

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?



Corporate Espionage

“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)



“\$400 million corporate espionage incident at DuPont” by Ericka Chickowski
(SC Magazine): <http://tinyurl.com/2tdny6> “Stolen laptops fuel industrial espionage fears for UK software firm” by John Leyden (The Register): <http://tinyurl.com/3b4uh9>

Covert Testing

... 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



Are You High?!?

- ◆ 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 Advace 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 yeahhhh...



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 cartridge port



Potential: XBOX

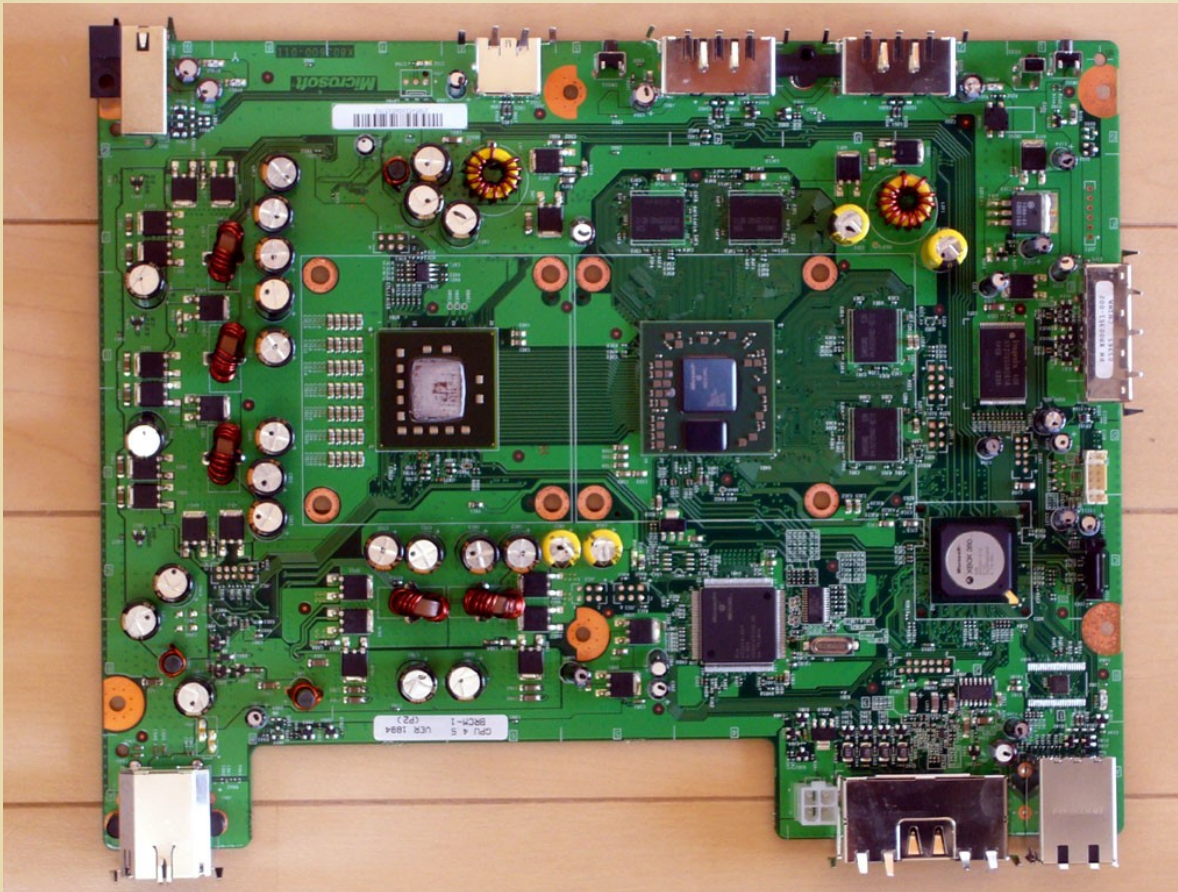


Add-ons:

- ◆ 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



Potential: XBOX 360

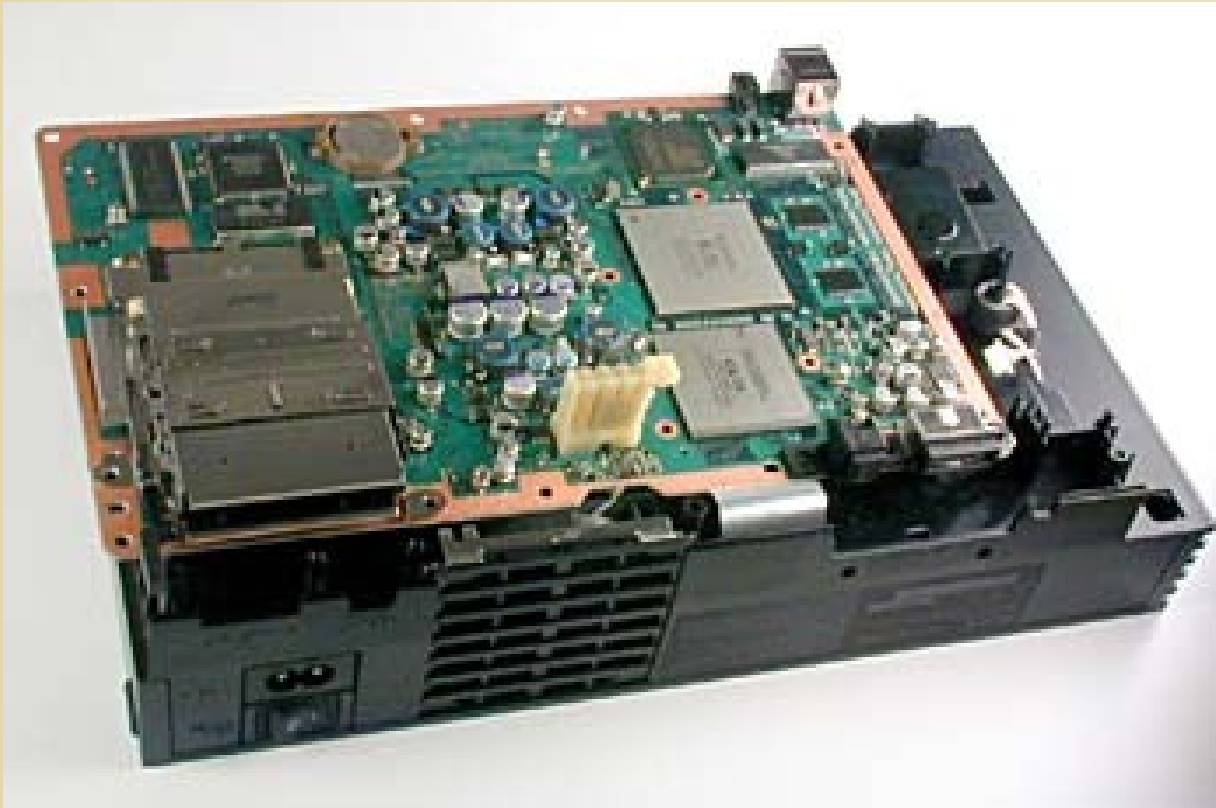


Add-ons / Mods:

- ◆ Upgrade HD 120G or more...
- ◆ 802.11G adapter
- ◆ XBL Vision (Web Camera)
- ◆ USB Keyboard / Mouse



Hardware: Playstation²

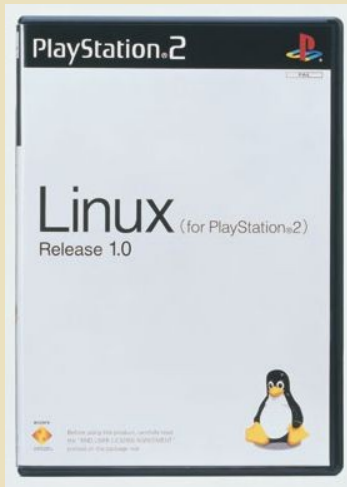


Under The Hood:

- ◆ 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)



Potential: Playstation²



Add-ons:

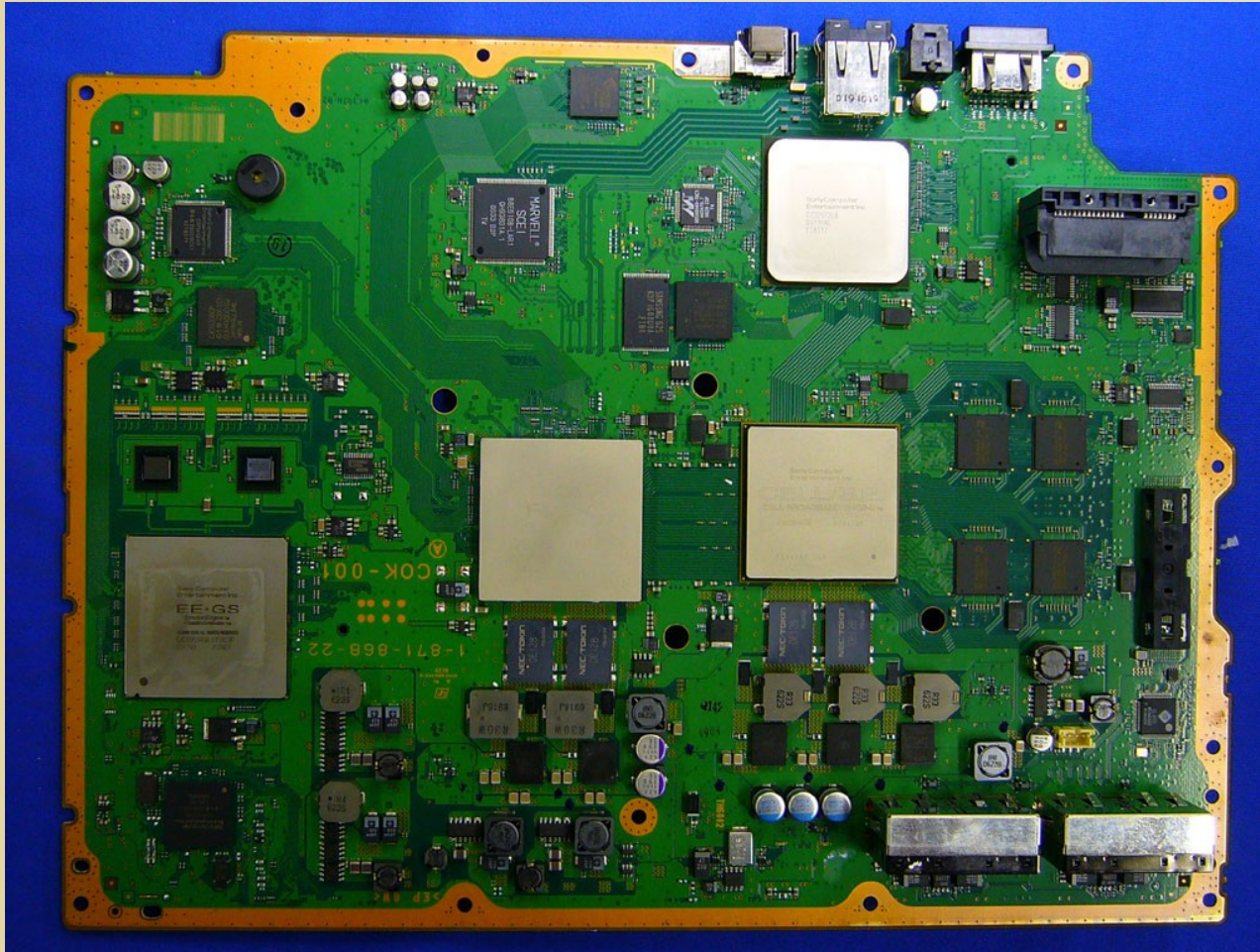
- ◆ Ethernet / Modem / HD assembly
- ◆ ~500G HD maximum**
- ◆ USB keyboard / mouse

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: Playstation³



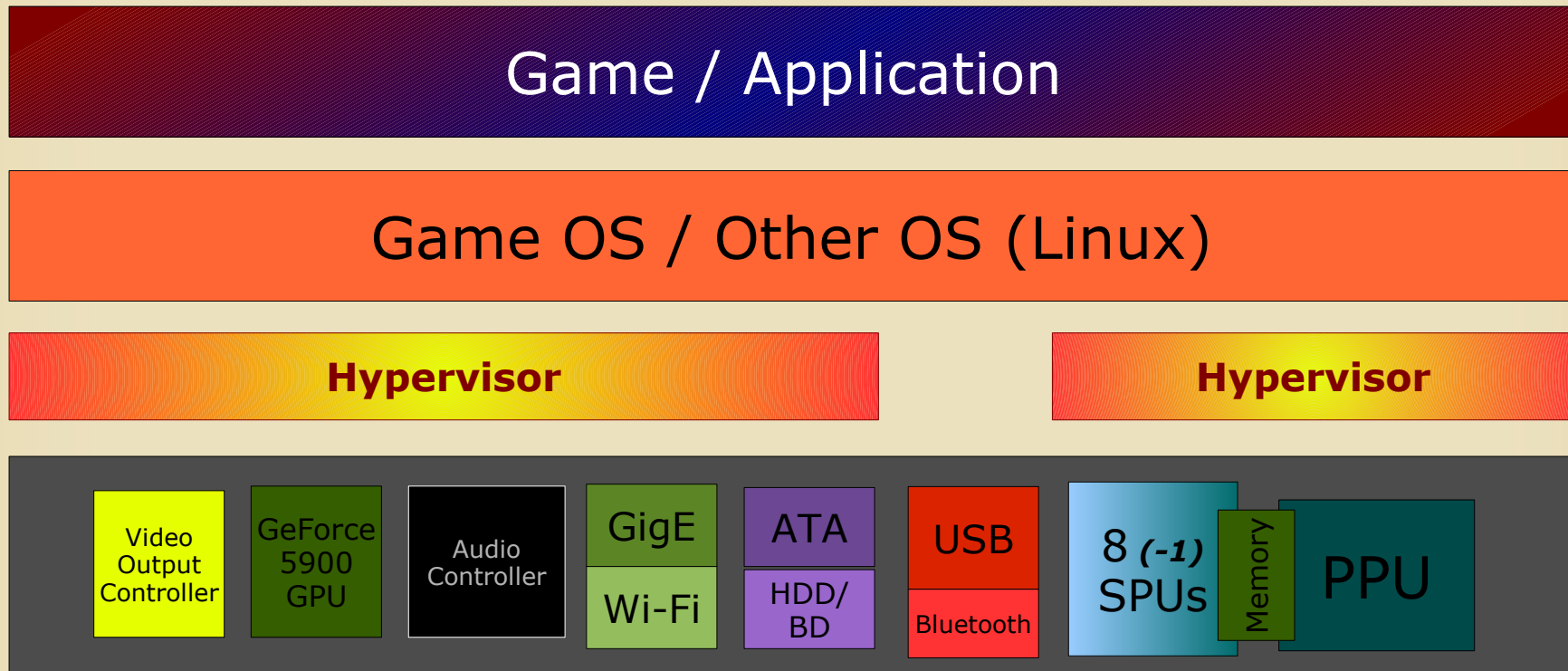
Under The Hood:

- ◆ **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)



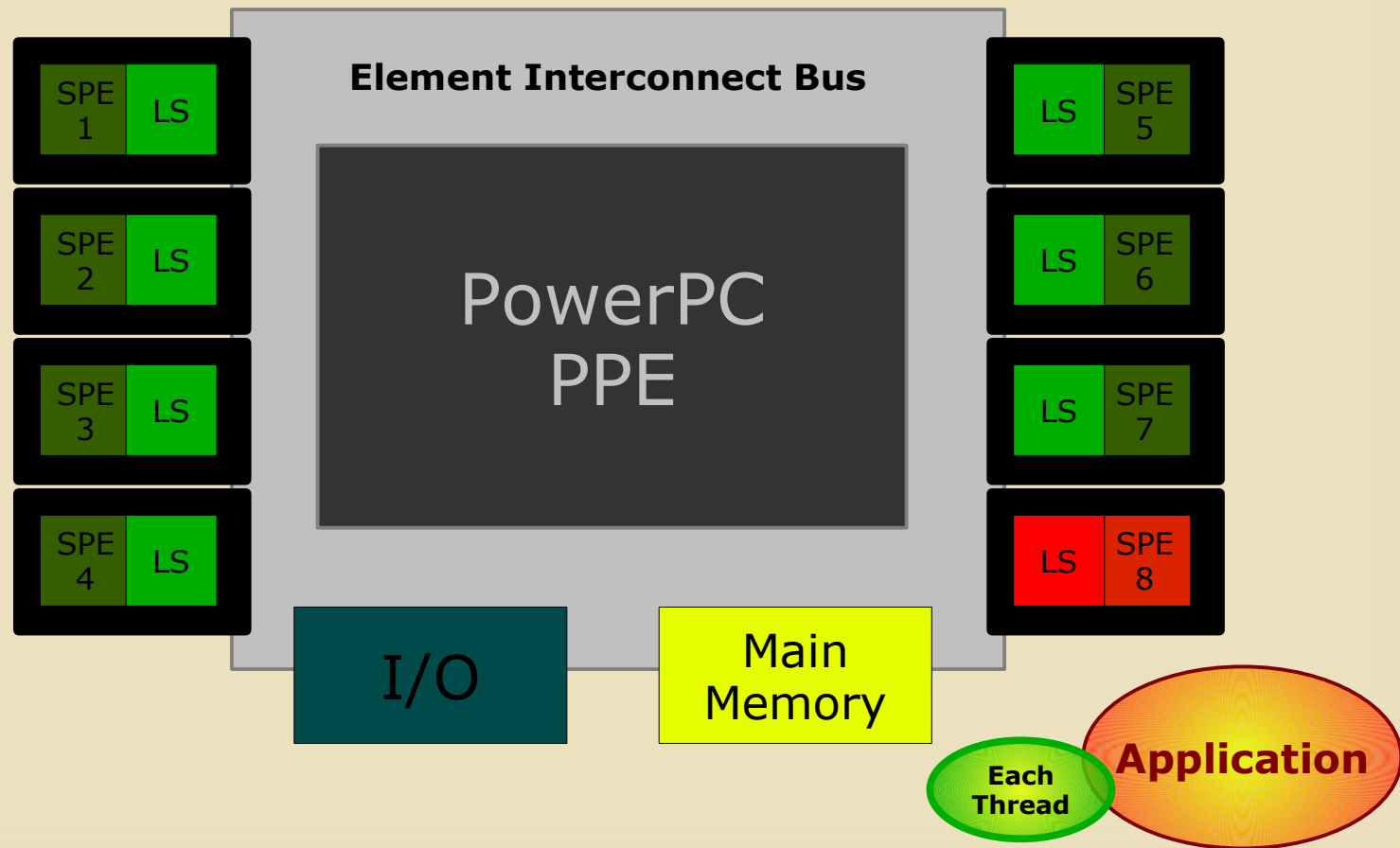
Hardware: Playstation³

Interaction with the PS3 Hypervisor



Hardware: Playstation³

PS3 Cell Processor Security



Potential: Playstation³



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

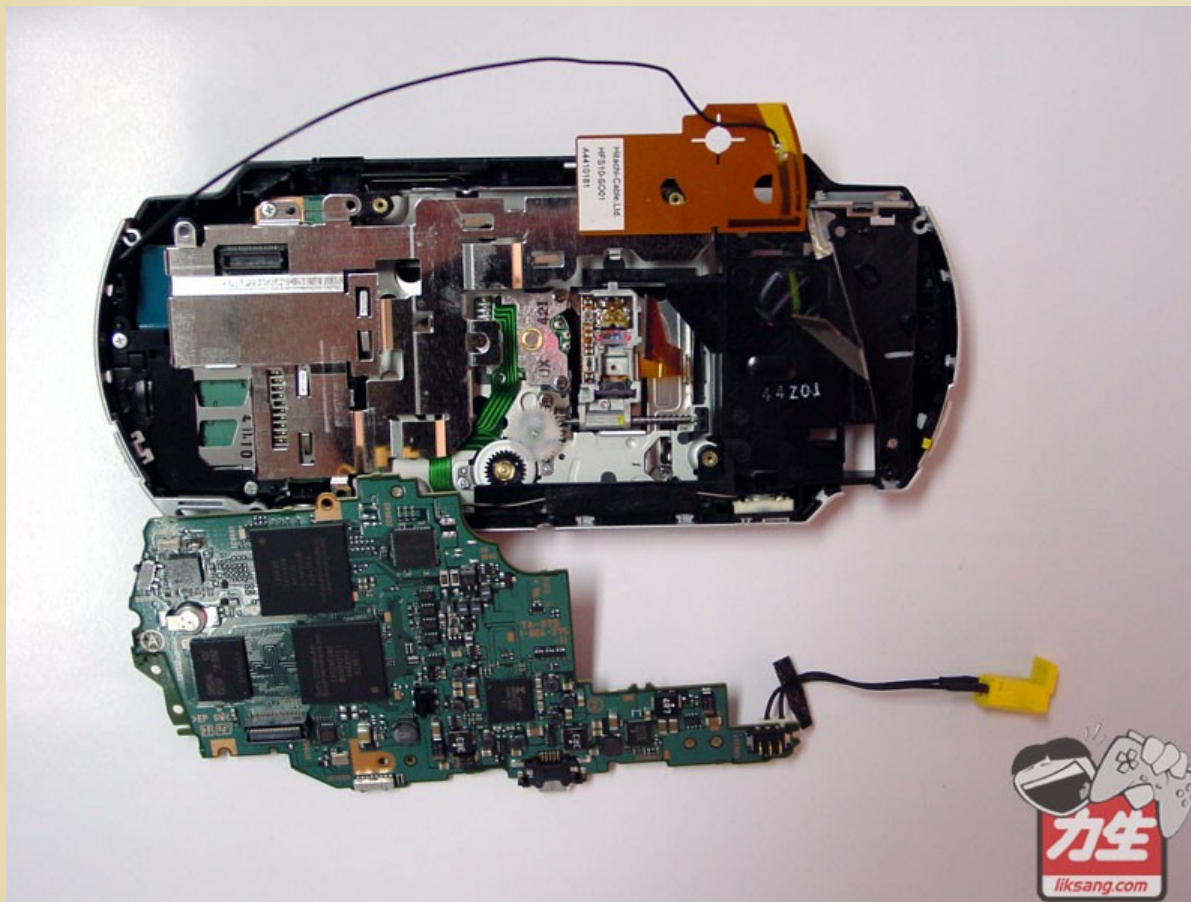
Tricks:

- ◆ 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



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



Potential: GameCube



Add-ons:

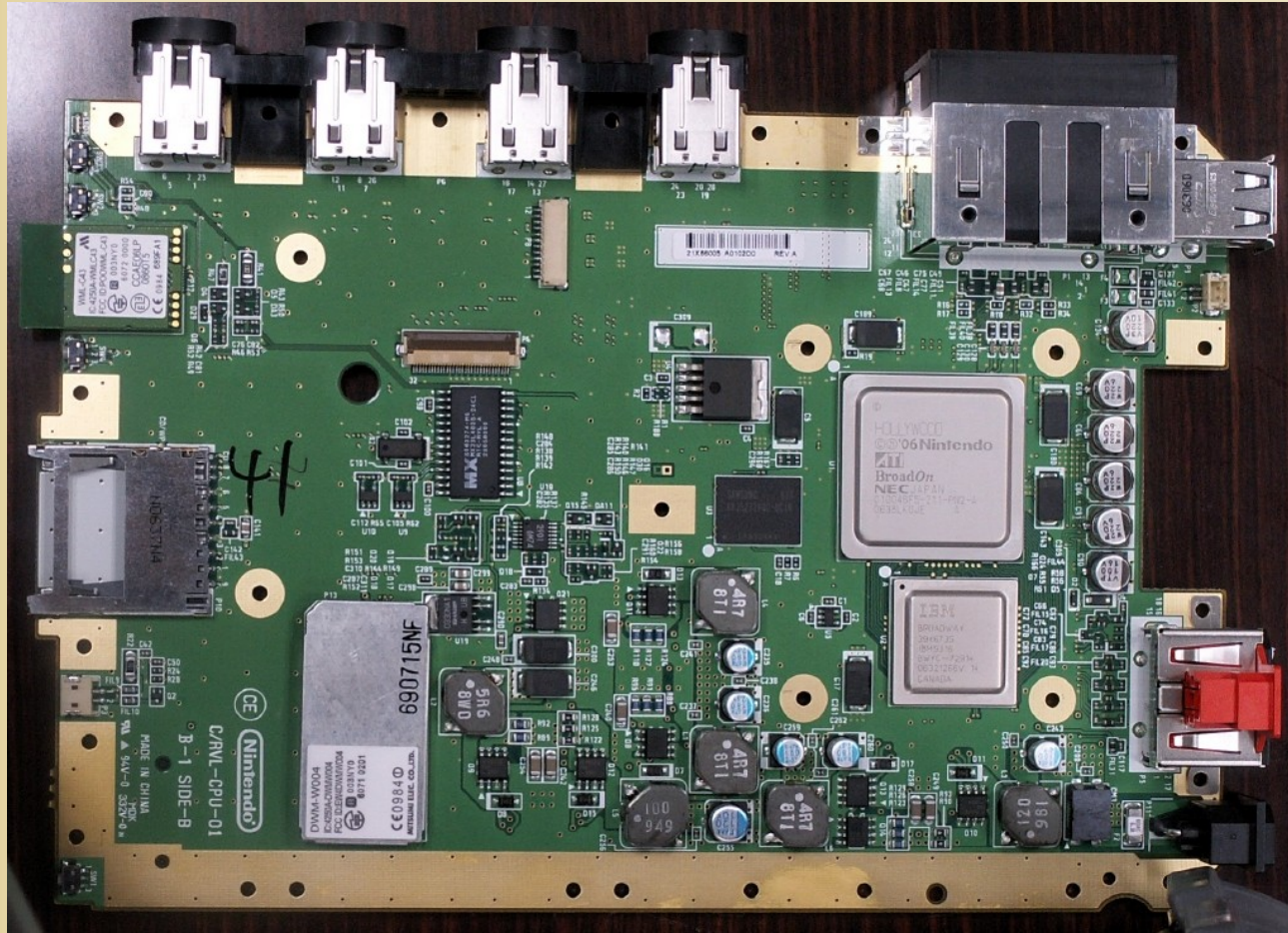
- ◆ Mod chips
- ◆ Keyboard / Analog stick

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)



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



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

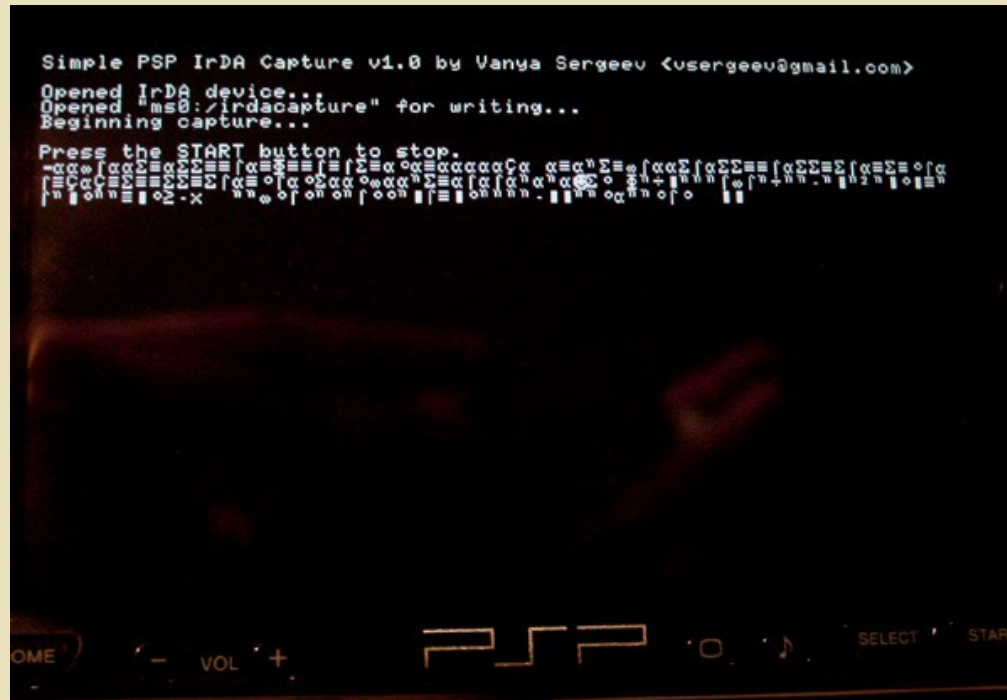
Homebrew is a term frequently applied only to video games that are produced by consumers on proprietary game platforms; in other words, game platforms that are not typically user-programmable, or use proprietary hardware for storage.

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.



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>

Homebrews of Note

[PSP] iR Commander



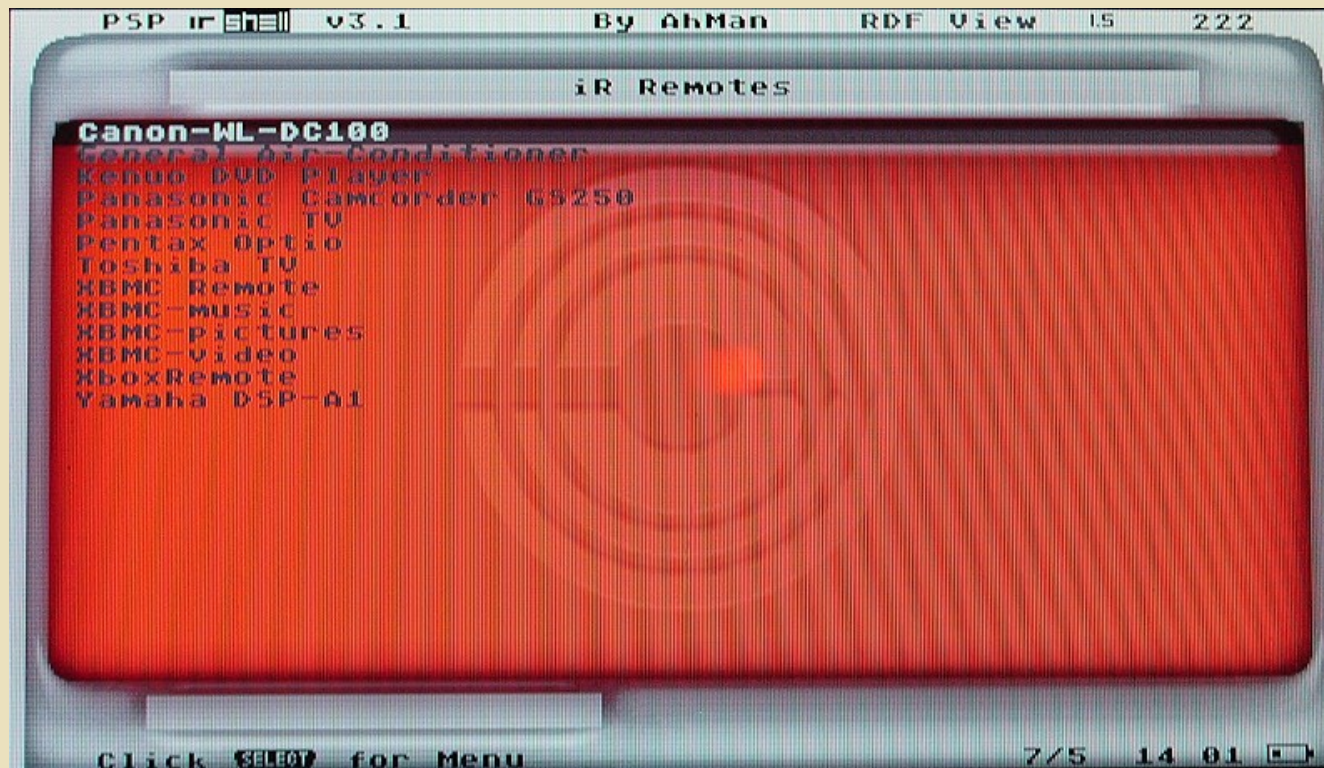
The newest version supports 2,000 controllable infrared devices – for 1.50 users. Check Major Malfunxion's “Old Skewl Hacking Infrared” for why this interesting.



To grab your device (Remote Central): <http://www.remotecentral.com>

Homebrews of Note

[PSP] iR Shell



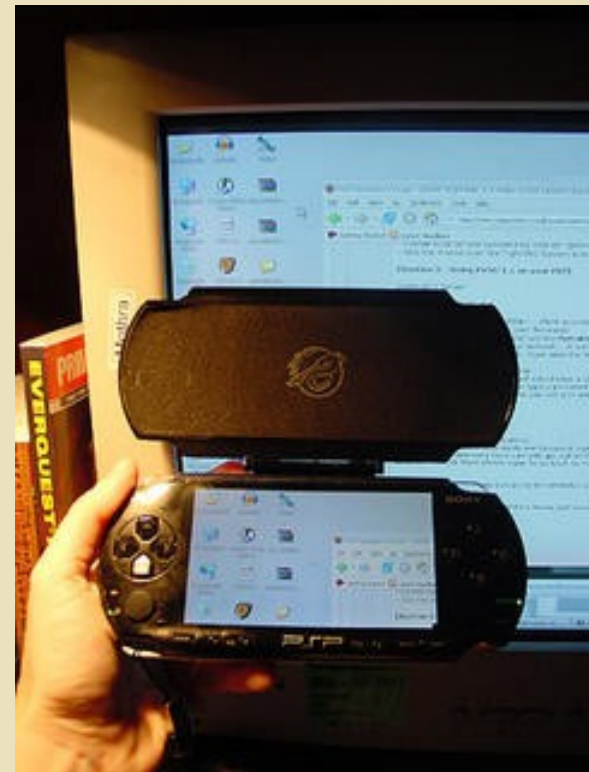
AhMan returns with another homebrew of interest. This one allows for ***more*** IR devices, performs ad-hoc WiFi transfers, throttles CPU speed, DevHook support, nethost redirection, and works on all homebrew-friendly firmwares.



Where to download (My QJ.net): <http://tinyurl.com/32xj99>

Homebrews of Note

[PSP] Portable VNC Viewer



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.



(((TightVNC Install & PSP VNC Video)))

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/>

Homebrews of Note

[PSP] SecureText

```
SECURETEXT V0.1                               GlobWare.com
ms0:/PSP/GAME/FILER/

..
Black.bmp
Blue.bmp
EBOOT.PBP
Green.bmp
Grey.bmp
Long.txt
LongButGood.txt
MENU.BMP
MyLog.txt
ReadMe.txt
ReadMe.txt.sec
ReadMe2.txt
ReadMe2.txt.sec
ReadMe3.txt
ReadMe3.txt.sec
Smaller.txt
Smaller.txt.sec
TEST3.TXT
TEST3.TXT.sec
Tiny.txt
Tiny.txt.sec

Files:23      Mode: 32      Bytes: 5055
X:SECURE  O:DESECURE/OPEN FOLDER  ^:UP  □:VIEW  L1:DELETE  R1:PASSWORD  START:EXIT
```

```
SECURETEXT V0.1                               GlobWare.com
ms0:/PSP/GAME/FILER/

..
Black.bmp
Blue.bmp
EBOOT.PBP
Green.bmp
Grey.bmp
Long.txt
LongButGood.txt
MENU.BMP
MyLog.txt
ReadMe.txt
ReadMe.txt.sec
ReadMe2.txt
ReadMe2.txt.sec
ReadMe3.txt
ReadMe3.txt.sec
Smaller.txt
Smaller.txt.sec
TEST3.TXT
TEST3.TXT.sec
Tiny.txt
Tiny.txt.sec

Source: ReadMe.txt.sec
Dest: Memory File
File: ReadMe.2.txt_

^1234567890- =
abcdefghijklmnop
nopqrstuvwxyz
[]\;'/./

X: SELECT  □: CAPS ON  L1: BACKSPACE  R1: DONE

Files:23      Mode: 32      Bytes: 6748
X:SECURE  O:DESECURE/OPEN FOLDER  ^:UP  □:VIEW  L1:DELETE  R1:PASSWORD  START:EXIT
```

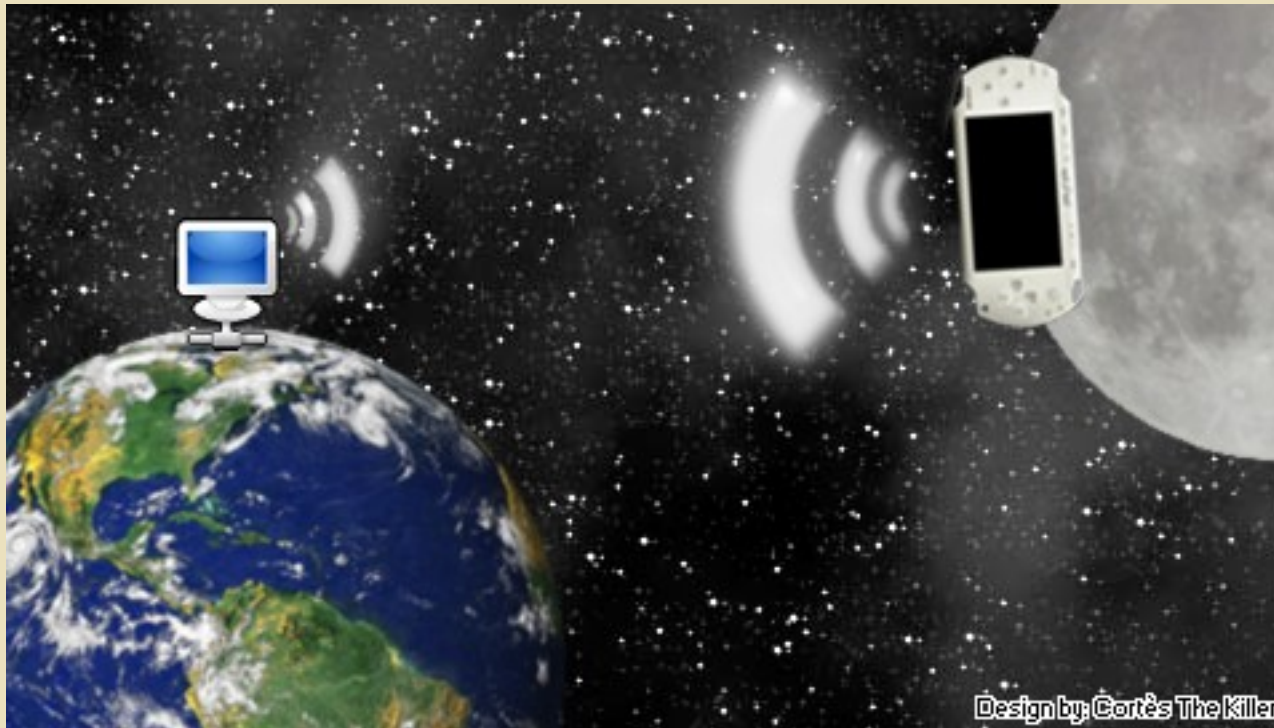
Allows the user to encrypt and decrypt – with RC4.



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>

Homebrews of Note

[PSP] AFKIM

```
Resolving
Resolved, Connecting
Connected, Identifying
&bitlbee
Welcome to the BitlBee gateway!

If you've never used BitlBee before, please do read the help
information using the [help] command. Lots of FAQ's are
answered there.
&bitlbee
Configuration saved
auto-connect = false
auto-reconnect = true
auto-join = true
auto-voice = 60
add

Add an Account
AIM
ICQ
MSN
GTalk
Yahoo

d, press [select] to add one.
```

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

```
Last login: Wed Aug 1 14:48:22 2007 from 54.239.15.100:22
PSP
NetBSD 3.0 (USERS) #0: Tue Feb 7 15:49:12 EST 2006
-[02/12/07]-(S%$g)-----
Pls to be looking in /home/old_users, and cleaning out your old dirs;
That jank has been sitting around for over a year now. We probably ;
out to start archiving accounts of people who haven't authed since ;
the move to the new machine. Call this cleanup in preparation for ;
the move to 757Labs. ;
-[07/01/07]-(S%$g)-----
Finally got alpine (Pine's replacement) to build. It's installed in ;
/opt, but is symlink'd to /usr/local/bin/alpine. If you need an ;
example .pinerc, let me know. I've figured out how, now, that you ;
can use IMAP, with all of your standard courier-imap folders, and ;
it'll only prompt you for your password once, when you open alpine. ;
```



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



(((PSPSSH Video)))

Where to download PSPSSH2 (ZX81's Website):<http://tinyurl.com/22fgmh>

(((PSPSSH Video)))



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/>

Homebrews of Note

[PSP] WiFi Sniffer



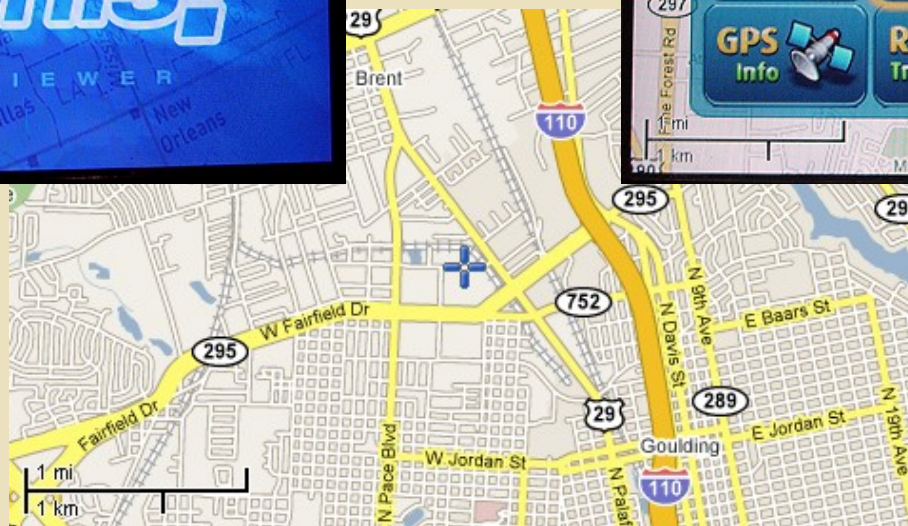
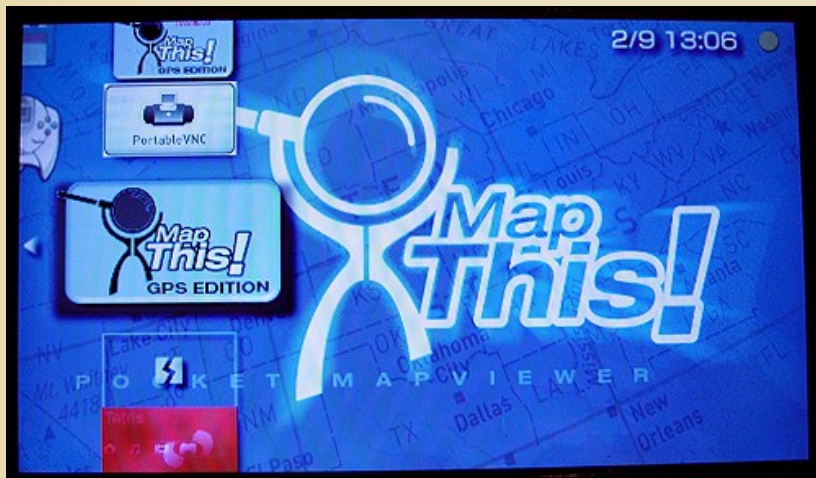
Jean Yves Lamoureux's basic WiFi Sniffer.



Where to download WiFi Sniffer (Max Console): <http://tinyurl.com/yoggvz>

Homebrews of Note

[PSP] MapThis!



(((MapThis! Video)))

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

(((MapThis! Video)))



YouTube version: <http://www.youtube.com/watch?v=jcMtIEFCZSo&>
To download this video go to <http://haksys.schleppingsquid.net/Files/index.php?path=DefCon15+Material/>

Homebrews of Note

[PSP] PSPInside

```
----< PSPInside V0.1multipurpose0 /-/itmen Productions >----
Trigger L/R : Tab -/+ | TrigL/R+Home : Quit

System | Memory | Disasm | Register | Syscalls | IRQs |
-----|-----|-----|-----|-----|-----|
Module list:
8805801c : sceKernelUtils
8805a950 : sceMemImd
8805abb4 : sceModuleManager
88063418 : sceInit
88068d0c : sceLoadExec
88077200 : sceSYSREG_Driver
8807ab54 : sceGPIO_Driver
8807c178 : scePWM_Driver
8807d3b4 : sceI2C_Driver

Segments:
8807c500 - 8807dbc4
8807abd0 - 8807dc10

Module 20 of 64 :
Module ID : 00ccf24d
Name : sceI2C_Driver
Attributes : 00001007
Module entrypoint : 8807d3b4
# of segments : 1
text seg. address : 8807c500
text seg. size : 000016c0
data seg. size : 00000040
bss seg. size : 0000001c
gp : 88085c00

Analog U/D : Thread -/+ | Square :
Select : Scrollmode | Cross :
Triangle : Load functions | Circle :
Start : USB on/off
```

```
*** PSPInside - TD.9g (c) 2005 by /-/itmen Mtion toolbox ***
Trigger L/R : Tab -/+ | TrigL/R+Home : Quit

<IRQs | Videoram | Patch? | Console | Profiler | Config >
-----|-----|-----|-----|-----|-----|
00000000 | 0 | (unknown)
00000000 | 0 | (unknown)
00000000 | 0 | (unknown)
00000000 | 0 | (unknown)
8807b1ee | 10200 | GPIO
00000000 | 0 | ATA_ATAPI
880f2c26 | 0 | UmdMan
8812a726 | 111 | MScm0
881838aa | 47756 | Wlan
00000000 | 0 | (unknown)
880c2c76 | 0 | Audio
00000000 | 0 | (unknown)

(unknown)
IrDA
mer0
mer1
mer2
mer3
id0

Calls 0
Common 00000000 GP 00000000
ctrlLevel 0 Enabled 0
k_lo 00000000 totalclk_hi 00000000
lock_hi FFFFFFFF
clock_hi 00000000
~0ead0e00
```

```
*** PSPInside - THE multipurpose PSP information toolbox ***
Trigger L/R : Tab -/+ | TrigL/R+Home : Quit

<Disasm | Register | Syscalls | IRQs | Videoram | Patch? >
-----|-----|-----|-----|-----|-----|
[InX] Kernel@RAM(4MB): 00000000
88000000 : c0 00 00 00 27 addiu $sp, 0x0($sp)
88000004 : 20 00 00 00 00 addiu $sp, 0x0($sp)
88000008 : 34 00 00 00 00 addiu $sp, 0x0($sp)
8800000c : 3c 00 00 00 00 addiu $sp, 0x0($sp)
88000010 : 28 00 00 00 00 addiu $sp, 0x0($sp)
88000014 : 28 00 00 00 00 addiu $sp, 0x0($sp)
88000018 : 28 00 00 00 00 addiu $sp, 0x0($sp)
8800001c : 1c 00 00 00 00 addiu $sp, 0x0($sp)
88000020 : 18 00 00 00 00 addiu $sp, 0x0($sp)
88000024 : 21 90 c0 00 00 addiu $sp, 0x0($sp)
88000028 : 14 00 00 00 00 addiu $sp, 0x0($sp)
8800002c : 20 00 00 00 00 addiu $sp, 0x0($sp)
88000030 : 20 00 00 00 00 addiu $sp, 0x0($sp)
88000034 : 14 00 00 00 00 addiu $sp, 0x0($sp)
88000038 : 14 00 00 00 00 addiu $sp, 0x0($sp)
8800003c : 3c 00 00 00 00 jal $zero, 0x8800c800
88000040 : 04 00 00 00 00 jal $zero, 4($sp)
88000044 : 21 20 00 00 02 addiu $a0, $zero
88000048 : 03 00 00 0e jal $zero, 0x88000fbc
8800004c : 21 10 40 00 addiu $a6, $zero
88000050 : 61 00 40 10 beq $a6, $zero, 0x880001d8
88000054 : 21 98 40 00 addiu $a3, $zero
88000058 : 10 00 64 33 andi $a5, 0x0018
8800005c : 01 88 15 3c lui $j, 0x8801

Analog U/D : Addr -/+ | Circle : Section change
Triangle : Enter address | Square : More functions
Cross : Memory(Addr.) | Start : Dump section /0ead0e00
Select : Scrollmode
```

/-/itmen 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/>

Lumines Downgrader

- ◆ 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...



[Lumines \(PlayStation Portable\)](#)
Platform: **Sony PSP**
Genre: **Action, Adventure**
Release Date: **2005**

\$0.01 - \$144.99
175 items for purchase

4.5/5 from 23 reviews

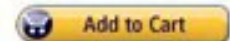
\$125.00
+ \$3.99 shipping

Used - Like New

Seller: **DAROGA28**

Rating: ★★★★★ **92% positive** over the past 12 months (24 ratings,) 30 lifetime ratings.

Shipping: In Stock. Ships from MI, United States Expedited shipping available See [shipping rates](#)

 Add to Cart

OR
[Sign in](#) to turn on 1-Click ordering.



Prices confirmed 04 July 2007 on Amazon.com and eBay.com

Homebrews of Note

[DS] DSFTP

```
DSFTP v2.2                                © 2006 Björn Giesler
                                           <bjoern@giesler.de>

Server running on port 21.
Screensaver: 60 seconds
Wake on Log: ON
Press A+B+X+Y for safe poweroff.
** New FTP control connection 2
** FTP conn 2 from 192.168.1.10.
User bjoern logged in (root=/, home=/, write=yes)
** Data conn 5 from 192.168.1.10.
** Closing data connection 5.
Storing /sshot0.ppm

IP 192.168.1.101 - 1 connections
```

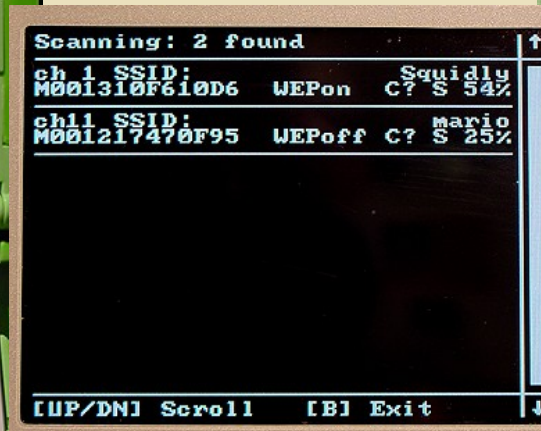
Björn Gieslers Webseiten's FTP server application.



Where to download DSFTP (Giesler.biz): <http://tinyurl.com/272pnf>

Homebrews of Note

[DS] Wifi Lib Test



Stephen Stair's bare-bones AP finder and packet capture application.



For more info: <http://www.akkit.org/>

Homebrews of Note

[DS] AirCrackDS

```
** HircrackDS **  
no /ptw.cap  
Recovering WEP KEY...
```



Retrohead's simple WEP cracking application.



Where to download AirCrackDS (1Emulation): <http://tinyurl.com/253471>

Homebrews of Note

[DS] AirePlayDS

```
AirePlayNDS "Early Build" by JSR
-----Debug-Print-----
Wifi Init!
Scan for AP!
Press A to stop Scanning!
Number of AP: 0

Scan Finished!
```

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



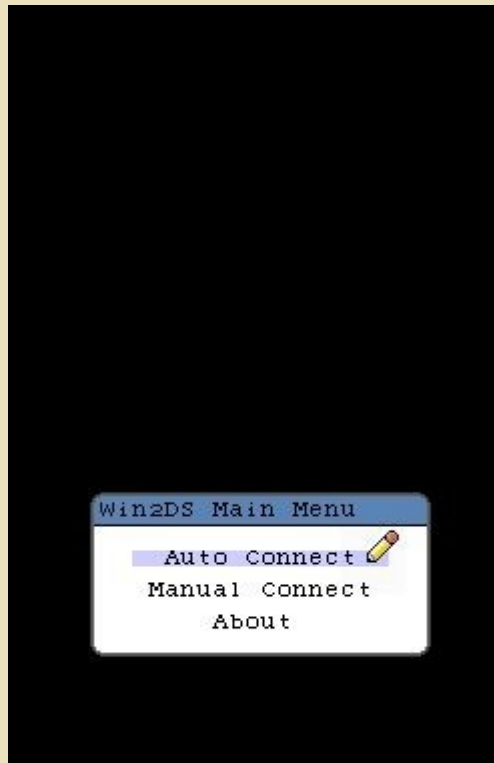
Pointless' custom protocol driven remote PC controller.



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>

Homebrews of Note

[DS] Lilou FTP Server

```
fat en cours d'initialisation
fat initialis 
Wifi lib test - Alain
Version 0.3a
Build Date:Jun 23 2007 19:54:30
Waiting for ARM7 to init..
ARM7 Init Confirmed.
Rename file failed %d
Wait Confirmed.
Picked: Launch Quick ftp server
Connection failed - Returning to
main menu
Returned from ftp server

Quick ftp server
Quick ftp client
ftp client bookmark
Connect to an AP
Configure wifi
Tools

[UP/DN]Move[A/Touch]Sel
```

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 Paralyser.



Where to download MoonShell (Infantile Paralyser):<http://tinyurl.com/ge6bs>

Concealment

... you put that console WHERE??
(No Goatses were hurt in this section)



Concealment



Who in this picture does ***NOT*** have a pocket video game on them?

Hint: Probably not the young geisha.



Concealment



**Do you know if game systems are allowed in your work spaces?
What about the customers? Is there a policy covering you??**



Concealment



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 ...



Fuzzy Finds

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.



Fuzzy Finds

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**.



Fuzzy Finds

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.**



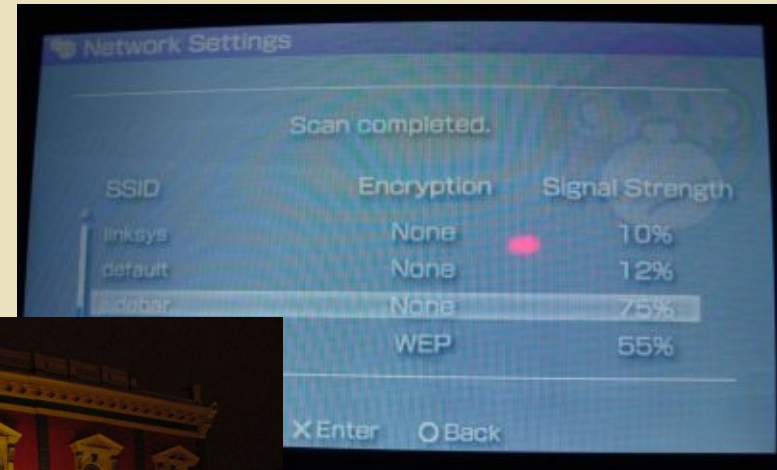
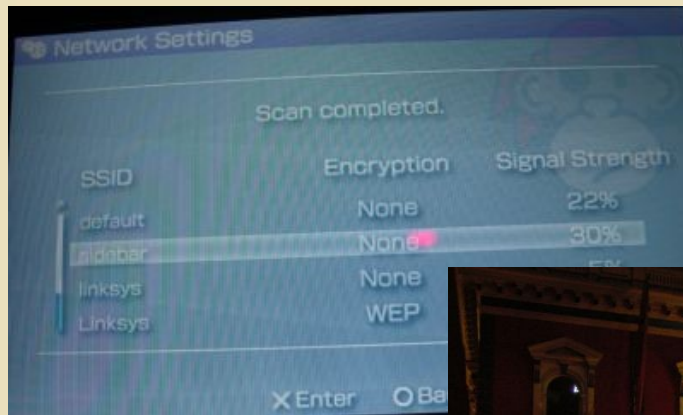
Fuzzy Finds

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...



Really Alternative



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.



Sources

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

