **Disponibilità** dei sistemi e della rete
3. **Integrità** dei contenuti trasmessi

SIP = Session Initiation Protocol è il principale e più diffuso protocollo di segnalazione per le reti VOIP sia Enterprise sia Provider.
Il suo funzionamento è molto simile al protocollo HTTP. Ma è un peer-to-peer

RTP = Real-time Transport Protocol. Protocollo di trasporto della voce codificata

Sicurezza nelle reti VoIP

Dallo RFC3261: *SIP non è un protocollo semplice da rendere sicuro. Il suo uso di intermediari, le numerose relazioni di fiducia e le operazioni che si compiono utente-utente rendono la sicurezza niente affatto facile*.

Data l'elevata diffusione del SIP e la difficoltà intrinseca a renderlo sicuro il protocollo si avvia a diventare il miglior candidato come UFBP = Universal Firewall Bypass Protocol

AGENDA

- Introduzione: il mondo VOIP
- Attacchi VOIP
- Frodi nel VOIP
- Contromisure
- ZRTP
- Symbiote
- Conclusioni

Categorie e attachi VOIP

- **Riservatezza**
  - Eavesdropping
    - Utilizzo di vulnerabilità per catturare il traffico RTP voce di una chiamata
  - (*sniffing*) Phreaking
    - Utilizzo di vulnerabilità per catturare il traffico di segnalazione VOIP, oppure uso criminale del CLI del chiamante
  - (*spoofing*) Call hijacking
    - Può riguardare sia la segnalazione sia il traffico voce, uso di tecniche differenti, come ENUM poisoning, DHCP spoof e altre tecniche di attacco
- **Integrità**
  - MITM
    - Estende le tecniche di dirottamento della segnalazione di una chiamata nascondendole al destinatario, permette il furto di identità
- **Disponibilità**
  - SPIT
    - Uso massivo di servizi di mailbox e chiamate estere gratuite tramite dialer per saturare la rete VOIP
  - DoS (*Denial of Service*)
    - Invio massivo di messaggi sia segnalazione tipicamente Invite, sia voce, RTP, per rendere indisponibile il canale di comunicazione

Tool utilizzati per attacchi VOIP

Azione Malevola	Tool
• Information gathering	• Smap, sipsack, svmap (sipvicius), sipscan
• Extension enumeration	• Svwar (sipvicius)
• Eaversdropping (MITM)	• Wireshark, ARPSpoof
• Telephone Tampering (MITM)	• RTPInsertsound
• Authentication Attack (MD5, Bruteforce)	• SIPCrack (SIPDump), SVCrack (sipvicoius) John the Ripper (Bruteforce)
• Denial of Service (DoS, DDoS)	• Inviteflood, RTPFlood, Teardown
• Spoofing Caller ID	• Svwar, Inviteflood
Altri attacchi correlati, XSS,SQL Injection…	Altri tool, Vomit, Metasploit, Cain&Abel, Voipong e diversi altri

Tutto ciò contribuisce a rendere il SIP il candidato migliore come UFBP

Esistono malware nel VOIP ?

- **Il caso Regin**
  - La compagnia Belgacom ha subito un pesante attacco portato da questo malware, molto insidioso perché modulare, crittografato e di difficile analisi.
  - La fonte era un server in Nord Europa e il dito è stato puntato su NSA e GCHQ come esecutori dell'attacco.
  - L'attacco ha prodotto furto di credenziali e hacking dei PBX di Belgacom e anche di radio basi.
- **Il caso Sality**
  - Attraverso una botnet distribuisce malware per azioni malevole. E' stato usato per distribuire un cracker per SIP che esegue attacchi per password cracking, discovering e PBX hacking
- **The Honeypot Project**
  - Dioanaea: honeypot per catturare malware,eseguire analisi e reagire. Ora capace di analizzare traffico SIP. A causa di vulnerabilità del codice può essere hackerata e utilizzata in modo malevolo

Skype è sicuro?

E’ senza dubbio il più diffuso sistema VOIP del mondo. Permette chiamate e conferenze audio\video, chat e trasferimento file **sicuri** ma….

- E’ stato ed è ancora veicolo di molte azioni malevole spesso nascoste
- Nel 2013 è stata resa nota una pesante vulnerabilità legata al furto dell’account attraverso l’email dell’utente da usare per rigenerare la password. Era nota da mesi ed è rimasta unpatched per diverse ore dopo l’ufficializzazione della scoperta
- Lo skype client per Linux esegue accessi al profilo di Firefox e allo storico della navigazione. Lo skype client per Mac esegue accessi alla Rubrica Indirizzi anche se l’integrazione è disabilitata
- In adesione al CALEA, la FCC e l’FBI possono ascoltare le conversazioni su Skype. Microsoft fornisce loro le chiavi di decifrazione
- Anche senza il CALEA, NSA, Russia e Cina possono accedere alle conversazioni e alle chat, Microsoft permette deliberatamente questo passando il ruolo dell’applicazione da client a server permettendo il flusso di dati non cifrati
- I ricercatori Biondi e Desclaux, legati a BlackHat, asseriscono con uno studio che Skype ha una backdoor e rimane “in funzione” anche quando è spento
- Altre vulnerabilità rendono Skype bersaglio di attacchi DoS, URL, buffer overflow…

AGENDA

- Introduzione: il mondo VOIP
- Attacchi VOIP
- Frodi nel VOIP
- Contromisure
- ZRTP
- Symbiote
- Conclusioni

Frodi nel VOIP

- **Definizione di frode nel VOIP**
- Qualsiasi utilizzo di una rete VOIP per evitare il pagamento di tariffe, in maniera parziale, totale, o scaricando i costi su altri utilizzatori o provider

Le frodi vengono attuate sfruttando debolezze nella rete VOIP delle vittime o utilizzando vulnerabilità nei sistemi integrati al VOIP

Il terreno per le frodi nel VOIP è molto fertile dato che spesso ci sono lacune normative che lasciano spazio a queste azioni in moltissimi paesi

Lo scopo di una frode nel VOIP è sostanzialmente di guadagnare in maniera fraudolenta

Tipi di frodi nel VOIP

- **Arbitrage**
  - Sfruttamento della complessità e diversità di tariffe tra Paesi diversi e re-routing delle chiamate
- **Buffer Overflow**
  - Utilizzo del buffer overflow sul metodo INVITE del SIP per causare crash del cient o iniettare codice
- **Bypass Fraud**
  - Inserimento di traffico non autorizzato nela rete di un provider, detto anche gateway fraud o SIM boxing
- **Call transfer fraud**
  - Hack del PBX vittima e trasferimento delle chiamate internazionali attraverso il proprio sistema VOIP
- **CNAM revenue pumping**
  - Utilizzo del CNAM dip per accoppiare la chiamata con servizi ad alto costo come conference service o sex line o circuiti satellitari
- **False answer supervision**
  - Chiamate effettivamente non risposte che non andrebbero tariffate compaiono con dei falsi messaggi di Supervision e vengono tariffate

Tipi di frodi nel VOIP

- **PBX Hacking**
  - Un classico e ancora uno dei più temuti. Sfruttamento di vulenrabilità del PBX per esguire un elevato numero di chiamate ad alto costo tramite ad esempio un dialer o bot
- **Premium rate services**
  - I premium-rate hanno una parte della chiamata a carico del provider. Vulenrabilità del sistema sfruttare per generare alti volumi di chiamate verso questi numeri
- **Revenue shared fraud**
  - Conseguenza spesso di un PBX hacking prende vantaggio dalla cooperazione tra carrier per iniettare traffico con chiamate verso rotte ad alta tariffa
- **Roaming Fraud**
  - Sfruttamento di reti wireless al di fuori del proprio Paese per routare le chiamate gratuitamente. Solitamente accoppiato al subscription fraud, grazie al ritardo di trasmissione dei CDR tra provider possono occerre diversi giorni per accorgersi del danno

Tipi di frodi nel VOIP

- **Subscription**
  - Tipicamente associato all'uso di identità falsa o rubata ha lo scopo di effettuare un alto numero di chiamate senza pagare
- **Shell Companies**
  - Provider che non vendono servizi ma li comprano da altri provider a credito e vi si connettono con un trunk. Dopo un primo periodo di attività leggittima la shell esegue un picco di utilizzo dei servizi. Quando il provider originale fattura i servizi la shell company scompare
- **Toll fraud**
  - Break di un PBX per effettuare chiamate verso numeri internazionali o reti satellitari o servizi ad alta tariffazione senza pagare
- **Traffic pumping**
  - Sfruttamento di accordi "rapina" tra carrier locali o di certi Paesi per tariffare provider nazionali quando le chiamate sono dirette ai clienti sottoscritti ai provider malevoli.
- **Unallocated number fraud**
  - Utilizzo di numeri non allocati nella tariffazione e routing delle chiamate verso questi numeri che generano alti guadagni. Circa il 32% delle chiamate fraudolente sono di questo tipo

Frodi nel VOIP

- **Chi è il bersaglio preferito delle frodi?**
- Tipicamente le grandi aziende o i provider

- Ma anche i privati: uno dei casi più famosi è la controversia tra AT&T e la signora Sue Smith chiamata a pagare una bolletta di 1,2 Milioni di $
- Tuttavia uno studio ha stabilito che 34 delle 50 principali banche sono state vittima di frodi tramite i sistemi VOIP

AGENDA

- Introduzione: il mondo VOIP
- Attacchi VOIP
- Frodi nel VOIP
- Contromisure
- ZRTP
- Symbiote
- Conclusioni

Cosa posso fare se vengo attaccato?

DON'T PANIC

Controlla i CDR (Call Detail Record)

Controlla i log del server VOIP

Avvisa le autorità

CAMBIA LE PASSWORD!!!

Protezione delle reti VOIP

- SVOIP = Secure VOIP
- SVOIP si propone di mettere in sicurezza i client che compongono una rete VOIP, ad esempio un telefono VOIP che cifra segnalazione e voce e trasmette su un network non sicuro

- VOSIP = Voice Over Secure IP
- VOSIP si propone di mettere in sicurezza la rete su cui viaggia il traffico VOIP, ad esempio un tunnel VPN cifrato. Anche un "vecchio" apparato non sicuro può usufruire della protezione della rete sicura

Quale approccio è "più sicuro" ?

La tendenza dei sistemi odierni data la grande mobilità acquisita e la difficoltà di creare reti cifrate distribuite su internet fa preferire SVOIP a VOSIP.

Tuttavia una combinazione delle due metodologie può aiutare a rendere sicura la vostra rete VOIP

Best Practice per la protezione

- Uso di Firewall IDS \IPS VOIP aware
- Uso di SRTP per la voce
- Uso di SBC (Session Border Controller) per demarcare la rete VOIP, controllare la segnalazione, gestire la cifratura e difendersi da una serie di attacchi specifici a segnalazione e traffico voce, nonché nascondere la rete interna
- Uso di cifratura TLS\SSL per la segnalazione
- Uso di strong password per i client
- Uso di tunnel cifrati per proteggere i client in mobilità o le reti remote, VPN, TLS o altri metodi

E contro le frodi come mi proteggo?

- La sicurezza andrebbe sempre pensata in fase di deployment del servizio VOIP integrata con la rete dati
- Allestire un buon sistema di analisi dei CDR che esamini la durata e le rotte delle chiamate specialmente di notte e nei weekend possibilmente in “real-time” con allarmi e blocchi temporanei di rotte sospette
- Azioni legali: difficili da applicare verso Paesi terzi e spesso le compagnie non denunciano le frodi dato che statisticamente solo l’1% delle azioni portano ad un risultato

- Eseguire periodicamente un VA per stabilire se ci sono vulnerabilità anche nel VOIP
- Validare le rotte verso altri provider e se il caso bloccare interi Paesi noti per essere fraudolenti ….
- Utilizzare codici di protezione per le chiamate ad alta tariffazione!!!
- Per privati e aziende bloccare tutti i numeri a servizi non necessari!!!
- SBC SBC SBC e ancora SBC !!

AGENDA

- Introduzione: il mondo VOIP
- Attacchi VOIP
- Frodi nel VOIP
- Contromisure
- ZRTP
- Symbiote
- Conclusioni

ZRTP

Zimmerman RTP
Tecnologia alternativa al TLS per cifrare una chiamata VOIP:

- Protocollo ZRTP definito da RFC 6189
- Sviluppato da P.Zimmerman (tra i creatori di PGP)
- Non dipende da strutture di cifratura come le PKI
- E' indipendente dal protocollo di segnalazione utilizzato
- La negoziazione delle chiavi di cifratura avviene "in band" dopo la sessione di comunicazione tra i client, es: segnalazione SIP
- La negoziazione delle chiavi avviene in maniera P2P tra gli endpoint
- La chiave (SAS), tipicamente randomicamente estratta dalla PGP Word List, viene presentata a vista ad entrambe gli interlocutori per conferma (contro MITM)
- Utilizzabile come plug-in dai client SIP esistenti
- Meccanismo di protezione contro attacchi di MITM
- Utilizzabile da server VOIP per creare una blackbox di cifratura

ZRTP

Quanto è sicuro ?

L'algoritmo di cifratura utilizza un sistema Entropy collection of random data.
SE la fonte di randomizzazione è debole è possibile attaccare la cifratura.
Il suggerimento è utilizzare fonti di randomizzazione in cui siano presenti messaggi voce registrati.
La randomizzazione dovrebbe avere sorgenti di messaggi audio fisiche, ad esempio il microfono stesso.
Il messaggio audio non viene inviato durante la validazione delle chiavi.

Nel 2013 scoperte 3 vulnerabilità critiche nella libreria ZRTPCPP che permettono di bypassare la sicurezza del protocollo

Colpite diverse implementazioni di ZRTP, tra cui SilentCircle, dello stesso Zimmerman

Verificare il livello di release della libreria PRIMA di utilizzarla

AGENDA

- Introduzione: il mondo VOIP
- Attacchi VOIP
- Frodi nel VOIP
- Contromisure
- ZRTP
- Symbiote
- Conclusioni

Symbiote, la frontiera ?

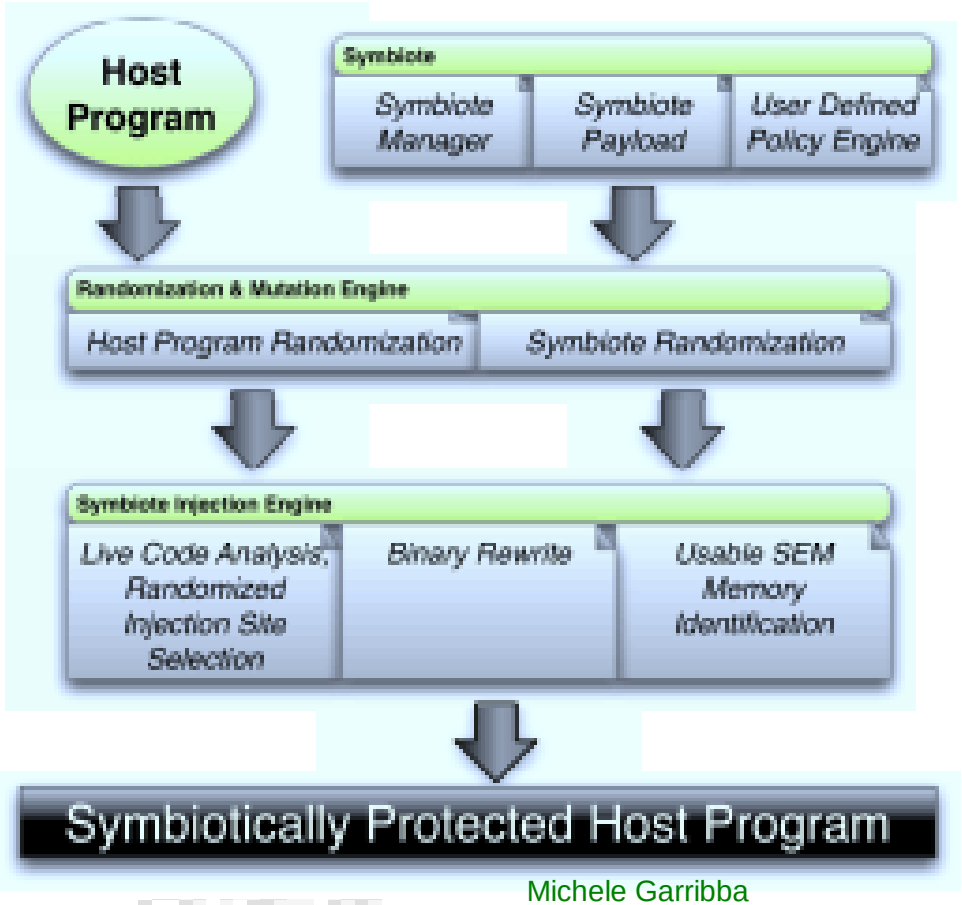
Nel 2013 il PhD Cui e il Prof. Stolfi della Columbia University, finanziati da DARPA, IARPA e DHS, eseguono un controllo di sicurezza, e scoprono che tutti i modelli di telefoni VOIP hanno vulnerabilità nel firmware. In particolare la parte che regola lo switch dello stato di Off-Hook.

Hanno dimostrato che è possibile iniettare codice in ciascuno dei telefoni Cisco ed eseguire un eaversdropping delle chiamate da qualsiasi parte del mondo.

L'attacco può essere condotto attaccando il circuito sotto riportato al telefono, uno qualsiasi di una compagnia e controllando il device da una app nel proprio smartphone.

Symbiote, la frontiera ?

Parte lo sviluppo di un framework che permette di mettere in sicurezza i telefoni VOIP.
Il progetto porta allo sviluppo di un software denominato Symbiote realizzando una difesa host-based del device.



Come un simbionte, il software risiede insieme al firmware nel device tramite il FRAK (Firmweare Reverse Analysis Konsole).

Esegue analisi randomica del comportamento del firmware

In caso di tentativo di inserzione di codice il Symbiote percepisce il cambio del comportamento e blocca l'azione

In caso di tentativo di rimozione del Symbiote, il device va in blocco

AGENDA

- Introduzione: il mondo VOIP
- Attacchi VOIP
- Frodi nel VOIP
- Contromisure
- ZRTP
- Symbiote
- Conclusioni

Conclusioni

- Il VOIP si diffonde sempre più e si integra sempre più con le reti e questo lo rende più suscettibile di attacchi e sfruttamento per azioni criminali.
- Pensare ad una difesa del VOIP separata dalla difesa del resto della rete è un approccio sbagliato
- Non esiste una rete VOIP sicura a priori. Così come le reti dati anche la rete voce necessita di un continuo aggiornamento delle tecniche di difesa
- Anche tra gli addetti ai lavori deve crescere la sensibilità alla protezione dei servizi VOIP data la delicatezza delle informazioni che viaggiano tramite la voce e ai danni economici da affrontare in caso di attacco