AAPL – Automated Analog Telephone Logging.

Using modern techniques and software to map the PSTN.

- Da Beave & Jfalcon -
Da Beave

• Work in the network security field @ Softwink, Inc.
• Author “Asterisk Hacking” and “Threat Analysis 2008” – Syngress Press
• Hacker/Programmer
• Author of iWar and various other “hacking” tools (X.25 tools, etc)
• Founder of 'Telephreak' (loose knit Asterisk/VoIP hackers).
• Check out www.telephreak.org (The BBS!)
• Founder of “The Deathrow OpenVMS cluster”
JFalcon

- First Federally Convicted Hacker in Alaska (1994)
- Professional consultant and hired gun to Fortune 500 companies
- Experimenter, Hacker and Inventor
Brief history....
Yes, we know who we're talking to......
“Hand scanning”

• Very slow....
• Pick up the phone dial and listen.
• Can be accurate, but that largely depends on the “hand scanners” knowledge base.
• Still a popular pass time for phreaks.

(See http://www.handscan.net)
Automated Wardialing (Old School)

- 1980's .....
Made you this guy....
Historical Problems with Automatic Wardialing

- Typically relied on standard PSTN/POTS connections. Telcos monitor for over utilization of their service and “flag” the line for further investigation.

- In some cases they'd shut down your POTS line leaving you to explain what you where doing.

- Modems are lame. Scan for carriers (data) or tones/fax. Multiple scans. You are limited by your hardware.

- Later generation CTI hardware? Cost prohibited then, now obsolete (ISA boards!) and need PRI.

- Sure – things like randomly dialing/random timing help, but still you end up missing a lot.
Still the 80' but enter the AppleCat

- Could generate and detect tones. Good for boxing and for this talk War dialing.
- Software like Cat's Meow/Phantom Access.
- Expensive and proprietary API (Later Firmware emulated Hayes command set.
- We'll talk about this later...
2002'ish. We can do it better. Sorta....
Enter VoIP: Less problems/different headaches. (The good)

• The world is your oyster. Cheap calls even if they supervise. If they don't, free or next to nothing.

• No longer bound to physical POTS lines.

• Less monitoring (in most cases).

• More calls and more “lines”.

• Still interesting things out there! (Routers, X.25 networks (you read that right), SCADA systems, Old school BBS's). Yup.
Enter VoIP: Less problems/different headaches. (The bad)

• Still bound to a crappy modem.
• Don't care how good it is......Do you really want to sit and listen to a modem?
• Not everything interesting has a carrier or tone.
• What software will you use?
• Sure, THC-SCAN and TONELOC rock... but what if you want to store to a database? Or lookup data on the tubes?
... and now a side note …

- 2004'ish I was doing a pentest which I needed some war dialing foo.
- Most *nix based “War dialers” blow.
- Didn't want to load a DOS emulator to run TONELOC.
- I'm certainly not going to “buy” commerical software.
- Besides, it's a war dialer. It'll only take me a week or so to complete.. Right?
iWar (Intelligent Wardialer - 2005)

• *nix based (OpenBSD/Linux/etc...)
• Written in C/ncurses frontend
• Tone location (like Toneloc)
• No limitation on the number of devices.
• MySQL/PostgreSQL/ASCII output support
• All your standard 80's bells/whistles.
• FTW! Errrr.. not quite...
ATA+Modem = Your technique is weaksauce.
This is the way we roll...errr.. rolled...

• An Old School wardialer with some chest hair!
T1/DS1 + Asterisk + VoIP == 48+ line modem bank in your face.

- Standard Asterisk -> Internet setup. T100P/Asterisk supplies the “telco” to the AS5200 (24 channels).
- *2 T100P == 48 channels.
- T100P connects via T1 loopback cable to AS5200. AS5200 is “fooled” into have PRI.
- iWar connects to AS5200 via TCP/IP. Modems are on different ports.
T1/DS1 + Asterisk + VoIP ==
48 line modem bank in your face (The good)

• 48+ modems in one box. Shotgun methodology!
• No crazy cabling!
• iWar get TCP/IP functionality!
• The fact that we're using a AS5200 isn't important.
• When ISP's fail your modem capacity goes up ($20.00 bucks for a AS5200).
• iWar uses local & remote modems all the same! Doesn't matter if the modem bank is local or across the Internet in Russia!
T1/DS1 + Asterisk + VoIP ==
48 line modem bank in your face (The bad)

• Limited by bandwidth for VoIP
  — but you always will be.

• YOU'RE STILL USING F*CKING MODEMS!
  • JUST MORE OF THEM!
But maybe there's a smarter way. (what the Applecat did right)

• It allowed you to scan for modems and tones at the same time.

• It had rudimentary voice detection and could detect clicks, beeps and buzzes.

• One NPA scan and you were fairly done (no rinse and repeat).
VoIP + DSP == PIMP

• VoIP + DSP isn't a new idea. We've seen lots of semi-working and poor implementation.
  • For example, trying to tie VoIP raw audio with software based modem. Cool idea, more than modems out there.
    • iWar has had IAX2 support, but it's been weak (no real DSP).
  • Then we ran into HD Moore (of Metasploit fame) and his Warvox project......
VoIP + DSP == PIMP

• Warvox uses a dialer (IAX2 protocol) to dial/record calls.
• A Ruby backend does the analysis (to look for tones/fax/modem/etc).
• Works as part of the Metasploit frame work.
• Working with HD Moore, iWar does the same thing – Just in C, and without the really nice GUI frontend/graphics. (iWar is curses, remember?)
Warvox Screen Shot (job)
Warvox Screen Shot (analysis)
VoIP + DSP == PIMP

• With iWar we decided to use a “signature” based system.

• Basically a configuration file to tell iWar “what to listen for”.

• Uses KissFFT (Fast Fourier Transform) – like Warvox, for back end signal processing.

• Since both write to “raw” files, it's easy to move iWar generated audio files to Warvox for reporting.
iWar/Warvox.

• You no longer need hardware!
• All VoIP/DSP work is now done in software!
• Detect modems, fax, clicks, tones... whatever......
iWar: Where do we go now?

• Limited to IAX2.
• Adding SIP support for both iWar and Warvox. Shouldn't be that bad. (PJSIP). Just need to dedicate the time.
• Backspoofing? iWar can do CNAM lookups via the Internet, which varies in accuracy. True backspoofing for real CNAM lookups.
• Speech to Text technology. Lumenvox, for example (“Hello?”... “Domino's Pizza”). HD has played with this.... easy enough...
• Software based “modem”.. to connect and banner analysis....
Improving Your Hit Ratio

• Backspoofing/CNAM dips/NANPA lookups:
  • Know before you dial.
  • Business/Residential/Government.
  • Able to identify Telco owned lines and Cellular carriers.
Improving Your Hit Ratio

• Better Tools = Better Results:
  • VoIP carriers allow multiple outbound trunks.
  • iWar/Warvox – One Scan == Multiple Results
  • Speech to Text processing way better now…
  • Database Backend = Ability to “Data mine”
Improving Your Hit Ratio

- Better Hardware:
- Just carriers? Setup a modem bank!
- Asterisk + chan_mobile: Use those free nights and weekends! (Bluetooth <-> DAHDI)
- Any FPGA/Embedded Hackers out there? Massive DSP processing power now…
Highway to hell passes through Capital Hill.

• Legislation against “CID spoofing” ongoing in various states and federal levels (iWar/Warvox supported).

• Single party consent and recording. iWar/Warvox “record” the call then analyze the audio. Violation?

• “Do Not Call” list / VSP’s terminating service – Go International! (Globalization)
CVS iWar now....
(a shameless plug)

- MySQL/PostgreSQL
- CNAM lookups
- IAX2 support (SIP soon?)
- TCP/IP remote mode (w & w/o authentication)
- HTTP based logging (log numbers over the tubes)
- Banner detection
- Save state/load state

- Random/Seq. Dialing.
- Random Timing between dials
- Traditional “tone” detection (serial/TCP)W/ serial true modem control (CTS/RTS)
- DSP/IAX2 with signature based configuration.
- Just to name a few....
Getting the WaR3Z

Warvox:
http://www.warvox.com

iWar:
http://www.softwink.com/iwar

(Probably best to use CVS code. CVS instructions are on the site)
Video: What's still out there!  
(Where's the popcorn)

Presentation location:
http://www.telephreak.org/DC17/defcon.pdf

Presentation movie location:
http://www.telephreak.org/DC17/defcon.mov