VoIP WiFi Phone Handset Security Analysis: We’ve met the enemy…and they built our stuff?!?

Shawn Merdinger

Security Analyst, TippingPoint

ShmooCon 2006

Obligatory Speaker Slide

- 8/05-present VoIP security analyst, TippingPoint, Division of 3Com
  - VOIPSA - www.voipsa.com
  - ZDI – www.zerodayinitiative.com
- 5/05-8/05 Independent security researcher
  - VoIP wifi phone started during this timeframe
- 1/01-5/05 Security researcher - Cisco Systems
  - STAT (Security Technologies Assessment Team)
  - SEO (Security Evaluation Office)

What you'll learn here today

- Overview of the VoIP Wifi phone market
- Basic threat model and vulnerability analysis applied to VoIP Wifi handsets
- Review previous project vulns disclosed
- New project vulns found (public today)
- Looking ahead: project roadmap and plans

Key Project Points

- Independent side project
  - My time, my dime
- Ongoing evaluation, adding more phones
- Vendor notification and response
  - 30 days plus notice before disclosure
  - All vendors notified via email
    - Chasing down vendors' security POC is no fun
    - No response from most vendors

Voices in the wilderness

"VoIP handsets are simply Internet-capable computers disguised as telephones. They are subject to the same security threats as other web-connected devices. Until the VoIP world gets serious about security, industry growth risks being stunted"

Carmi Levy
Senior Research Analyst
Info-Tech Research Group

June, 2005

Agenda

- Motivation
- Emerging VoIP trends
- VoIP wifi phone marketplace
- What does “secure” mean anyway?
- VoIP wifi phone threat modeling
- Level one methodology
- WiFi phone testing
- Future testing

Motivation

- Fun project in-between jobs
  - Got first phone and found vulnerabilities – I wonder how bad it is across vendors?
- Professional development
  - Focusing on VoIP for almost a year
- Project Goals
  - Disclose real issues in 15-20 shipping VoIP WiFi phones
    - Break-up “theoretical VoIP attacks” chatter
    - Expect simular vulnerabilities across multiple vendors
  - Outline VoIP WiFi phone threat analysis and methodology
  - Phased approach, gradual increase in sophistication

Emerging VoIP security trends

- Cavalier attitude
  - “Look how much **money** we’re going to **make/save**!”
  - Doing things their own way, not following standards
    - Vonage UDP/5061, Skype “just trust us”
- Oversimplification of VoIP threats and risks
  - VoIP complexity + real-time needs + Internet issues
- Huge concerns about sniffing
- Common industry lines one hears
  - “VoIP is more secure because it's on your internal network”
  - “Proprietary protocols are harder to hack”
  - “Our solution is secure because it’s encrypted end-to-end”

Emerging VoIP security trends

- Many attacks largely dismissed as “theoretical”
- ***Very few publicized*** VoIP security breaches
  - Likely low disclosure rate -- any legal requirements?
- Not many free VoIP security tools now
  - Protocol robustness (mostly SIP)
    - PROTOS, SIPp, SipSak, IETF SIP “torture tests”
  - Sniffing (Vomit, VoiPong, Cain & Abel, Ethereal, SCAPY)
  - Growing security community interest
    - Protocol analysis, phones vulns (Cisco 7940), tools (Send SIP Fun)
    - Community needs more presentations and tools

Agenda

- Motivation
- Emerging VoIP trends
- **VoIP wifi phone marketplace**
- What does “secure” mean anyway?
- VoIP wifi phone threat modeling
- Level one methodology
- WiFi phone testing
- Future testing
- Questions

VoIP wifi phone marketplace

- Types of 802.11b VoIP wifi phones
  - Pure-play SIP (this project)
  - Proprietary protocols or backend gear
    - Spectralink, Cisco, Vocera, Blackberry, Skype
  - Dual-mode handsets
    - WiFi to cellular “on-the-fly” switch-off
  - Specialized devices (everything else)
    - Game consoles, Kiosks
    - PDAs of all kinds (e.g. Nokia 770 tablet, MagPie PDA)
    - OpenPeak Simple Remote – TV remote with SIP client

As WiMax mesh networks gain traction, expect to see VoIP
WiFi all over, and in unique devices

VoIP devices – early 2006

VoIP WiFi phone marketplace

- Where are VoIP Wifi phones used?
  - Government, Financial/Trading, Businesses, Healthcare, Education
  - Individuals at home, work, hotspots…***planes*** ☹
- Emergency communications - Katrina
  - Bush/Nagin Vonage call – only service available
  - Jeff Pulver - http://pulverblog.com/archives/002817.html
- VoIP and ISP provider add-on
  - Azulstar mesh network - Hitachi WIP-5000
  - Vonage, BroadVoice - UTStarcom F1000
  - Skype – Netgear, Accton,

Marketplace security impact

- End user confusion
  - Many VoIP WiFi phone manufacturers
  - Lots of re-branded phones
  - Hard to find firmware, support, documentation
- Testing challenges
  - Variety of OS, web servers, FTP and TFTP clients
  - Multiple configuration options
  - Hard to obtain detailed specifications, source, etc.
  - Several trivial to DoS with simple scans/probes/attacks
  - Targeting features like email client, SMS, etc.

Agenda

- Motivation
- Emerging VoIP trends
- VoIP wifi phone marketplace
- **What does “secure” mean anyway?**
- VoIP wifi phone threat modeling
- Level one methodology
- WiFi phone testing
- Future testing
- Questions

What does “secure” mean anyway?

It is impossible to ensure a product is “secure”
One can only really say it is not vulnerable to specific threats

- Security features do not make a device itself secure
- Seems most folks really care about features
- “Caught between fear and greed”
  - Market drives development timetables, resources, headcount
  - Insatiable demand for new features (internal & external)
  - (Most) vendors reluctant to test beyond feature validation
- Big questions - No easy answers
  - Product security vulnerability cost? (company + customer)
  - Where do you draw the line with internal security testing?

Agenda

- Motivation
- Emerging VoIP trends
- VoIP wifi phone marketplace
- What does “secure” mean anyway?
- **VoIP wifi phone threat modeling**
- **Level one testing methodology**
- WiFi phone testing
- Future testing
- Questions

Thinking like an attacker

- Rules? We don’t need no stinkin’ rules…
- All the time in the world, none of the constraints
- Exploit anything
- Abuse all access and features
- Use any tools or techniques available
- Ignore protocol (Step 1: *grep* for “must not”)
- Leverage vendor info, tools, documents, support

VoIP WiFi phone threat modeling

Questions that focus the analysis

- What type of phone?
- What is the attacker profile and goals?
- What kind of OS, applications are used?
- Are there known vulnerabilities in phone?
- Can any features can be misused?

Level one methodology

- Level one is
  - “First look” from attacker’s perspective
  - Risk and the threats from
    - Basic configuration, open ports, services, developer leftovers
    - Basic feature misuse
- Level one is not
  - Attacking crypto
  - Analyzing protocol implementation
  - Various phone configurations
  - Attacking features
  - Physical attacks via USB

Level one methodology

- Defining the target
  - IP address
- Defining the “Level one” attacker
  - Location → remote
  - Skill level → low to medium
  - Tools → free, Opensource, publicly available
  - Goals
    - See how it works, gather information for next phases
    - Identify OS, ports, services, features, “unique stuff”
    - Read/Modify config (SIP servers, DNS, address book, logins)
    - Remote access to HTTP daemon, undocumented debug ports

Level one methodology

- Network access threat vectors – How simple?
  - What if the attacker can just access the IP address?
  - How will he identify phone OS, ports and services?
  - What attacks can he perform against those services?
  - What further remote network access via phone?
- Device access threats
  - What can the attacker do if he can change the phone’s configuration?

Agenda

- Motivation
- Emerging VoIP trends
- VoIP wifi phone marketplace
- What does “secure” mean anyway?
- VoIP wifi phone threat modeling
- Level one methodology
- **WiFi phone testing**
- Future testing
- Questions

Testbed

- VoIP WiFi phone
  - “Out-of-the-box” default settings
  - Linksys WRT54G AP
- Attacker
  - Firefox and Internet Explorer
  - Snmpwalk
  - Telnet, netcat
  - Nmap
    - Opensource contribution by submitting OS signature of unidentified phones - http://www.insecure.org/nmap/

WiFi phones: Level One

November, 2005 - CSI

- Cisco 7920
- Hitachi WIP-5000
- UTstarcom F1000
- Senao SI-680H
- ZyXel W2000 (Ver. 1)

January, 2006 - ShmooCon

- ZyXel W2000 (Ver. 2)
- ACT P202S
- Senao SI-7800H
- MPM HP-180W
- Clipcomm CP-100E
- Clipcomm CPW-100E

Cisco 7920

- Only non-SIP phone evaluated (had one ;)
- Version and OS
  - 7920.3.3-01-07 on VxWorks
- Vulnerabilities
  - **Undocumented port**, UDP/17185 VxWorks WDB remote debugging (wdbrpc)
  - **SNMP daemon** enabled, read/write with “public,” “private” via SNMP.
- Exploitation
  - **Undocumented port** allows debug access
  - **SNMP** attacks can read/write device configuration

Cisco 7920

- Workarounds
  - **SNMP and wdbrpc** service cannot be disabled
  - **SNMP** does not allow community string modification
- Vendor response
  - Same day response from Cisco PSIRT
  - Coordination on fixes and public advisory

Hitachi WIP-5000

- Version and OS
  - V1.5.6 on FreeBSD 4.3
- 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

Hitachi WIP-5000

- Exploitation
  - **HTTP index page** discloses too much information (device, routing, firmware, etc.)
  - **HTTP** no default login credentials
  - **SNMP** read/write using any credentials
  - **Undocumented open port TCP/3390 -** Unidata Shell?
  - **Hardcoded admin password via keypad**
- Workarounds
  - **HTTP daemon index page -** disable webserver

Hitachi WIP-5000

- Workarounds
  - **HTTP daemon –** change default no credential login
  - **SNMP daemon** cannot be disabled, nor can the read/write community strings be changed
  - **Undocumented open port TCP/3390** cannot be disabled
  - **Hardcoded admin password via keypad** cannot be changed
- Vendor response
  - No direct response, but fixed
  - www.hitachicable.co.jp/infosystem/security/pdf/917076.pdf
- Comments
  - AzulStar ISP mesh network phone

UTStarcom F1000

- Version and OS
  - S2.0 on VxWorks
- Vulnerabilities
  - **Undocumented SNMP daemon** enabled, read/write using “public/private” community string
  - **Undocumented Telnet** root VxWorks login “target/password”
  - **Undocumented rlogin** unauthenticated VxWorks shell
- Exploitation
  - **SNMP** attacker can read/modify phone MIB
  - **Telnet and rlogin** debugging, direct memory dumping/injection, read/write configuration, enable/disable/restart services, reboot

UTStarcom F1000

- Workarounds
  - **SNMP** cannot be disabled, credentials cannot be changed
  - **Telnet** cannot be disabled, user/pass is changeable
  - **Rlogin** cannot be disabled, no authentication can be enabled
- Vendor response
  - None
- Comments
  - Vonage is shipping this phone as of late December, 2005

Senao SI-680H

- Version
  - 0.03.0839 on VxWorks
- Vulnerability
  - **Undocumented port**, UDP/17185 VxWorks WDB remote debugging (wdbrpc)
- Exploitation
  - **Undocumented port**, UDP/17185 debug access
- Workaround
  - **Undocumented port**, UDP/17185 cannot be disabled
- Vendor response - None

ZyXel W2000 (Version 1)

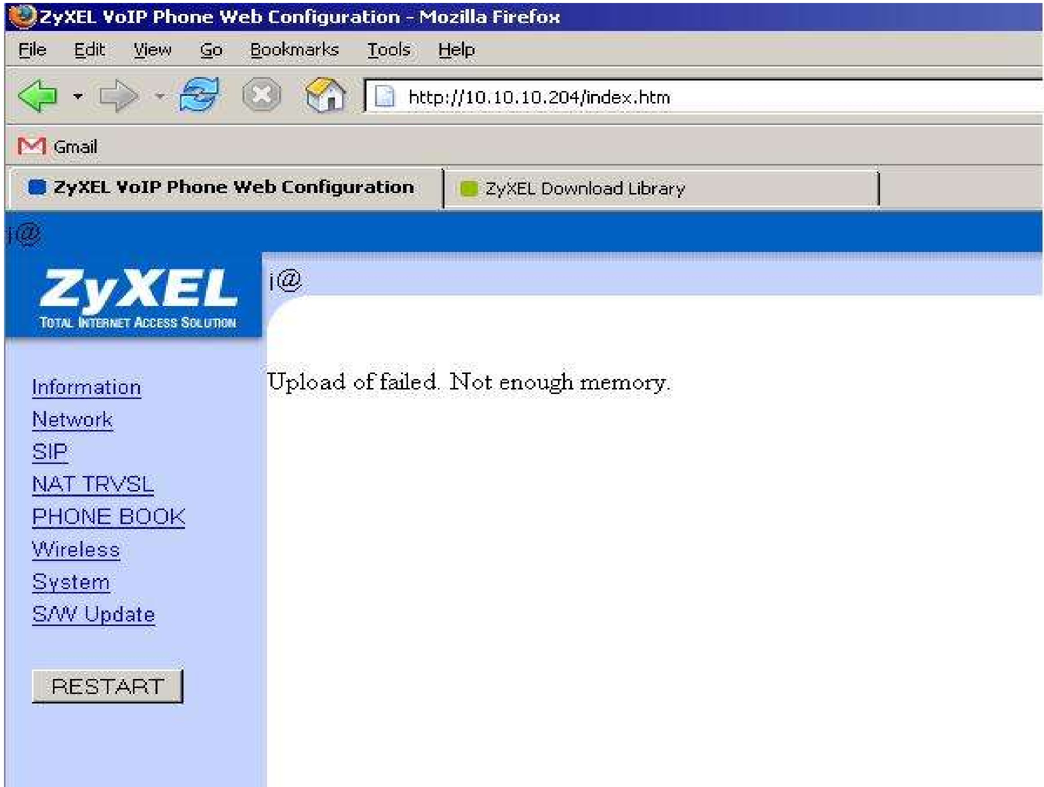
- Version
  - Wj.00.10 on VxWorks
- Vulnerabilities
  - **Hardcoded DNS to two servers in Taiwan**
  - **Undocumented open port** UDP/9090 provides MAC and firmware version on connect
- Exploitation
  - **Undocumented open port** UDP/9090 provides attackers an easy way to identify the device firmware

ZyXel W2000 (Version 1)

- Exploitation (cont’d)
  - **Hardcoded DNS servers**
    - DoS of NTP servers hoses **ZyXel phones worldwide**
    - Control DNS requests and route to 0wn3d SIP gateways
- Workarounds
  - **Undocumented open port** UDP/9090 cannot be disabled
  - **Hardcoded DNS servers** cannot be modified
- Vendor response - None

ZyXel W2000 (Version 2)

- Firmware version was BETA, hardcoded DNS, UDP/9090
- Upgrading firmware failed on at %99 with “Not enough memory” error using Firefox
- My new $200 brick
- Response from ZyXel
  - “Use IE”
  - Gee, not documented!
  - RMA time


ZyXEL VoIP Phone Web Configuration - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://10.10.10.204/index.htm
Gmail
ZyXEL VoIP Phone Web Configuration
ZyXEL Download Library
i@
ZyXEL
TOTAL INTERNET ACCESS SOLUTION
i@
Information
Network
SIP
NAT TRVSL
PHONE BOOK
Wireless
System
S/W Update
RESTART

Upload of failed. Not enough memory.

ZyXel W2000 (Version 2)

- Second W2000
- Version
  - WV.00.02 on VxWorks
- Vulnerabilities
  - **Undocumented open port** UDP/9090 provides MAC and firmware version on connect
- Exploitation
  - **Undocumented open port** UDP/9090 provides attackers an easy way to identify the device firmware and MAC

ACT-P202S

- American Century Telecommunications
- Version and OS
  - 1.01.21 on VxWorks (also runs JAVA applications)
- Vulnerabilities
  - **Undocumented port**, UDP/17185 VxWorks WDB remote debugging (wdbrpc)
  - **Undocumented port**, TCP/513, rlogin
  - **Undocumented port**, TCP/7, echo
- Exploitation
  - **Undocumented port**, UDP/17185 debugging access
  - **Undocumented port**, TCP/513 rlogin

ACT-P202S

- Workaround
  - **Undocumented ports** cannot be disabled
- Vendor response – exchanged email, answered questions, etc.
- Comments
  - HTTP daemon on TCP/9999
  - Hardcoded NTP server in Taiwan
  - Snip from ACT email response
    - Got IANA lesson?

> “Port 17815 - reserved for debugging purpose
> Port 513 - reserved for telnet access
> Port 7 - allow others to ping”

Senao SI-7800H

- Version
  - 0.03.0001 on VxWorks
- Vulnerability
  - **Undocumented port**, UDP/17185 VxWorks WDB remote debugging (wdbrpc)
- Exploitation
  - **Undocumented port**, UDP/17185 debug access
- Workaround - None
- Vendor response - None

MPM HP-180W

- Version
  - WE.00.17 on VxWorks
- Vulnerabilities
  - **Undocumented open port** UDP/9090 provides MAC and firmware version on connect
- Exploitation
  - **Undocumented open port** UDP/9090 provides attackers an easy way to identify the device firmware and MAC
- Workaround - None
- Vendor Response - None

Clipcomm CP-100E

- Version
  - 1.1.60 (050221) on VxWorks
- Vulnerabilities
  - **Undocumented open port** TCP/60023 allows remote access to two debugging accounts: Clip and USH.
- Exploitation
  - Reboot, factory reset, call trace, write to registers, dump memory, modify configuration, etc.
- Workaround - None
- Vendor Response - None

Clipcomm CPW-100E

- Version
  - 1.1.12 (051129) on VxWorks
- Vulnerabilities
  - **Undocumented open port** TCP/60023 unauthenticated remote access to two debugging accounts: Clip and USH.
- Exploitation
  - Reboot, factory reset, call trace, write to registers, dump memory, modify configuration, etc.
  - Debug CLI to <u>call another phone number</u> (snoop, 1-900, etc)
- Workaround - None
- Vendor Response - None

Level one testing summary

- Default accounts, passwords
- Inability to change credentials
- Inability to disable services
- Extraneous services
- Development debug access
- Hardcoded DNS and NTP servers
- DoS doing simple scans and probes (hard ***not*** to)
- Difficulty finding and upgrading firmware (risky)
- Poor documentation
- Lackluster response from majority of vendors

Level one testing summary

- Depending on the phone, an attacker may
  - Login with default or hardcoded credentials
  - Remote access via extraneous services
    - Debugging, trace calls, snooping, reset phone
    - Modify configuration: SIP servers, DNS
    - Modify phonebook for social engineering
  - DoS or control routing to hardcoded Taiwan DNS
  - SNMP
  - Brick phone with bad image (or maybe even a good one)

Agenda

- Motivation
- Emerging VoIP trends
- VoIP wifi phone marketplace
- What does “secure” mean anyway?
- VoIP wifi phone threat modeling
- Level one testing methodology
- WiFi phone testing
- **Future testing**
- Questions

Future testing – Level 2

- More phones to finish Level 1 (15-20 phones total)
- Level 2 testing
  - Upgrade all phones with fixed
  - Profile increased attacker skill level, more tools
  - Deeper application (HTTP daemon)
  - More port scans, vulnerability scanners
  - Targeting protocol implementation
    - SIP: Protos SIP, IEFT torture tests, SipSak, SIPp scenarios
    - TCP stack: “Typical” floods, Naptha, ISIC
- Map attacks to VOIPSA Threat Taxonomy
  - “Visualize” coverage, demonstrate applied to evaluation

Future Testing – Level 3

- Advanced attacks against individual phones
  - Targeting specific features
    - Email clients, client Web browsers, SMS, JAVA
  - Targeting non-802.11b network access
    - Bluetooth
    - USB
  - Skype

SIP or Skype Phones Q1 2006

- UTStarcom F3000 – ordered, delivery soon
- Zultsys WIP2 – scoping
- Linksys WIP330 – Q1 2006
- Netgear – Q1 2006
- Accton – Q1 2006

Think broadly...and contribute

- Current security analysis needs
  - ATAs, Wired VoIP phones, Softphones, PDAs
  - PBXs (D-Link, LinksysOne, provisioning)
  - Asterisk
- Protocol fuzzing
  - SIP, MGCP, RTCP, etc.
  - Proprietary protocols

Questions?

Thanks!

shawnmer@gmail.com