Demystifying..
Game Console Security

Over 10 years of Ownage unraveled

blasty <peter@haxx.in> (@bl4sty)

Introduction / Outline

- Game consoles from 2003 till 2013
- Yes, this includes handhelds as well.
- Won’t bore you with much architectural information, just juicy hax and anecdotes.

Who am I?

- Hacker
- Console/homebrew scener
- Avid CTF Player (Eindbazen/NL)
- Twiizers / failOverflow / Eindbazen
- HITB Groupie

Game Consoles?

- Kiddies like to play videogames.
- So do adults, heh.
- What goes on inside of these boxes? :)

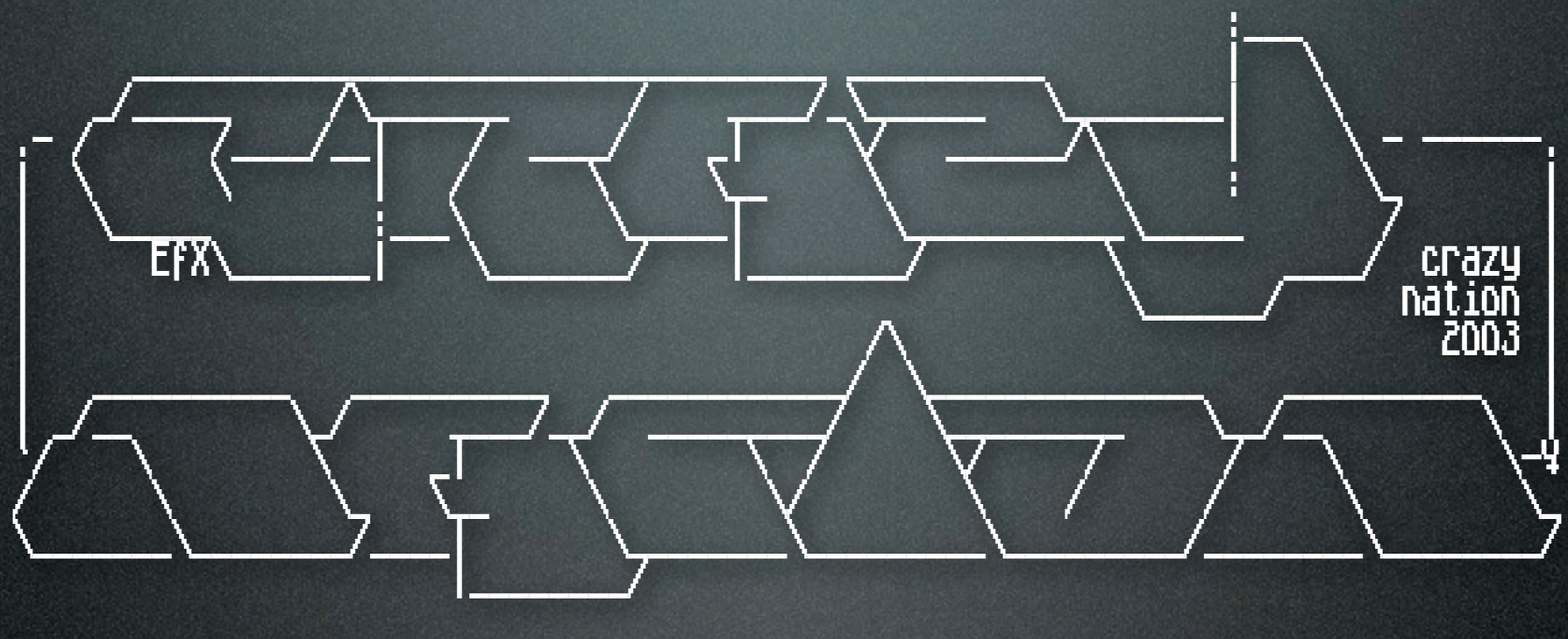
Entities

- Hackers (curious people)
- Homebrewers (application & game dev for alt. systems)
- Warezers (free games)
- Companies ($$$)
- Lots of overlap between those ;-)

2001 - Nintendo Gamecube

IBM PowerPC “Gekko” @ 486 MHz
24MB main, 16MB aux, 3mb gfx
ATI “Flipper” GPU

August 2003 - PSUL



CRAZY NATION PRESENTS

PSUL 1.1 - GAMECUBE CODE UPLOADER

.oOo. RELEASE NOTES .oOo.

YYYYYEEEEEESSSSSSSSSSSSSSSSSSSS!!!!!!!!!!!!!!!!!

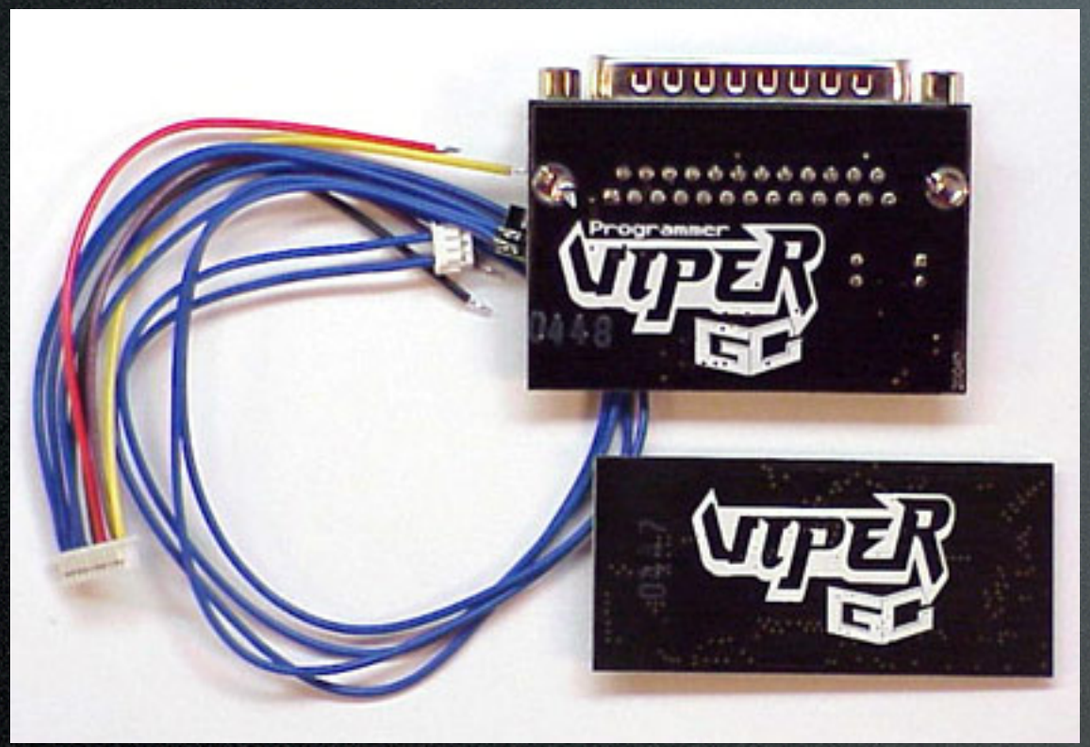
I had this dream, to run code on my dear sweet cube...
And one day I met this guy... Crusader of Kalisto, that made the dream comes true... He is the man behind the PSO backdoor discovery and exploited it at first, so he has my eternal love respect and devotion ;-)

BBA + PSO = HAX!


NINTENDO
GAMECUBE
BROADBAND ADAPTER
HI SPEED PORT


NINTENDO
GAMECUBE
PHANTASY STAR™
ONLINE
ファンタシースターオンライン
EPISODE I&II
Includes free 30 day Hunters Licence subscription fee*
Offline split screen action for up to 4 players
SEGA
PAL
LICENSED BY
Nintendo

ViperGC Modchip



IPL/BIOS Encryption

- Boot flash connected to EXI bus
- EXI is just SPI
- ROM Comms is ciphered using LFSR
- Accidentally clocks out shift register during dummy clocks..
- Can be used to recover keystream and replace the BIOS/Firmware

Mentalcube's COBRA

Utopia's ANACONDA

Once again we are proud to say :

"An alle : Maulhalten, jetzt, sofort !"

-- The senior members of Utopia present you today : --

- Anaconda04 -

A viperfree Cobra04 DVD-R boot core recode in pure assembly!

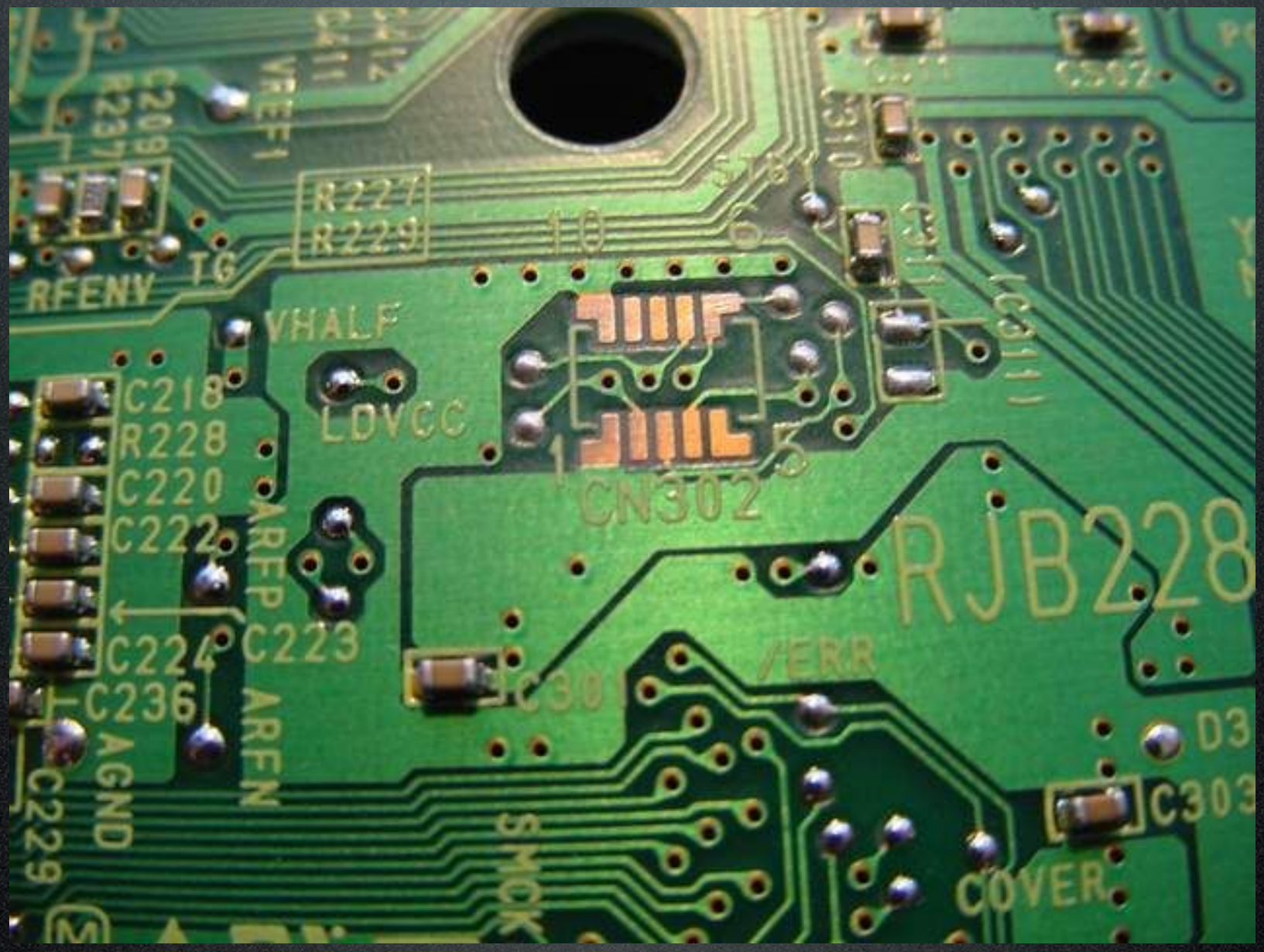
Gamecube DI Debug

- DI bus is used for sending commands from PowerPC to DVD drive. (Drive Interface)

- Unlock debug features using
  “**FF 01 MATSHITA 02 00**” and
  “**FF 00 DVD-GAME 03 00**”

- “**FE 01 01 00** <OFFS> <LEN> <DATA>”
  can be used to poke into drive mem.

CN302 Debug Port



First used in the famous XenoGC Modchip

2004 - Nintendo DS

ARM9 @ 66MHz, ARM7 @ 33mhz
4MB RAM, 256K VRAM

Code Execution (NDS)

- Communications with cartridge are mostly encrypted..
- .. but retrieving the header is done in plaintext. Header is protected by simple CRC16 checksum
- Entrypoint for ARM7/ARM9 CPU's can be pointed into 0x08000000 region to jump to data on GBA cart.

Code Execution (2)
Cartridge Passthtrough

Dumping NDS(i) BIOS

- ROM/BIOS mapped at 0x00, we can't read it. :-(
- However, we can execute it.. SVC code lives here.
- Code executed from this region *can* read itself..

Dumping NDS BIOS (2)

- We fill all general purpose registers with a pointer to BIOS/ROM region we normally can't access.
- We init a timer & jump randomly into the BIOS/ROM region and interrupt after a couple of instructions (based on timer IRQ)
- We examine registers to see if we hit an LDR(h/b) by accident which leaks BIOS region data :-)

2006 - Playstation 3

Cell CPU, 3.2ghz PowerPC, 8 SPU's. 256MB XDR RAM, 256MB GDDR3 VRAM, Bluray, WiFi

OtherOS Pwnage

- OtherOS was a nice feature by Sony to run alternative operating systems on PS3.
- geohot claimed first blood through a memory bus glitch attack.
- Hypervisor exposed. Sony cancels OtherOS. Hackers enraged.

PSJailbreak

- Run arbitrary code in LV2 context
- Based on exploit in the USB stack.
- Device emulates a HUB with multiple devices attached
- Triggers a use-after-free vulnerability in USB descriptor parsing.
- Reversed and cloned in record time.

fail0verflow @ 27c3 (december 2010)

- ECDSA Failure
- Linux showed booting on PS3 Slim (lightning talk)
- Lots of media buzz..

PS3 Aftermath

“ props to fail0verflow for the asymmetric half
no donate link, just use this info wisely
I do not condone piracy
if you want your next console to be secure,
get in touch with me. any of you 3.
it'd be fun to be on the other side.”

-- geohot

Legal Troublez.

- Sony starts sending out all kinds of subpoenas.
- Sony ramps up for sue'ing some individuals.

Legal Troublez (2)

DOCUMENT REQUESTS

1. All information and documents related to the use of your service(s) to register, create, maintain and/or use the Twitter account associated with Twitter Usernames “KaKaRoToKS”, “gnihsub”, “pytey”, “bl4sty”, “marcan42”, and “fail0verflow”, located respectively at <http://twitter.com/kakarotoks>, <http://twitter.com/gnihsub>, <http://twitter.com/pytey>, <http://twitter.com/bl4sty>, <http://twitter.com/marcan42>, and <http://twitter.com/fail0verflow>.

EFF To the rescue..

- Hooks us up with a lawyer.
- Lawyer is a pretty helpful and informative dude, but won't keep working for free forever. :-(:-P
- .. luckily most subpoena's get initially quashed

EFF To the rescue.. (2)

" I was informed today by EFF that the judge was furious that Sony had served subpoenas before she decided whether to allow them or not.

As a consequence, she quashed all of the subpoenas, and directed Sony to inform the recipients that the subpoenas were withdrawn. "

EFF To the rescue.. (3)

" Here's some good news for you. Take a look at p. 10 of 17 (see header) -- a complete and indefinite suspension of subpoenas regarding the individual defendants. Although you aren't (I think) named specifically, I think the intent is clear: Sony is losing interest in the individual defendants. "

\o/

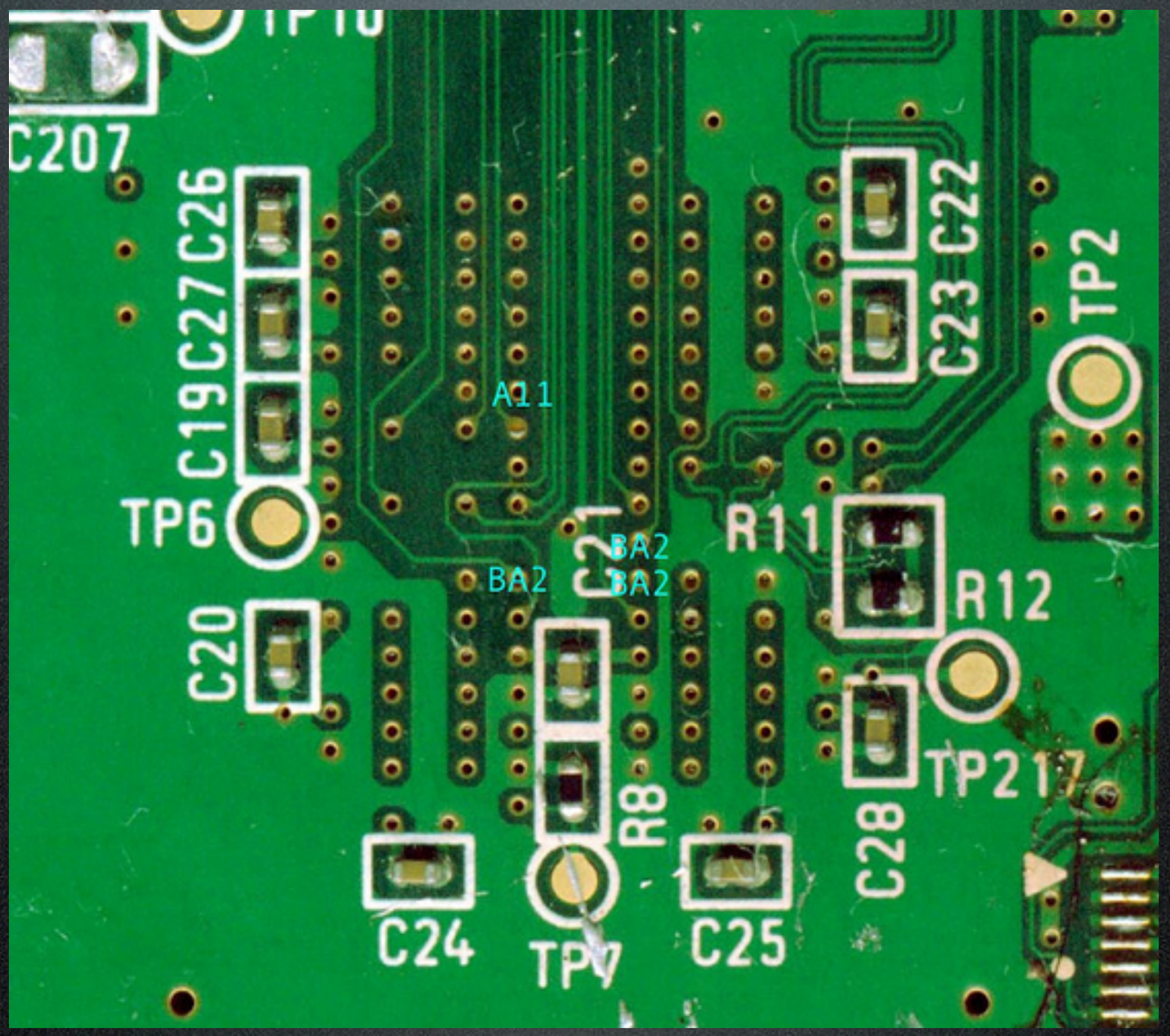
Sony Legal Roundup

- Nobody gets into any real shit(tm)
- Geohot and one US based failOverflow member settle with Sony never to touch/break a sony product again. ;-)
- Looks like Sony Computer Entertainment of Europe was less interested in suing people than Sony Computer Entertainment of America was. ;-)

2006 - Nintendo Wii

PowerPC “Broadway” processor, ATI “Hollywood” GPU, 64MB GDDR3, NAND Flash, SD storage, WiFi

Tweezer Attack



Starlet in Hollywood

- It turns out, Nintendo burried a security processor in the GPU die.
- The GPU's codename is "Hollywood", hence the nickname "Starlet" for the security CPU.
- Based on ARM926EJS.
- OS Running on starlet is called "IOS". Not to be confused with Cisco/iPhone

Trucha Bug Fakesigning

- Nintendo fucked up. Bigtime.
- Comparing a **binary SHA1 hash** using **strncmp()** is **not** a good idea.
- Vulnerability was attempted to keep a secret for a while.

Twilight Hack

- Classic stack smash in Zelda: Twilight Princess save file data.
- EPWNAAAAAAAA.....
- Allows for arbitrary code execution on the PowerPC

Twilight Hack

The Homebrew Channel

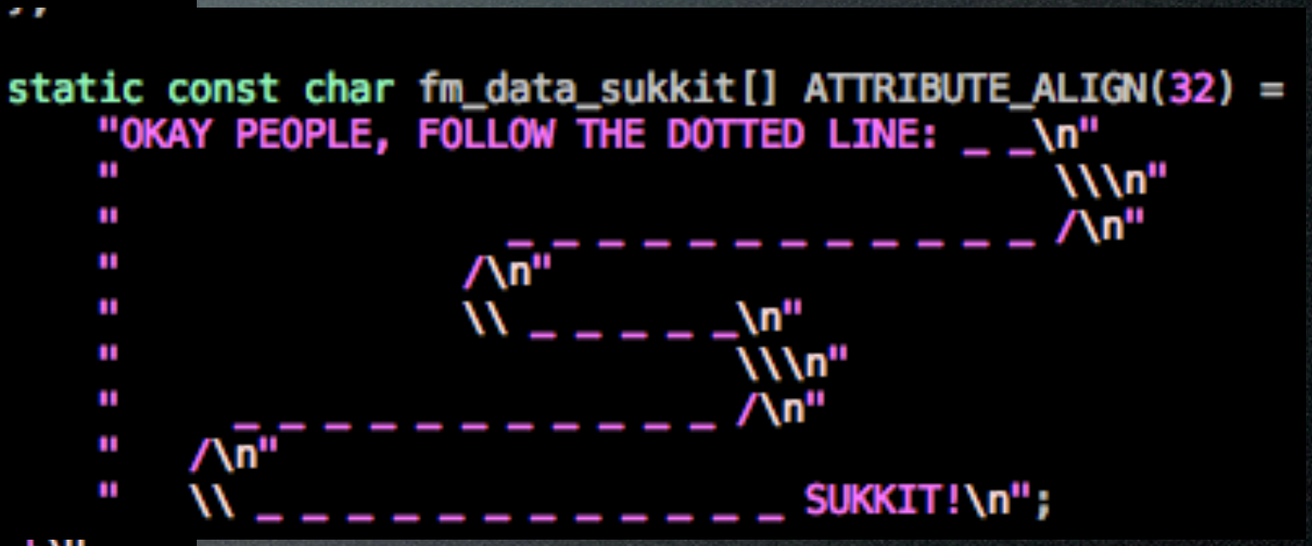
BootMii

- Bootloader (BOOT2) replacement for Nintendo Wii consoles with vulnerable bootrom. (trucha bug)
- Allows for lowlevel NAND backup and recovery
- Powered by mini (custom IOS firmware) and ceiling_cat (barebones graphical PPC frontend)

Bootmii (2)

C3lL1NG_C4T UI interface

Frustrating Researchers

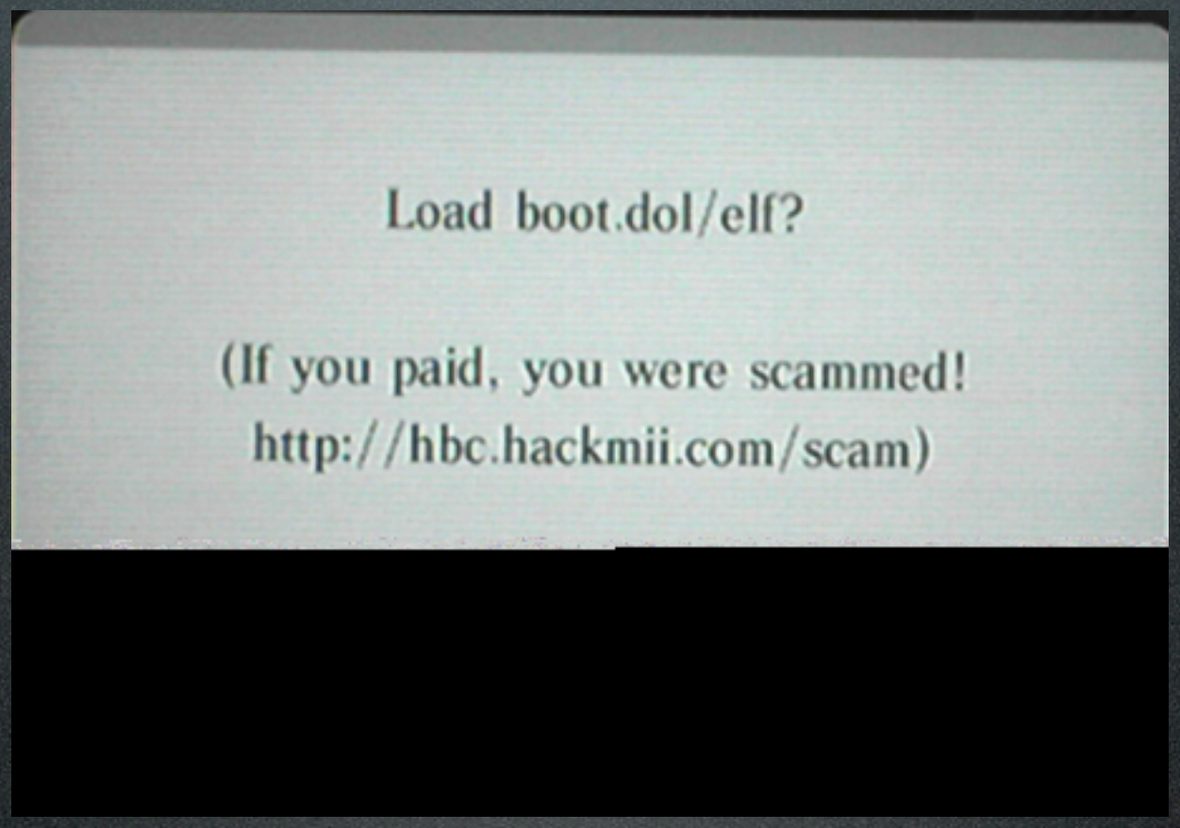


"If they try to pick our stuff apart, they're gonna have a bad time"

BannerBomb

- Exploit for savegame “banner” data by comex.
- Got killed by Nintendo, and then revived by comex.
- First exploit that didn’t require a specific commercial game to function.

BannerBomb


Load boot.dol/elf?
(If you paid, you were scammed!
http://hbc.hackmii.com/scam)

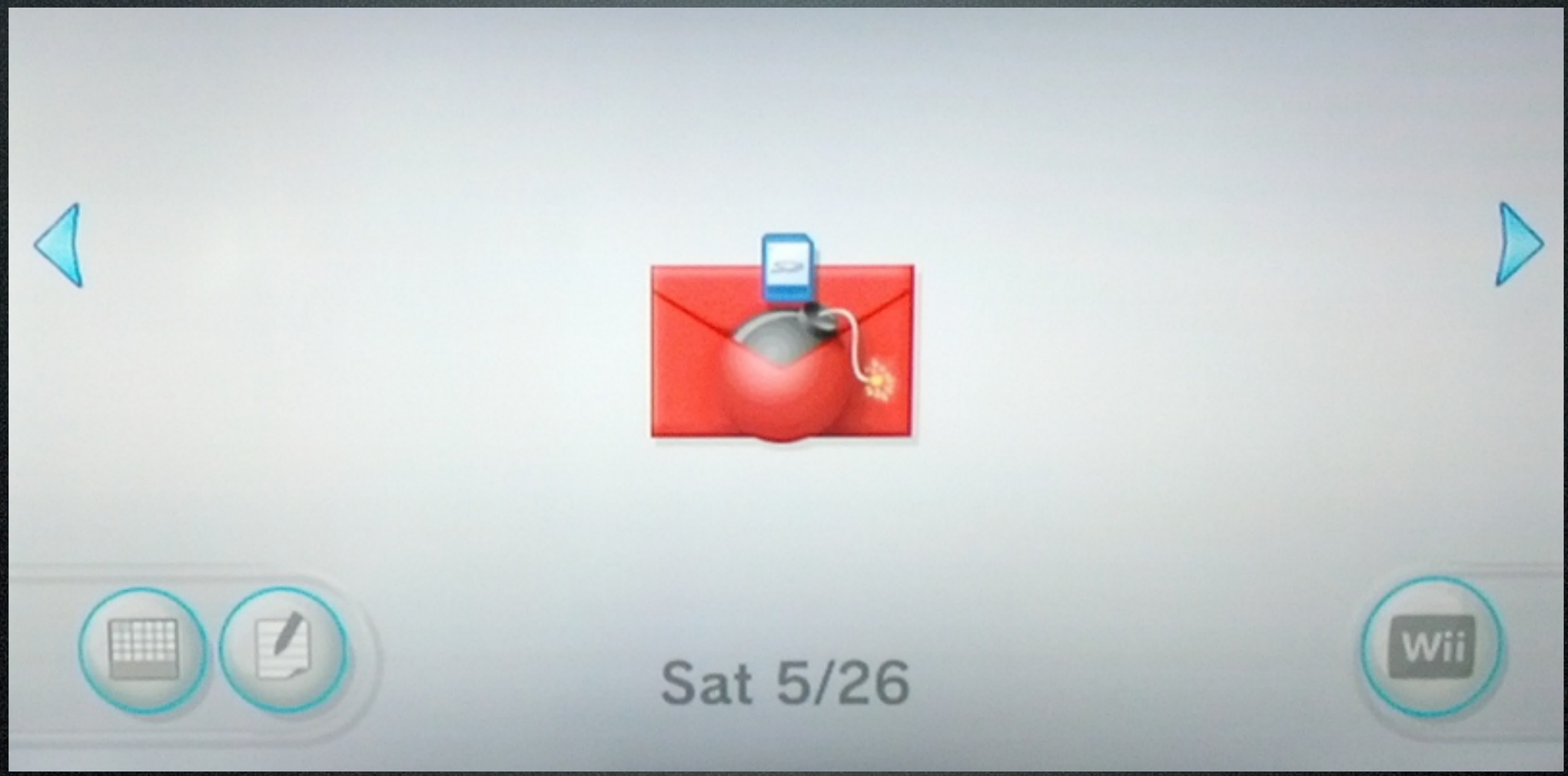
LetterBomb

- Crafted by tueidj and yours truly.
- Latest exploit that doesn't require a game.
- Exploits a buffer overflow in the email file format
- Still works on recent consoles. Use http://please.hackmii.com to liberate your Nintendo Wii today!

Crafting a LetterBomb

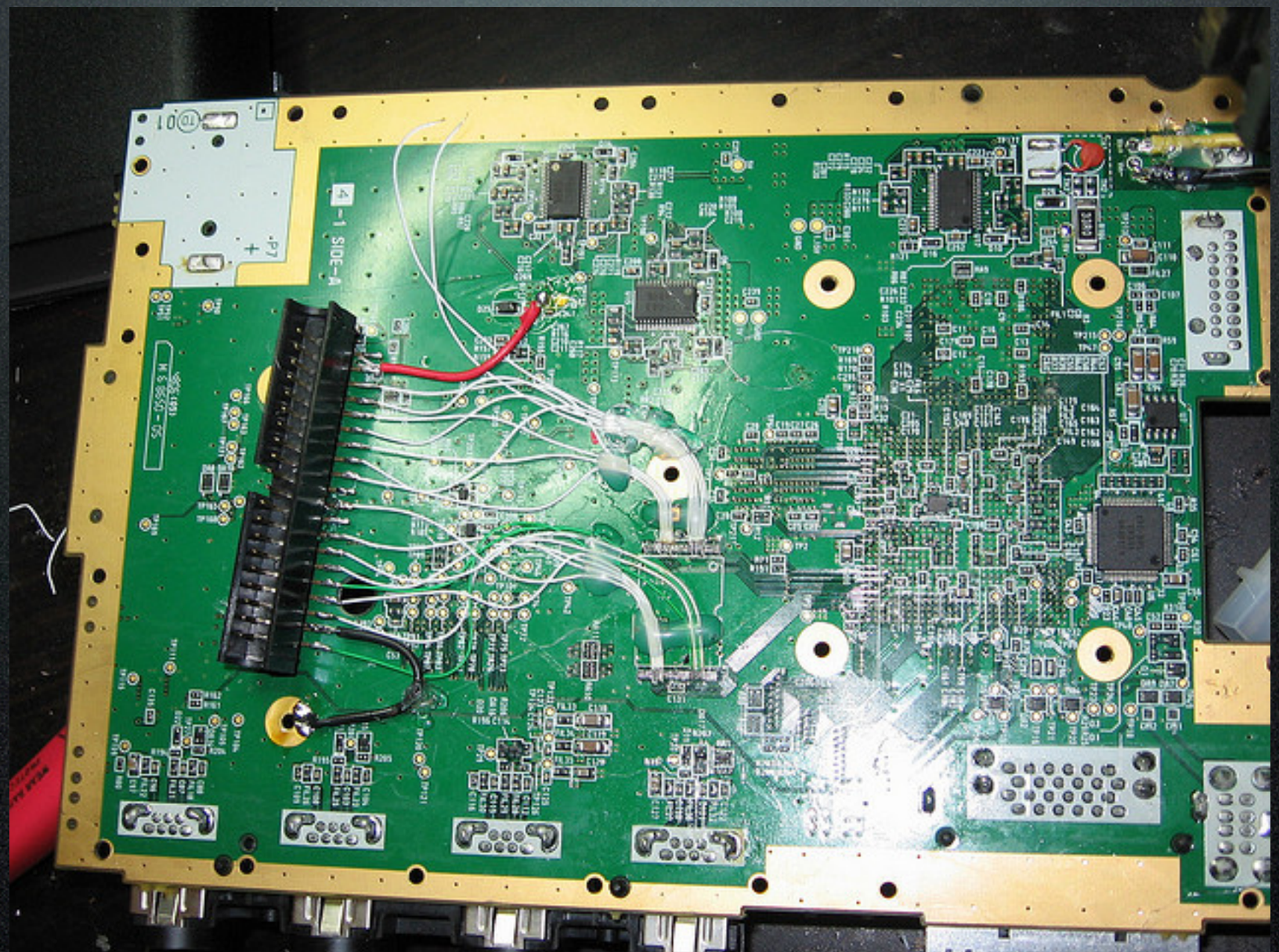
- When there's no space left on your Wii NAND.. it will backup email messages to your SD card..
- Encrypted using AES-128-CBC with a NULL key and IV from header of file..
- Signed using HMAC key based on Wii WiFi MAC Address..

LetterBomb



Put “boot.elf” in root of SD, click bomb, kick back!

Wii PrOn



Nintendo DSi (2008)

ARM9 @ 133MHz, ARM7 @ 133mhz
16MB RAM, NAND, Camera’s

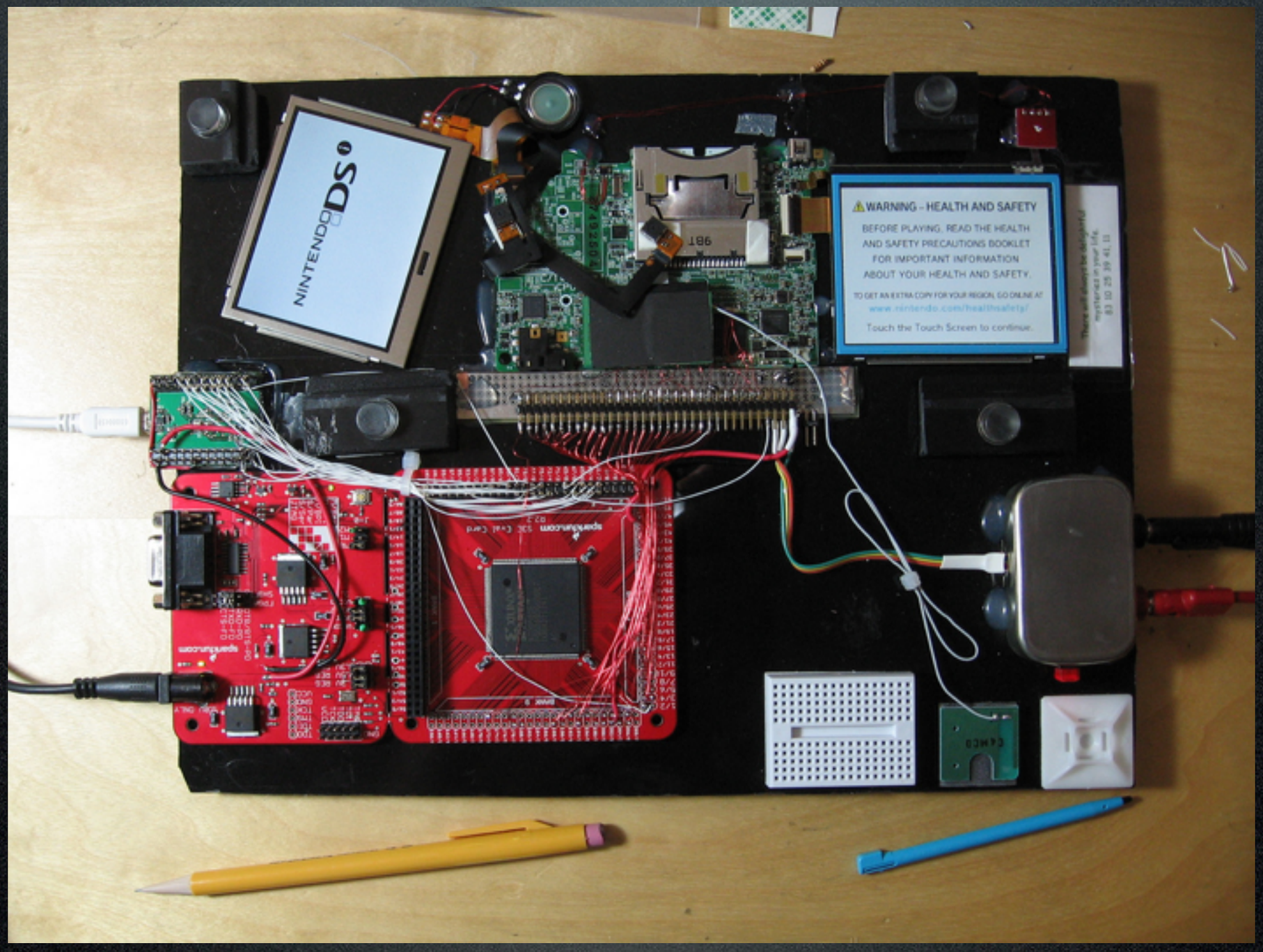
Savegame Exploits

- I started trying to break savegame checksums for various DSi games.
- Most are simple addition- or CRC16-based checksums, *yawn*.
- Managed to break some DSi compatible game by overflowing a profile name :-)

Savegame Exploits (2)

- Classic Wordgames was the first cart based game by Ubisoft to be exploited.
- Coincidentally, another game by Ubisoft, “My Healthy Cooking Coach” suffered from the same bug.
- yellows8 exploited 4 more DSiWare games. (Sudoku, Guitar Rock tour, Legends of Exidia and Fieldrunners)

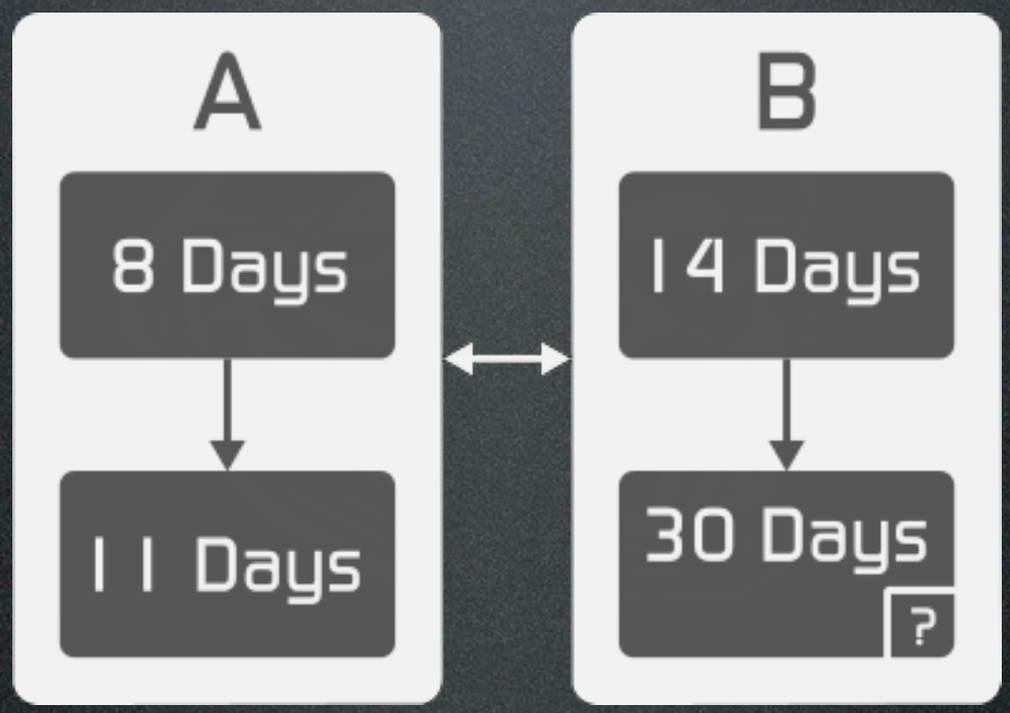
(FC)RAM Attack!



Courtesy of scanlime / Beth Scott

WiiU (2012)

- Yet another beefed up gamecube ;-)
- failOverflow claims first blood in form of mysterious SHA1 hashes and teaser images



WiiU DRC


```
#!/usr/bin/python

from wiiu_rpc import *
from utils import *

rpc=wiiu_rpc_client()

rpc.OSCancelThread(0x255bcdc8)

alloc = rpc.read32(rpc.sym("MEMAllocFromDefaultHeapEx"))
fb = rpc.fc(alloc, 854*480*4*2, 0x1000)

print "ALLOC'D FB @ 0x%08x" % fb

rpc.GX2SetDRCBuffer(fb, 854*480*4*2, 2, 0x41a, 1)
```

The Next Generation

- PS4
- Xbox One
- Both based on AMD Technology
- Yay, x86_64, we should know this by now.
- PS4 Devkits are based on FreeBSD
- Microsoft is redoing their game disc DRM system in a haste.

Conclusion

- Consoles are toys for big boys (and girls) too!
- Manufacturers are stepping up their security game, but often still leave glaring holes.
- The prestige of cracking a security/ DRM system is worth much more than being able to run copied games ;-)

Thanks for listening!

Questions? Feedback?

E-mail: **peter@haxx.in**

twitter: **@blasty**