hackers 2 hackers conference III

voip (in)security

luiz eduardo
cissp, ceh, cwne, gcih

H2HC

who am I?

- networking guy
- security guy
- employed by Aruba Networks
- wlan network for defcon, blackhat & ccc
- regular speaker at cons
- founder, dc55.org
- and...

agenda

- intro
- voip a, b, c...
- protocols
- architectures
- attacks
- vowlan
- tools
- conclusion

before we start....

```
    szPassword[i++] = ch;
    _putch( '*' );
>   } while( 1 );
```

intro

- voip
  - not that new.... being developed since the early 90s
- why voip?
  - save $
  - pstn integration
  - save $
- why voip security?
  - people USE IT (regardless if they know/want to or not)
  - because iphreakers are out there & technology is accessable (just like back in the day)
  - security practices are undergoing development
  - “sometimes” security isn’t top priority

voip a, b, c...

- voip : voice over internet protocol
- endpoint : softphone/ hardphone
- call : has a signaling and a media channel
- poe : anyone?
- pstn : public switched telephone network
- gateway = a bridge between two different voice network types
- directory services = translates an “alias” to an endpoint device

protocols / signaling

- sip: session initiation protocol
  tcp/udp ports 5060/5061
- sccp: skinny client control protocol
  tcp 2000/2001
- rtcp: real-time transfer control protocol
  dynamic udp
- mgcp: media gateway control protocol
  udp 2427/2727 – for pstn integration

protocols/ media

- rtp: real-time transport protocol
  udp 5004
  (it's got problems with nat-t, so use STUN)
- srtp: secure rtp, uses AES

h.323

“Some kind of high powered mutant never even considered for mass production. Too weird to live , and too rare to die”

ok, it did go to mass production, but, from what movie is this quote from?

h.323

- signaling
  - h.235 (security)
  - h.225 + q.931 (management)
  - RTCP

- media
  audio/ video: RTP

codecs

* too many... seriously...

http://www.voip-info.org/wiki-Codecs

architectures

- intelligent endpoints
  - i.e: h.323, sip
- device control
  - i.e: sccp, mgcp
- p2psip
- hybrid

attacks

- knowing your enemy...
- network/ voip attacks according to cia triad
- vowlan
- social threats

footprinting

- samspade
- google + google hacking
- ending-up on the company's website
  job-listings, switchboard phone number, etc...

  www.hackingvoip.com
- nmap (what option should be used?)

what for??

enumeration, what is out there?

- names
- extensions
- configuration

use netcat... sip is similar to http
filenames can give out important info
config files can give out MORE important info

- and, never forget SNMP...

so.... what are the 3 well-known security principles?

- confidentiality

- integrity

- availability

confidentiality attacks

- eavesdropping
  - problem: it's "sniffable", recordable, redirectable
  - (possible) solution: encryption for the media channel
- enumeration
  - problem: send messages to the servers (i.e. sip via nc) / configuration transferred by tftp/ftp, filenames
  - (possible) solution: encryption for the signaling channel / protocol change ☹

integrity attacks

- caller-id spoofing
  - problem: easily spoofable/ not always checked / systems rely on caller-id for authentication (i.e. cellphone voicemail)
  - (possible) solution: not trust caller-id(s)
- signaling manipulation
  - problem: malicious signal injection / call redirection/ call teardown/ endpoint freak-out
  - (possible) solution: encryption for the signal channel / change protocol to use authentication

availability attacks...

- amplification attacks
  - problem: smurf-attack like problems
  - (possible) solution: use of authenticated protocols/ rate-limit /shapping
- protocol fuzzing
  - problem: some of the stacks on endpoints (mainly hardphones) are somehow imature / phones reboot/ freeze, etc...
  - (possible) solution: open-source soft phones and hard phone firmware, check forums/ mailing lists

...availability attacks

- flooding
  - problem: send lots of voip signaling packets or simple network packets (i.e: tcp syn) / device crash/ call quality problems, etc...
  - (possible) solution: protect/ firewall the voip infrastructure, rate-limit / shaping
- signaling manipulation (again)
  - problem: malicious signal injection / call redirection/ call teardown/ endpoint freak-out (again)
  - (possible) solution: encryption for the signal channel / change protocol to use authentication (again)

vowlan

vocera
Sprint
Pocket PC
onex
symbol
Avaya IP Softphone
Pocket PC
NOKIA
Avaya one-X
AVAYA
onex
Menu
Back
NOKIA
Wireless IP
03/22 火
10:21
CLR
END
SymPhone
View Tools Help
(425) 467-9485
Ready (Global)
1
ABC 2
DEF 3
GHI 4
JKL 5
MNO 6
PRS 7
TUV 8
WXY 9
*
0
#
AVAYA
onex
space

vowlan

- wlan problems are the same
- voip problems don't change either
- combine both... and...
- but, people are gonna use it.... why? $$ and many options (dual-mode phones/ pdas / even softphones)
- people love cellphones, but not the bill
- concerns: QoS being addressed in 802.11e and management frame security/encryption 802.11? (anyone?)

vowlan – identity awareness is key

service delivery based on who, what, when, where and how

- Identity aware
  I am Matt Green, the employee
- Device aware
  I am Matt Green with a laptop with no viruses or worms
- Traffic aware and QoS
  I am Matt Green with a laptop using a soft phone with QoS
- Time aware
  I am Matt Green with a laptop using a soft phone with QoS at 1:40 pm
- Location aware
  I am Matt Green with a laptop using a soft phone with QoS at 1:40 p.m. in the clinic

social threats

- spit
  spam over internet telephony
  - impersonation (phone)
  - sometimes contacts are obtained by account harvesting, enumeration
  - different from spam, interrupts the user immediately
- voiphishing
  collect people's information (HOW?)
  - mitm
  - eavesdropping
  - impersonation again (email)

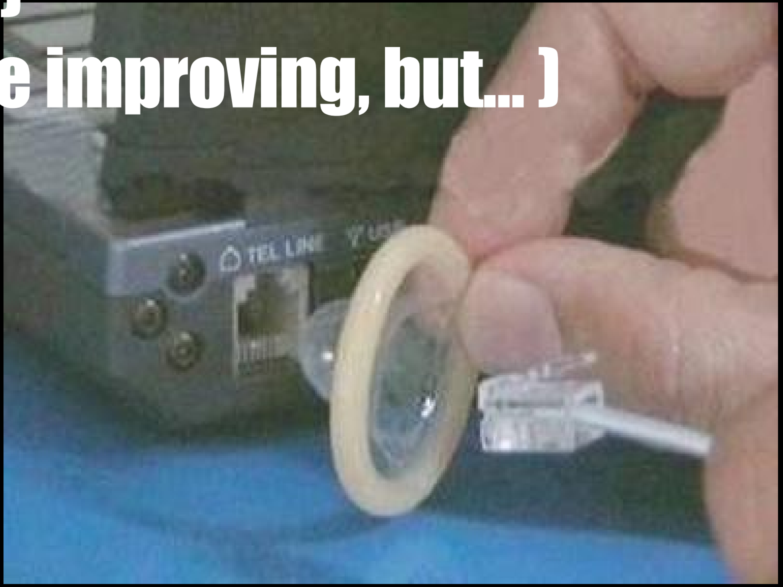
ok, ok, but HOW???* or trixbox + social engineering

tools

- eavesdropping: wireshark , cain & abel, vomit,
- directory enumeration: sipcrack, enumiax, sipscan
- caller-id spoofing: most softphones, spoofcard.com (some providers allow pstn access based on caller id)
- signaling manipulation: sip-redirectrtp + rtpproxy (for mitm)
- flooding: scapy, inviteflood, iaxflood, udpflood, rtpflood
- fuzzing: PROTOS (for SIP, HTTP, SNMP), ohrwum - rtp, fuzzy packet rtp w/ arp poisoner, etc
- amplification: scapy or any packet (re)player
- forced call teardown: most are sip bye injection tools

conclusion/ use protection

- when possible, secure the voip network infrastructure and the bounderies via security policies
- encryption (and try to make it based on voip mechanisms)
- authentication (where you can)
- protocol challenges (things are improving, but...)
- don't trust caller-id(s)
- traffic shapping
- zfone
- and let's not forget, privacy....



quem quer dinheeeiro?

- sip ports?
- sccp? (not the certification, the protocol)
- old name for wireshark?
- opensource tool shown on Matrix Reloaded?
- what tool was used to exploit the system?
- on Matrix 1, what's Neo's apartment number?
- what's the name of the famous "hacker quarterly" magazine?

][@#]@[*^&@^#

comments/ questions?

obrigado!

luiz eduardo

luiz [at] arubanetworks.com