Voip Security Tools & Attacks

Shawn Merdinger

CONfidence Security Conference
Krakow, Poland
12 May, 2007

Obligatory Speaker Slide

- Shawn Merdinger
- Independent consultant & security researcher
- Past employment
  - Cisco Systems Security Technologies Assessment Team (STAT)
  - Tippingpoint's Digital Vaccine Team
- Current projects
  - Consulting with SecureLogix (VoIP security assessments and pen-testing services)
  - Cisco Press technical editor
  - VOIPSA Technical Advisor, etc.
- Personal website: www.voipninja.com

Thoughts so far…

- Wow! Krakow, Poland is so cool and I expect a bright future for information technology here!
- A special ‘thank you’ to CONfidence staff ☺
  - Fantastic speaker treatment!
    - Flights, meet at airport, apartment, dinner and drinks, checking to make sure everything is OK
    - Awesome communication all the way!
- No “politics” talk is a good thing…
  - We are technical people sharing academic information to enable better security for systems

Objectives Today

- VoIP Technology Overview
- VoIP Security Risks and Attack Examples
- VoIP Security Tools

Key Points

- My focus is on SIP protocol and product vulnerabilities
- All information today is public
- No exploits released in this presentation
- Several Cisco examples but not “beating up” Cisco!
- Please use information in legal and ethical manner ☺

Why Should We Care?

- VoIP on your desk in business, home, hotel
- “Usurping 100 years of trust” in traditional telephone reliability and dependability
- Scary attacks
  - Quiet, stealthy, targeted attacks for espionage
  - DoS phone systems in critical times
    - After Hurricane Katrina - VoIP very important (google search: voip katrina site:.mil)
    - US school VoIP phone alert systems in every classroom (school shootings, etc.)
- Typical IT attitude and vendor sales materials say “VoIP is just another network application”
  - So, VoIP phone calls are about as secure as email ☹

What comprises a VoIP system?

- VoIP = Voice Over Internet Protocol
- Signaling = Call setup
- Media = Call voice stream content
- Endpoints = Phones (soft, hard, wifi, dual-mode)
- Network Services = Infrastructure, TFTP, routers
- Call control = Call setup, tear down, manage
- Directory servers = user/number lookups, etc.
- SBC = Session Border Controllers for trust boundaries at carrier/provider level
  - Note: very few SBC vendors – “Acme Packet” is biggest

What do we mean by VoIP?

- Skype
- Google, Jabber, Dialpad
- Vonage, Sunrocket
- Asterisk geeks
- SMB - LinksysOne, etc.
- Residential cable/DSL VoIP part of “triple play”
- Enterprises
- Call centers
- Illegal VoIP!
  - China, India, Latin America, Bangladesh, etc.

Bangladeshi VoIP operator hiding in New York?

March 2, 2007 · In: **VoIP Regulation**

The continuing VoIP shutdown in Bangladesh can apparently be attributed at least partly to a change in ruling parties. One of the

What is the VoIP attraction?

- Cost cutting
  - Long distance
- Collaboration, presence, conference calls
- Integration with office productivity suites like Microsoft Office 2007
- Gaining momentum in all areas
- Showing up on television shows like Fox *24*
  - Chloe's VoIP security video clip ☺

What Protocols?

- Signaling
  - SIP – Session Initialization Protocol
    - Most popular, clear text, HTTP-like
  - SDP – Session Description Protocol
    - SDP is encapsulated within SIP
  - MGCP – Media Gateway Control Protocol
  - SCCP “Cisco Skinny”, Nortel UNISTIM, etc.
  - H.323, etc.
- Media
  - RTP and Secure RTP – Realtime Transfer Protocol
- IAX2 - “eeks” - Asterisk combined signal/media

Security Issues - General

- All built on top of commercial OS
  - Linux, Windows, Vxworks, etc.
- Poor security design, patching, processes
- Dependent on other software and services
  - Web servers, TFTP, DHCP, etc.
- Inherit network issues like layer 2 attacks, ARP spoofing, etc.
- Latency is huge risk
    - More than 150 milliseconds delay = horrible sound
    - More delay as layers of security are added into networks

Social Engineering VoIP Attacks

- SPIT – SPAM over IP Telephony
  - Predicted to get bad...
- VoIP Phishing - “Vishing” to some
  - Already happening, Blackhat (Jay Schulman)
  - Used in conjunction with targeted emails, 800 #
  - Spoofing caller ID for call backs, etc.
    - Bank of America MP3 of vishing recording
- Google Maps - Click to Call
  - Crafty harassment tool
  - Connect two parties using your Web browser
    - Caller ID spoofed on both sides!
    - Web browser will show status

Attacks against VoIP Devices

- Problems with phones
  - Low memory, CPU, poor implementations & design
  - Flood SIP phones with INVITE requests, etc.
  - Attacking phone webservers, other services
  - “Standard” tools like Nmap can crash phones
- Problems with PBXs
  - Flooding TCP, SIP REGISTER, etc.
  - NAPTHA is your friend…
    - TCP state manipulation and resource starvation
    - Bindview RAZOR Team (Simple Nomad and others)
  - ISIC = IP Stack Integrity Checker (also IP6SIC)
    - Guaranteed to break something…really.

Hitachi WIP-5000

- Version and OS
  - V1.5.6 on Linux
- Vulnerabilities
  - **HTTP index page** discloses software version, phone MAC address, IP address and routing
  - **HTTP** no default login credentials
  - **SNMP** enabled, read/write using any credentials
  - **Undocumented open port TCP/3390** Unidata Shell
  - **Hardcoded admin login "0000"** on device keypad

  - Good vendor response and issues fixed
  - It's a high quality phone and my favourite!

- **Other phones' security issues....**
  - Interoperability, stability, quality, no vendor response, bricking phone during firmware upgrade, etc.

2007 VoIP Phone Vulns

- Cisco Unified IP Phone
  - SSH server with hard coded default admin account and default password that is used for debugging
- Linksys WIP 330 VoIP wireless phone crash from Nmap scan
- Cisco 7905 VoIP phone crashing from Dug Song's arpspoof (part of dsniff)

2006 Phone Vulns (by me)

- [Full-disclosure] Senao SI-7800H VoIP wireless phone wdbrpc debug service UDP/17185
- [Full-disclosure] Clipcomm CPW-100E VoIP wireless handset phone open debug service TCP/60023
- [Full-disclosure] ZyXel P2000W (Version 2) VoIP wireless phone undocumented port UDP/9090
- [Full-disclosure] ACT P202S VoIP wireless phone multiple undocumented ports/services
- [Full-disclosure] MPM HP-180W VoIP wireless desktop phone undocumented port UDP/9090
- [Full-disclosure] UTstarcom F1000 VoIP Wifi phone multiple vulnerabilities

And a few more (by me)

- [Full-disclosure] Senao SI-680H VoIP Wifi phone undocumented open port
- [Full-disclosure] Zyxel P2000W (Version1) VoIP Wifi phone multiple vulnerabilties
- [Full-disclosure] GrandStream GXP-2000 VoIP Desktop Phone multiple undocumented UDP ports and DoS
- [Full-disclosure] PolyCom IP-301 VoIP Desktop Phone HTTP server DoS and undocumented TCP port 42
- [Full-disclosure] Linksys SPA-921 VoIP Desktop Phone HTTP Server DoS

These are all low-hanging fruit across multiple vendors

Goal: Chum the waters to get security people interested

Attacks - Confidentiality

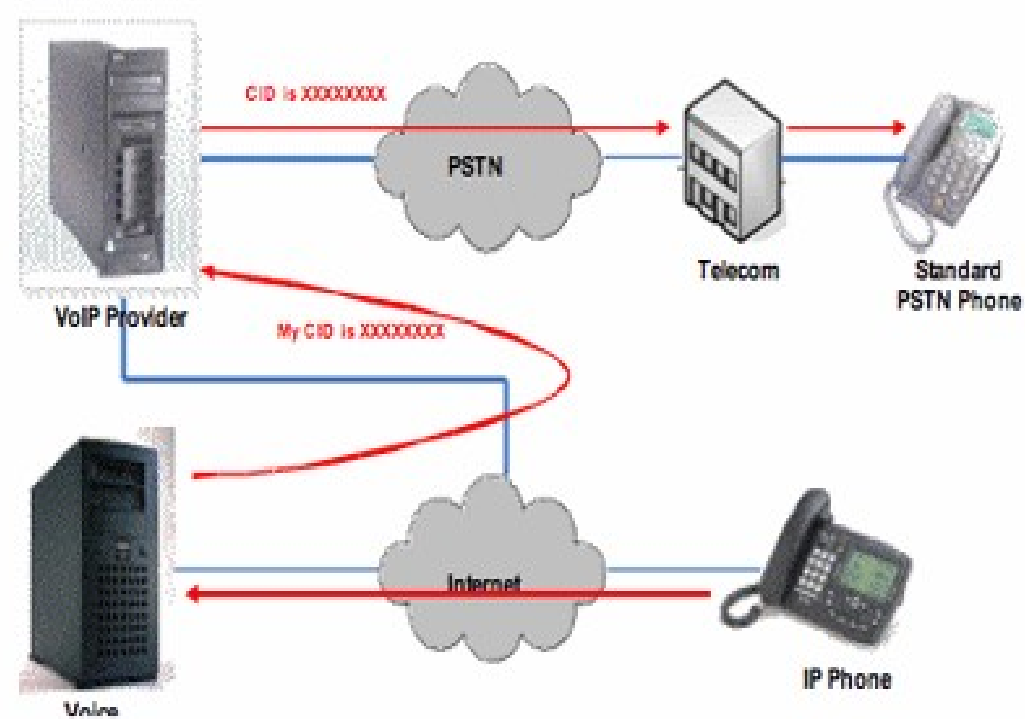
- Most VoIP media streams are unencrypted
  - Only 5% deployments use encryption at all (word of mouth)
  - RTP streams can be sniffed and converted to WAV using tools like Cain& Abel, Wireshark, VOMIT
- Archives of VoIP (banks, stock brokers, etc.) will become a very attractive attack vector
  - Biometric theft – *Sneakers* movie: “my voice is my password”
  - Extraction of sensitive information (DTMF tones)
  - Modification/deletion of recorded calls
  - Lack of encrypted call archives, secure storage, etc.

Attacks – Trojan images

- Trojan images
  - GPL people pushing vendors to release source
    - Example: Linksys WIP 300
      - Linux, ARM processor
      - Potential for custom attacker images, binaries, etc.
      - Nmap on a Linux based VoIP phone
        - Why is my phone scanning my network?
  - Softphones trojaned?
    - We can expect this very soon…probably this year

Attacks – Caller ID Spoofing

- Common today and trivial to execute
- Commercial services like spoofcard.com
- Roll your own with Asterisk and SIP provider



Attacks - Fuzzing

- Very beginning of this type of testing
- Many products impacted by protocol fuzzing
- Very few vendors engaging in proactive testing
  - Boundless, infinite testing space
- Many fuzzers released and specialized
  - Commercial: Codenomicon, Mu Security, Breakingpoint Systems (HD Moore)
  - Free PROTOS suites (SIP, SNMP, etc.)
  - Oracle Fuzzer (think VoIP archive servers here)

SIP Fuzzing Impact to Cisco

- Cisco Security Advisory: Multiple Product Vulnerabilities Found by PROTOS SIP Test Suite (Feb. 2003)
- Cisco Security Advisory: SIP Packets Reload IOS Devices with support for SIP (Jan. 2007)
- Cisco Security Advisory: Multiple Vulnerabilities in Cisco PIX and ASA Appliances (Feb. 2007)
  - “Inspection of malformed Session Initiation Protocol (SIP) packets”

VoIP Security Tools – VOIPSA List

- VOIPSA – Voice over IP Security Association
- www.voipsa.org
  - Non-vendor affiliated, open community effort
  - Mailing list, blog, best practices, threat taxonomy
  - VoIP Security Tool List
    - Maintained by Dustin Trammell and myself
    - Open source and commercial VoIP security tools
  - Divided into categories: Sniffing, Scanning, Flooding, Fuzzing, Media and Signal Manipulation, misc.
- **Bolded tools are what I recommend you start learning first**

Tools - Sniffing

- AuthTool - determine the password of a user by analyzing SIP traffic.
- **Cain & Abel – Sniff and reconstruct RTP media calls. (Windows)**
- Oreka - Oreka is a modular and cross-platform system for recording and retrieval of audio streams.
- PSIPDump - psipdump is a tool for dumping SIP sessions
- **VoiPong - VoIPong is a utility which detects all Voice Over IP calls on a pipeline (bootable CD)**
- VOMIT - converts Cisco Skinny into a wave file
- **Wireshark - Formerly Ethereal**

Tools – Scanning

- enumIAX - An IAX2 (Asterisk) login enumerator using REGREQ messages.
- SIP Forum Test Framework (SFTF) – Test devices for common errors – “SIP torture tests”
- **SIPcrack - SIPcrack is a SIP protocol login cracker.**
- SIPSCAN - SIPSCAN is a SIP username enumerator that uses INVITE, REGISTER, and OPTIONS methods.
- **SiVuS - A multi-use SIP scanner. (Windows)**
- SMAP - SIP Stack Fingerprinting Scanner

Tools - Flooding

- IAXFlooder - A packet flooder that creates IAX packets.
- **INVITE Flooder - Send a flurry of SIP INVITE**
- kphone-ddos - Flooding attacks with spoofed SIP packets
- RTP Flooder - Creates "well formed" RTP packets
- **SIPBomber - SIPBomber is sip-protocol testing tool**
- SIPNess - SIPness Messenger is a SIP testing tool
- SIPp - SIPp is a free Open Source test tool / traffic generator for the SIP protocol.
- **SIPsak - SIP swiss army knife.**

Tools - Fuzzing

- **Asteroid - a set of malformed SIP testcases**
- Fuzzy Packet - Fuzzy packet is a tool to manipulate messages through the injection, capturing, receiving or sending of packets generated over a network. Can fuzz RTP and includes built-in ARP poisoner.
- Ohrwurm - ohrwurm is a small and simple RTP fuzzer.
- **PROTOS SIP and H.323 Suites - malformed messages designed by the University of OULU in Finland.**
- **Sip-Proxy - Acts as a proxy between a VoIP UserAgent and a VoIP PBX. Exchanged SIP messages pass through the application and can be recorded, manipulated, or fuzzed.**

Tools – Signal Manipulation

- **BYE Teardown - spoofing the SIP BYE message from the receiving party.**
- RedirectPoison - monitor for an INVITE request and respond with a SIP redirect response, causing the issuing system to direct a new INVITE to another location.
- **Registration Adder - bind another SIP address to the target, effectively making a phone call ring in two places**
- Registration Eraser - denial of service by sending a spoofed SIP REGISTER message to convince the proxy that a phone/user is unavailable.
- Registration Hijacker - spoof SIP REGISTER messages to cause all incoming calls rerouted to the attacker.

Tools – Signal Manipulation (cont'd)

- **SIP-Kill - Sniff for SIP-INVITEs and tear down the call.**
- SIP-Proxy-Kill - Tears down a SIP-Session at the last proxy before the opposite endpoint in the signaling path.
- SIP-RedirectRTP - Manipulate SDP headers so that RTP packets are redirected to an RTP-proxy.
- SipRogue - a multifunctional SIP proxy that can be inserted between two talking parties

Tools – Media Manipulation

- **RTP InsertSound - this tool takes the contents of a .wav or tcpdump format file and inserts the sound into an active conversation.**
- **RTP MixSound - this tool takes the contents of a .wav or tcpdump format file and mixes the sound into an active conversation.**
- RTPProxy - Wait for incoming RTP packets and send them to a desired destination.

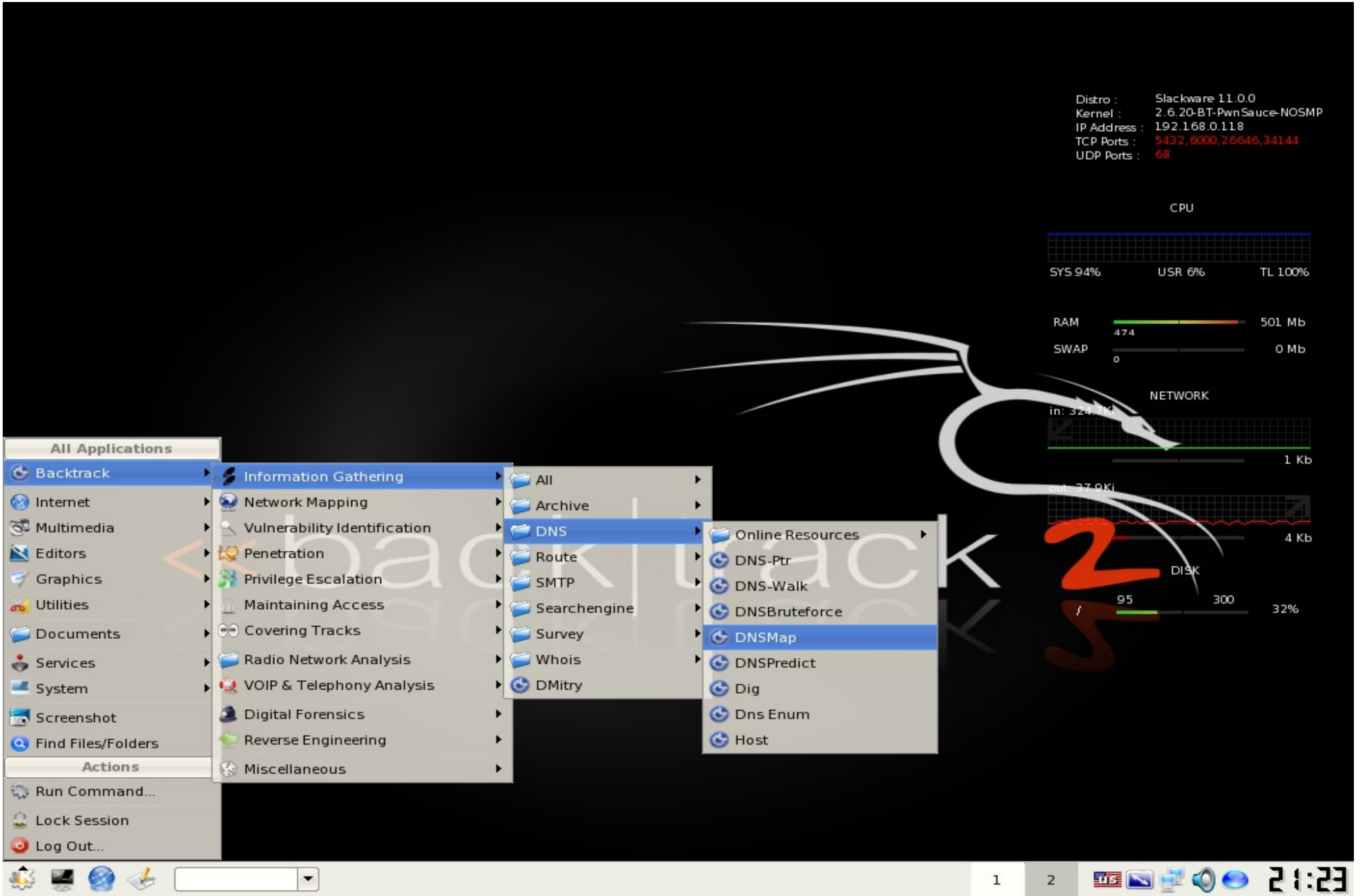
Tools - Other

- **iWar - IAX2 protocol Wardialer for Asterisk PBX**
- **SIP-Send-Fun - Sip Send Fun exploits specific vulnerabilities such as add/delete message waiting light on VoIP phones**
- **Spitter - A set of tools for Asterisk to perform VoIP spam testing.**

1st Linux Live CD with VoIP Tools

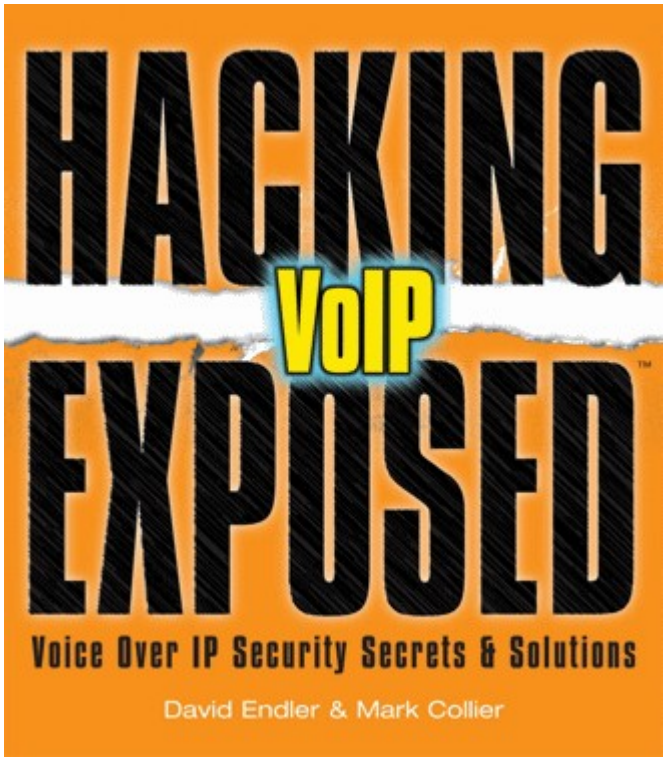
- Backtrack 2
  - Released with 5 VoIP security tools
  - SIPSak, SIPcrack, SIPdump, SIPp, SMAP
  - 300 other security tools
  - Bootable CD, does not touch hard drive
  - http://backtrack.offensive-security.com/

BackTrack 2 Screenshot



Book: Hacking VoIP Exposed

- By Dave Endler and Mark Collier
- Available now, and has a companion website
- Many tools are written by Mark Collier and Mark O'Brien from SecurLogix
- Solid book
- I may assist writing next one



Mitigation Strategies

- Call signaling – use TLS
- Call Media – use SRTP
- Secure management protocols and practices
- VLANs for IP phones, no TFTP if possible
- Careful with “VoIP aware” firewalls, IDS/IPS as this is a new market and effectiveness is questionable – plus latency impact
- Run tools and attacks yourself because your vendor most probably does not!
- Ask vendor which tools from VOIPSA they run ☺

Emerging trends in 2007

- Toll fraud by insiders (industry and company)
- More product vulnerabilities…duh…
  - iPhone (predict security issue 1 week after release)
  - Dual-mode VoIP phones unstable – Nokia E91, etc.
- Lots more attack tools, and refining of current tools, such as media injection and sniffing
  - Dustin Trammell, SecureLogix VoIP Team (including me)
- Espionage…of course
- US Military
  - New Pentagon VoIP deployment
  - Avaya VoIP call from general at Pentagon to pilots in F-16 attack jet en route to target…scary stuff

Thank you!

Questions?

Contact: shawnmer@io.com

www.voipninja.com