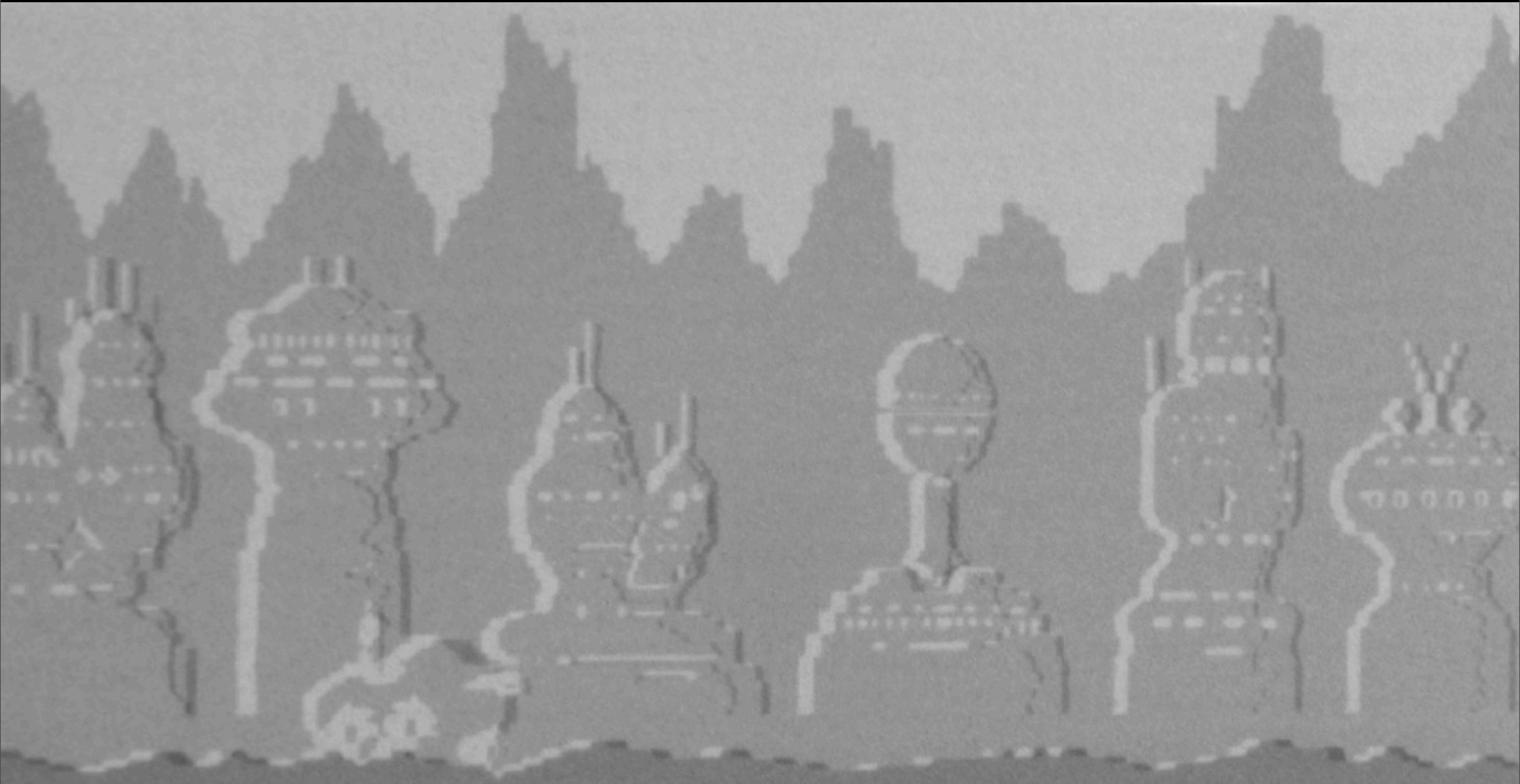
The Pitfalls and Perils of Poor Security

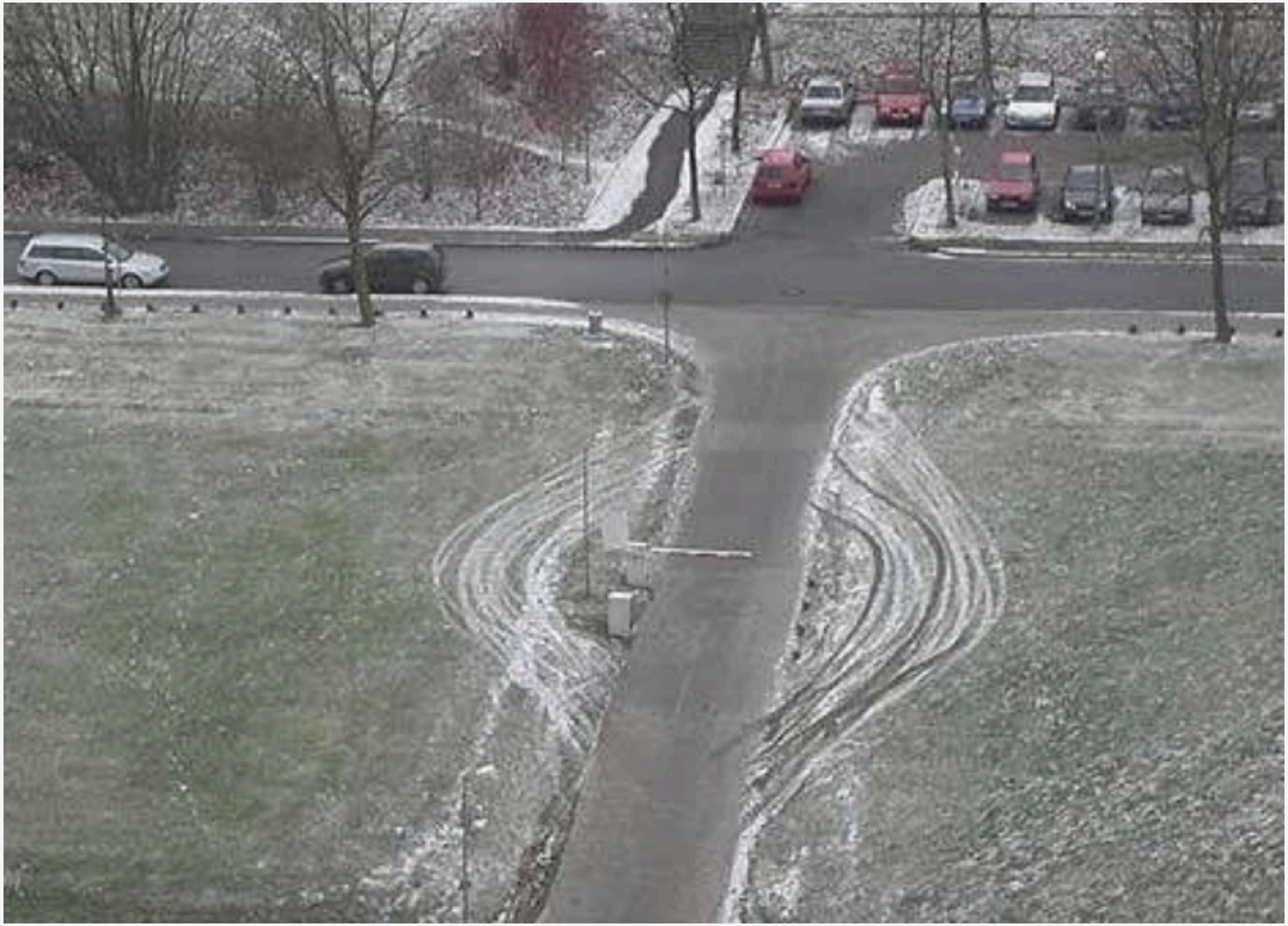


Joe Grand
Grand Idea Studio, Inc.
www.grandideastudio.com

We Are Part of the Problem

- Electronics industry is plagued by insecurity
- We are trained to think like engineers
- We are not trained to think like hackers
- We are constrained by budget and time-to-market
- Security is an afterthought (if at all)
- Our response to attacks/discoveries is antiquated
  - Denial of any issue (and refusal to fix it)
  - Knee-jerk reactions

The Hacker Mindset



Why Hardware Hacking?

- Cloning/counterfeiting
  - Specific theft of information/data/IP for marketplace advantage
- Theft of service/PII
  - Malicious intent, malware
  - Extract $$$, CC/PINs, passwords
- Bypass security features/privilege escalation
  - Defeating protection measures/gaining increased control of a system
  - Jailbreaking, expanding functionality of a device, use as an entry point into a network to further an attack
- Forensic analysis/intelligence
  - What is that hardware? Who designed it? How to extract data?
- Security competency
  - Test hardware security schemes for failures/weaknesses

Types of Hackers

Resource	Curious Hacker	Academic	Organized Crime	Government
Time	Limited	Moderate	Large	Large
Budget ($)	< $1000	$10k - $100k	> $100k	Unknown
Creativity	Varies	High	Varies	Varies
Detectability	High	High	Low	Low
Target/Goal	Challenge	Publicity	Money	Varies
Number	Many	Moderate	Few	Unknown
Organized?	No	No	Yes	Yes
Release info?	Yes	Yes	Varies	No

P. Kocher, Crypto Due Diligence, RSA Conference 2002

Attack Surfaces

- Chip/Silicon
- Printed Circuit Board (PCB)
- Embedded Systems

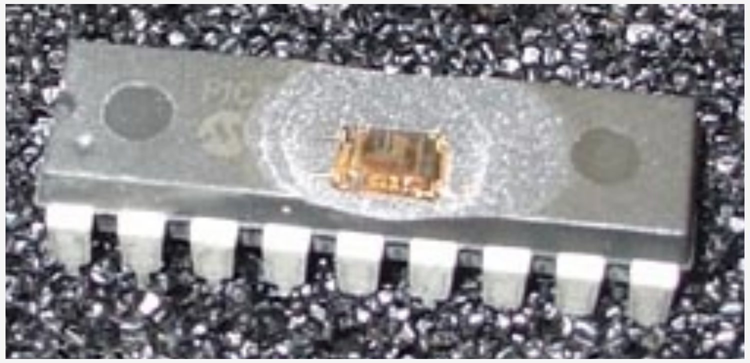
* Important to focus on the types of attack, not the product or vendor

* Only a sampling is shown here (just because you're not mentioned doesn't mean you're secure!)

Chip/Silicon

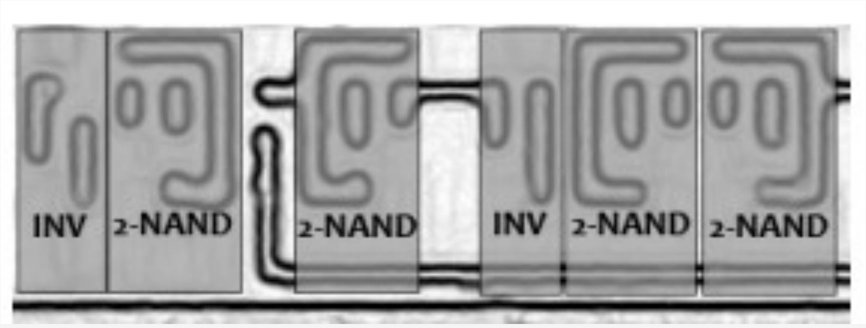
Chip Hacking

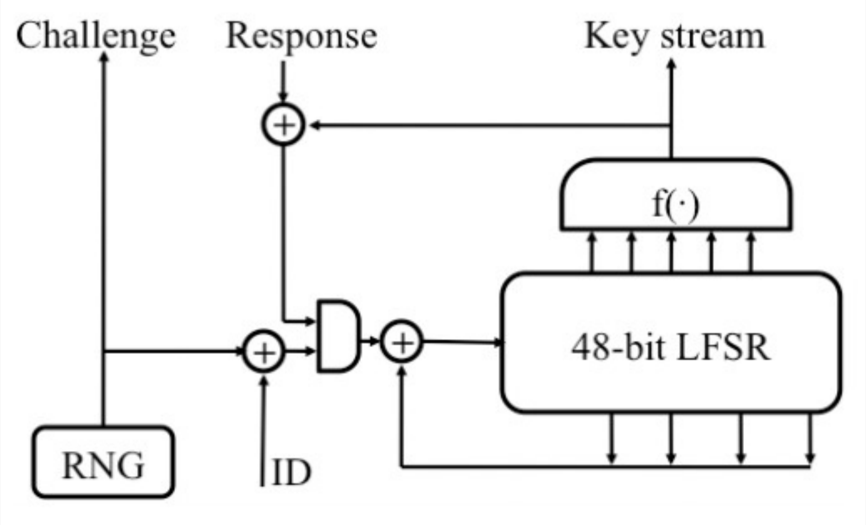
- Simple imaging to gather clues (identify counterfeits, backdoors)
- Cutting or repairing silicon structures (security fuses, traces)
- Retrieve contents of Flash, ROM, FPGAs, other non-volatile devices
- Key/algorithm extraction from ICs

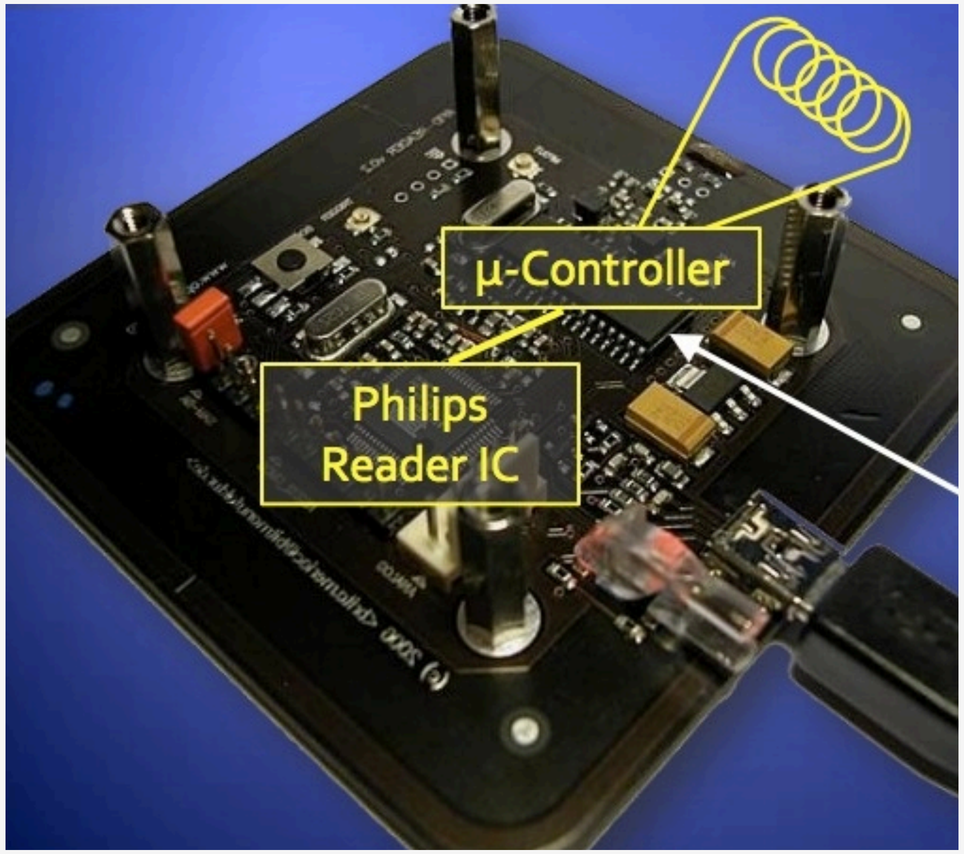


Mifare Classic (RFID)

- Karsten Nohl, David Evans, Starbug, Henryk Plotz
  - www.cs.virginia.edu/~evans/pubs/usenix08/usenix08.pdf
- Reconstructed & defeated proprietary Crypto-1 cipher w/ die images & protocol analysis
- ~400 2-NAND gate equivalents

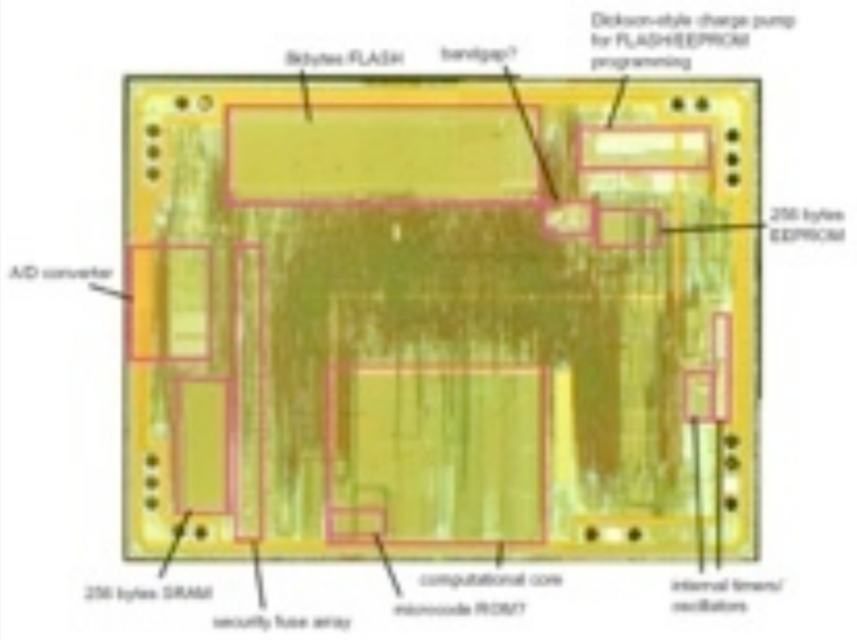






Microchip PIC Configuration Fuses

- Configuration fuses (including code protection bit) can be erased from some devices with UV light
  - "Hacking the PIC18F1320," www.bunniestudios.com/blog/?page_id=40
- Flash floating-gate transistor structures similar to UV-erasable EPROMs

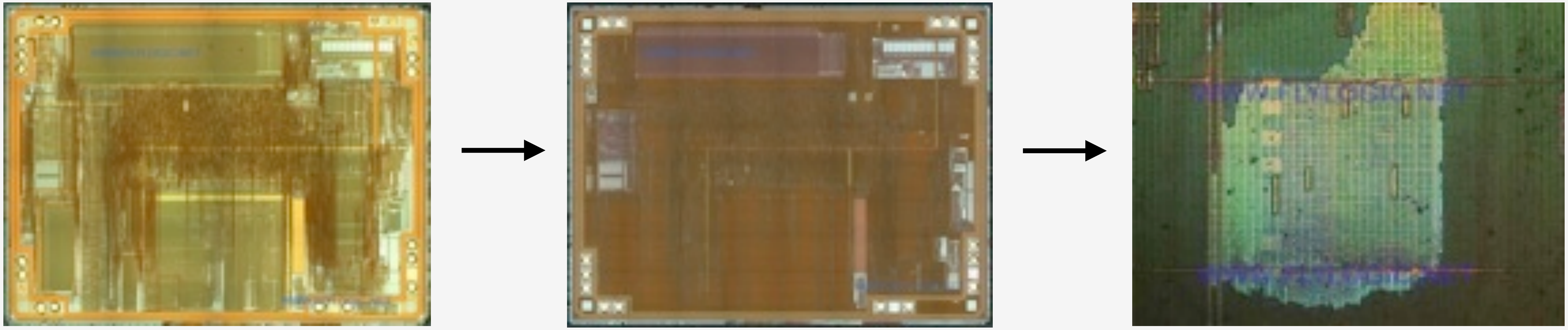


→

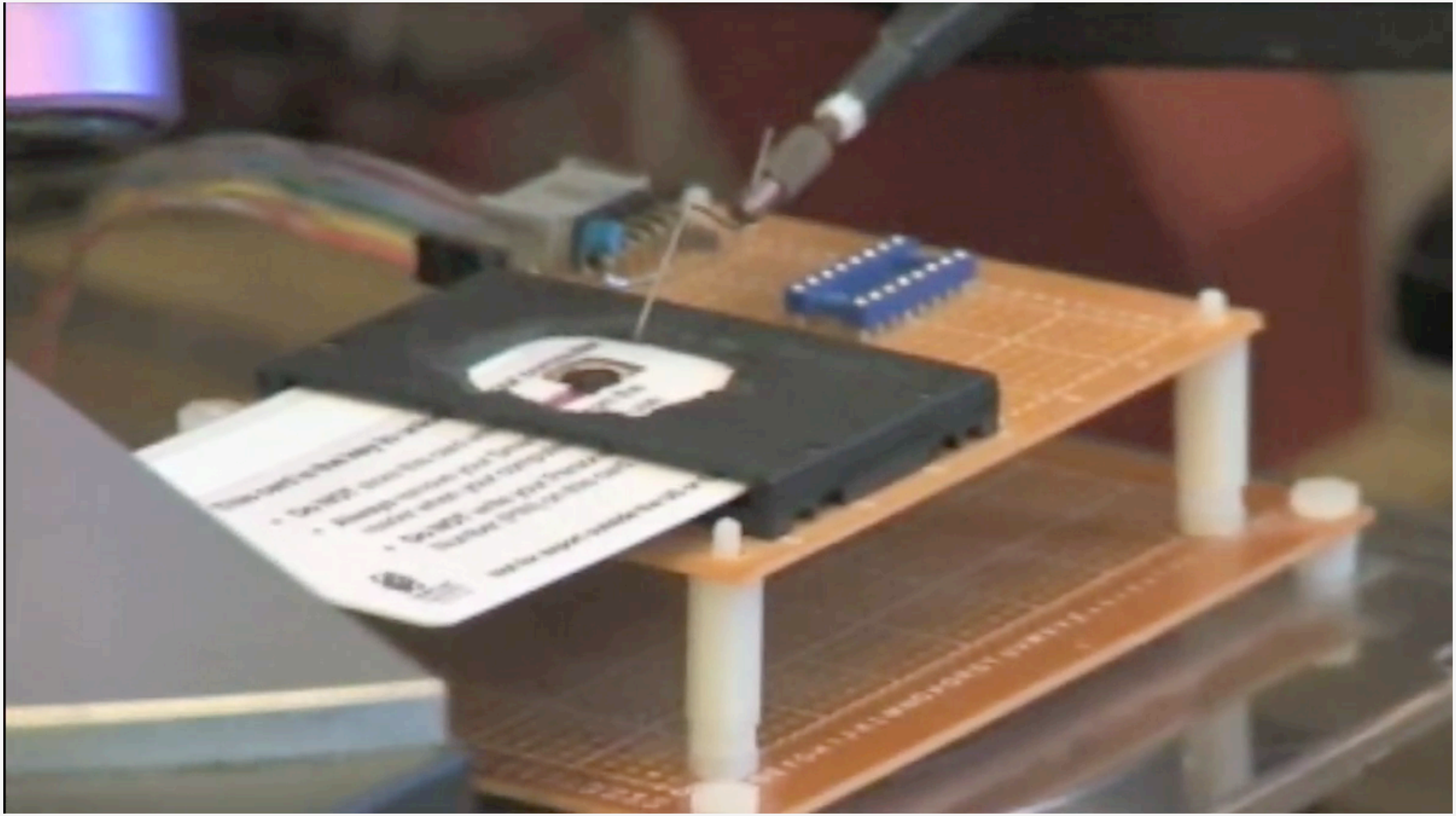
→

Microchip PIC Configuration Fuses 2

- Microchip revised die with additional metal fill
  - Many vendors now use active mesh to prevent probing
- Makes the attack slightly more difficult...
  - "Unmarked die revisions: Part I," https://web.archive. org/web/ 20131220115300/http://www.flylogic.net/blog/?p=9
  - "...Part II," https://web.archive.org/web/20071215020712/http:// www.flylogic.net/blog/?p=12



Satellite TV Smart Card

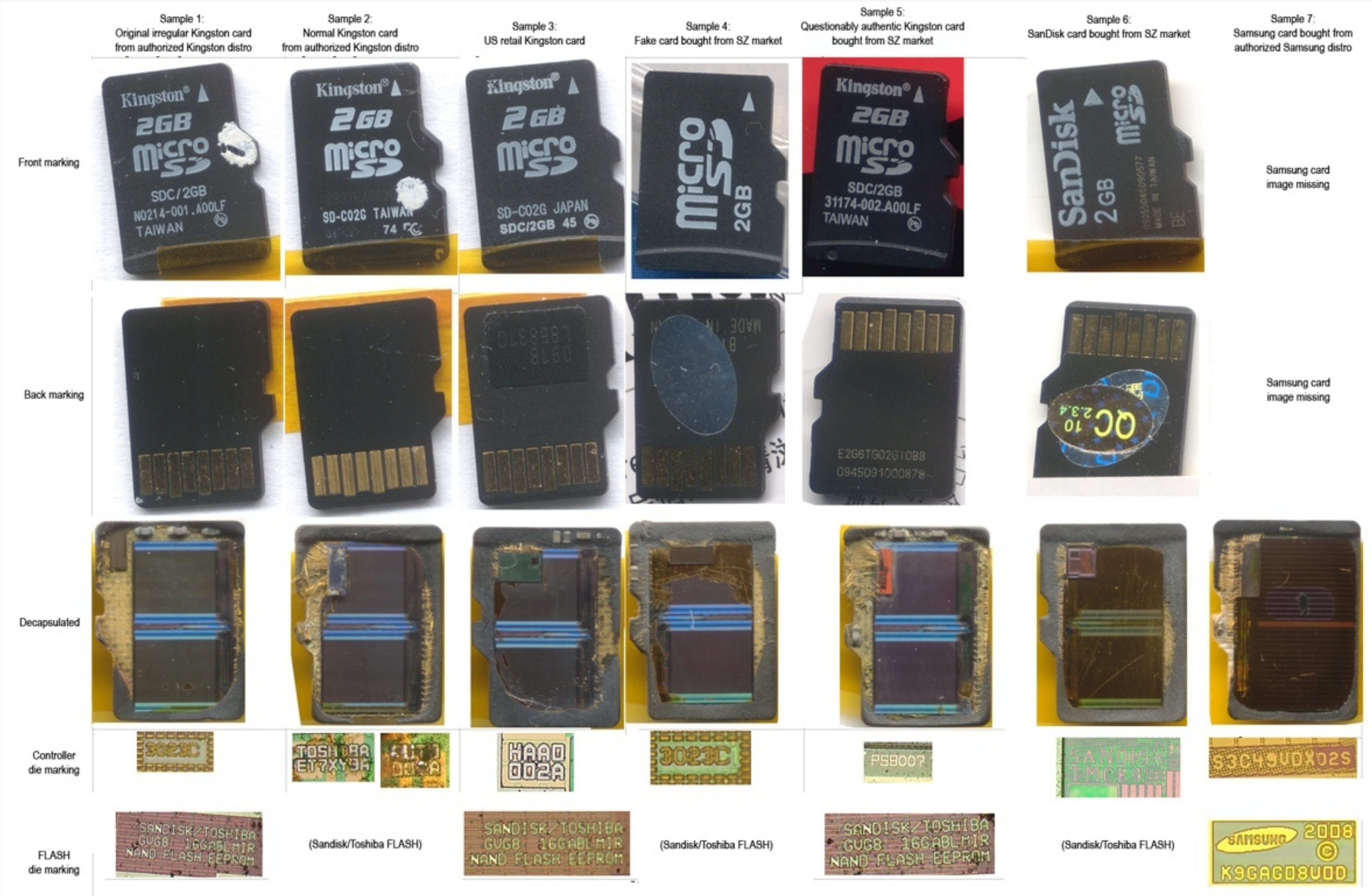


www.wired.com/video/hack-a-sattv-smart-card/1813637610

Counterfeits and Quality Control

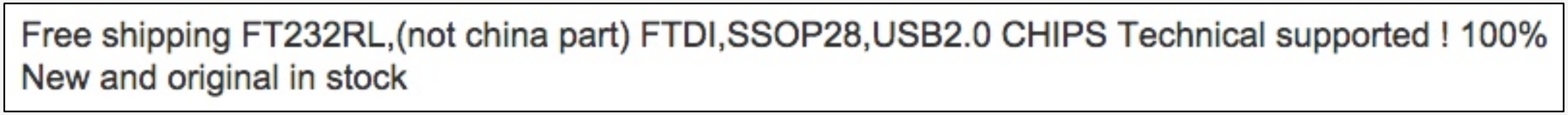
- For highest assurance, use authorized distributors
  - But, what happens if/when non-genuine parts enter legitimate supply chain?
- Krieg, Dabrowski, Hobel, Krombholz, & Weippl, Hardware Malware, 2013, www.morganclaypool.com
- Chris Tarnovsky, Spotting Fake Chips in the Supply Chain, http://blog.ioactive.com/2013/04/spotting-fake-chips-in-supply-chain.html
- Bunnie Huang, On MicroSD Problems, www.bunniestudios.com/blog/?page_id=1022
  - Questionable quality control of Kingston MicroSD cards
    - Including authorized manufacturers/distributors
  - Many different versions, all repackaged/remarked of Toshiba/SanDisk Flash

Counterfeits and Quality Control 2


Sample 1:
Original irregular Kingston card from authorized Kingston distro
Sample 2:
Normal Kingston card from authorized Kingston distro
Sample 3:
US retail Kingston card
Sample 4:
Fake card bought from SZ market
Sample 5:
Questionably authentic Kingston card bought from SZ market
Sample 6:
SanDisk card bought from SZ market
Sample 7:
Samsung card bought from authorized Samsung distro
Front marking
Back marking
Decapsulated
Controller die marking
FLASH die marking
Kingston 2GB microSD
SDC/2GB
N0214-001.A00LF
TAIWAN
SD-C02G TAIWAN
74
SD-C02G JAPAN
SDC/2GB 45
microSD 2GB
SDC/2GB
31174-002.A00LF
TAIWAN
SanDisk 2GB microSD
MADE IN TAIWAN
BE
Samsung card image missing
0918
E2G6TG02G10BB
0945091000878
QC 10 2.3.4
Samsung card image missing
3023C
TOSHIBA ET7XY9A
HAAD 002A
3023C
PS8007
SANDISK
S3C49VDX02S
SANDISK/TOSHIBA GVG8 16GABLMIR NAND FLASH EEPROM
(Sandisk/Toshiba FLASH)
SANDISK/TOSHIBA GVG8 16GABLMIR NAND FLASH EEPROM
(Sandisk/Toshiba FLASH)
SANDISK/TOSHIBA GVG8 16GABLMIR NAND FLASH EEPROM
(Sandisk/Toshiba FLASH)
SAMSUNG 2008 © K9GAG08U0D

Counterfeits and Quality Control: FTDI

- Extremely popular, heavily counterfeited part for USB-to-serial UART interface
- New FTDI driver released through Window's Automatic Update (~October 2014)
  - Renders non-genuine FT232RL devices inoperable by changing PID to 0 (writing to memory in a fashion not supported by legitimate devices)
- Huge debate within the security/electronics community
  - http://hackaday.com/2014/10/22/watch-that-windows-update-ftdi-drivers-are-killing-fake-chips/
  - www.eevblog.com/forum/reviews/ftdi-driver-kills-fake-ftdi-ft232/

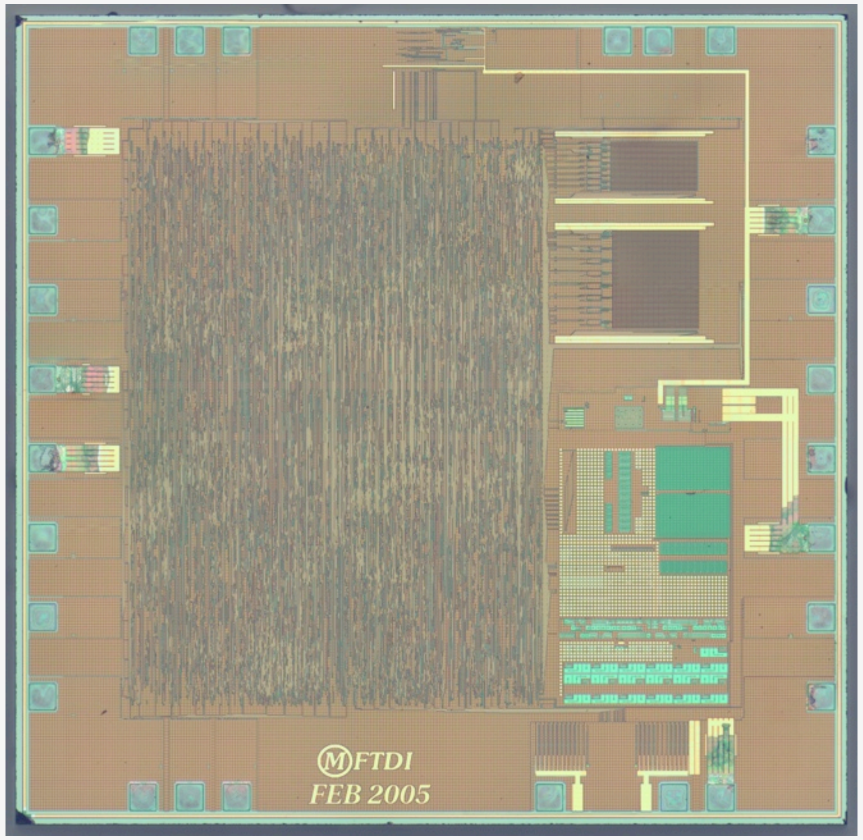


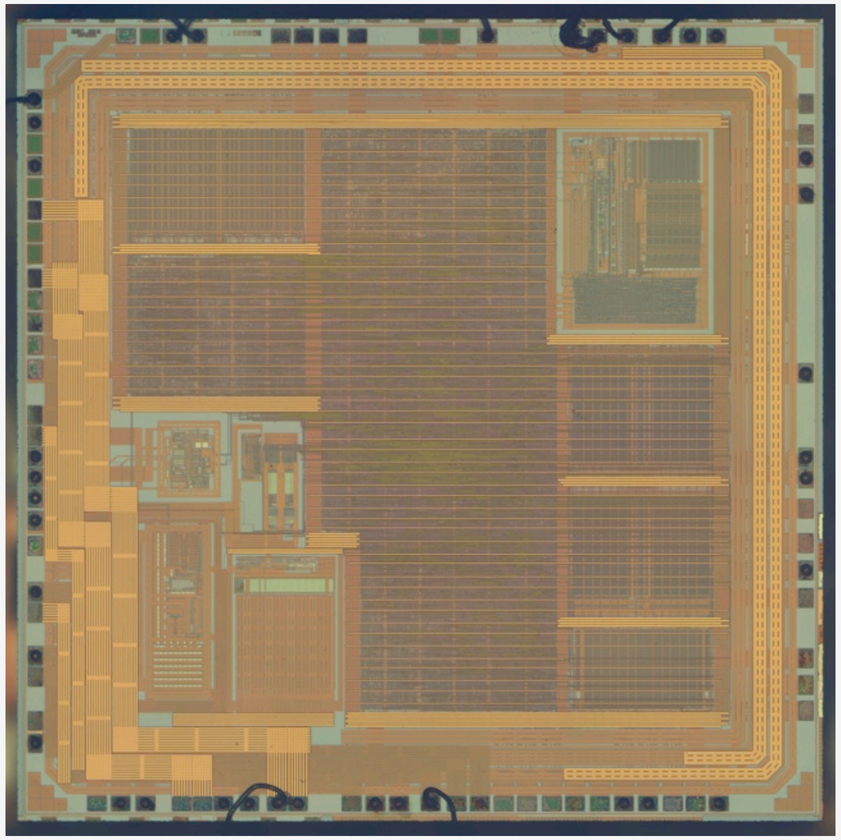
Free shipping FT232RL,(not china part) FTDI,SSOP28,USB2.0 CHIPS Technical supported ! 100% New and original in stock

www.aliexpress.com/item/Free-shipping-FT232RL-not-china-part-FTDI-SSOP28-USB2-0-CHIPS-Technical-supported-100-New-and/2039225609.html

Counterfeits and Quality Control: FTDI 2

- Update modified to disallow non-genuine devices in a non-invasive way
  - www.ftdichipblog.com/?p=1053
- Comparison of genuine v. non-genuine yields hacked-together masked ROM MCU emulating the interface
  - http://zeptobars.ru/en/read/FTDI-FT232RL-real-vs-fake-supereal

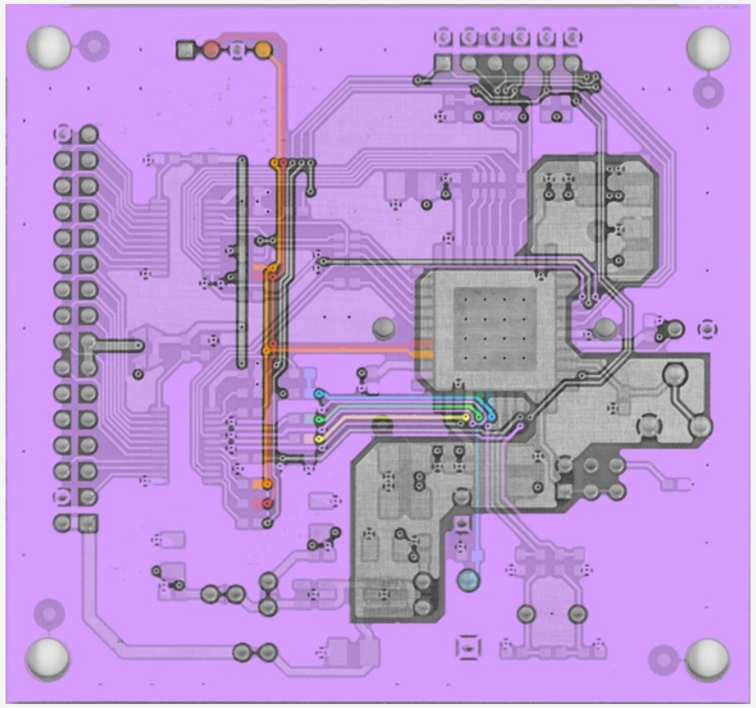


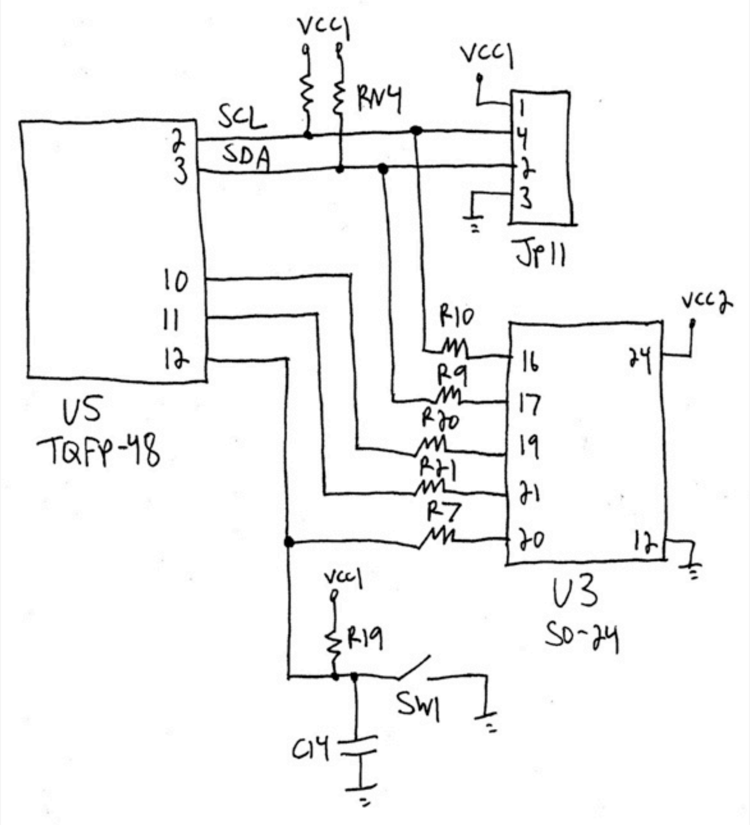


Printed Circuit Board (PCB)

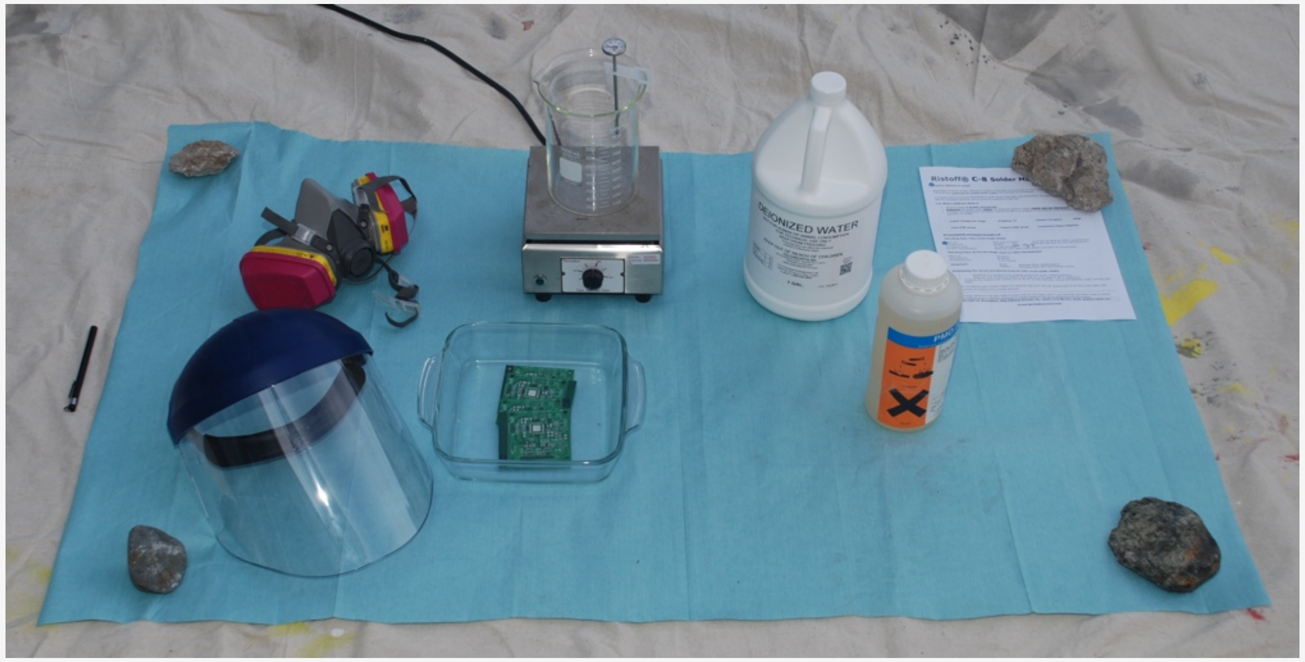
PCB Deconstruction

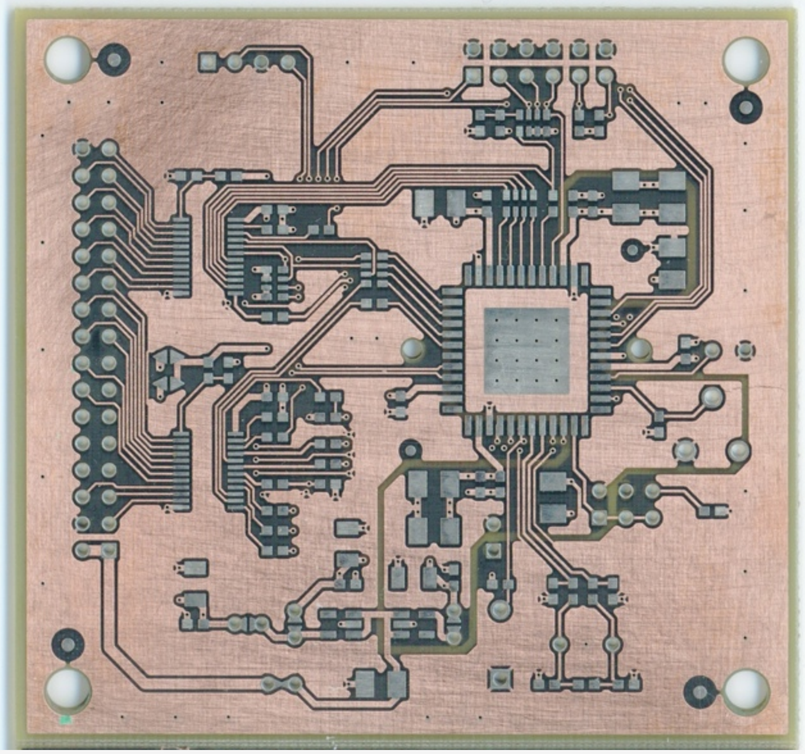
- Why?
  - Determine system or subsystem functionality
  - Security research/verification
  - Forensic analysis/intelligence
  - Clone a design
  - Inject new (malicious) behavior
- How?
  - Access to copper layers
  - Analyze layout rules/features
  - Trace component interconnections



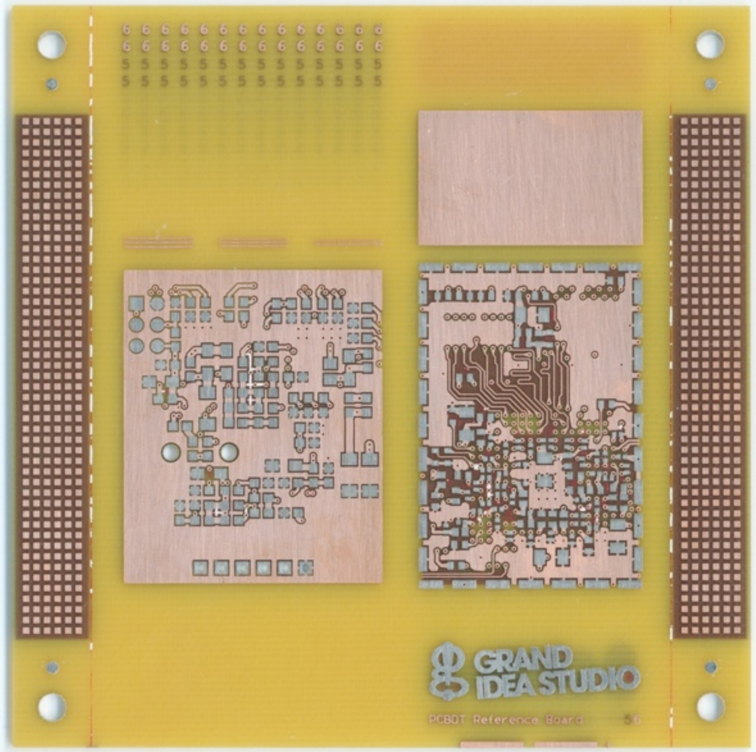


Solder Mask Removal: Chemical





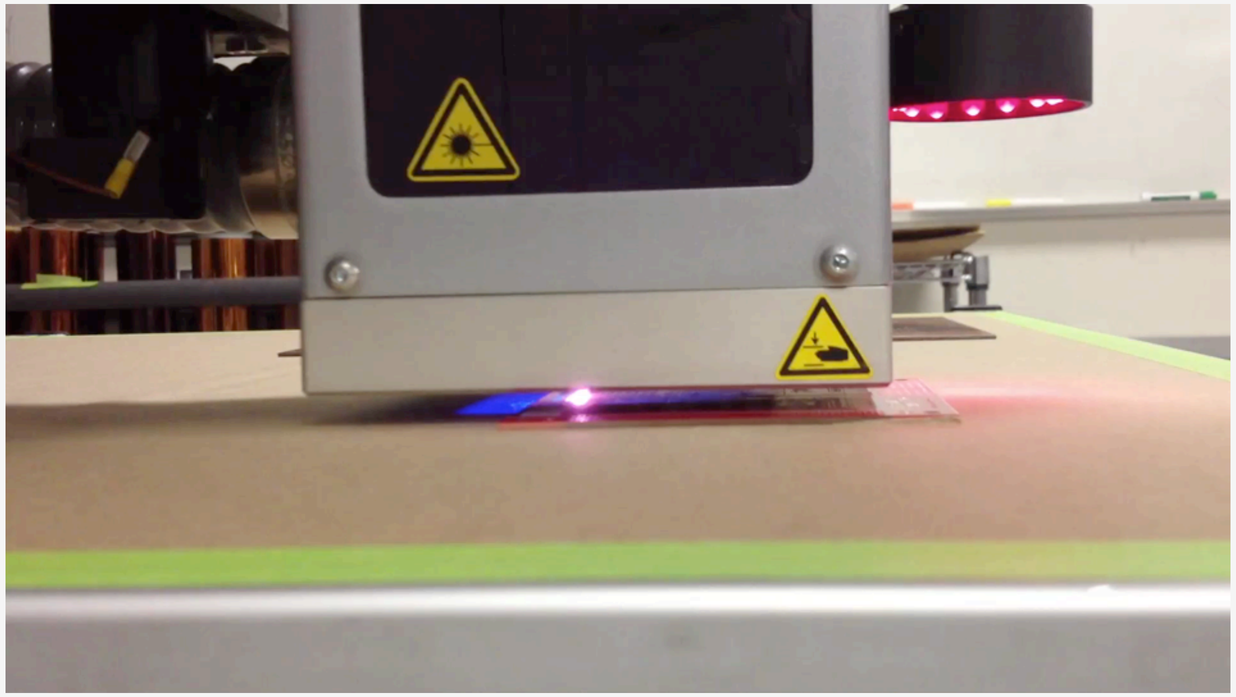
Ristoff C-8 @ 90 min., 130°F

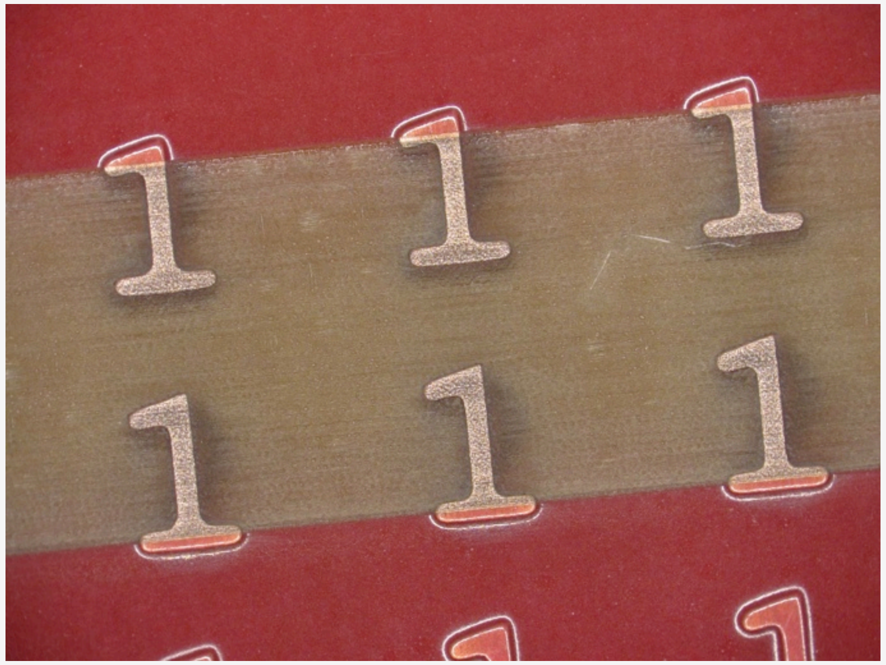


Magnastrip 500 @ 75 min., 150°F

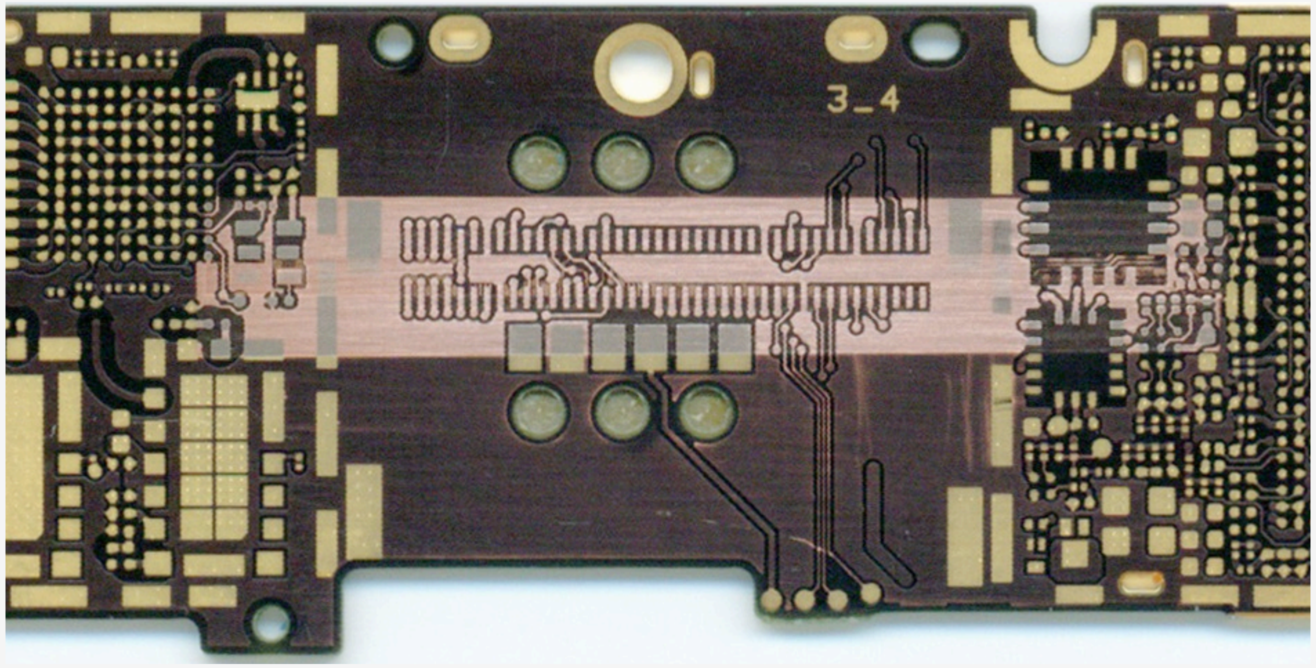
Solder Mask Removal: Laser

[redacted]



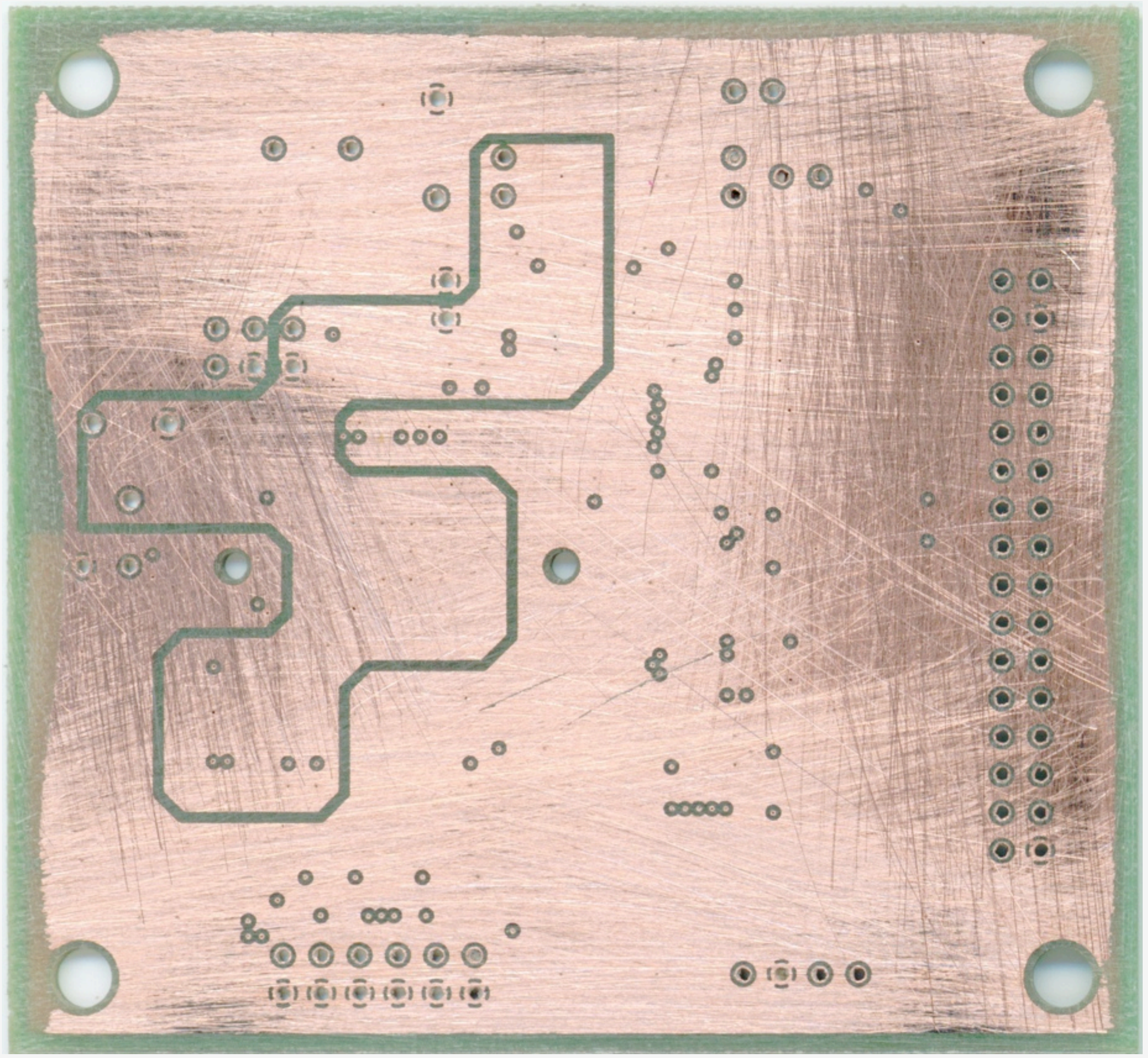


PCBDT Reference Board



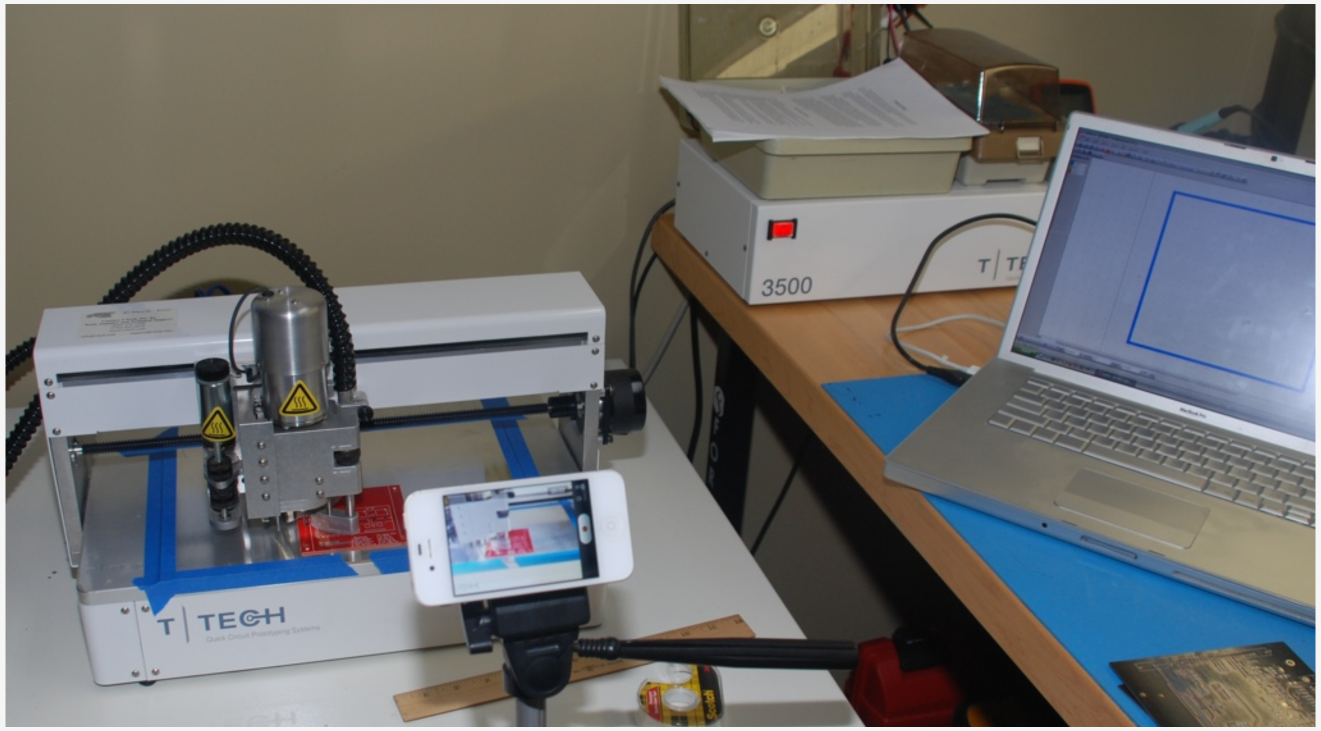
iPhone 4 16GB Logic Board

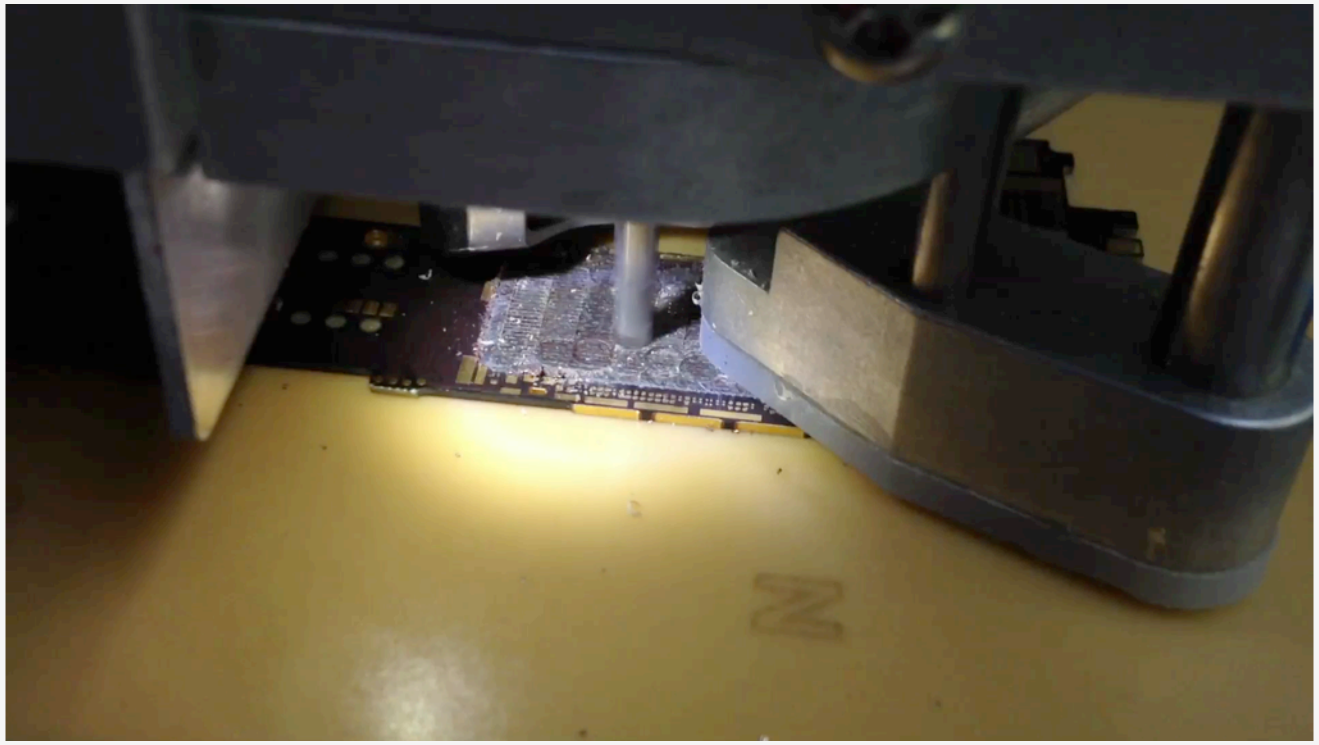
Delayering: Sandpaper/Rubbing Stone

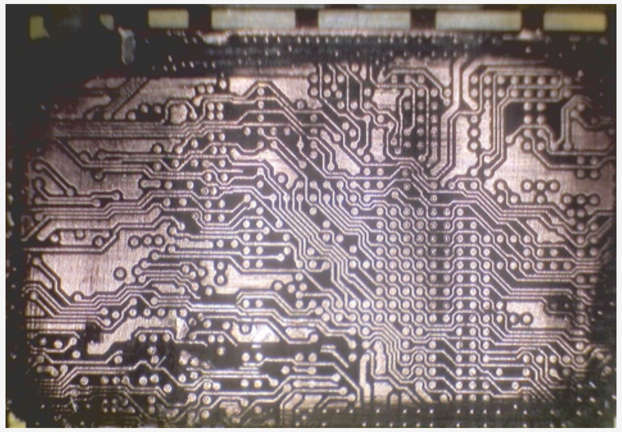


60/80 grit rubbing stone + 220 grit sandpaper

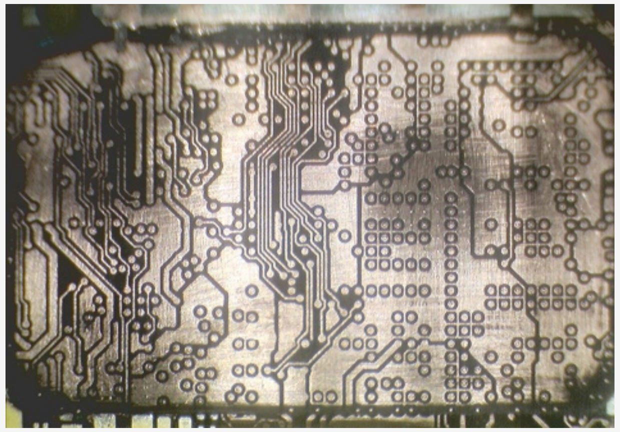
Delayering: CNC Milling



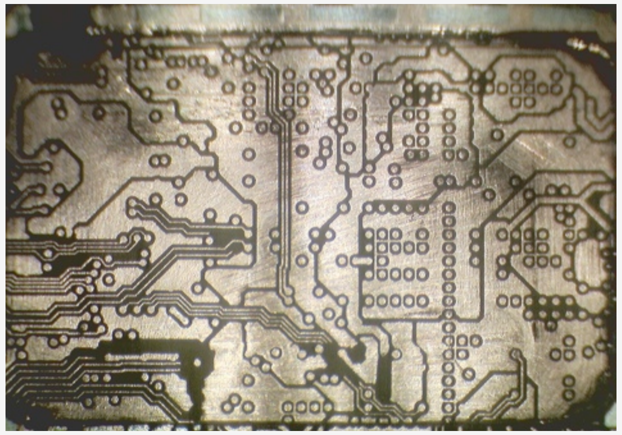




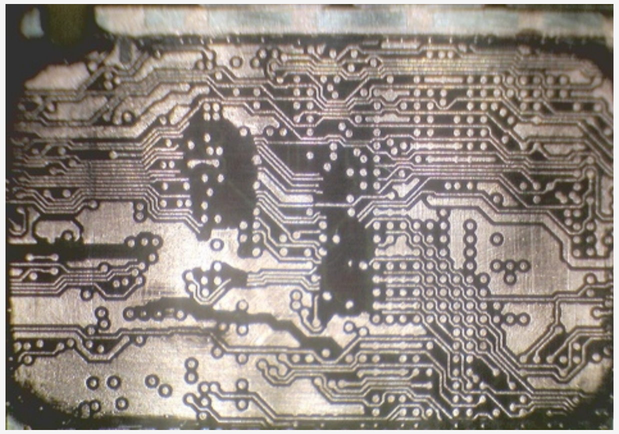
2



3

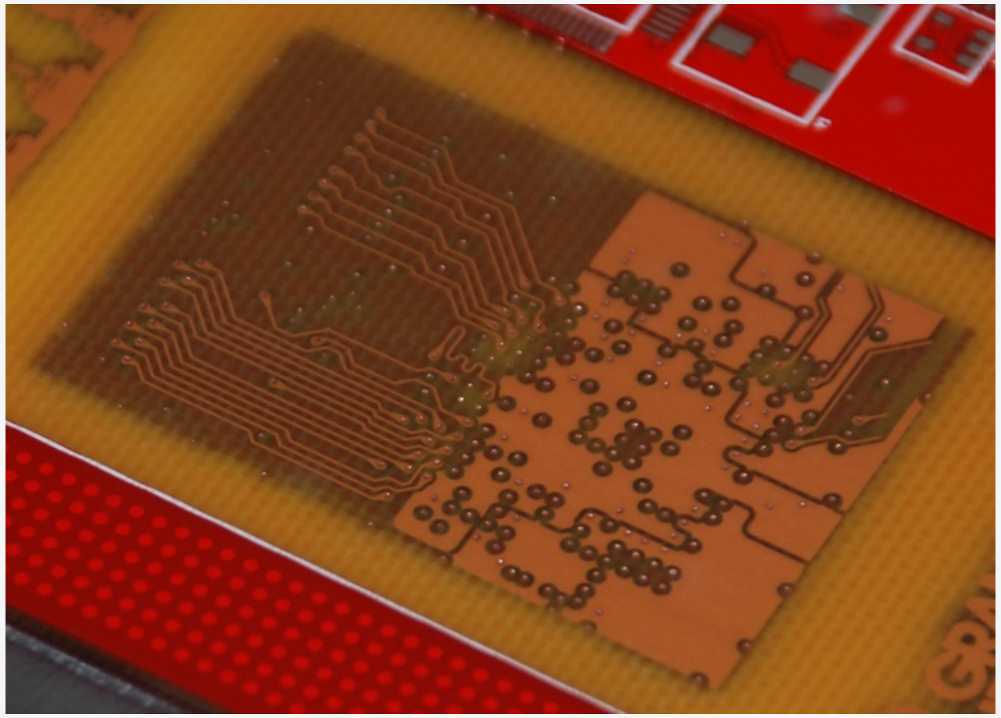


4

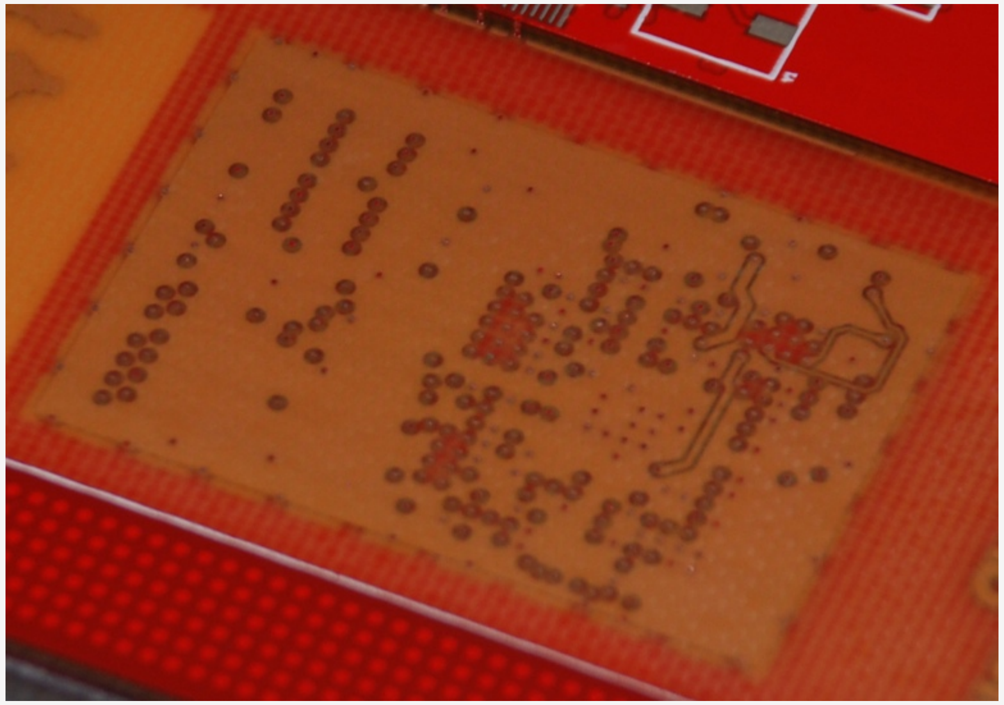


5

Delayering: Surface Grinding

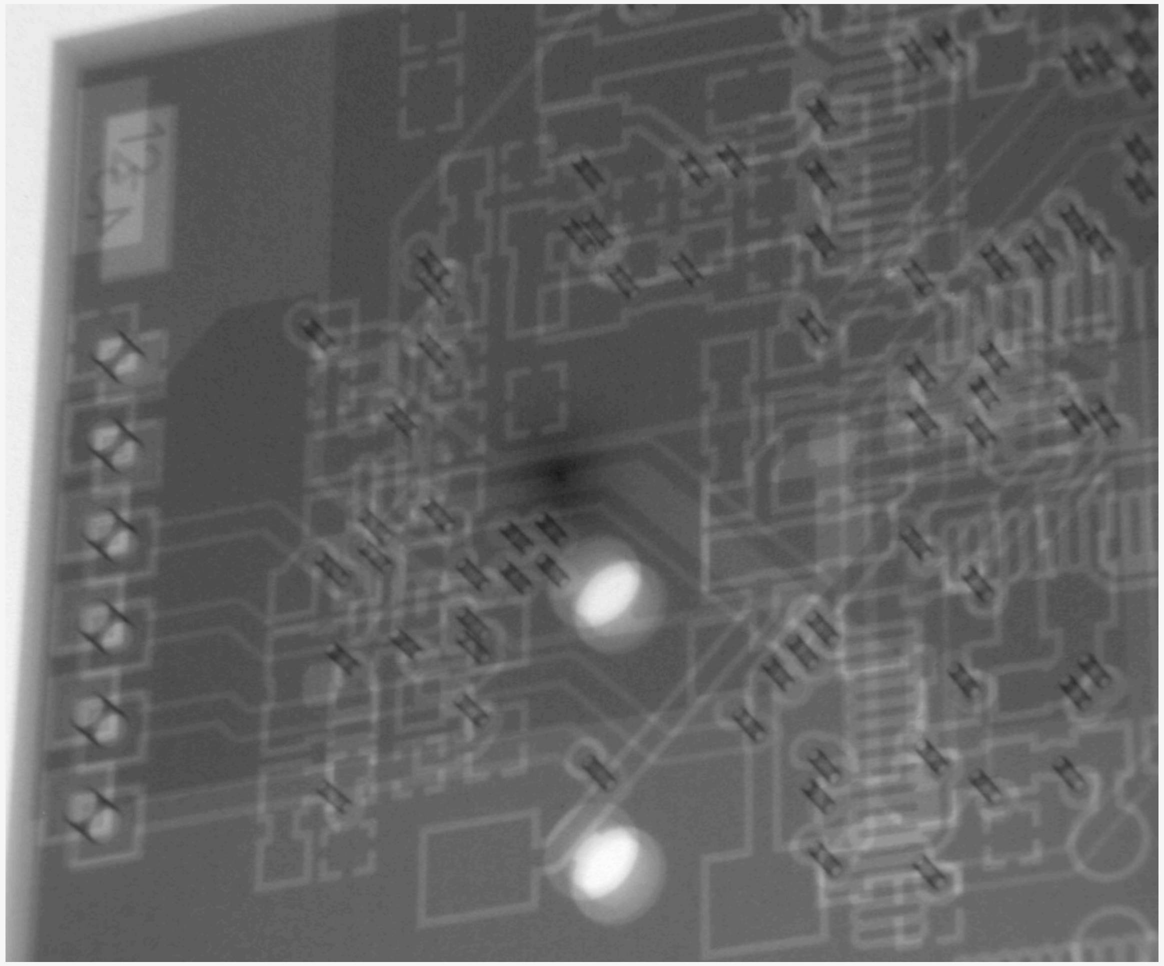


3

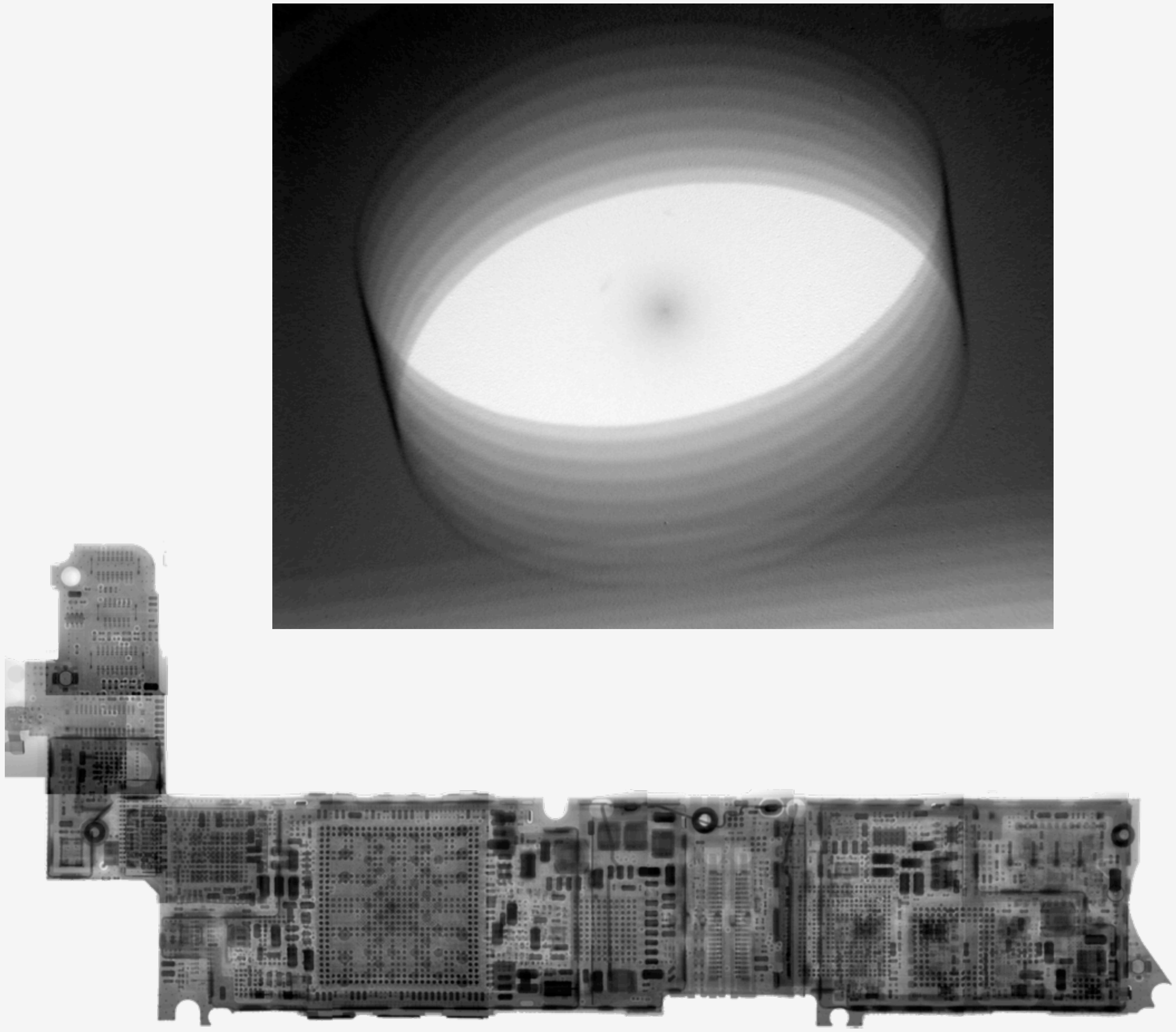


4

Imaging: X-Ray (2D)

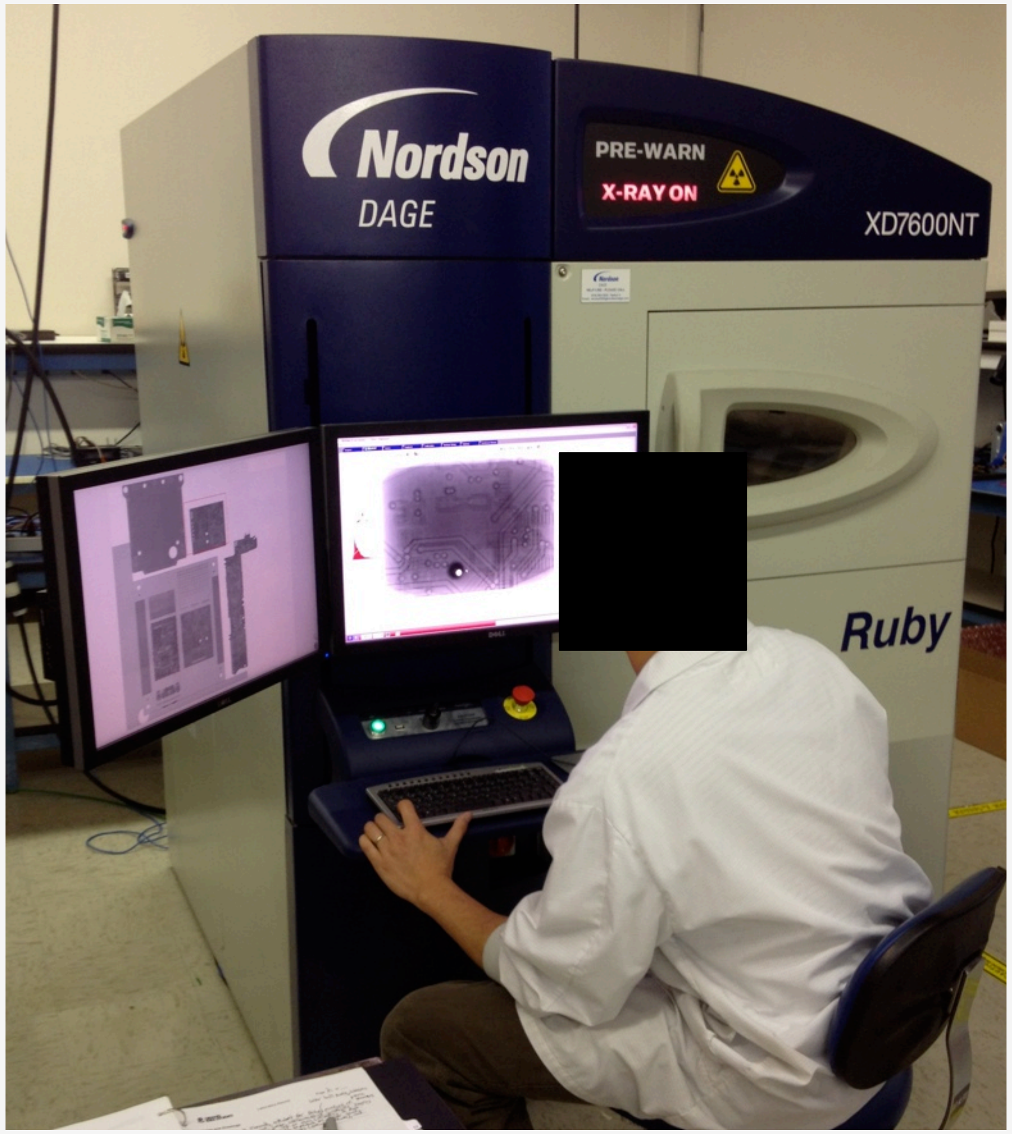


Emic 2 Text-to-Speech Module

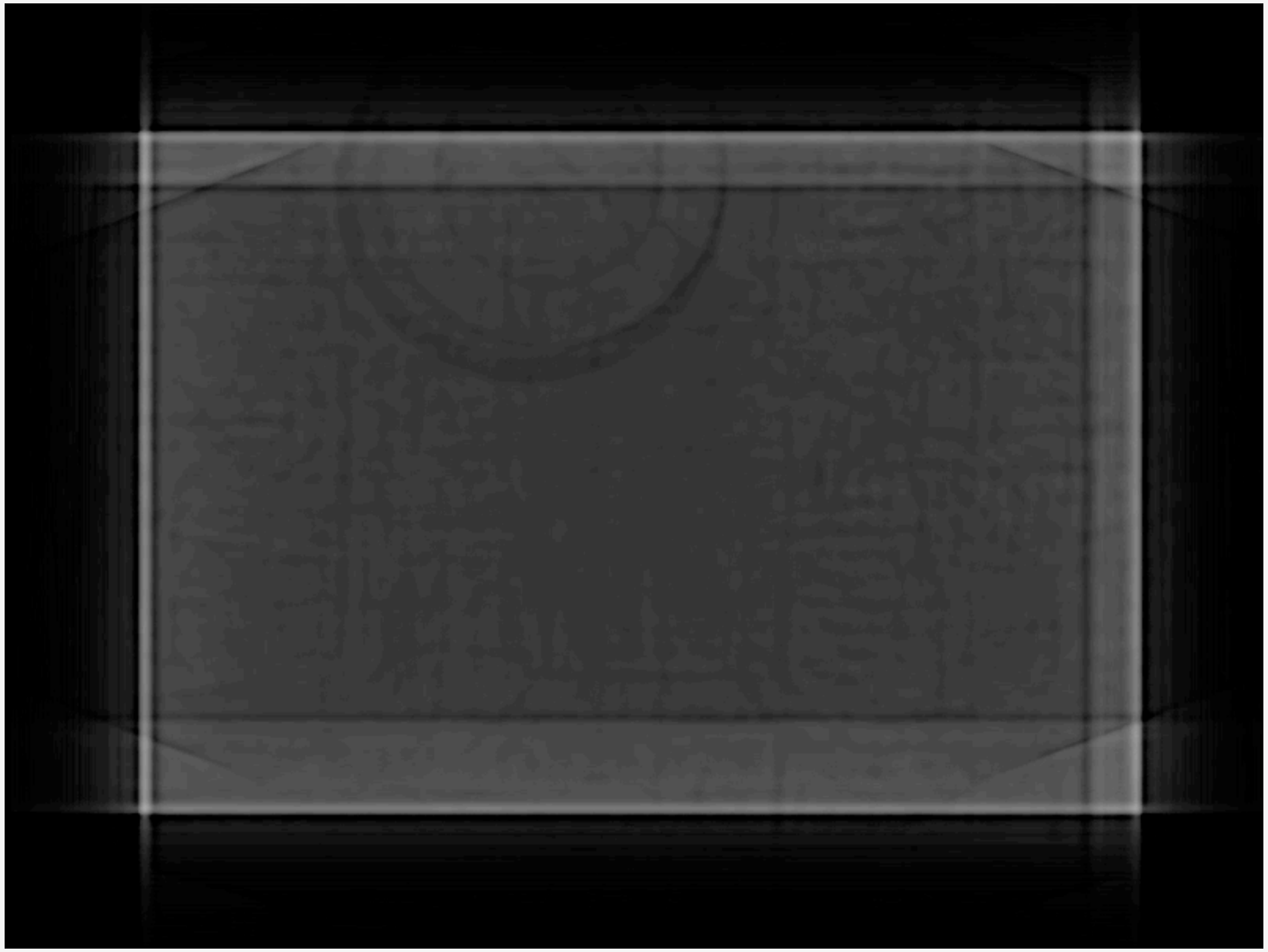


iPhone 4 16GB Assembled

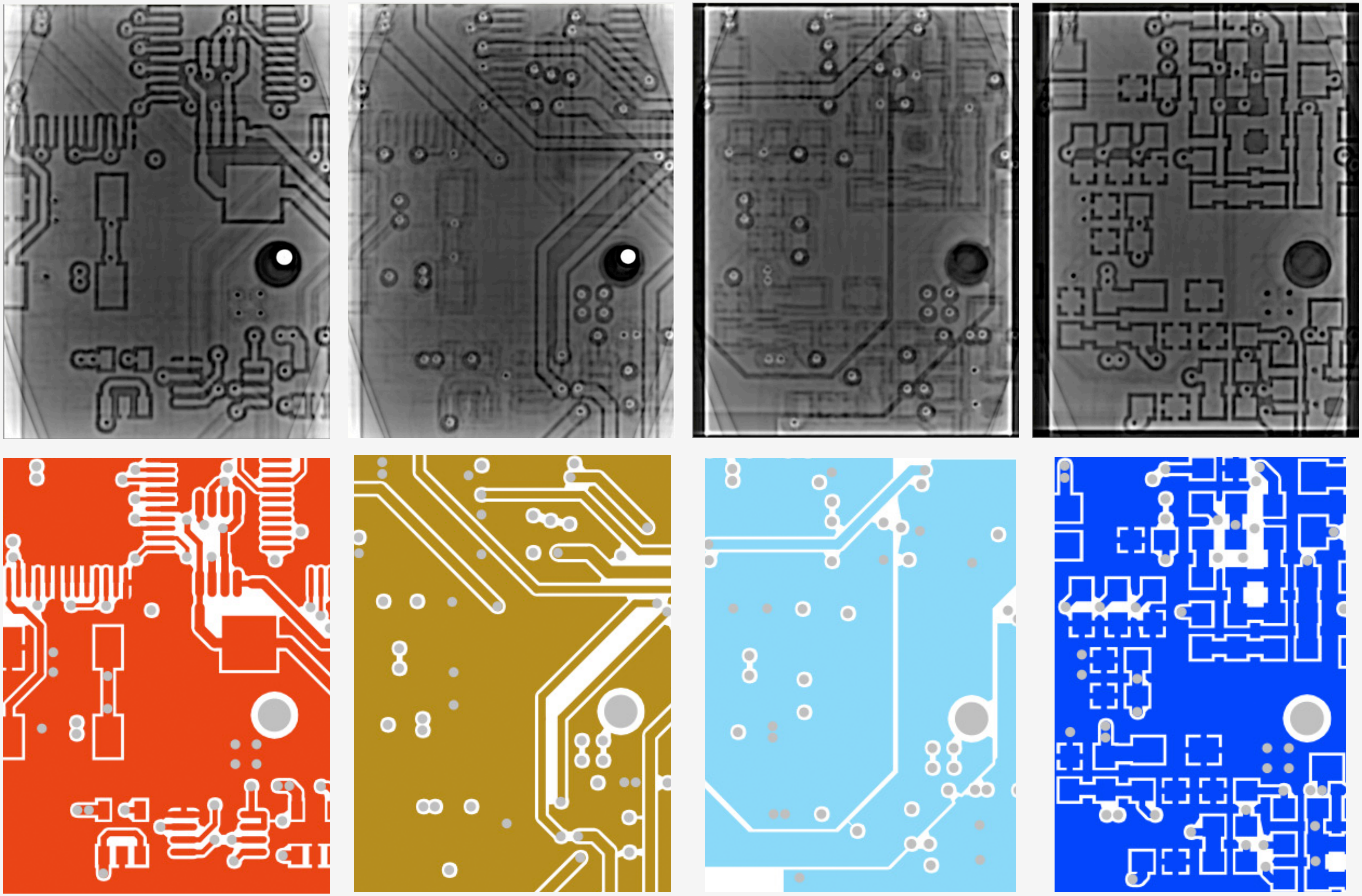
Imaging: X-Ray (3D/CT)



[redacted]



Imaging: X-Ray (3D/CT) 2



Emic 2 Text-to-Speech Module (5/8" x 7/8" area)

Embedded Systems

Hack All the Things

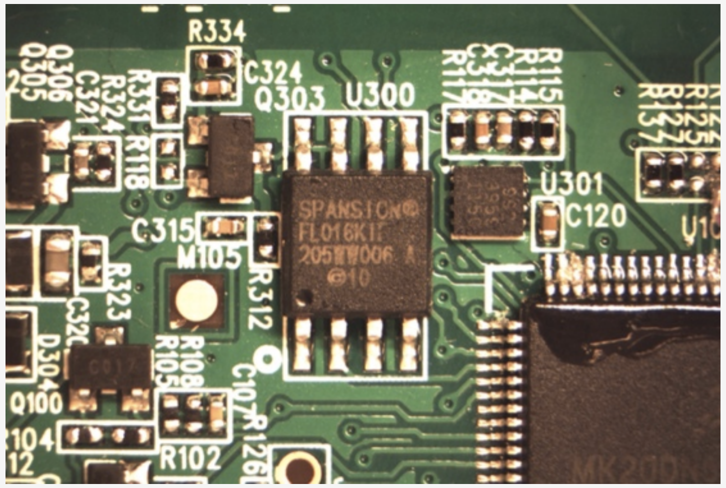
- The Internet of Things becomes "Hack All the Things"
- Any interface may be vulnerable
  - Wired: Serial/UART, USB, Ethernet, CAN, I2C/SPI
  - Wireless: WiFi, Bluetooth, ZigBee, ANT+, "Generic" RF
  - Programming/debug: JTAG, PIC ICSP, TI Spy-Bi-Wire, Freescale BDM, AVR ISP
  - Most implementations transmit data in the clear and have no authentication
    - Some may have password protection or be obfuscated/disabled
  - Vendors may not realize/be aware/care that data streams can be monitored/manipulated
- Other common weaknesses
  - Unsecured Linux implementations, hardcoded credentials/ backdoors, unauthenticated/unencrypted firmware updates

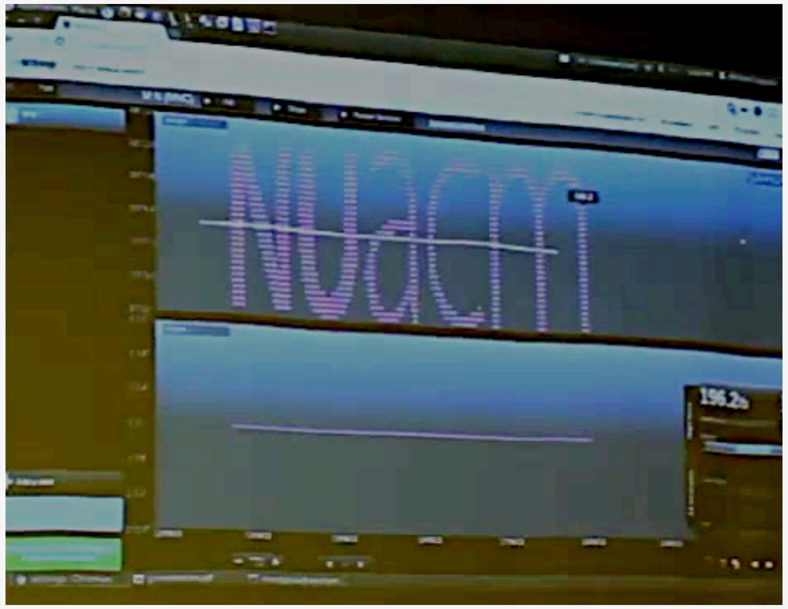
Hack All the Things 2

- GTVHacker Wiki
  - www.gtvhacker.com
  - Blu-ray players, cameras, home automation, media players, mobile devices, NAS, printers, refrigerator, televisions, thermostats
- Craig Heffner
  - www.devttys0.com
  - Routers, access points, IP cameras
  - Finding and Reversing Backdoors in Consumer Firmware, EE Live! 2014, www.devttys0.com/wp-content/uploads/2014/04/FindingAndReversing Backdoors.pdf
- Six Ways to Kill by Hacking
  - www.googlehupf.at/rluh/wp-content/uploads/ITSecX_6WaysToKill_EN.pdf

Withings WS-30 Wireless Scale

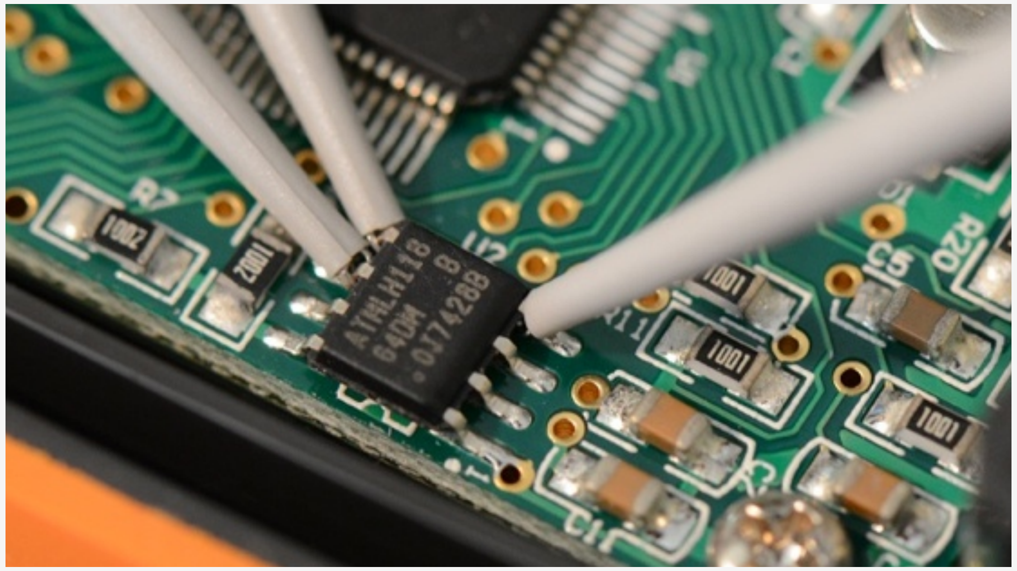
- Can authenticate to database as scale & spoof data
  - Michael Copolla, SummerCon 2013
  - http://poppopret.org/2013/6/10/summercon-2013-hacking-the-withings-ws-30/
- Obtain firmware image during WiFi device update
- Reverse engineer firmware w/ IDA (ARM Cortex-M4)
- Challenge/response secret key stored in plaintext in external SPI Flash





Agilent U1241A True RMS Multimeter

- Changing one byte in Serial EEPROM unlocks higher model (U1242A) features
  - www.eevblog.com/forum/projects/agilent-u1241a-to-u1242a-hack/
- Trial and error
  - Dump memory contents, change each byte, see what happens
  - Once the correct byte was located (new features enabled but not configured), adjusted value of that byte only

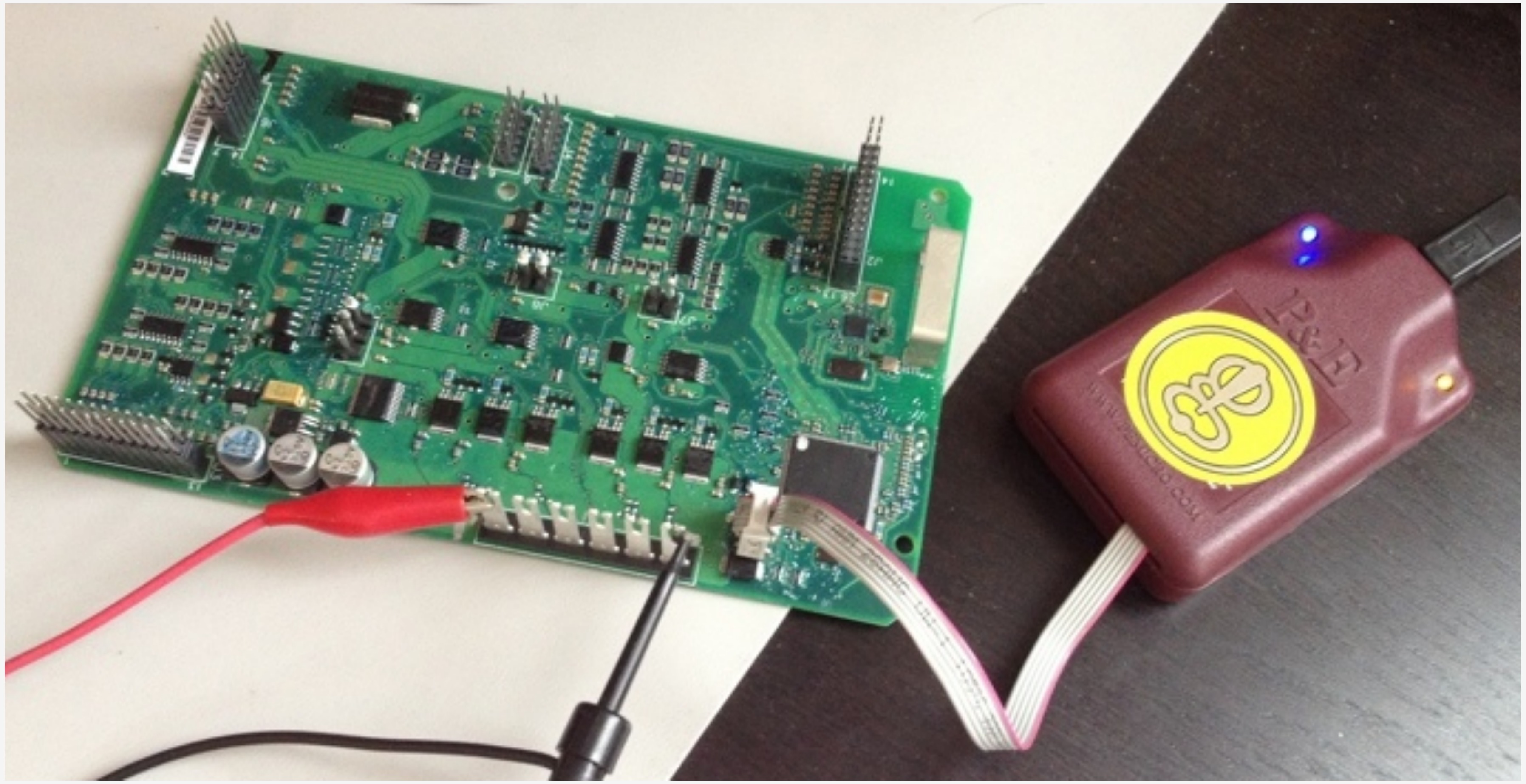


Ford Electronic Control Units (ECUs)

- For Charlie Miller & Chris Valasek's Car Hacking
  - Complete firmware extraction
  - Allowed arbitrary code execution
  - Helped to understand typical CAN traffic/functionality
  - Remote access/exploitation research in progress
  - https://www.defcon.org/html/links/dc-archives/dc-21-archive.html#Miller
  - http://illmatics.com/car_hacking.pdf
- Standard, off-the-shelf development tools
  - Freescale CodeWarrior for S12(X) v5.1 + P&E Multilink USB Rev. C

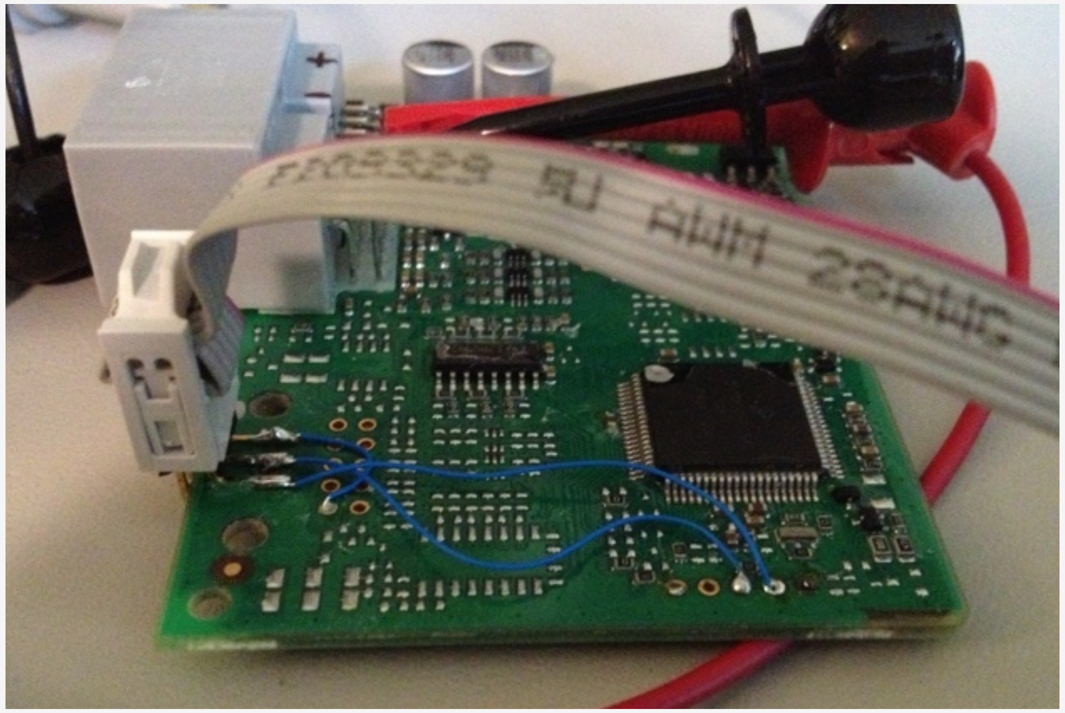
Ford Electronic Control Units (ECUs) 2

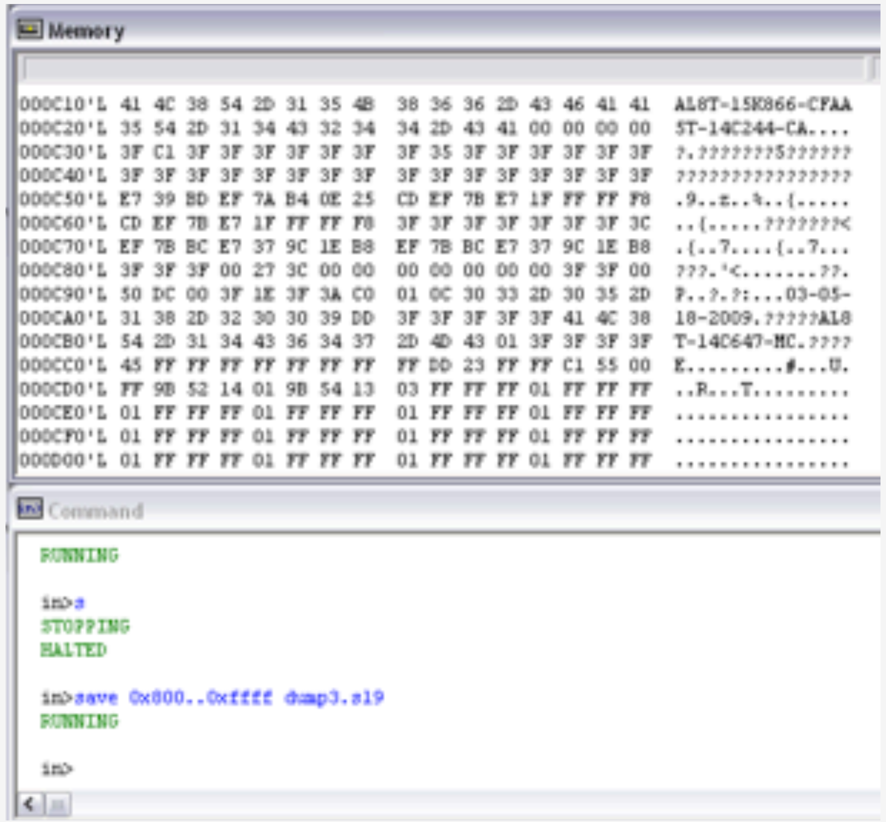
- BDM connector footprint close to part
- No code protection enabled
- Used debugger to manually dump code chunks
- Can load and execute new/modified code



Ford Electronic Control Units (ECUs) 3

- No BDM connector footprint
- Added a BDM connector and wired directly to MCU pins
- Watchdog timer kept resetting the part
  - Changing register to disable internal WDT didn't work
  - Could have been looking for certain data on the CAN bus
- Used debugger to manually dump code in chunks before reset





```
000C10'L 41 4C 38 54 2D 31 35 4B  38 36 36 2D 43 46 41 41  AL8T-15K866-CFAA
000C20'L 35 54 2D 31 34 43 32 34  34 2D 43 41 00 00 00 00  5T-14C244-CA....
000C30'L 3F C1 3F 3F 3F 3F 3F 3F  3F 35 3F 3F 3F 3F 3F 3F  ?.???????5??????
000C40'L 3F 3F 3F 3F 3F 3F 3F 3F  3F 3F 3F 3F 3F 3F 3F 3F  ????????????????
000C50'L E7 39 BD EF 7A B4 0E 25  CD EF 7B E7 1F FF FF F8  .9..z..%..{.....
000C60'L CD EF 7B E7 1F FF FF F8  3F 3F 3F 3F 3F 3F 3F 3C  ..{.....???????<
000C70'L EF 7B BC E7 37 9C 1E B8  EF 7B BC E7 37 9C 1E B8  .{..7....{..7...
000C80'L 3F 3F 3F 00 27 3C 00 00  00 00 00 00 00 3F 3F 00  ???.'<.......??.
000C90'L 50 DC 00 3F 1E 3F 3A C0  01 0C 30 33 2D 30 35 2D  P..?.?:...03-05-
000CA0'L 31 38 2D 32 30 30 39 DD  3F 3F 3F 3F 3F 41 4C 38  18-2009.?????AL8
000CB0'L 54 2D 31 34 43 36 34 37  2D 4D 43 01 3F 3F 3F 3F  T-14C647-MC.????
000CC0'L 45 FF FF FF FF FF FF FF  FF DD 23 FF FF C1 55 00  E.........#...U.
000CD0'L FF 9B 52 14 01 9B 54 13  03 FF FF FF 01 FF FF FF  ..R...T.........
000CE0'L 01 FF FF FF 01 FF FF FF  01 FF FF FF 01 FF FF FF  ................
000CF0'L 01 FF FF FF 01 FF FF FF  01 FF FF FF 01 FF FF FF  ................
000D00'L 01 FF FF FF 01 FF FF FF  01 FF FF FF 01 FF FF FF  ................
```

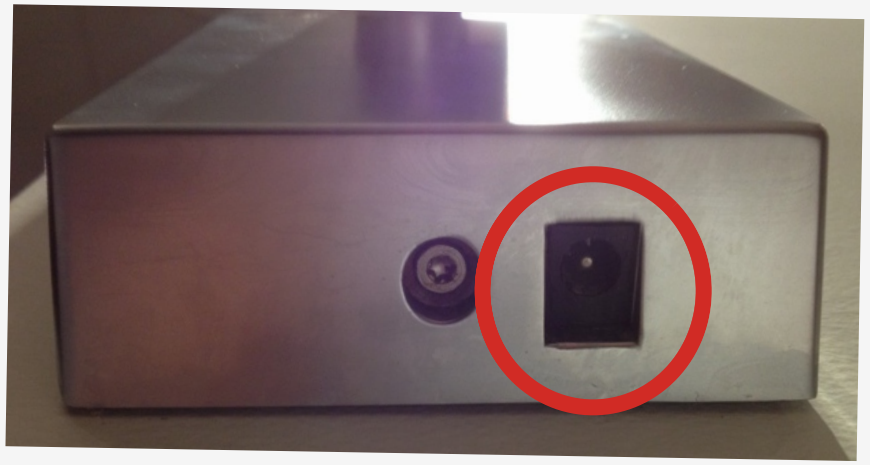
```
RUNNING

in>s
STOPPING
HALTED

in>save 0x800..0xffff dump3.s19
RUNNING

in>
```

Ford Electronic Control Units (ECUs) 4

www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/

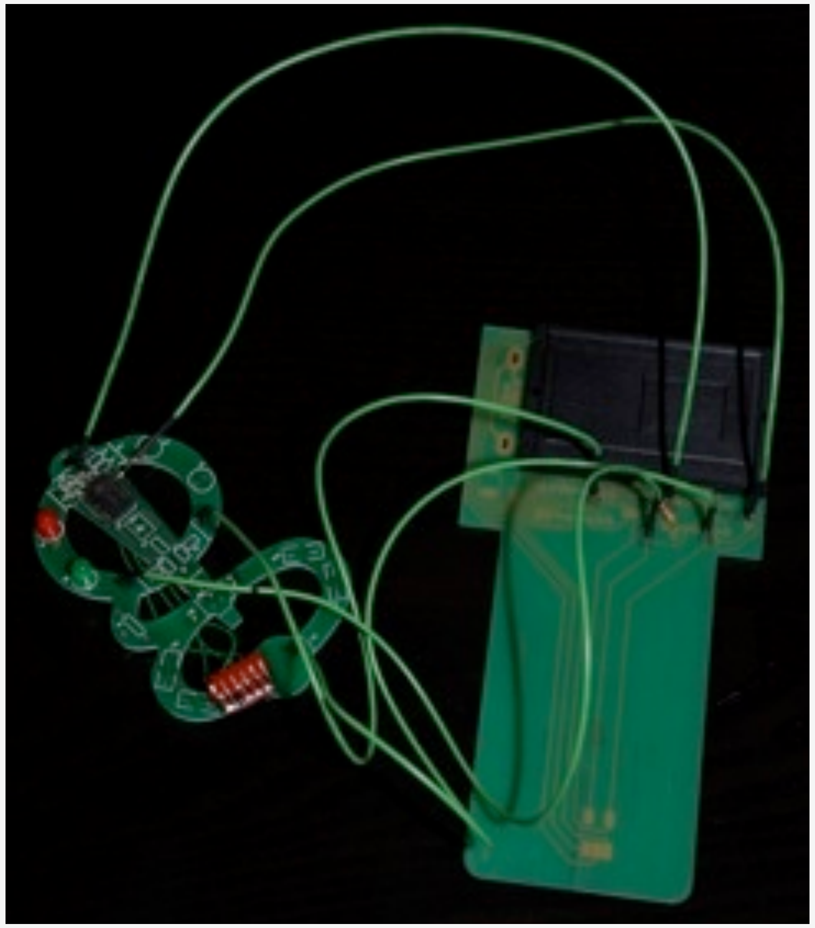
Hotel Room Locks

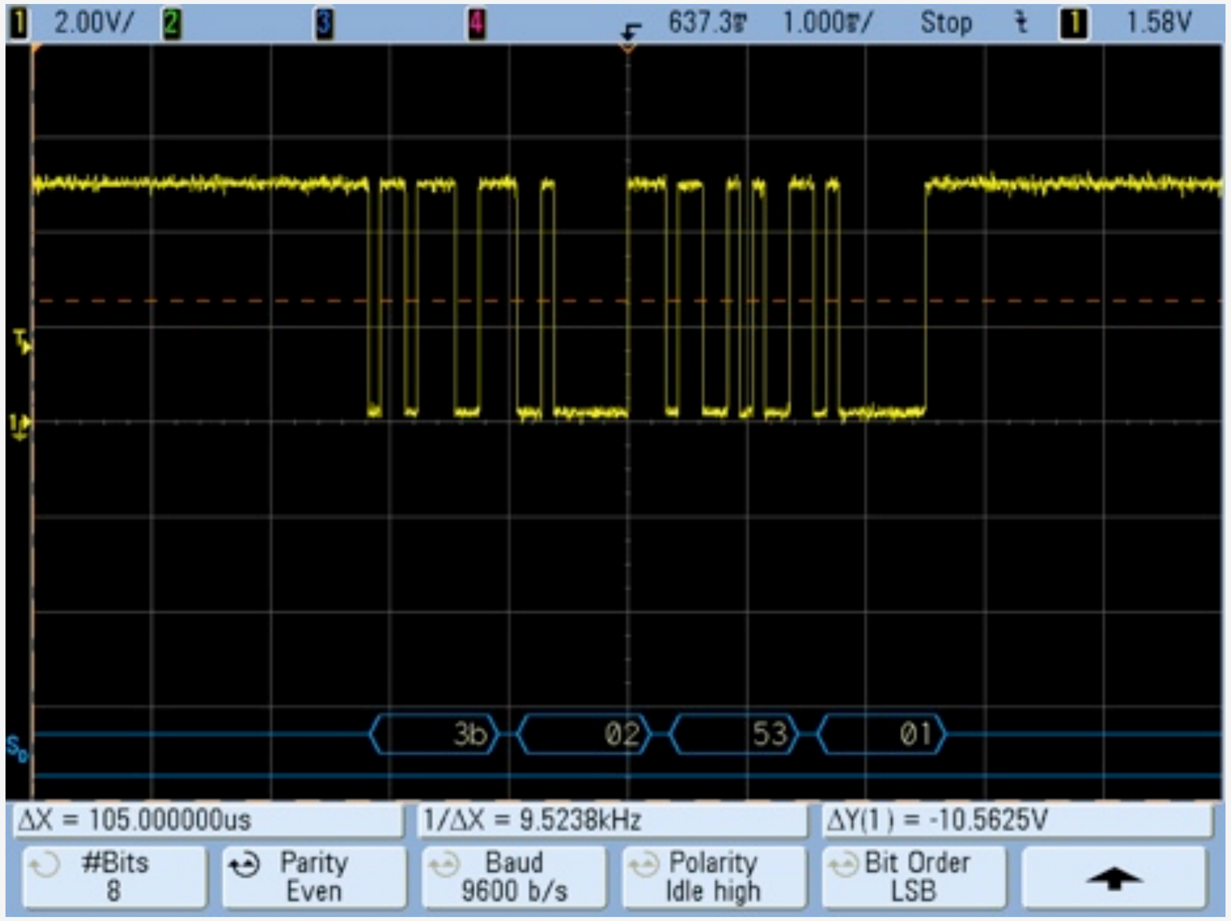
- Cody Brocious, My Arduino can beat up your hotel room lock, BH USA 2012
  - Onity HT lock system, 4 million installed since 1993
  - Read 32-bit sitecode (unique per property) from memory via 1-wire interface
  - Open lock using that same sitecode
  - http://daeken.com/blackhat-paper



SFMTA Smart Parking Meter

- Grand, Tarnovsky, Appelbaum, BH USA 2009
  - Smartcard-based stored value card
  - Monitored communications of legitimate card
  - Created custom smartcard to allow unlimited parking
  - www.grandideastudio.com/portfolio/smart-parking-meters/





1 2.00V/ 2 3 4 637.3ms 1.000ms/ Stop 1 1.58V

3b 02 53 01

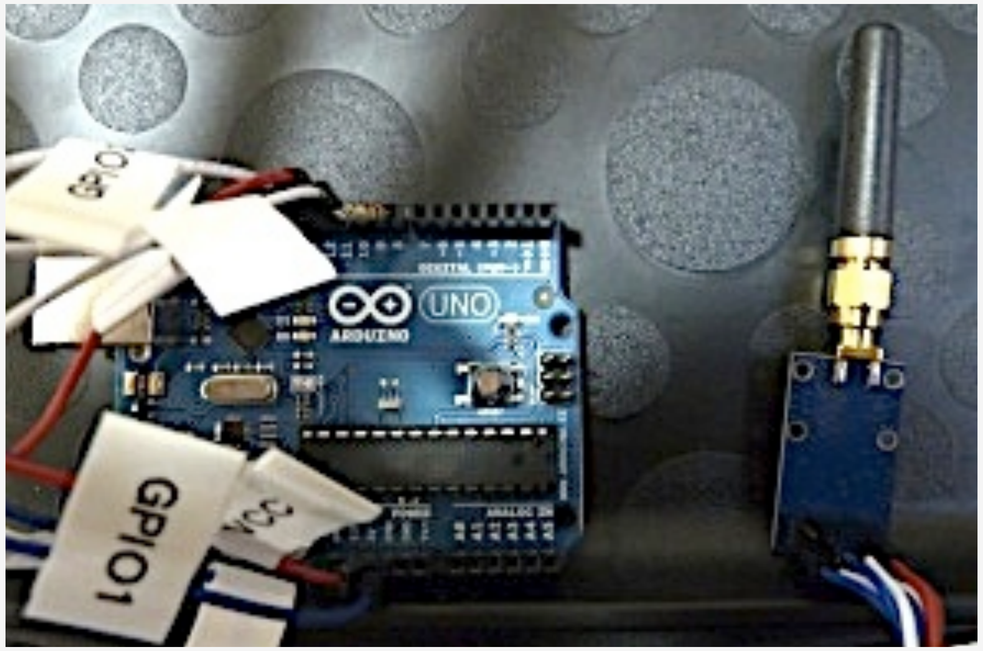
ΔX = 105.000000us 1/ΔX = 9.5238kHz ΔY(1) = -10.5625V

#Bits 8 | Parity Even | Baud 9600 b/s | Polarity Idle high | Bit Order LSB

SFMTA Smart Parking Meter 2

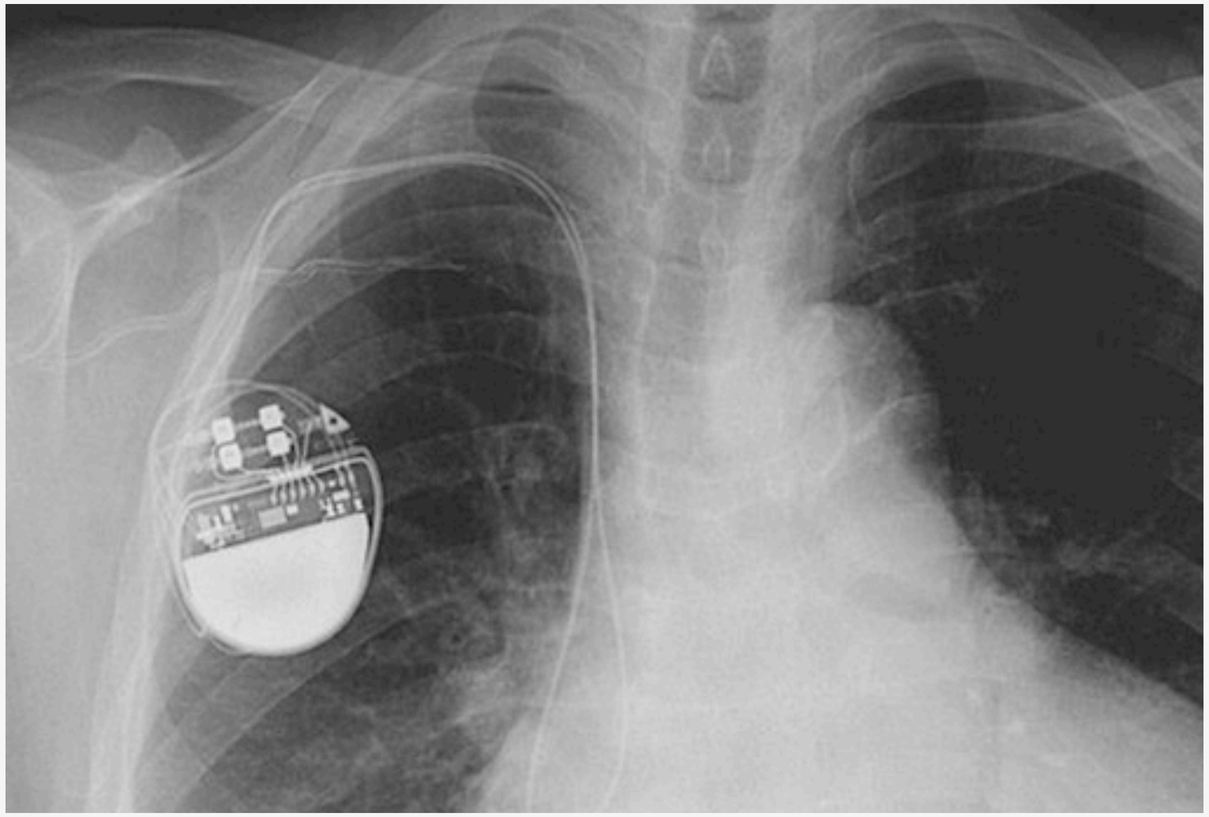
Medical Devices

- Medtronic Implantable Insulin Pump
  - Unauthenticated, remote insulin dispensing
  - Change blood sugar levels on display
  - Download all historical data
  - https://media.blackhat.com/bh-us-11/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_Slides.pdf



Medical Devices 2

- Pacemaker/Implantable Cardiac Defibrillator
  - – Unencrypted communications
  - – Extract private information
  - – Change/disable settings
  - – Send HV shock/induce fibrillation
  - – www.secure-medicine.org/public/publications/icd-study.pdf



Automated Teller Machines (ATMs)

- Barnaby Jack's "Jackpotting ATMs," July 2010
  - Physical access to ATM circuitry (using master key)
  - JTAG interface to PC running Windows CE
  - Injected explorer.exe
  - Reverse engineered file system for vulnerabilities
  - Found flaw in remote update authentication
    - No more physical access required!
  - Uploaded rootkit
  - Results: Spit out money, read card data, etc.
  - https://media.blackhat.com/bh-us-10/video/Jack/BlackHat-USA-2010-Jack-JackpottingATM-video.m4v

Automated Teller Machines (ATMs) 2

Best Practices

Best Practices

- Avoiding the Top 10 Security Flaws
  - http://cybersecurity.ieee.org/center-for-secure-design/avoiding-the-top-10-security-flaws.html
- Compartmentalization
  - Distribute design documentation on a need-to-know basis
  - Be aware of where/how documentation appears online
- Network Configuration
  - Close unused ports/daemons, learn about common network exploits
- Encryption
  - For both data at rest and in motion
  - Consider key management, cipher type, on-chip support
  - Please don't roll your own!

Best Practices 2

- Secure Coding
  - Properly handle undefined behavior, memory leaks, buffer overflows, off-by-one, etc.
- Secure Boot/Code Signing
  - Only execute authenticated code (verified origin/integrity)
- On-Chip Debugging
  - Disable or remove completely for production units
- Security Fuses
  - Easy to enable, makes the attacker work harder

Best Practices 3

- Side-Channel Prevention
  - Unintentional leakage from system
  - Consider power/EM, timing, thermal
- Anti-Tamper Mechanisms
  - Physical security for embedded systems
  - Resistance, evidence, detection, response

Final Thoughts

- People put undeserved trust in hardware
  - In reality, all HW should be untrusted and suspect unless proven/ verified otherwise
- The line is now blurred between HW & SW
  - Provides more attack vectors, allows non-HW hackers to get into the game
- It's so easy, even hackers are getting annoyed
  - [Dailydave] Junk Hacking Must Stop!, Sept. 22, 2014
- Everyone in the industry has to make an effort towards security
  - Vulnerability can happen at any point in the lifecycle
  - We're all responsible!

The End.