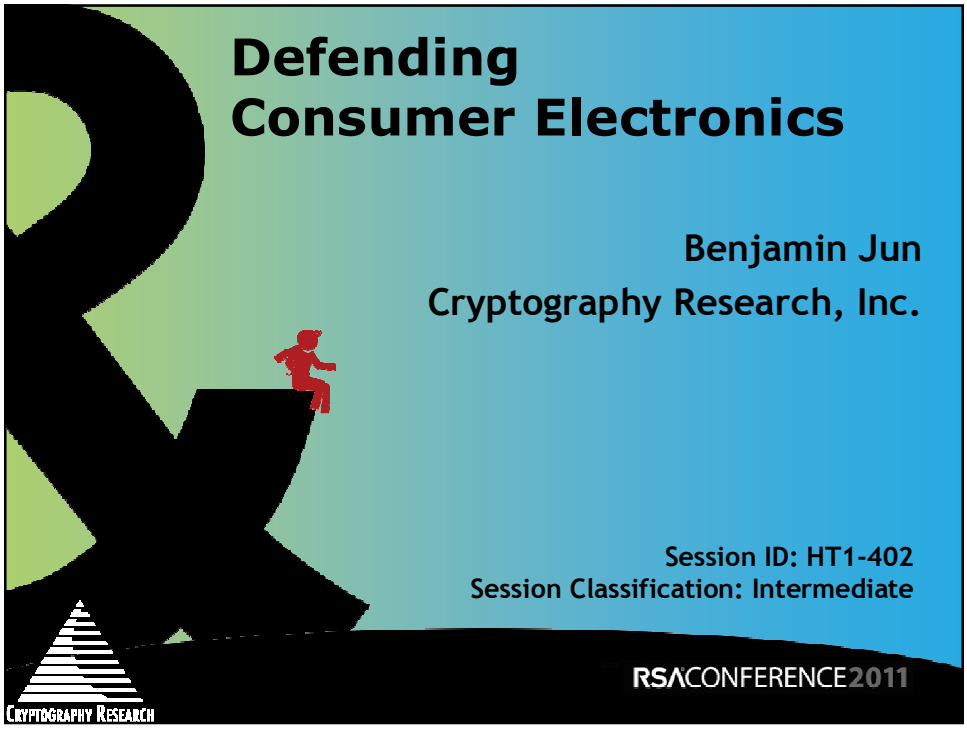


Defending Consumer Electronics

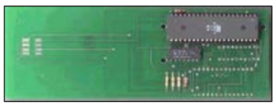
- Security challenges
- Learning from open source
- Attacks!
- Putting it together: Boot protection

RSA 2011 CONFERENCE

Cryptography Research

Consumer electronics threats

- Content piracy
  - Unauthorized content access



Pay TV security card emulator

Key redistribution

RSA 2011 CONFERENCE

CRYPTOGRAPHY RESEARCH

Consumer electronics threats

- Content piracy
  - Unauthorized content access
- Financial fraud
  - Extract, use payment key(s)

ATM skimming device

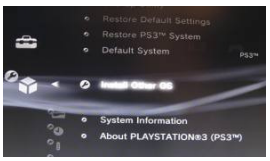
Joe Grand, Jacob Appelbaum, Chris Tarnovsky
"Smart" Parking Meter Implementations, Globalism, and You (2009)

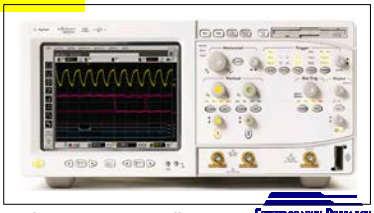
RSA 2011 CONFERENCE

CRYPTOGRAPHY RESEARCH

Consumer electronics threats

- Content piracy
  - Unauthorized content access
- Financial fraud
  - Extract, use payment key(s)
- Modified functionality
  - Feature unlock, jailbreak, linux





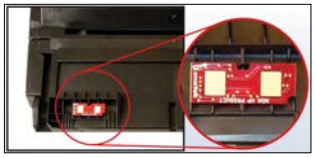
Agilent 54833D Oscilloscope

RSA 2011 CONFERENCE

CRYPTOGRAPHY RESEARCH

Consumer electronics threats

- Content piracy
  - Unauthorized content access
- Financial fraud
  - Extract, use payment key(s)
- Modified functionality
  - Enable unauthorized features, linux
- Device cloning
  - Sell interoperable device



Unauthorized toner chip

"RAZR V3" Battery

RSA 2011 CONFERENCE

CRYPTOGRAPHY RESEARCH

Consumer electronics threats

- Content piracy
  - Unauthorized content access
- Financial fraud
  - Extract, use payment key(s)
- Modified functionality
  - Enable unauthorized features, linux
- Device cloning
  - Sell interoperable device

Mobile first, PCs to follow

Try this at home!

Learn from open-source embedded products

RSACONFERENCE2011

Look to open-source embedded projects

- Not (really) a security compromise…
  - Learn techniques to control and use HW
  - Efforts involve reverse engineering

- Good engineering lessons
  - Fast way to explore embedded environments
  - Fun! Good return on $ / time

µClinux

RSA 2011 CONFERENCE

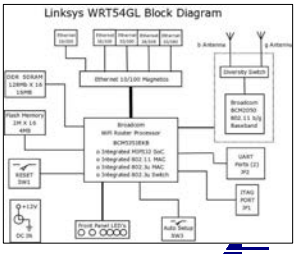
Microsoft; mindupdate; Make magazine

CRYPTOGRAPHY RESEARCH

Linksys WRT54GL

- $60 home wireless router
  - Linksys released open source SW

- Why mod?
  - Modify parameters (xmit power, etc.)
  - Add more firewall setttings, mesh networking, QoS, metering, etc.
  - Linux on cheap, low power platform



- Thriving hobbyist community
  - DD-WRT (www.dd-wrt.com)
  - OpenWRT (www.openwrt.org)
  - Note: buy the WRT54GL

RSA 2011 CONFERENCE

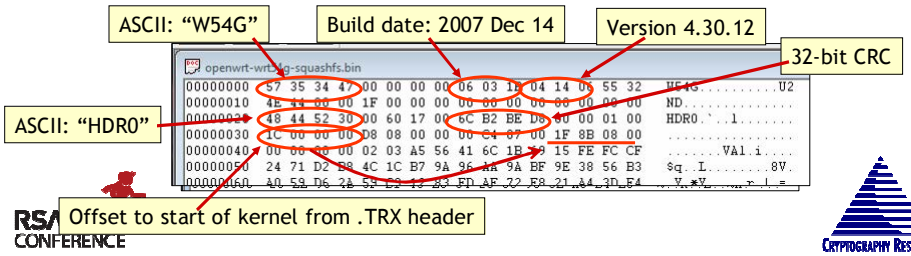
Linksys (Cisco Systems)
The Consolidated Hacking Guide for the Linksys WRT54GL, "ByteEnable", www.linuxelectronics.com

CRYPTOGRAPHY RESEARCH

FW reflash of Linksys WRT54GL

- Upgrade to OpenWRT firmware
  - Download OpenWRT whiterussian rc5, squash fs
    http://downloads.openwrt.org/whiterussian/rc5/bin/openwrt-wrt54g-squashfs.bin
  - Use (unsecured) FW update mechanism
  - Reboot, use www interface to set root pw
  - SSH in!

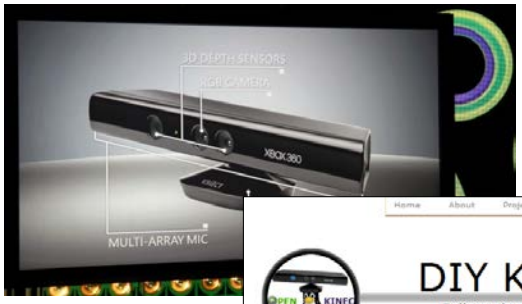
Stock Linksys FW: "4.30.12 1/10/2008" **OpenWRT FW: whiterussian rc5, squash FS**

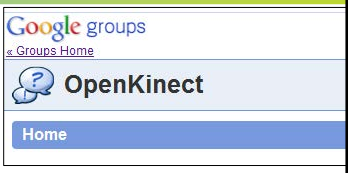


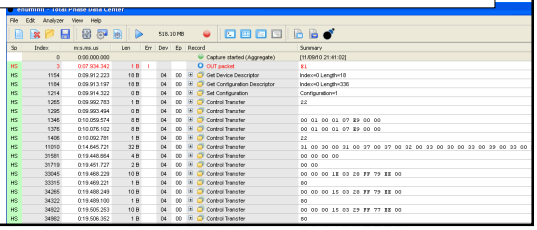
RSA CONFERENCE

CRYPTOGRAPHY RESEARCH

Example: Microsoft Kinect



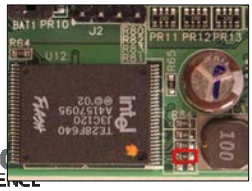




RSA 2011 CONFERENCE

Example: Linksys NSLU2

- Ethernet SMB (Windows) fileserver for USB disks ($70)
- HW mods:
  - Overclocking
  - RAM upgrade
  - Add debug ports
  - Add wifi



http://www.nslu2-linux.org/wiki/HowTo/AddAThirtyFourPinUniversalConnector http://www.nslu2-linux.org/wiki/HowTo/OverClockTheSlug David Hicks, http://www.nslu2-linux.org/wiki/HowTo/AddInter

No surprise to embedded developers…

- Nearly all products based on commodity cores, reference designs
  - WRT54GL: Broadcom BCM5352E
  - NSLU2: Intel IXP420 XScale (ARM)
- Small number of development environments
  - Linux, uC Linux, VxWorks
  - Good development, cross-compilation, debugging tools
- Hardware incrementally “free”
  - Differentiating features governed by software
  - Software modifications have interesting results!

Why follow these projects?

- Infrastructure type projects
  - "Boot linux on _____", "repurpose _____"
  - Understand debugging, porting tools
- Patch type projects
  - "Get in, get system to do _____, get out."
  - SW reverse engineering
- Hardware extension projects
  - "Add ___ HW feature"
  - HW reverse engineering

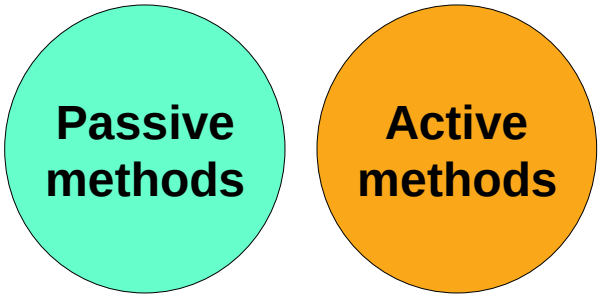
RSA 2011 CONFERENCE

Extracting Information

RSACONFERENCE2011

Extracting information

- Goal: Gather information
  - Reverse engineering is about making hypotheses
  - … and finding ways to confirm them !



Bus I/O

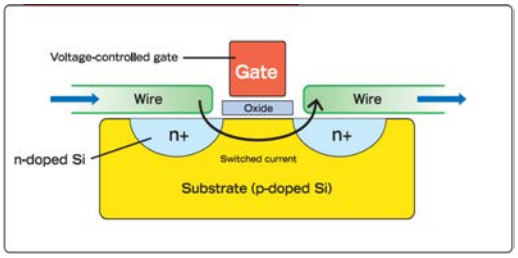
- Observe protocol
  - Protocol elements
  - Error handling
  - Crypto?
- Replay messages
  - Understand stateful protocol elements
  - Create test harness
- Perturb messages
  - Alter data fields, message order

SCSI Analyzer

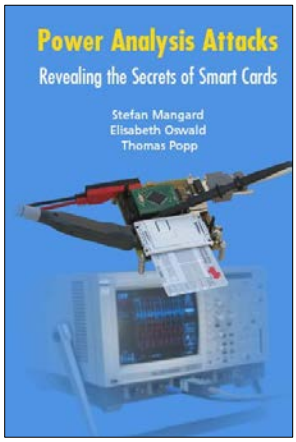
USB Analyzer

Information leakage

Integrated circuits consume power as they operate.



Typical MOS Transistor

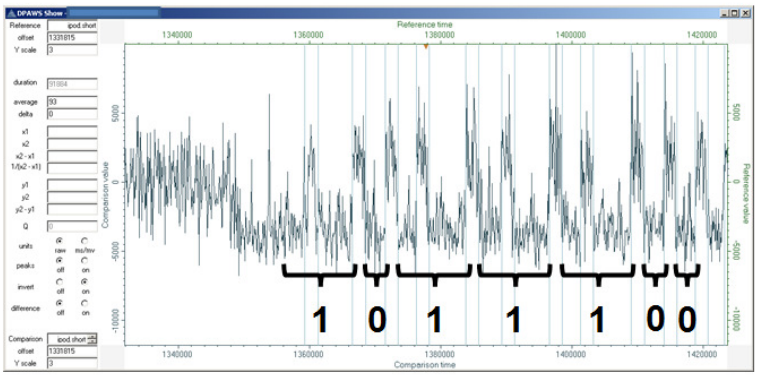


Mangard, Oswald, Popp
www.dpabook.org

RSA 2011 CONFERENCE

CRYPTOGRAPHY RESEARCH

Simple Power Analysis (SPA)

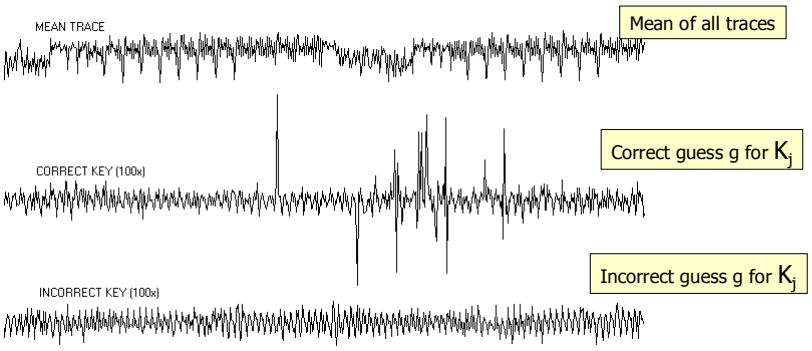


PDA device performing ECC curve multiplication, emissions recorded at 972.05MHz using antenna (E field). ECC secret key "double" and "add" operations have different emission structures. Differentiating these allows recovery of ECC secret key (scalar input to curve multiplication). With this setup, keys can currently be recovered at distances up to about 10 feet.

RSA 2011 CONFERENCE

CRYPTOGRAPHY RESEARCH

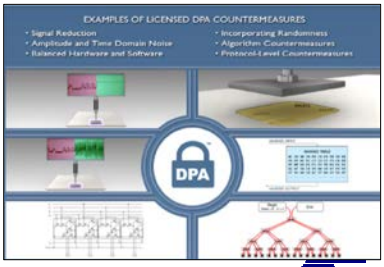
Differential Power Analysis (DPA)



- **To read more about DPA**
  - **www.cryptography.com/dpa**
  - **www.dpabook.org**

Defenses against power analysis

- Categories
  - Obfuscation
  - Leak Reduction
  - Balanced HW / SW
  - Amplitude & Temporal Noise
  - Incorporating Randomness
  - Protocol Level CM
- Certifications / Requirements
  - Common Criteria
  - CAC, E-Passport, HSPD-12
  - FIPS 140-3 draft



Cryptography Research

Code dump

- Using the SoC
  - Ask SW to read it for you!
  - Use JTAG debug interface
- Physical tap
  - I/O bus or external reader
- With a code dump…
  - Recognize processor type
  - Disassemble, probe for implementation weakness
  - Search for keys (high entropy)

GALEP-4 programmer/reader

USB - JTAG connector

FW_WRT54GL_4.30.12.3_US_EN_code.bin

```
00000000  57 35 34 47 00 00 00 00 07 0C 14 04 1E 0C 55 32
00000010  4E 44 00 00 1F 00 00 00 00 00 00 00 00 00 00 00
00000020  48 44 52 30 00 E0 2C 00 F3 9F DA C3 00 00 01 00
00000030  1C 00 00 00 30 B9 0A 00 00 00 00 00 1F 8B 08 08
00000040  08 1E 6A 47 02 03 70 69 67 67 79 00 EC 7D 0D 74
00000050  1C 57 95 E6 ED 57 DD 52 DB 6E C7 25 A9 2D B5 6D
00000060  25 EE 96 4B 3F B1 45 E8 04 25 68 98 5E A8 B4 E5
```

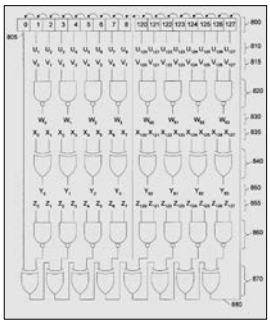

Die imaging

- Imaging the ROM
  - Optical microscope / FIB: automated imaging of ROM
- Imaging digital logic
  - Use automated tool to image + recover netlist
  - Easier if crypto area small, design has good structure
  - One reference: Nohl, Starbug, Plotz, *Mifare Security*, CCC 2007
- Comment: Imaging techniques have some errors
  - Requires human interpretation + correction
  - …AES with a few errors is obviously AES

Memory images: Hector Xeno
FIB: University of Cambridge Department of Materials Science Device Materials Group

Imaging countermeasures

- Hide stuff
  - Shield layers
  - Camouflage cells
- Add an entropic array
  - "Grown" from design rules and random seed
  - Internal entropy / lack of structure
  - Makes imperfect reverse engineering results useless



Example EA

RSA 2011 CONFERENCE

Cryptography Research

US patent 6,640,305

Active Attacks

RSACONFERENCE2011

Active attacks

- "Standard" attacks and defenses apply…
  - Protocol / network attacks
  - Filesystem attacks
  - OS attacks
- Plus, attacker has direct physical access!

Debug tools

- JTAG analyzer
  - Full debug interface
  - Boot code replacement
  - In-target flash/ROM reading + programming

EJTAG In-target analyzer

First Silicon Solutions, ISA-MIPS

ARM JTAG debugger interface

Olimex Ltd., ARM-USB-OCD

Glitching tools

- What if computing platform is not reliable?

Hand tuned analog glitcher

Riscure VC Glitcher

Thermal attack

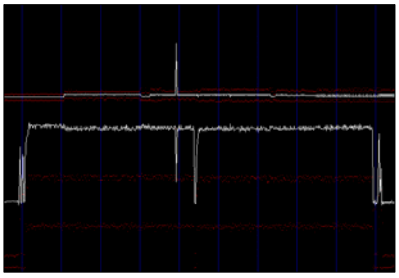
Arbitrary waveform generator

Glitching example

```
; This routine is used to output a 4-byte result
; DPTR points to first byte of data
result_out:  MOV R0, 3             ; set loop counter
result_loop: CALL #putch           ; call UART routine
             INC DPTR              ; increment pointer
             DJNZ R0, #result_loop ; conditional loop
             RET
```

Fault induction

- What things can happen?
  - Induce a computational fault
  - Change value being read/stored
  - Break into/out of an execution loop
  - Change program counter
- Apply externally or to specific circuit element on chip (laser)
- Surprises
  - More repeatable than you think…



Glitch impulse & power trace during successfully-glitched RSA CRT

Boot Attacks

Bootloaders

- Bootstrap embedded system
  - Initialize environment and peripherals
  - Decrypt / decompress flash
  - Authenticate code

"Let's start at the very beginning
A very good place to start
When you read you begin with A-B-C
When you sing you begin with do-re-mi"
- Maria

Example: Bootloader with code signatures

- Boot ROM with code authentication
  - Reset vector jumps to boot ROM
  - Verify RSA cert (hash of PK can be hard-coded)
  - Hash and verify payload, FAIL on error
  - Decrypt + decompress payload to RAM
  - Clear all other RAM
  - Jump to payload

- HW requirements
  - Force jump to internal boot ROM on reset
  - JTAG and other execution vectors off by default
  - Development/test: skip bootloader if fuse unblown

Bootloaders are hard!

- Challenges
  - "Instant on" requirements
  - Crypto bootstrap
  - Low power mode
  - Developer access
  - Recovering from corrupted image
  - MMU behavior
  - Key management
  - Support for different HW versions
  - Secure fuse reads
  - Forward compatibility
  - … and many more …

Checkpoint Charlie (1986)

RSA 2011 CONFERENCE

CRYPTOGRAPHY RESEARCH

Ways to load code

- Grab control of program counter with buffer overflow, glitch, protocol errors, …
- Suspend/resume with memory image change
- Replace device public key
  - "Savegame" buffer overflow in "007" Xbox game (2003)
  - Makes public modulus divisible by 3

```
BE00000080      mov esi, 80000000
AD              lodsd                   ; 0x00000032
81EE03000000    sub esi, 00000003
3DBD1B4BA4      cmp eax, A44B1BBD
75F2            jne 00000032            ; scan RAM for public key
8176FFD68BD72D xor dword ptr [esi-0], 2DD78BD6  ; modify last 4 bytes of public key
```

- Recover private key and sign your own code
  - PS3 DSA signature attack, CCC 2010

RSA 2011 CONFERENCE

CRYPTOGRAPHY RESEARCH

http://xbox-linux.sourceforge.net/docs/xbe/analysis.h

Conclusions

RSACONFERENCE2011

Consumer electronics challenges

- Devices:
  - Are in physical possession by attacker
  - Have flat memory architectures
  - Are used offline
- Developer tools == attacker tools
- High threat systems require security support in HW & SW

RSA 2011 CONFERENCE

Cryptography Research
www.spiritegris.com

Play with an open-source embedded project!

- Get a feel for HW and SW at block level
- Learn a few nuts and bolts
- Understand developer / attacker tools
- Have fun!

µClinux

RSA 2011 CONFERENCE

Images: Microsoft; mindupdate; Make magazine

CRYPTOGRAPHY RESEARCH

Contact Information

For more information, or to discuss how Cryptography Research can help with a security problem:

Benjamin Jun
ben@cryptography.com
415.397.0123
www.cryptography.com

CRYPTOGRAPHY RESEARCH

RSA 2011 CONFERENCE

CRYPTOGRAPHY RESEARCH