Hacking WITH the iPod Touch
Thomas Wilhelm
a.k.a. Hacker Junkie
Personal Experience

- Penetration Tester / Project Manager
  - Fortune 20 Company
  - Internal and External System
  - Network Architectures

- Certifications:
  - ISSMP, CISSP, SCSECA, SCNA, SCSA, NSA-IEM, NSA-IAM
Personal Experience

- Associate Professor
- Colorado Technical University
- What I Teach: Information System Security
- Undergrads and Graduate Programs
Personal Experience

- Masters Degrees:
  - Computer Science, Management (InfoSec)
  - Doctoral Student - Capella University
- Information Technology
  - Specialization: Information Assurance & Security
- National Center of Academic Excellence in Information Assurance Education (CAEIAE)
Personal Experience

- Author
Objectives

- Jailbreaking the iPod Touch / iPhone
- Using iPod Touch as PenTest Platform
- Hacking with the iPod Touch
- iPod Touch as an Attack Vector
- Conclusion
Jailbreaking

- Legal Issues
- Jailbreaking Tools
Jailbreaking
Legal Issues

- EFF Proposed Exception

- Proposed Class #1: Computer programs that enable wireless telephone handsets to execute lawfully obtained software applications, where *circumvention is accomplished for the sole purpose of enabling interoperability* of such applications with computer programs on the telephone handset.

Jailbreaking
Legal Issues

- DMCA Violation

  “Apple is opposed to the proposed Class #1 exemption because it will destroy the technological protection of Apple’s key copyrighted computer programs in the iPhone™ device itself and of copyrighted content owned by Apple that plays on the iPhone, resulting in copyright infringement, potential damage to the device and other potential harmful physical effects, adverse effects on the functioning of the device, and breach of contract.”

Jailbreaking
Legal Issues

- Outcome?
  - Copyright Office will be making a decision in October regarding exception
  - Apple’s License Agreement still in effect, regardless of outcome
Jailbreaking
Legal Issues

- System & Network Hacking
  - Standard iPhone / iPod Touch is fairly neutered
- Bad Laws:
  - Sierra Corporate Design, Inc. v. David Ritz - “Ritz’s behavior in conducting a zone transfer was unauthorized within the meaning of the North Dakota Computer Crime Law” - Judge Rothe-Seeger, Case number 09-05-C-01660
  - $63K judgement
Jailbreaking

Jailbreaking Tools

- QuickPwn.com
Jailbreaking

Jailbreaking Tools

- Default Install
  - Cydia
  - Installer

- First Things First...
  - OpenSSH / TouchTerm
iTouch as PenTest Platform

- Operating System
- Package Managers / Repositories
- System Tools
- Usability
**iTouch as PenTest Platform**

**Operating System**

- Darwin - Kernel Version 9.4.1
- Open Source
- POSIX compliant
- Includes code from NEXTSTEP and FreeBSD
- Single UNIX Specification version 3 (SUSv3) Compliant

**Conclusion:** iPod Touch == UNIX System
iTouc as PenTest Platform
Package Managers / Repositories

- Cydia
  - Port of Debian APT
  - 30+ repositories
- Apple’s App Store
  - Download applications from the iTunes Store
iTouch as PenTest Platform

System Tools

- Development Platform
  - GCC - GNU Compiler Collection
    - Headers available via Cydia
iTouch as PenTest Platform
System Tools

- Scripting Languages
  - Perl
  - Python
  - Ruby (on Rails)
  - ...and of course shells
iTouch as PenTest Platform

System Tools

- Network Tools
  - OpenSSH
  - Inetutils (ftp, inetd, ping, rlogin, telnet, tftp)
  - Network-cmds (arp, ifconfig, netstat, route, traceroute)
  - Wget
iTouch as PenTest Platform
System Tools

- Network Tools (continued)
  - Stealth MAC
  - Stunnel
  - TCPdump
iTouch as PenTest Platform

Usability

- Shell Window
- 13 Lines
- 57 characters

```
Interesting ports on 141.13.134.52:
Not shown: 993 filtered ports
PORT STATE SERVICE
22/tcp open ssh
25/tcp closed smtp
53/tcp open domain
70/tcp closed gopher
80/tcp open http
113/tcp closed auth
3128/tcp closed Elite
Nmap done: 1 IP address (1 host up) scanned in 54.42 seconds.
```

iPod:
iTouch as PenTest Platform

Usability

- Keyboard takes up a lot of real estate
- Solution: Remote SSH (when possible)
Hacking with the iPod Touch

- Statistics
- Information Gathering
- Vulnerability Identification
- Vulnerability Exploitation
- Web Hacking
- Privilege Escalation
- Maintaining Access
- Demonstration
Hacking with the iPod Touch

Statistics

- SECTOOLS.ORG
  - 9 / Top 20 Tools (+ Nmap)
- JTR BENCHMARK: FreeBSD MD5
  - MacBook Pro 2.8 GHz Intel Core Duo
    - 7674 c/s real, 7690 c/s virtual
- iPod Touch
  - 577 c/s real, 617 c/s virtual
Hacking with the iPod Touch
Information Gathering

- Safari
- Nmap
  - System & Application Footprinting
  - Banner Grabbing
- Telnet / Netcat
  - Verification & Enumeration of Nmap Results
Hacking with the iPod Touch
Vulnerability Identification

- Missing!
  - No Vulnerability Scanners (possible Nessus tunnel?)
  - Grabs Low Hanging Fruit... but saves a lot of time
Hacking with the iPod Touch
Vulnerability Exploitation

- Metasploit
  - Exploit Code & Shellcode
- Scapy
  - Packet Manipulation
Hacking with the iPod Touch

Web Hacking

- Nikto
  - Web Server Scanner
- Medusa
  - Application Access Brute Forcer
  - (http.mod, web-form.mod)
Hacking with the iPod Touch
Privilege Escalation

- Pirni
  - ARP Spoofing and Network Sniffer
  - Berkeley Packet Filter (example: "tcp dst port 80")
- John the Ripper
  - Password Brute Force Attack
- Medusa
  - Brute Force Network Authentication
Hacking with the iPod Touch
Maintaining Access

- Netcat
  - Read and Write Data Across Network Connections
  - Backdoor / File Transfer
- OpenSSH
  - Secure (Reverse) Shell
- Problem - Active Processes
Hacking with the iPod Touch
Demonstration

- ARP Spoofing & Traffic Gathering
iTouch as an Attack Vector

- Rogue System
- Social Engineering
iTouch as an Attack Vector

Rogue System

- Advantages
  - Small, Compact, Innocuous
- Disadvantages
  - Power
  - Wireless Only
  - $299 Base Price (More than I paid for my EeePC)
iTouch as an Attack Vector
Demonstration

- Rogue System
iTouc as an Attack Vector
Social Engineering

- iPod Touch vs. Laptop
  - Assume it’s a Phone
  - Unaware of its use as a hacking platform
  - “Texting” is socially acceptable
  - Compact - Easy to Hide
iTouch as an Attack Vector

Demonstration

- Social Engineering
Conclusion

- Personal Thoughts
- Shout-Outs
- Reminder
- List of Tools
Conclusion

Personal Thoughts

- Worthwhile Hacking Platform?
- What Could be Better?
- iPod Touch vs. iPhone?
- What Does the Future Hold?
Conclusion

Shout Outs

- DC303 - Robot Mafia
- Sudosu - Colorado Tech Security Club
- My Family
Conclusion

Links

- forums.heorot.net
- quickpwn.com
- cydia.saurik.com
- developer.apple.com
Conclusion

(Gentle) Reminder
Conclusion

List of Tools

adv-cmds
APT
AutomaticSSH
Backgrounder
Base Structure
Berkeley DB
Bourne Again Shell
bzip2
Core Utilities
csu
Cydia Installer
Darwin CC Tools
Darwin Tools
Debian Packager
Dev-Team
developer-cmds
Diff Utilities
diskdev-cmds
dns2tcp
Docs
Find Utilities
Gawk
gettext
GNU C Compiler
GNU Cryptography
GNU Debugger
GNU Privacy Guard
GnuPG Errors
grep
gzip
iBrowser
inetutils
iPhone Firmware
less
libffi
libgcc
libnet
libpcap
libutil
libxml2
libxslt
Link Identity Editor
Make
mDNSResponder
Metasploit
Mobile Substrate
nano
Netatalk
netcat
network-cmds
New Curses
Nmap
OpenSSH
OpenSSL
perl
pcre
pimri
Python
readline
Ruby
RubyGems
SBSettings
sed
shell-cmds
SpoofMAC
Stealth MAC
Stumbler Plus
Stunnel
Sudo
system-cmds
Tape Archive
tcpdump
unzip
Vi IMproved (VIM)
wget
whois
WinterBoard
XML Parser Toolkit

Added Manually:
libssh2
john the ripper
scapy
medusa

Apple Store:
TouchTerm
Ping
Speed Test
Hacking WITH the iPod Touch

Thank you for attending!

Q&A Session Afterwards... Punch and Pie.