



23C3 – Berlin 2006
Who can you trust?



VoIP (in)security

through OSS tools and real life news

Alessio L.R. Pennasilico
mayhem@alba.st
<http://www.recursiva.org>

Security Evangelist @ alba.st
Board of Directors or Hactivist of :
AIPSI, AIP, Italian Linux Society, ISSA,
LUGVR, Metro Olografix, Recursiva.org,
OpenGeeks/OpenBeer, Sikurezza.org,
no1984.org, Italian Pirat Partiet,
Spippolatori, CLUSIT, IT-ISAC, VoIPSA.

VoIP Risks are real



Cpt. Crunch explained why telephony world was(is) very vulnerable. Nowadays many people think VoIP is safe as telephony ... **WRONG!**



Real risks exist, on traditional and IP telephony, and were on newspapers' first page:

- × **VoIP specific tools to attack VoIP infrastructures**
- × **E.A. Pena arrested for selling stolen VoIP traffic**
- × **Criminals eavesdropping Greek Vodafone cust.**



VoIP multiplies the risks of phone nets and IP nets.

Phones use DHCP, TFTP, UDP flows, often no auth, usually data is in clear text ... :0

So many “legacy” IP tools are working out of the box: ettercap (hi naga ;P) , tcpdump, wireshark (formerly ethereal), netcat, nmap and so on ...

... but VoIP one's works better!



Oreka eavesdrops many protocols and codecs.

Everything is stored in a MySQL db and it has a nice web interface to query the db ;P

Ohrwurm is a fuzzer ...

we know it works (really) too fine :(

netcat = **sipsak**, nemesis = **scapy**, nmap = **smap**,
nessus = **sivus**, and so on ...



Packet Gen & Packet Scan

Shoot

Sipness

Sipshare

Sip scenario

Siptest harness

Sipv6analyzer

Winsip Call Generator

Sipsim

Mediapro

Netdude

SipBomber

RTP Flooder

Invite flooder

RTP injector

Sipscan

reg. hijacker eraser/adder

Fuzzy Packet

Iax Flooder

Cain & Abel

SipKill

SFTF

VoIPong

SipP



- ✓ **Pay attention to risk analysis and planning!**
- ✓ Divide in multiple VLAN
- ✓ Implement QoS
- ✓ Be extremely careful in AAA
- ✓ Use cryptography ! (TLS, SRTP)
- ✓ Use “clever” devices (can mitigate mitm, garp, spoofing, flooding and other known attacks)
- ✓ Application level Firewall
- ✓ Avoid single point of failure



<http://www.voipsa.org>

<http://www.voip-info.org>

<http://misitano.com/pubs/voip-ictsec.pdf>

<http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58.zip>

http://www.it-observer.com/articles/1134/tackling_voice_security_threat

<http://www.webcrunchers.com/crunch/esq-art.html>

<http://www.nytimes.com/2006/06/08/technology/08voice.html>

<http://www.schneier.com/blog/>

<http://www.cloudmark.com/press/releases/?release=2006-04-25-2>

<http://www.usdoj.gov/usao/nj/press/files/pdffiles/penacomplaint.pdf>

<http://www.usdoj.gov/usao/pae/News/Pr/2005/feb/Moore.pdf>

Scholz - Attacking VoIP Networks



23C3 – Berlin 2006
Who can you trust?



Thank you!

**Questions, maybe answers,
and beers will be in the lounge ;P**

Alessio L.R. Pennasilico
mayhem@alba.st

These slides written by Alessio L.R. Pennasilico aka mayhem. They are subjected to Creative Commons Attribution-ShareAlike 2.5 version; you can copy, modify, sell. "Please" cite your source and use the same licence :)