Advanced Hardware Hacking Techniques

DEFCON 12

Friday, July 30

Joe Grand (Kingpin)

`joe@grandideastudio.com`

Agenda

- The "What" and "Why" of Hardware Hacking
- Enclosure & Mechanical Attacks
- Electrical Attacks
- Final Thoughts and Conclusions

What is Hardware Hacking (to me)?

- Doing something with a piece of hardware that has never been done before
  - Personalization and customization (e.g., "hot rodding for geeks")
  - Adding functionality
  - Capacity or performance increase
  - Defeating protection and security mechanisms (**not** for profit)
- Creating something extraordinary
- Harming nobody in the process

Why Hardware Hacking?

- Curiosity
  - To see how things work
- Improvement and Innovation
  - Make products better/cooler
  - Some products are sold to you intentionally limited or "crippled"
- Consumer Protection
  - I don't trust glossy marketing brochures...do you?

Hardware Security Myths

- Many security-related products rely on misconceptions to remain "secure"
- Hardware hacking is hard
- Consumers lack the competency or courage to void their warranty
- Therefore, hardware is "safe"

Gaining Access to a Product

- Purchase
  - Buy the product from a retail outlet (with cash)
- Evaluation
  - Rent or borrow the product
- Active
  - Product is in active operation, not owned by attacker
- Remote Access
  - No physical access to product, attacks launched remotely

Attack Vectors

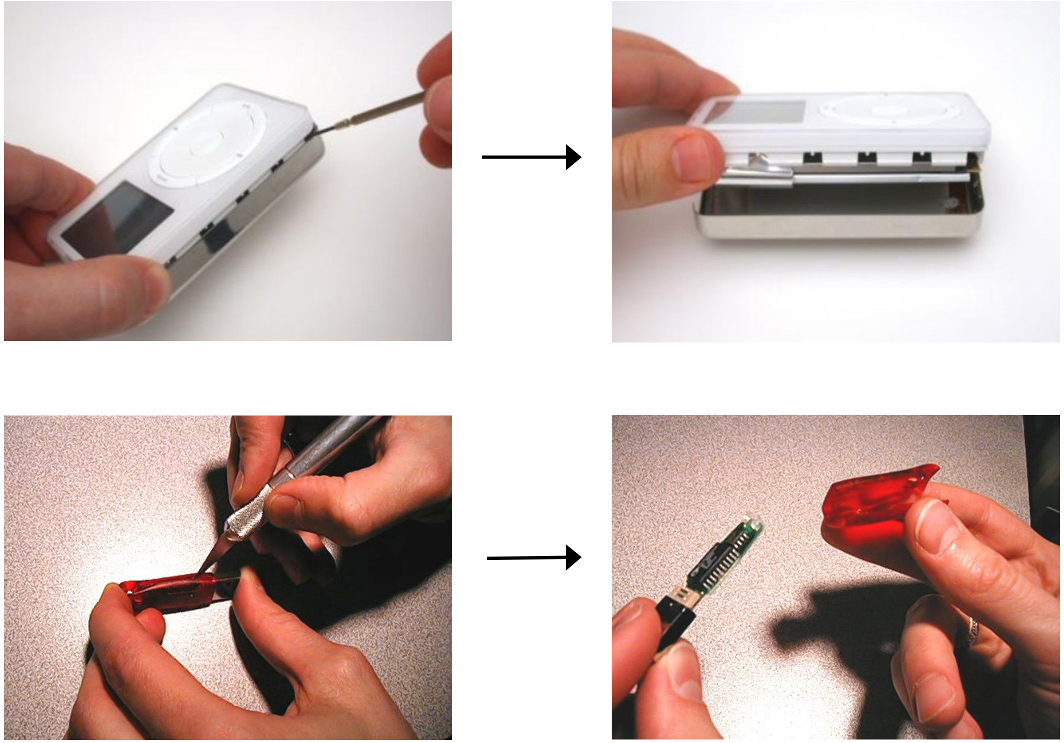
- Interception (or Eavesdropping)
  - Gain access to protected information without opening the product
- Interruption (or Fault Generation)
  - Preventing the product from functioning normally
- Modification
  - Tampering with the product, typically invasive
- Fabrication
  - Creating counterfeit assets of a product

Enclosure & Mechanical Attacks

- Opening Housings
- External Interfaces
- Anti-Tamper Mechanisms
- Conformal Coating and Epoxy Encapsulation Removal

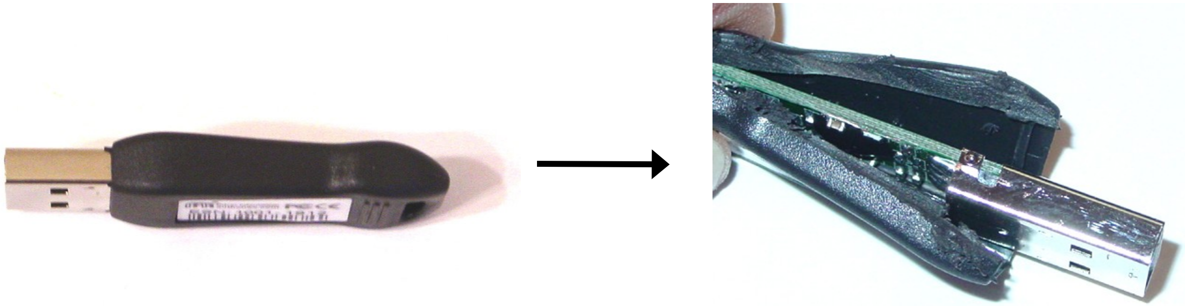
Opening Housings

- Goal is to get access to internal circuitry
- Usually as easy as loosening some screws or prying open the device



Opening Housings 2

- If glue is used to seal housing, use heat gun to soften glue and pry open with a knife
  - Some designers use glue with a high-melting point - enclosure will melt/deform before the glue does
- Some devices are sonically-welded to create a one-piece outer shell
  - If done properly, will require destruction of device in order to open it



Opening Housings 3

- Security bits and one-way screws
  - Used to prevent housings from being easily opened
  - Ex.: Bathroom stalls, 3.8mm and 4.5mm security bit for Nintendo and Sega game cartridges/systems
  - To identify a particular bit type, visit **`www.lara.com/reviews/screwtypes.htm`**
  - Bits available at electronics stores, swapmeets, online

External Interfaces

- Usually a product's lifeline to the outside world
  - Manufacturing tests, field programming/upgrading, peripheral connections
  - Ex.: JTAG, RS232, USB, Firewire, Ethernet
- Wireless interfaces also at risk (though not discussed here)
  - Ex.: 802.11b, Bluetooth
- Any interface that connects to a third-party may contain information that is useful for an attack
  - Could possibly obtain data, secrets, etc.

External Interfaces 2

- Look for obfuscated interfaces
  - Ex.: Proprietary or out-of-the-ordinary connector types, hidden access doors or holes
- Many times, test points just hidden by a sticker

External Interfaces 3

- Use multimeter or oscilloscope to probe and determine functionality
  - Logic state of pins can help with an educated guess
  - Ex.: Pull pins high or low, observe results, repeat
- Monitor communications using H/W or S/W-based protocol analyzer
  - USB: SnoopyPro
  - RS232 and parallel port: PortMon
- Send intentionally malformed/bad packets to cause a fault
  - If firmware doesn't handle this right, device could trigger unintended operation useful for an attack

External Interfaces: Backdoors

- Architecture-specific debug and test interfaces (usually undocumented)
- Diagnostic serial ports
  - Provides information about system, could also be used for administration
  - Ex.: Intel NetStructure crypto accelerator administrator access [1]
- Developer's backdoors
  - Commonly seen on networking equipment, telephone switches
  - Ex.: Palm OS debug mode [2]
  - Ex.: Sega Dreamcast CD-ROM boot

External Interfaces: JTAG

- JTAG (IEEE 1149.1) interface is often the Achilles' heel
- Industry-standard interface for testing and debugging
  - Ex.: System-level testing, boundary-scanning, and low-level testing of dies and components
- Can provide a direct interface to hardware
  - Has become a common attack vector
  - Ex.: Flash memory reprogramming on Pocket PC devices (**`www.xda-developers.com/jtag`**)

External Interfaces: JTAG 2

- Five connections (4 required, 1 optional):
  - ← TDO = Data Out (from target device)
  - → TDI = Data In (to target device)
  - → TMS = Test Mode Select
  - → TCK = Test Clock
  - → /TRST = Test Reset (optional)
- H/W interface to PC can be built with a few dollars of off-the-shelf components
  - Ex.: **`www.lart.tudelft.nl/projects/jtag`**, **`http://jtag-arm9.sourceforge.net/circuit.txt`**, or **`ftp://www.keith-koep.com/pub/arm-tools/jtag/ jtag05_sch.pdf`**

External Interfaces: JTAG 3

- JTAG Tools (`http://openwince.sourceforge.net/jtag`) serves as the S/W interface on the PC
- Removing JTAG functionality from a device is difficult
  - Designers usually obfuscate traces, cut traces, or blow fuses, all of which can be repaired by an attacker

Anti-Tamper Mechanisms

- Primary facet of physical security for embedded systems
- Attempts to prevent unauthorized physical or electronic tampering against the product
- Most effectively used in layers
- Possibly bypassed with knowledge of method
  - Purchase one or two devices to serve as "sacrificial lambs"

Anti-Tamper Mechanisms 2

- Tamper Resistance
  - Specialized materials used to make tampering difficult
  - Ex.: One-way screws, epoxy encapsulation, sealed housings
- Tamper Evidence
  - Ensure that there is visible evidence left behind by tampering
  - Only successful if a process is in place to check for deformity
  - Ex.: Passive detectors (seals, tapes, glues), special enclosure finishes (brittle packages, crazed aluminum, bleeding paint)

Anti-Tamper Mechanisms 3

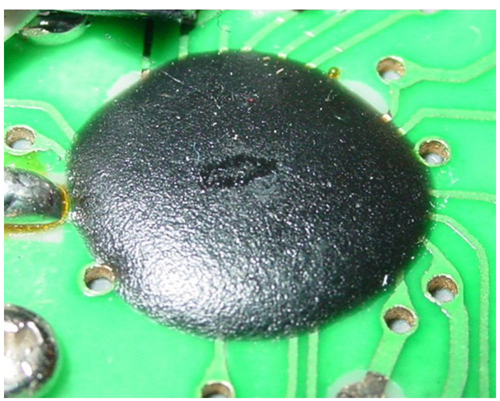
- Tamper Detection
  - Enable the hardware device to be aware of tampering
  - Switches: Detect the opening of a device, breach of security boundary, or movement of a component
  - Sensors: Detect an operational or environmental change
  - Circuitry: Detect a puncture, break, or attempted modification of the security envelope

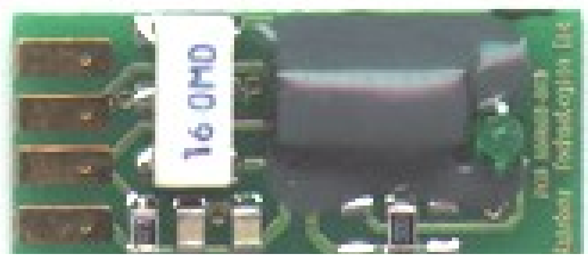
Anti-Tamper Mechanisms 4

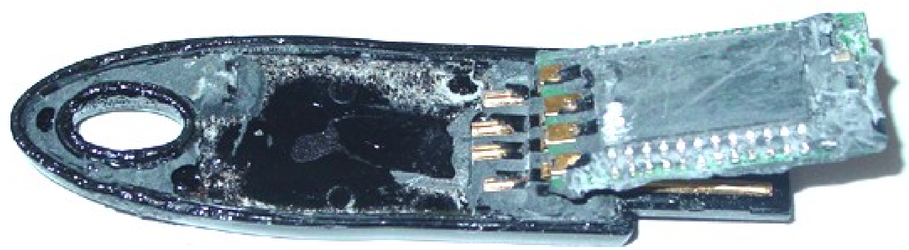
- Tamper Response
  - Countermeasures taken upon the detection of tampering
  - Ex.: Zeroize critical memory, shutdown/disable/destroy device, enable logging features
- *Physical Security Devices for Computer Subsystems* [3] provides comprehensive attacks and countermeasures
  - Ex.: Probing, machining, electrical attacks, physical barriers, tamper evident solutions, sensors, response technologies

Conformal Coating and Epoxy Encapsulation Removal

- Encapsulation used to protect circuitry from moisture, dust, mold, corrosion, or arcing
- Epoxy or urethane coatings leave a hard, difficult to remove film





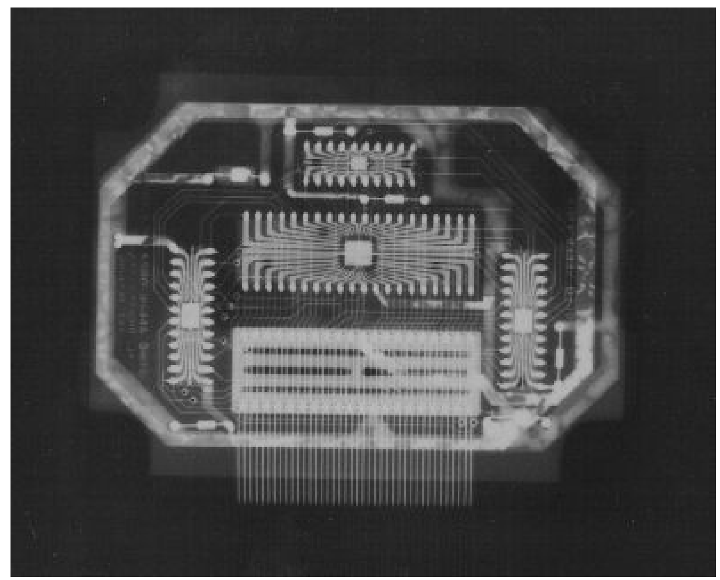


Conformal Coating and Epoxy Encapsulation Removal 2

- The good news: The coatings are not specifically designed for security
  - Can usually be bypassed with special chemicals like MG Chemicals' 8310 Conformal Coating Stripper (`www.mgchemicals.com`)
- Brute force approach: Dremel tool and wooden skewer as a drill bit
  - Doesn't damage the components underneath coating
  - Might remove the soldermask, but not a big deal...

Conformal Coating and Epoxy Encapsulation Removal 3

- When all else fails, use X-ray to determine location of components or connections



Electrical Attacks

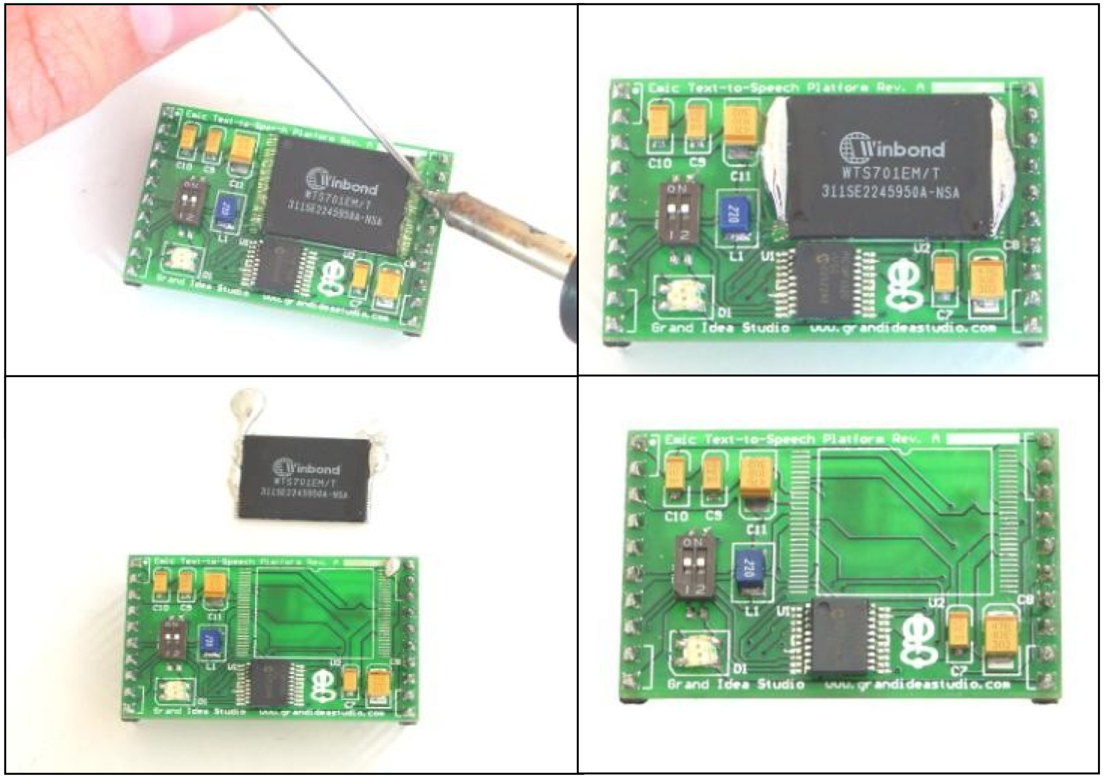
- Surface Mount Devices
- Probing Boards
- Memory and Programmable Logic
- Chip Delidding and Die Analysis
- Emissions and Side-Channel Attacks
- Clock and Timing

Surface Mount Devices

- Harder to work with than through-hole devices
  - Ex.: Fine-pitched packages, tiny discrete components
  - Don't get discouraged
- Human hands have more resolution than the naked eye can resolve
  - A microscope can go a long way to solder components
- Circuit Cellar, July 2004: Build your own computer-controlled, temperature-adjusting SMT oven

Surface Mount Devices 2

- Easy to desolder using ChipQuik SMD Removal Kit (**`www.chipquik.com`**)

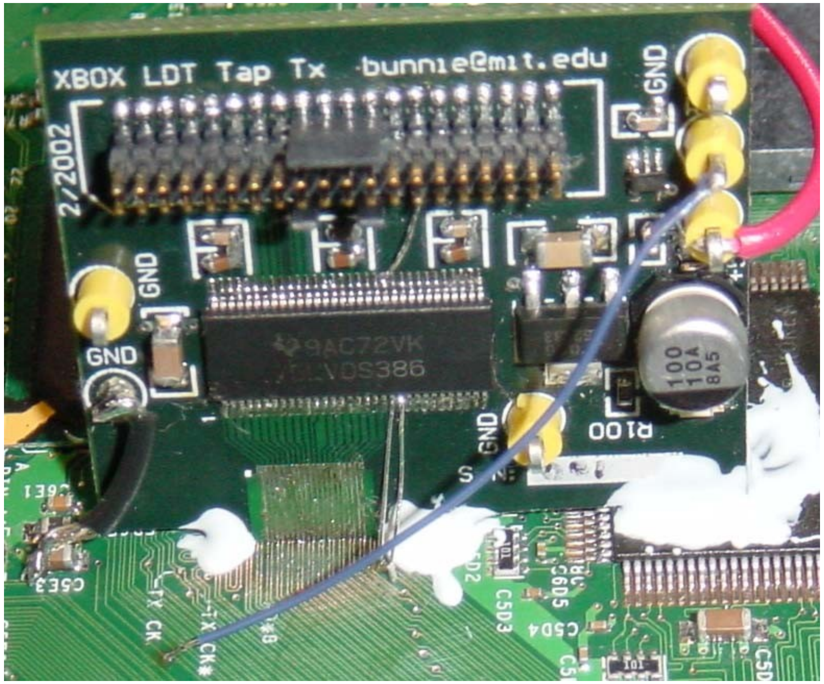


Probing Boards

- Look for test points and exposed traces/bus lines
- Surface mount leads and points are usually too small to manually probe
- Many ways to access:
  - Solder probe wire onto board using microscope
  - Use an SMD micrograbber ($5-$50)
  - Use a probe adapter (> $100) from **`www.emulation.com`**, **`www.ironwoodelectronics.com`**, or **`www.advintcorp.com`**
  - Build your own probe

Probing Boards 2

- Ex.: Tap board used to intercept data transfer over Xbox's HyperTransport bus [4]



Memory and Programmable Logic

- Most memory is notoriously insecure
  - Not designed with security in mind
  - Serial EEPROMs can be read in-circuit, usually SPI or I^2C bus (serial clock and data) [5]
- Difficult to securely and totally erase data from RAM and non-volatile memory [6]
  - Remnants may exist and be retrievable from devices long after power is removed
  - Could be useful to obtain program code, temporary data, crypto keys, etc.

Memory and Programmable Logic 2

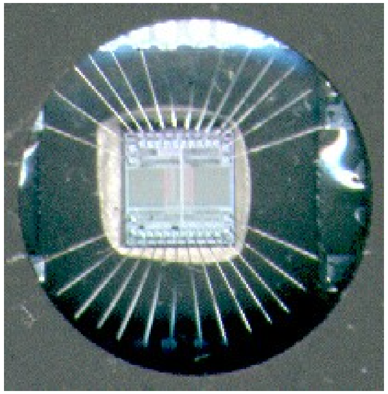
- SRAM-based FPGAs most vulnerable to attack
  - Must load configuration from external memory
  - Bit stream can be monitored to retrieve entire configuration
- To determine PLD functionality, try an I/O scan attack
  - Cycle through all possible combinations of inputs to determine outputs

Memory and Programmable Logic 3

- Security fuses and boot-block protection
  - Enabled for "write-once" access to a memory area or to prevent full read back
  - Usually implemented in any decent design
  - Might be bypassed with die analysis attacks (FIB) or electrical faults [7]
  - Ex.: PIC16C84 attack in which security bit is removed by increasing VCC during repeated write accesses

Chip Decapping and Die Analysis

- Analysis of Integrated Circuit (IC) dies is typically the most difficult area for hardware hacking
- With access to the IC die, you can:
  - Retrieve contents of Flash, ROM, FPGAs, other non-volatile devices (firmware and crypto keys stored here)
  - Modify or destroy gates and other silicon structures (e.g., reconnect a security fuse that prevents reading of the device)



Chip Decapping and Die Analysis 2

- The good thing is that IC designers make mistakes, so tools are needed
  - Failure analysis
  - Chip repair and inspection
- What tools?
  - Chip Decappers
  - Scanning Electron Microscope (SEM)
  - Voltage Contrast Microscopy
  - Focused Ion Beam (FIB)

Chip Decapping and Die Analysis 3

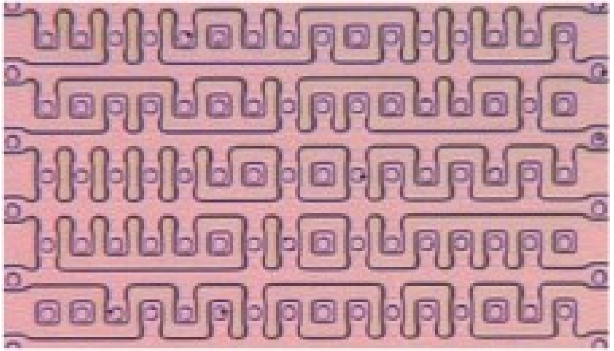
- Equipment available on the used/surplus market
- Access to tools in most any large academic institution
- Reverse engineering and analysis services exist (still high priced, $10k-$20k)
  - Can provide functional investigation, extraction, IC simulation, analyze semiconductor processes, etc.
  - Ex.: Semiconductor Insights (**`www.semiconductor.com`**) and Chipworks (**`www.chipworks.com`**)

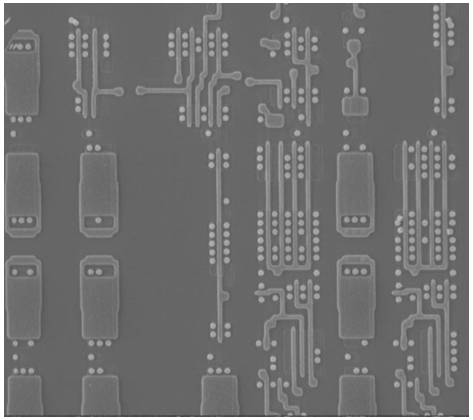
Chip Decapping and Die Analysis: IC Decapsulation

- Decapsulation tools used to "delid" or "decap" the top of the IC housing
- Uses chemical or mechanical means (or both)
- Will keep the silicon die intact while removing the outer material
- Ex.: Nippon Scientific (**`www.nscnet.co.jp/e`**), Nisene Technology Group (**`www.nisene.com`**), ULTRA TEC Manufacturing (**`www.ultratecusa.com`**), approx. $30k new, $15k used

Chip Decapping and Die Analysis: Scanning Electron Microscope

- Used to perform sub-micron inspection of the physical die
- Metal or other material layers might need to be de-processed before access to gate structures
- Depending on ROM size and properties, can visually recreate contents

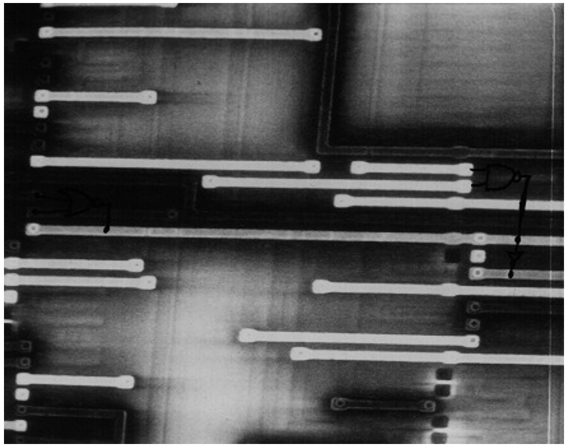




(Photos from ADSR Ltd. and FIB International)

Chip Decapping and Die Analysis: Voltage Contrast Microscopy

- Detect variances of voltages and display them as contrast images
  - Performed with a SEM
- Ex.: Could extract information from a Flash ROM storage cell



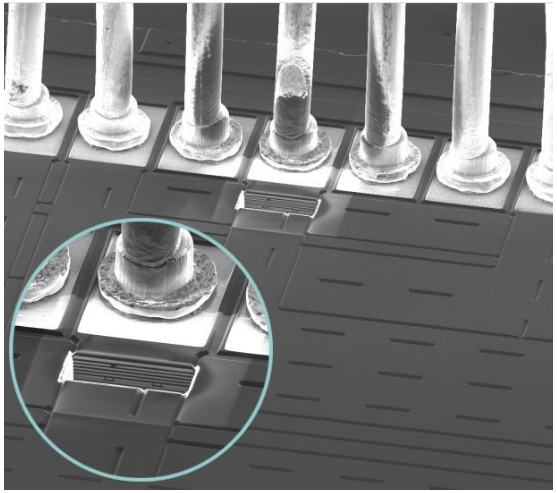
(Photo from `http://testequipmentcanada.com/VoltageContrastPaper.html`)

Chip Decapping and Die Analysis: Focused Ion Beams

- Send a focused stream of ions onto the surface of the chip
  - Beam current and optional use of gas/vapor changes the function
- Cutting
  - Ex.: Cut a bond pad or trace from the die ($1k-$10k)
- Deposition
  - Ex.: Add a jumper/reconnect a trace on the die ($1k-$10k)

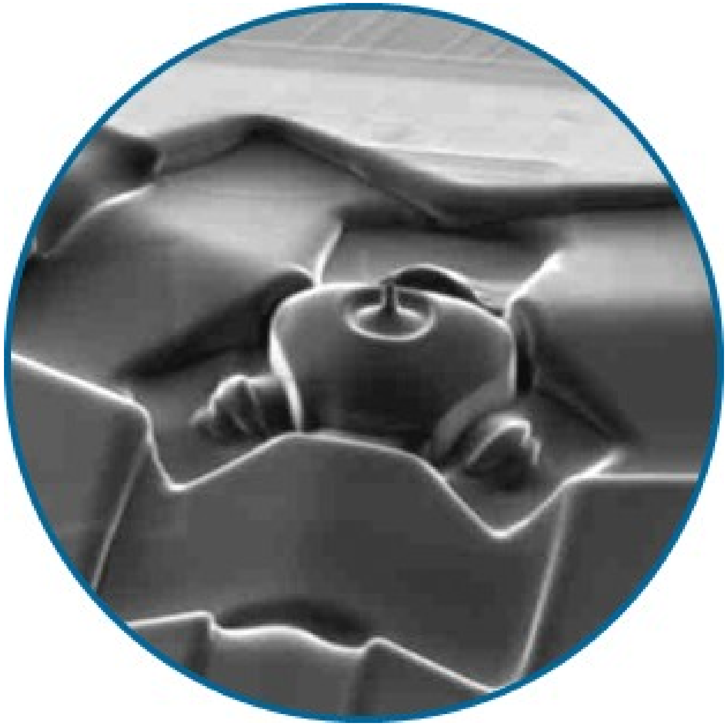
Chip Decapping and Die Analysis: Focused Ion Beams 2

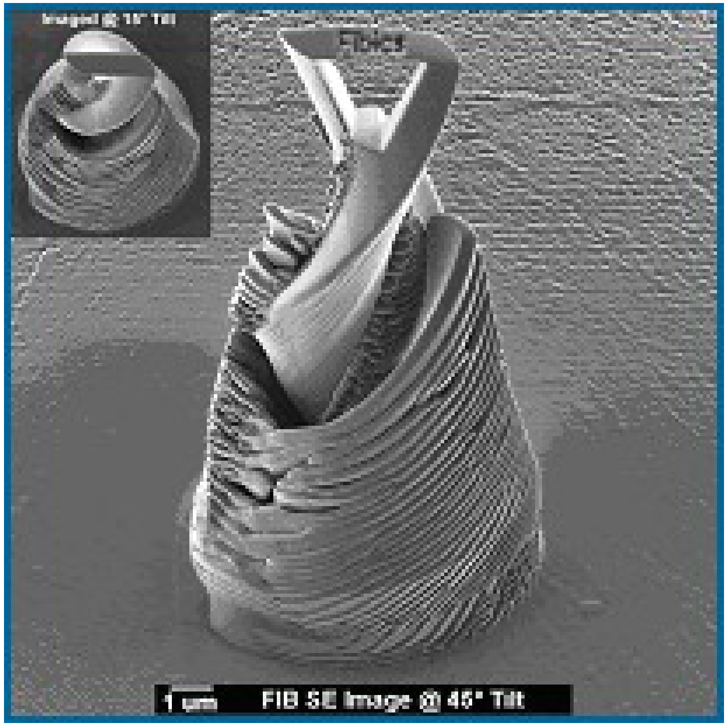
- Imaging
  - High-resolution image of die structure
- Ex.: Fibics Incorporated (**`www.fibics.com`**) or FIB International (**`www.fibinternational.com`**)



(Photos from Fibics Incorporated)

Chip Decapping and Die Analysis: Focused Ion Beams 3





(Photos from Fibics Incorporated)

Emissions and Side-Channel Attacks

- All devices leak information
  - EMI (electromagnetic interference) from circuits (TEMPEST) [8, 9]
  - Power supply fluctuations
  - Visible radiation from LEDs and monitors [10, 11]
- Can be monitored and used by attacker to determine secret information
- Devices may also be susceptible to RF or ESD (immunity)
  - Intentionally injected to cause failure

Emissions and Side-Channel Attacks: Power Supply

- Simple Power Analysis (SPA)
  - Attacker directly observes power consumption
  - Varies based on microprocessor operation
  - Easy to identify intensive functions (cryptographic)
- Differential Power Analysis (DPA) [12]
  - Advanced mathematical methods to determine secret information on a device

Clock and Timing

- Attacks rely on changing or measuring timing characteristics of the system
- Active (Invasive) timing attacks
  - Vary clock (speed up or slow down) to induce failure or unintended operation
- Passive timing attacks
  - Non-invasive measurements of computation time
  - Different tasks take different amounts of time

Security Through Obscurity

- "Security through obscurity" does **not** work
  - Provides a false sense of security to designers/users
  - Might temporarily discourage an attacker, but it only takes one to discover it
- Weak tactics to look out for when hacking "secure" hardware products:
  - Encoded forms of fixed data
  - Scrambled address lines through extra logic
  - Intentionally messy/lousy code
  - Spurious and meaningless data ("signal decoys")

Hardware Hacking Challenges

- Advances in chip packaging
  - Ultra-fine pitch and chip-scale packaging (e.g., BGA, COB, CIB)
  - Not as easy to access pins/connections to probe
  - Discrete components can now easily be inhaled
- Highly-integrated chips (sub-micron)
  - Difficult, but not impossible, to probe and modify
- High speed boards
  - Processor and memory bus > hundreds of MHz
  - Serial bus speeds approaching Gigabit/sec.

Hardware Hacking Challenges 2

- Cost of equipment
  - Advanced tools still beyond the reach of average hobbyist (probing, decapping, SEMs, etc.)
  - "State of the art" defined by what hackers can find in the trash and at swapmeets
- Societal pressures
  - Hardware hacking is practically mainstream, but "hacker" is still a naughty word

Conclusions

- Hardware hacking is approaching a mainstream activity
- Plays an important role in the balance between consumers and corporations (e.g., The Man)
- Think as a designer would
- Nothing is ever 100% secure
  - Given enough time, resources, and motivation, you can break anything
- The possibilities are endless
- Have fun!

References

1. J. Grand, et al, "Hack Proofing Your Network: 2nd Edition," Syngress Publishing, 2002, **www.grandideastudio.com/files/books/hpyn2e_chapter14.pdf**
2. J. Grand (Kingpin), “Palm OS Password Lockout Bypass,” March 2001, **www.grandideastudio.com/files/security/mobile/palm_backdoor_debug_advisory.txt**
3. S.H. Weingart, "Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defenses," *Workshop on Cryptographic Hardware and Embedded Systems*, 2000.
4. A. Huang, "Hacking the Xbox: An Introduction to Reverse Engineering," No Starch Press, 2003.
5. J. Grand (Kingpin), "Attacks on and Countermeasures for USB Hardware Token Devices," *Proceedings of the Fifth Nordic Workshop on Secure IT Systems*, 2000, **www.grandideastudio.com/files/security/tokens/usb_hardware_token.pdf**
6. P. Gutmann, "Secure Deletion from Magnetic and Solid-State Memory Devices," *Sixth USENIX Security Symposium*, 1996, **www.usenix.org/publications/library/proceedings/sec96/full_papers/gutmann/index.html**

References 2

7. S. Skorobogatov, "Breaking Copy Protection in Microcontrollers," **`www.cl.cam.ac.uk/~sps32/mcu_lock.html`**
8. W. van Eck, "Electronic Radiation from Video Display Units: An Eavesdropping Risk?" *Computers and Security*, 1985, **`www.jya.com/emr.pdf`**
9. J.R. Rao and P. Rohatgi, "EMPowering Side-Channel Attacks," IBM Research Center, **`www.research.ibm.com/intsec/emf-paper.ps`**
10. Joe Loughry and D.A. Umphress, "Information Leakage from Optical Emanations," *ACM Transactions on Information and System Security v.5, #3*, August 2002, **`www.applied-math.org/optical_tempest.pdf`**
11. M. Kuhn, "Optical Time-Domain Eavesdropping Risks of CRT Displays," *Proceedings of the 2002 IEEE Symposium on Security and Privacy*, May 2002, **`www.cl.cam.ac.uk/~mgk25/ieee02-optical.pdf`**
12. P. Kocher, J. Jaffe, and B. Jun, "Overview of Differential Power Analysis," **`www.cryptography.com/resources/whitepapers/DPATechInfo.PDF`**

Appendix A: Additional Resources

- J. Grand, et al, "Hardware Hacking: Have Fun While Voiding Your Warranty," Syngress Publishing, January 2004.
- J. Grand, "Practical Secure Hardware Design for Embedded Systems," *Proceedings of the 2004 Embedded Systems Conference*, 2004, **www.grandideastudio.com/files/security/hardware/practical_secure_hardware_design.pdf**
- A. Huang, "Keeping Secrets in Hardware: the Microsoft XBox Case Study," *Massachusetts Institute of Technology AI Memo 2002-008*, May 2002, **http://web.mit.edu/bunnie/www/proj/anatak/AIM-2002-008.pdf**
- F. Beck, "Integrated Circuit Failure Analysis - A Guide to Preparation Techniques," John Wiley & Sons, 1998.
- O. Kömmerling and M. Kuhn, "Design Principles for Tamper-Resistant Smartcard Processors," *USENIX Workshop on Smartcard Technology*, 1999, **www.cl.cam.ac.uk/~mgk25/sc99-tamper.pdf**
- R.G. Johnston and A.R.E. Garcia, "Vulnerability Assessment of Security Seals", *Journal of Security Administration*, 1997, **www.securitymanagement.com/library/lanl_00418796.pdf**

Appendix B: Related Web Sites

- Cambridge University Security Group - TAMPER Laboratory, **www.cl.cam.ac.uk/Research/Security/tamper**
- Molecular Expressions: Chip Shots Gallery, **http://microscopy.fsu.edu/chipshots/index.html**
- Bill Miller's CircuitBending.com, **http://billtmiller.com/circuitbending**
- Virtual-Hideout.Net, **www.virtual-hideout.net**
- LinuxDevices.com - The Embedded Linux Portal, **www.linuxdevices.com**
- Roomba Community - Discussing and Dissecting the Roomba, **www.roombacommunity.com**
- TiVo Techies, **www.tivotechies.com**

Appendix C: Tools of the Warranty Voiding Trade

- Bright overhead lighting or desk lamp
- Protective gear (mask, goggles, rubber gloves, smock, etc.)
- ESD protection (anti-static mat and wriststrap)
- Screwdrivers
- X-ACTO hobby knife
- Dremel tool
- Needle file set

Appendix C: Tools of the Warranty Voiding Trade 2

- Wire brushes
- Sandpaper
- Glue
- Tape
- Cleaning supplies
- Variable-speed cordless drill w/ drill bits
- Heat gun and heat-shrink tubing
- Center punch

Appendix C: Tools of the Warranty Voiding Trade 3

- Nibbling tool
- Jigsaw
- Wire stripper/clipper
- Needle-nose pliers
- Tweezers
- Soldering iron w/ accessories (solder sucker, various tips, etc.)
- Basic electronic components

Appendix C: Tools of the Warranty Voiding Trade 4

- Microscope
- Digital and analog multimeters
- Adjustable power supply
- Device programmer
- UV EPROM eraser
- PCB etching kit
- Oscilloscope
- Logic Analyzer

Appendix D: Where to Obtain the Tools

- The Home Depot (`www.homedepot.com`)
- Lowe's (`www.lowes.com`)
- Hobby Lobby (`www.hobbylobby.com`)
- McMaster-Carr (`www.mcmaster.com`)
- Radio Shack (`www.radioshack.com`)
- Digi-Key (`www.digikey.com`)
- Contact East (`www.contacteast.com`)
- Test Equity (`www.testequity.com`)

Thanks!

Joe Grand (Kingpin)

joe@grandideastudio.com