Digital Forensics Alumni

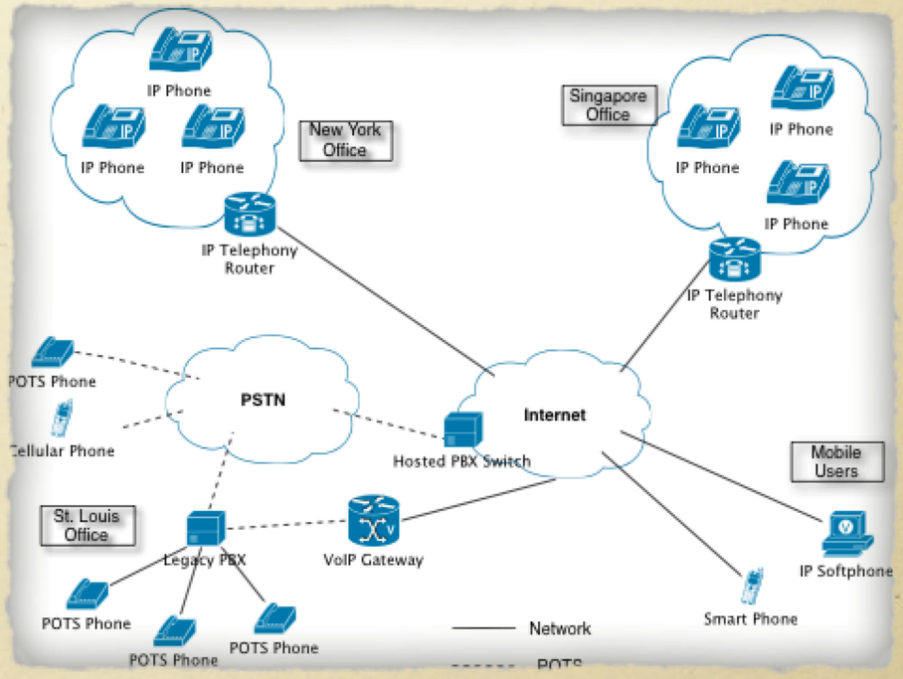
OPEN DAY 2015

VoIP e UC Forensics

spunti di riflessione sulla sicurezza della comunicazione unificata al tempo del Cloud

Marco Carlo Spada - m.c.spada@mash.it - *2/7/2105*

1871-2015
cos'è cambiato?

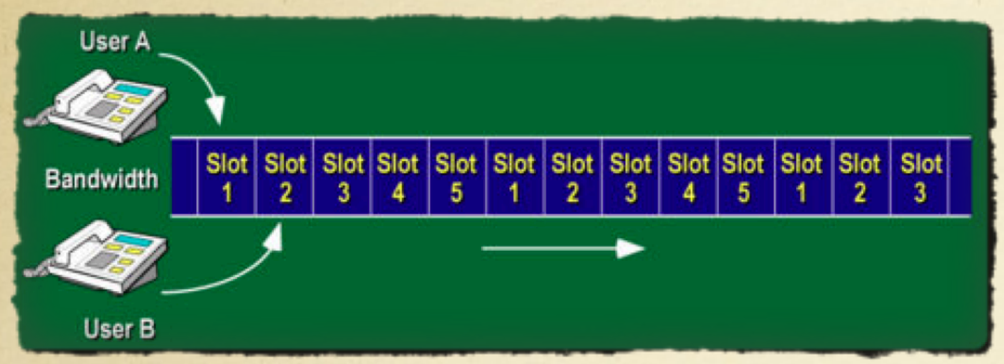


VoIP e UC forensics - Marco Carlo Spada

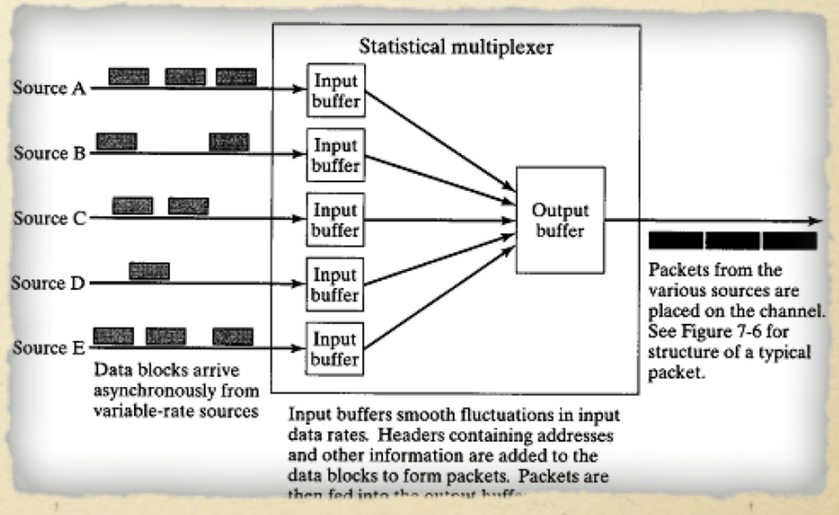
Digital Forensics Alumni OPEN DAY 2015

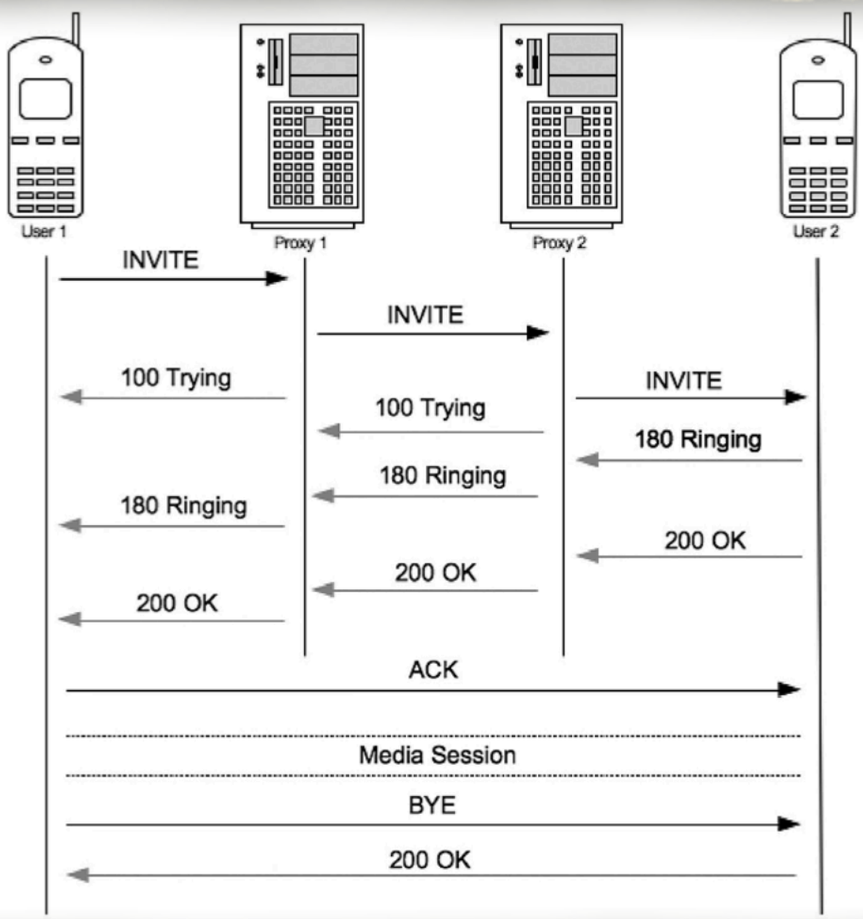

dall'intervista all'ing.
Giuseppe Cappelli
Napoli
2010
(Archivio storico Telecom Italia)

TDM: time division multiplexing



STDM: statistical time division multiplexing





- prima fase: segnalazione
- seconda fase: “media session”

UC e VoIP sono “applicazioni”…

- DHCP, DNS, TFTP, BOOTP, CDP, RADIUS, NTP, SNMP, HTTP(S), TLS/SSL, STUN,
- SIP, H323, SCCP
- RTP, SRTP

…che forniscono i seguenti servizi:

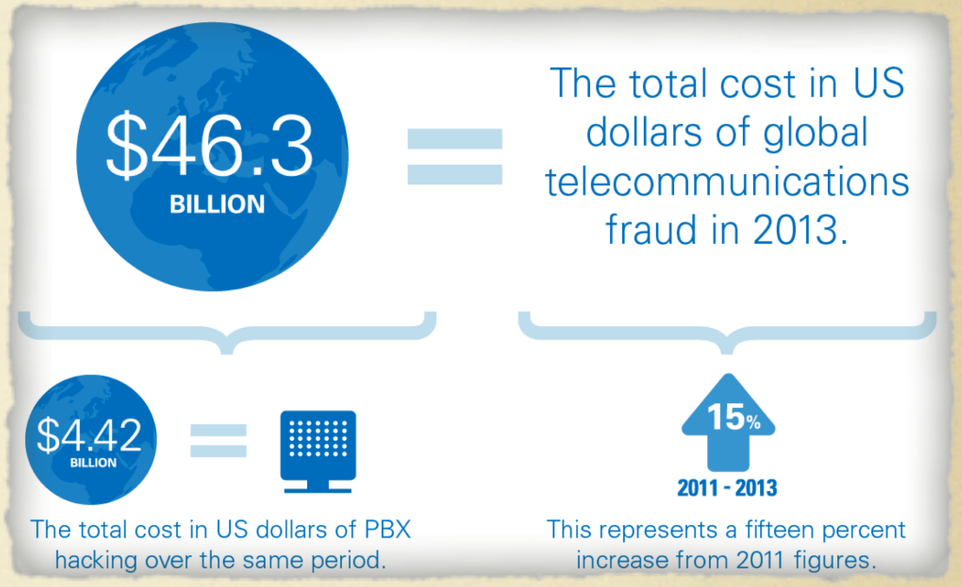
- “di terminale”: follow-me, dnd, wait, call-transfer, conference, page
- “di centrale”: DISA, Voice-Mail, AA, IVR, ACD, CTI, DID

Il tutto “sopra” i protocolli:

- L4 (in prevalenza UDP)
- L3 (IPv4 - IPv6)
- L2 (IEEE 802.3, 802.1x, 802.1q, 802.11)

Minacce contro i sistemi di telefonia

- Furto di chiamate (toll fraud)
- Intercettazione delle chiamate
- Spoofing del chiamante
- Voice Spam/Phishing/Stalking
- TDoS - Denial of Service Telefonico
- Furto di dati: log delle chiamate, rubriche telefoniche, registrazioni in casella vocale)



Queste minacce valgono indistintamente sia per gli impianti su IP che per gli impianti basati su PBX proprietari. Però riguardo al traffico di rete (protocollare e di comunicazione) alle vulnerabilità relative ai dispositivi (PBX e teminali) si aggiungono tutte le vulnerabilità relative ai servizi di rete su cui essi si appoggiano.

Come esempio:

- http://spectrum.ieee.org/telecom/security/the-athens-affair

> Five weeks after the first messaging failures, on 4 March 2005, Ericsson alerted Vodafone that unauthorized software had been installed in two of Vodafone's central offices. Three days later, Vodafone technicians isolated the rogue code. The next day, 8 March, the CEO of Vodafone Greece, Giorgos Koronias, ordered technicians to remove the software.

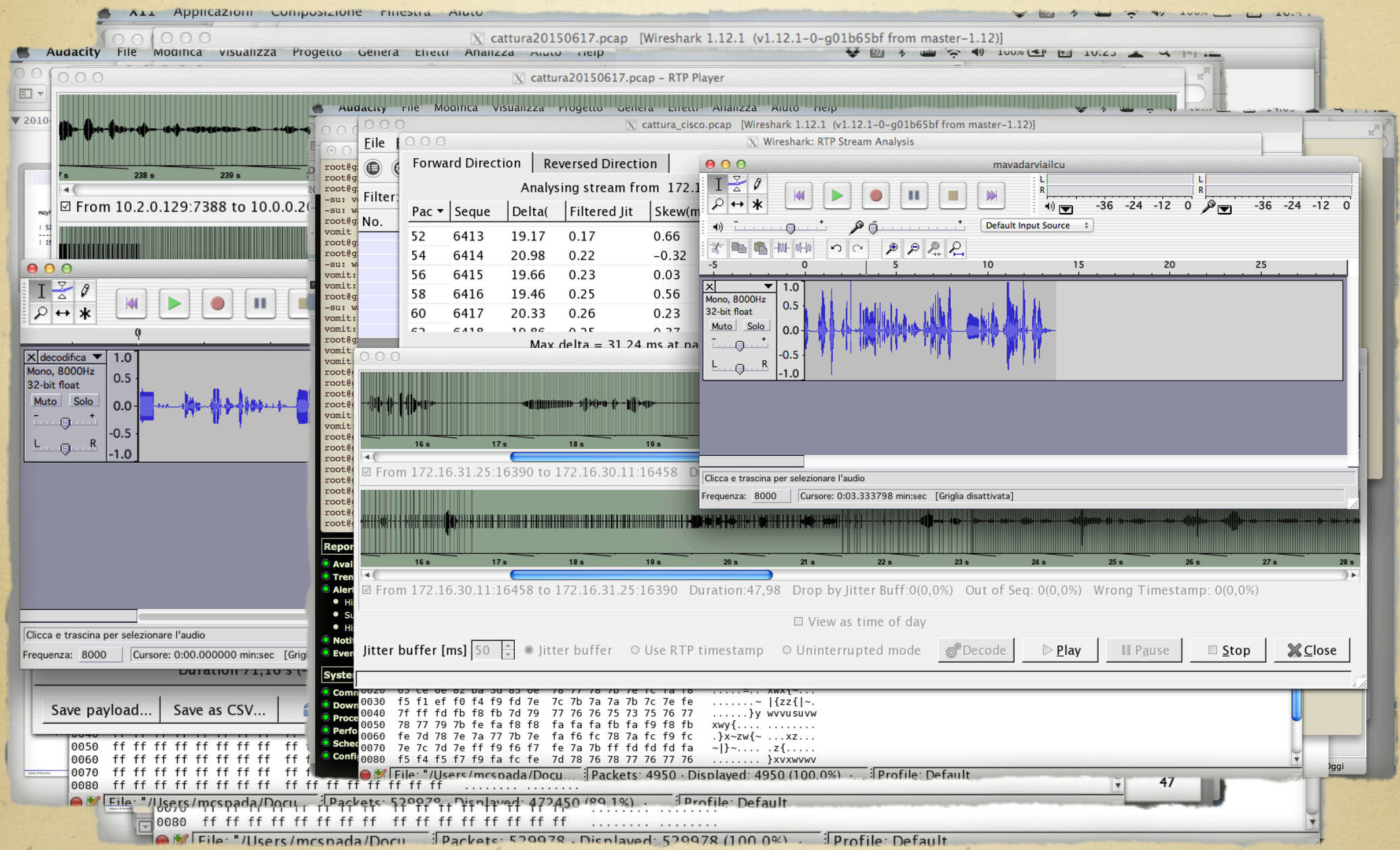
- Vulnerabilità CVE-2012-5445 (17/10)

Possibile intercettare telefoni VoIP Cisco

Una modifica al vostro telefono VoIP Cisco lo può trasformare in uno strumento per intercettazioni remote. Ancora più preoccupante è il fatto che - a differenza delle vulnerabilità di sicurezza che riportiamo ormai sempre più frequentemente - Cisco non ha ancora trovato una soluzione al problema.

I telefoni VoIP Internet venduti da Cisco Systems, sono infatti vulnerabili ad attacchi che permettono di **attivare un'intercettazione remota e ascoltare le telefonate private, oltre a far diventare il telefono una sorta di cimice o microspia per ascoltare le conversazioni che si tengono nella stessa stanza in cui è posizionato il telefono**.

Proof of concept…

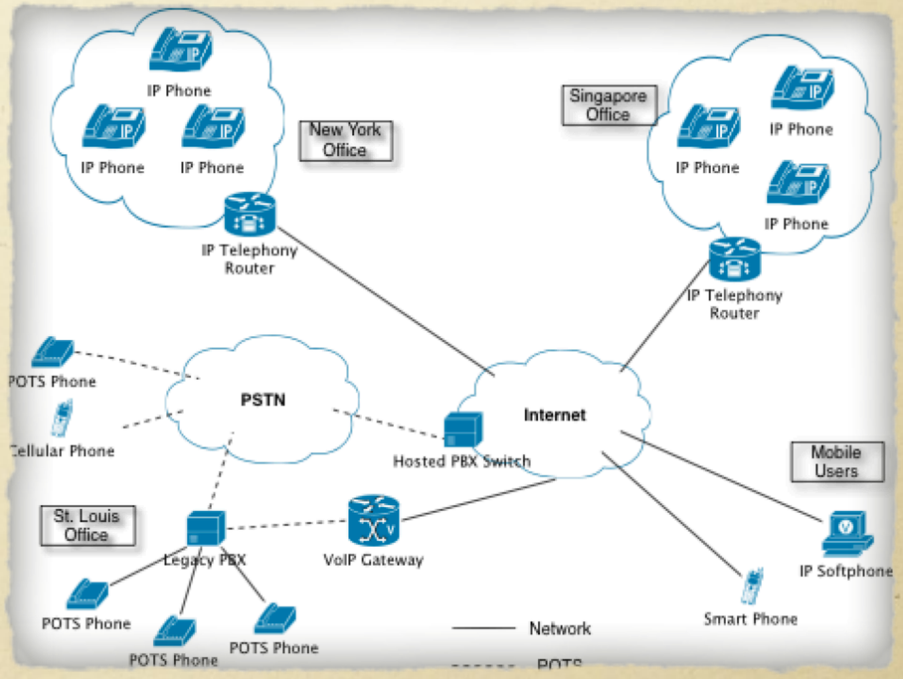


Conclusioni

- considerazioni sotto il profilo della sicurezza:
  - la sicurezza del sistema dipende prevalentemente da quella dei servizi su cui poggia
  - in caso di installazioni distribuite vanno usate le VPN o sistemi di crittografia
  - in installazioni su fornitori esterni (es. PBX in Cloud) va concordata
  - PBX e terminali possono essere oggetto di attacco

- considerazioni sotto il profilo della forensics
  - gli impianti VoIP si “prestano” ad intercettazioni sui nodi
  - PBX e terminali possono essere esaminati per raccogliere elementi di prova

1871-2015
cos'è cambiato?



VoIP e UC forensics - Marco Carlo Spada

Digital Forensics Alumni OPEN DAY 2015

Riferimenti bibliografici

Pubblicazioni:

- PBX Security and Forensics, A practical Approach - Iosif I. Androulidakis - Springer
- Hacking Exposed: Unified Communications & VoIP Security Secrets & Solutions - Mark Collier, David Endles - MacGraw-Hill
- Unified Communications Forensics - Nicholas Grant & Joseph W Shaw II - Syngress

Siti:

- http://www.litaliachiamo.it/242/come-funzionava
- http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab09/clb09.pdf
- https://github.com/sandrogauci/sipvicious
- http://www.viperlab.net/tools/vast
- http://spectrum.ieee.org/telecom/security/the-athens-affair
- http://www.telefonosottocontrollo.com/intercettare-telefoni-voip-cisco/
- https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-5445
- https://en.wikipedia.org/wiki/Comparison_of_VoIP_software
- https://www.overthewire.com.au/news/how-to-protect-yourself-from-toll-fraud


That's all Folks!