Thinking Outside of the Console (Box)

Squidly1

gameconsolez@gmail.com / haksys.schleppingsquid.net

DefCon 15 / August 04, 2007
HAXO(RED)

See G. Mark FMI see him @ Hacker Jeopardy

SaveDarfur.org

Crisis ongoing. Read up & help
Squidly1

- Computer Network Defense Team Lead (US Navy)
- Former Red Team Lead
- Independent security researcher
- GSEC
- Software engineering student
- Wireless explorer
- Heavy gamer
- Fervent g33k
Covert Testing

- Used by legitimate vulnerability assessment firms and Red Teams in order to better help companies and organizations learn how to protect themselves. The focus of these testing methods is to help said entity identify possible intrusions, faulty equipment / software, bad security practices, ineffective policies – among other things. At the end of the assessment phase a report is presented to the entity in order to set into motion an informed plan for fixing the discovered deficiencies.

- Used by other companies and governments in order to serve their own gain. Corporate espionage anyone?
“The U.S. Department of Justice (DOJ) pulled the covers off a previously-sealed case of corporate espionage by a former DuPont scientist who stole $400-million in intellectual property from his employer.”

- SC Magazine (16 Feb 2007)

“A UK-based hi-tech firm that's become the victim of "industrial espionage" is offering a reward for information leading to the arrest of those responsible for stealing its computer hardware. Thieves who stole a number of laptops from VBi Triscan Systems also lifted hard disks from the fuel management firm's servers... Executives at the ... firm fear the thefts were aimed at gathering trade secrets rather than just routine blogs.”

- The Register (20 Apr 2007)
... And then you have people like us ...

: P

We have no allegiance, no political motive and no fiscal gain - just looking and passing through - kthxbai

“hacker ethic” entry in Jargon File: http://tinyurl.com/qu2ck
“Is there a Hacker Ethic for 90s Hackers?” by by Steven Mizrach: http://tinyurl.com/24tzs
After I modified my first XBOX and bought my first PSP I experienced the realization that the newer generation game consoles could be so much more than ... game consoles.

Prior to 2002 there was very little going on in the console hacking arena, outside of relatively crude hardware modifications and game cheating.

Since then the game industry has moved forward in using even more powerful main processors and GPUs, in order to both satisfy and build up gamer desires for 'the next best thing.'

Now we have true computers with the ability to network... to share... to probe... to perform vulnerability scans... to find YOUR network... to get on YOUR network... and...?
Stimulation

- Sixth & Seventh Generation game consoles
- Hand-held game systems
- Ubiquitous online connectivity (wired / wireless)
- ...but it's just a video game console...
- OMG! It's a video game console on MY network!! WTF!!!
Goals

- Cover the three key features a covert tester looks for in penetration hardware, and why game consoles can fit the bill.
- Look at the evolution of homebrew applications on various game systems, especially those that expand system usage.
- Show how a couple of game systems can be used to infiltrate your network, or collect data.
- Suggest things you can do to mitigate this threat.
- Open discussions on what the future holds…
Three Important Things

... or what is important to the covert tester?
Three Important Things

- **Power**
  (Potential)
- **Programmability**
  (Flexibility)
- **Concealment**
  (Plausible Deniability)
POWER!!!

... or what might this baby do?
Sixth Generation Systems

Primary platforms:

- Sony Playstation2 (26 Oct 2000)
- Microsoft XBOX (15 Nov 2001)
- Nintendo GameCube (18 Nov 2001)
- Nintendo GameBoy Advance SP (Sept 2004)
- Nintendo Wii * (08 Dec 2006)
Seventh Generation Systems

Primary platforms:

- Sony Playstation3 (17 Nov 2006)
- Sony Playstation Portable (24 Mar 2005)
- Microsoft XBOX 360 (22 Nov 2005)
- Nintendo Wii (08 Dec 2006)
- Nintendo DS / DS-Lite (21 Nov 04 / 11 June 06)
Squidly1's Systems

- Playstation3 (60G)
- Playstation2 (40G)
- Playstation
- PSP (1.50, 3.40OE-A)
- GameBoy
- XBOX 360 (120G)
- XBOX (300G)
- Wii
- DS Lite (M3 Movie Player Lite Pro, Passcard)
- GameBoy Advance SP
Hardware & Potential

... G33k pr0n, awww yeaahhh...
Hardware: XBOX

Under The Hood:

- An Intel 733Mhz custom PIII
- 64M DDR SDRAM
- 250 Mhz custom nVidia GPU (NV2X) + 200Mhz media processor
- 10/100 Ethernet
- Proprietary USB ports
- DVD optical drive
- 8~10G hard drive
- Proprietary memory cartidge port

Xbox System Specifications (Xbox Reporter): http://tinyurl.com/f6p2h
Potential: XBOX

Add-ons:
- Upgrade to 1.3G Celeron
- Upgrade 128MRAM
- 802.11B/G adapter
- Dual HDs / 320G max HD
- USB Keyboard / Mouse
Hardware: XBOX 360

Under The Hood:

- An IBM PowerPC (3 symmetrical cores) 3.2G ea.
- 512M GDDR3 RAM
- **500 Mhz Xenos custom ATI GPU**
- 10/100 Ethernet
- USB ports
- DVD optical drive
- 20~120G hard drive
- Proprietary memory cartridge port

Xbox 360 System Specifications (Team Xbox): http://tinyurl.com/af6x9
Potential: XBOX 360

Add-ons / Mods:
- Upgrade HD 120G or more...
- 802.11G adapter
- XBL Vision (Web Camera)
- USB Keyboard / Mouse
Hardware: Playstation²

Under The Hood:

- Toshiba 300MHz R5900 MIPS IV Processor
- 32M Direct RAMBUS RAM
- 150Mhz GPU
- USB / Firewire
- DVD optical drive
- MS Pro Duo, Compact Flash (I & II) and SD (standard & mini)

PS2 System Specs: http://www.linux-mips.org/wiki/PS2
**Potential: Playstation²**

**Add-ons:**
- Ethernet / Modem / HD assembly
- ~500G HD maximum**
- USB keyboard / mouse

**Tricks:**
- 70 node Beowulf cluster
  * Customized code blocks to the GPU allowed for processing speeds up to 1 Gflop – per machine.
- Oh, yeah, it runs Linux

Hardware: Playstation

Under The Hood:

- Cell Broadband Engine processor (heterogeneous, 1 control CPU, 8 computational SPEs) ~3.2Ghz ea
- 256M XDR RAM (3.2Ghz) / 256M GDDR3 RAM (700Mhz)
- 550 Mhz custom GeForce 5900 nVidia GPU
- 10M~1G Ethernet / 802.11B/G
- USB ports
- DVD/BluRay optical drive
- 20~60G hard drive **
- MS Pro Duo, Compact Flash (I & II) and SD (standard & mini)

PS3 System Specifications (PS3Source): http://tinyurl.com/2ehe6l
Interaction with the PS3 Hypervisor

Game / Application

Game OS / Other OS (Linux)

Hypervisor

- Video Output Controller
- GeForce 5900 GPU
- Audio Controller
- GigE
- Wi-Fi
- ATA
- HDD/BD
- USB
- Bluetooth
- 8 (-1) SPUs
- Memory
- PPU

PS3 Hypervisor Details (IBM CBE Team & Sony Linux Dev Team)
Hardware: Playstation³

PS3 Cell Processor Security

Element Interconnect Bus

PowerPC
PPE

I/O

Main Memory

Each Thread

Application

Cell Processor Security (IBM CBE Whitepaper)
Potential: Playstation

Add-ons:
- 250G+ hard drive (2.5” Serial ATA) **
- MS Pro Duo, Compact Flash (I & II) and SD (standard & mini) – max size?
- InFeCtuS firmware (hardware) downgrader **
- BlueTooth or USB keyboard / mouse

Tricks:
- Runs Linux, many flavors
- And there are a few clusters...
- Crack crypto – Single Precision is best... See Folding@Home zoom!

InFeCtuS Downgrader: http://tinyurl.com/2bugql
Gartner's Steve Prentice fears criminals could use PS3 for crypto cracking (TechTarget ANZ): http://tinyurl.com/yoeqlk
Hardware: PSP

Under The Hood:
- a MIPS R4000-based CPU (1~333Mhz)
- 32M RAM + 4M DRAM
- 166 Mhz GPU has 2 MiB embedded memory
- 802.11B Ad-Hoc / Infra Modes
- IrDA transmit / receive
- Mini-USB and custom serial
- UMD optical drive
- MemoryStick Pro Duo drive
Potential: PSP

Add-ons:
- PSP PS-290 GPS Unit
- PSP PS-260 Microphone
- PSPj-15003 Camera
- 8 GB MS Pro Duo (need firmware 2.81 or higher)
Potential: PSP

Mods:
- Hirose connector for expansion of antenna

PSP WiFi Module: RIP Lik-Sang
PSP with external antenna (Engadget): http://tinyurl.com/2eo9fa
Hardware: GameCube

Under The Hood:

- 485Mhz Gekko (custom) IBM PowerPC CPU
- 40M RAM (total)
- 162Mhz ATI / Nintendo Flipper GPU
- Proprietary optical disc
- Proprietary memory cards

GameCube System Specifications (PSReporter): http://tinyurl.com/28jsgy
Potential: GameCube

Add-ons:
- Mod chips
- Keyboard / Analog stick

Trick:
- Linux - again...
Hardware: Wii

Under The Hood:

- 729Mhz Boardway IBM PowerPC CPU
- 88M RAM (total)
- 243Mhz Hollywood ATI GPU
- 802.11B/G
- 512M Flash memory
- SD memory
- USB 2.0 ports
- Optical drive
  (No DVD support)

Wii System Specifications (Wii-Volution): http://tinyurl.com/3xj7lo
Hardware: DS-Lite

Under The Hood:

- Two 32-bit processors: [main] ARM 946E-S (67 MHz) [co] ARM 7 TDMI (33MHz)
- 4M main RAM / 656K VRAM
- 802.11B / Ni-Fi protocol (Mitsumi MM3205B module)
- SD removable memory storage
- Microphone
- Touch sensitive display
- GBA (Slot 2) and NDS (Slot 1) ports

DS-Lite System Specifications (Embedded): http://tinyurl.com/37h2a3
Potential: DS-Lite

Add-ons:
- Removable memory storage
  - SD, CompactFlash, MicroSD **
- Flash ROMs / Mod cards

Trick:
- Linux...? Limited, but it's here, too!
Programmability & Flexibility

... or what can I make this thing do??
Native Vulnerabilities

- Sony Playstation Portable (PSP)
  - Firmwares 1.00 & 1.50
  - Custom Firmwares
  - Gateway Firmwares: 2.71, 3.02, 3.50
  - Vulnerable games: Lumines, Grand Theft Auto: Liberty Cities

- Nintendo DS

- Nintendo DS-Lite

Both units are open enough that one only needs to plug in some custom hardware... Done.
Native Vulnerabilities

◆ Microsoft XBOX
  - Font handler / no mod checks
  - XBOX Dashboard
  - A20# memory handling flaw
  - Games run in Kernel Mode
  - Vulnerable games
    007 Agent Under Fire
    MechAssault
    Splinter Cell (and many more)

◆ Playstation3
  - Internet browser flaw?!?!?
  - 'Controlled' PS2 game 'crash'?!?

At current, neither of these approaches is all that promising. Besides, who wants to brick a $600 system to find out??

Check out Michael Steil's talks on the XBOX security flaws (GoogleVideo): http://tinyurl.com/2n8y62
and Chaos Communication Congress 22 (22C3 Info Page): http://tinyurl.com/34b22k
Linux Is Everywhere

- The only sustained exceptions to this rule are:
  1. Nintendo Wii
  2. Microsoft Xbox360 **
     (only “works” on X360 kernels 4532 & 4548)
- But is it “Game Over” when Linux is installed??
Game Console Coding

While In Linux:
- Take your pick – C, Python, Perl, etc.

After Modification:
- Python (PSP, XBOX and DS)
- Lua (PSP and DS)
- Assembler (PSP**)
- C (PSP**)
- BASIC (DS)
Homebrew is a term frequently applied only to video games that are produced by consumers on proprietary game platforms; in other words, game platforms that are not typically user-programmable, or use proprietary hardware for storage.

Sometimes games developed on official development kits, such as Net Yaroze or PS2 Linux are included in the definition. Some, however, also refer to all non-commercial, "home-developed" games for open architectures as homebrew games, though these typically go under more frequently used labels, such as freeware.

“Homebrew” definition (Wikipedia): http://tinyurl.com/yzfxkz
Homebrews of Note

[PSP] IrDA Capture

Shows “IrDA Sample” by Vanya Sergeev snagging raw IR signals from two universal remotes. The same trick can be done with any other IR device – like your PDA.

Where to download (PSP-Homebrew): http://tinyurl.com/34zfzg
[PSP] iR Commander

The newest version supports 2,000 controllable infrared devices – for 1.50 users.
Check Major Malfunction's "Old Skewl Hacking Infrared" for why this interesting.

To grab your device (Remote Central): http://www.remotecentral.com
AhMan returns with another homebrew of interest. This one allows for *more* IR devices, performs ad-hoc WiFi transfers, throttles CPU speed, DevHook support, nethost redirection, and works on all homebrew-friendly firmwares.

Where to download (My QJ.net): http://tinyurl.com/32xj99
AhMan's VNC controller for the PSP. Allows you to control computers, even password protected ones, with your PSP. Can be also used with iR a keyboard.

Where to download (ZX81's Website): http://tinyurl.com/2pgvo8
PortableVNC Video

YouTube version: http://www.youtube.com/watch?v=t0cQrx8IOyg
To download this video go to http://haksys.schleppingsquid.net/Files/index.php?path=DefCon15+Material/
[PSP] SecureText

Allows the user to encrypt and decrypt – with RC4.

For more information (GlobWare): http://tinyurl.com/25xux5
Homebrews of Note

[PSP] HTTPd / FTPd

Need to set up a quickie web (by Elxx) or FTP (by ZX-81/PSPKrazy) server?
Works really well, too.

Where to download HTTPd (PSPUpdates): http://tinyurl.com/2y2u6y
FTPd (ZX81’s Website): http://tinyurl.com/3a3ro9
[PSP] AFKIM

IRC, AIM, ICQ, MSN, GTalk, Yahoo! on your PSP. 14 iR keyboards are supported. Thanks Danzel!

Where to download AFKIM (Danzels Internets): http://localhost.geek.nz/
Homebrews of Note

[PSP] PSPSSH

Zx-81’s port of the DropBear (Matt Johnston) SSH2 client / server application.

Where to download PSPSSH2 (ZX81’s Website): http://tinyurl.com/22fgmh
YouTube version: http://www.youtube.com/watch?v=Xw59RWVRNHA
To download this video go to http://haksys.schleppingsquid.net/Files/index.php?path=DefCon15+Material/
Jean Yves Lamoureux's basic WiFi Sniffer.

Where to download WiFi Sniffer (Max Console): http://tinyurl.com/yoggvz
Homebrews of Note

[PSP] MapThis!

Where to download MapThis! (DCEMU): http://deniska.dcemu.co.uk

(( MapThis! Video )))
Homebrews of Note

[PSP] PSPInside

//hitmen Console's PSPInside – the tool for determining what your PSP is thinking... Can you say buffer overflow??

Where to download PSPInside (Hitmen Console): http://www.hitmen-console.org/
Less than a week after discovery, game sellers on Amazon and eBay began gouging PSP gamers with prices far over what they were selling at prior to the announcement. On eBay people were actively bidding for $60-$45 copies.

The median prices the week before were $12 - $15.

Prices confirmed 04 July 2007 on Amazon.com and eBay.com
Björn Gieslers Webseiten's FTP server application.

Where to download DSFTP (Giesler.biz): http://tinyurl.com/272pnf
Stephen Stair's bare-bones AP finder and packet capture application.

For more info: http://www.akkit.org/
[DS] AirCrackDS

Retrohead's simple WEP cracking application.

Where to download AirCrackDS (1Emulation): http://tinyurl.com/253471
[DS] AirePlayDS

JSR's packet injection code. At the Alpha stage at the moment.

Where to download AirePlayDS (1Emulation): http://tinyurl.com/yuj3ot
Homebrews of Note

[DS] DSOrganize

DragonMinded's general purpose organizer, IRC client and web viewer.

Where to download DSOrganize (DragonMinded): http://tinyurl.com/mv58h
Homebrews of Note

[DS] PointyRemote

Pointless' custom protocol driven remote PC controller.

Where to download PointyRemote (1Emulation): http://tinyurl.com/eanps
Homebrews of Note

[DS] Win2DS

A small VNC-type program by Bill Blaiklock (Sintax).

Where to download Win2DS (1Emulation): http://tinyurl.com/2f6s5z
[DS] Lilou FTP Server

Lilou's FTP server / client application.

Where to download Lilou FTP Client/Server (Lilou's Blog): http://blog.dev-scene.com/lilou/
Homebrews of Note

[DS] MoonShell

General interface replacement by Infantile Paralysiser.

Where to download MoonShell (Infantile Paralysiser): http://tinyurl.com/ge6bs
Concealment

... you put that console WHERE??
(No Goatses were hurt in this section)
Who in this picture does *NOT* have a pocket video game on them?

Hint: Probably not the young geisha.
Do you know if game systems are allowed in your work spaces? What about the customers? Is there a policy covering you??
Altoids tins ain't just for holding those curiously strong gum pieces anymore...
Concealment

Are they playing a game, or not?
Other Tidbits

... last minute goodies ...
The following ports were detected, on a v1.50 PSP:

- **25 [SMTP]** - Simple Mail Transfer Protocol is a protocol for sending electronic mail messages between computers. (TCP) Open
- **110 [POP3]** - Post Office Protocol 3. Mail server protocol commonly used on the internet. (TCP) Open
- **123 [NTP]** – Network Time Protocol (UDP). Listening

Research on www.netbsd.org shows that the network architecture on the PSP is based on NetBSD, giving it a robust communications capability.

**IDS Goodies:** PSP MAC addresses begin with **00:01:4A**, and they will generally look for **fj00.psp.update.playstation.org (130.94.58.55)** if an update is requested.
The following ports were detected, on an Xbox360:

- 25 [SMTP] – An unknown service is running on this port. (TCP) Open
- 110 [POP3] – An unknown service is running on this port. (TCP) Open
- 1030 [IAD1] – A communications service, acting as webserver is on this port. (TCP) Open

“It was possible to crash the remote host by sending a specially malformed TCP/IP packet with invalid TCP options. Only the version 2.6 of the Linux Kernel is known to be affected by this problem” (hmmm)...

IDS Goodies: X360 MAC addresses begin with 00:12:5A.
The following ports were detected, on a Playstation³:

- **25 [SMTP]** - Simple Mail Transfer Protocol is a protocol for sending electronic mail messages between computers. (TCP) Open
- **110 [POP3]** - Post Office Protocol 3. Mail server protocol commonly used on the internet. (TCP) Open

“The remote host accepts loose source routed IP packets.”
“The remote host is vulnerable to an 'Etherleak' - the remote ethernet driver seems to leak bits of the content of the memory of the remote operating system”

**IDS Goodies:** PS3 MAC addresses begin with **00:15:C1**, and they will generally look for **fj00.ps3.update.playstation.org (129.250.162.55)** if an update is requested.
The following ports were detected, on the Wii and DS Lite:

Nothing... Seems that both units shut down all wireless when not expecting to use it. Still checking for 802.11x radiation signature fluctuation. Could be part of their power-saving functionality...
I believe that I am the first person to actually use my PSP (or any wireless device) to assist in a pub crawl... Found the **Sidebar** in San Diego.
Chaos Computer Congress - 22nd & 23rd
- **Nintendo DS:** Mario Manno, Tobias Gruetzmacher, Marcel Klein
- **Console Hacking 2006:** Felix Domke
- “**Xbox**” and “**Xbox 360**” **Hacking:** Michael Steil and Felix Domke

**Sources**

- PSPUpdates.net
- MaxConsole
- DCEmu.co.uk
- NeoFlash.com
- PS2Dev
- dev-scene.com/NDS
- Sony's Playstation Forums
- XboxHacker Forums
- Xbox-Scene
- Anathema (PS3 browser exploit)
- PSP Vault
- IBM / Sony CBE Engineers & their programming support sites
- Individual developer websites

*THANKS for all the hard work guys!!!*