

Myths and Misconceptions about Hardware Hacking

Andrew "bunnie" Huang, PhD
bunnie@xenatera.com
Xenatera LLC

Analog Reconversion Discussion Group
May 28, 2003

Outline

- ◆ Hardware hacking myths (introduction)
- ◆ Why these myths are not true today
 - The "Technology Divide"
 - Moore's Law
- ◆ Today's hardware hacking technology
- ◆ The cost of overhauling an A/D converter
- ◆ The cost of building your own A/D converter

Hardware Hacking Myths

- ◆ Hardware development is beyond the reach of individual hobbyists
 - Requires corporate funding
 - Requires a team of engineers
- ◆ Mass-production of hardware hacks requires corporate funding
 - Requires massive capital infrastructure

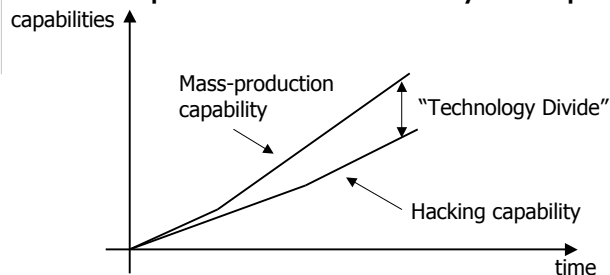
4/22/03

Copyright © 2003 Xenatera LLC

3

How Myths Come About

- ◆ The Technology Divide
 - Differential between mass production capabilities and hobbyist capabilities



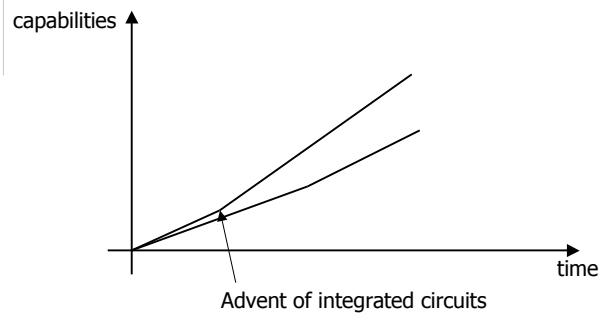
4/22/03

Copyright © 2003 Xenatera LLC

4

The Technology Divide

◆ The advent of integration set hacking technology back...



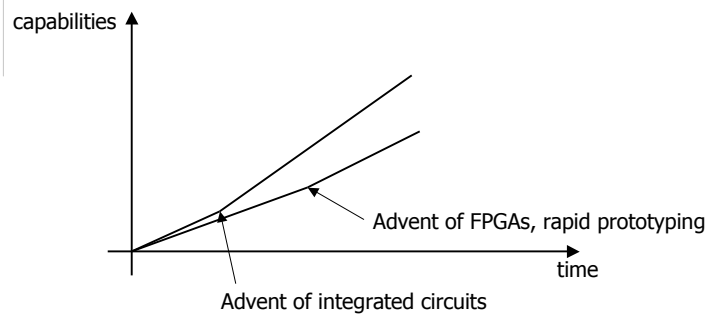
4/22/03

Copyright © 2003 Xenatera LLC

5

The Technology Divide

◆ But even corporations need economical solutions to their prototyping needs...



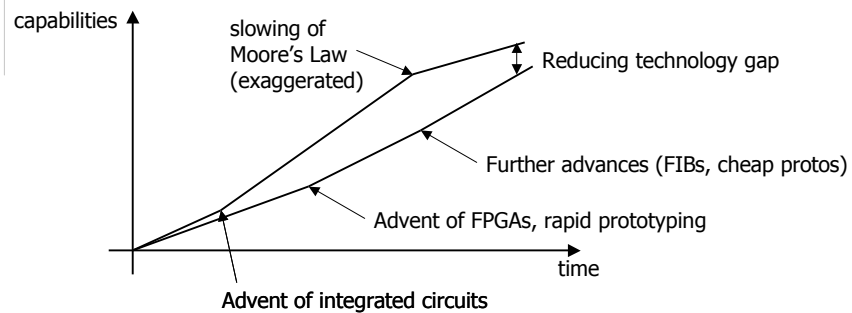
4/22/03

Copyright © 2003 Xenatera LLC

6

The Technology Divide

◆ ...and the economic slowdown has only increased that need



4/22/03

Copyright © 2003 Xenatera LLC

7

Today's Hacking Challenges

- ◆ High Integration Chips
- ◆ High Speed Boards
 - 200 MHz+ board interconnect
- ◆ High Density Packaging
 - 1000-pin BGA-style packages

4/22/03

Copyright © 2003 Xenatera LLC

8

The Renaissance of Hacking

- ◆ Economic downturn of early 2000 is a blessing to hardware hackers
 - Technology pace slows down
 - Price competition brings rapid proto prices into the sub-\$100 range
 - ◆ 4-layer boards for \$50
 - ◆ BGA attach and inspect for \$100
 - ◆ FPGAs for \$10
 - Excess inventory drives down prices
 - IC analysis services are slashing prices
 - ◆ Decap and photograph for \$100's

4/22/03

Copyright © 2003 Xenatera LLC

9

The Renaissance of Hacking

- ◆ No single trend solves the problems facing hackers
 - Synergy of multiple trends is re-enabling hardware hacking

4/22/03

Copyright © 2003 Xenatera LLC

10

Hardware Hacking Trends

- ◆ Cheap PCBs
- ◆ FPGAs
- ◆ Soldering Myths and Techniques
- ◆ Probing Boards
- ◆ IC Analysis Tools
- ◆ Backdoors and Manufacturability
- ◆ Turnkey mass-production
- ◆ Sideband signal attacks

4/22/03

Copyright © 2003 Xenatera LLC

11

Cheap Printed Circuit Boards

- ◆ Custom PCBs used to cost \$100's of dollars to fabricate
- ◆ Now:
 - "no-touch" services and internet ordering has created intense price competition
 - 2-layer board costs about \$20-30/ea
 - 4-layer board costs about \$50/ea
 - ◆ Note: min order quantity is usually 2

4/22/03

Copyright © 2003 Xenatera LLC

12

Cheap PCBs

- ◆ What does this mean for hackers?
 - Enables hackers to use latest fine-pitch SMD technology, including BGAs to some extent
 - Enables hackers to build custom test equipment
 - ◆ Orders of magnitude less cost than general purpose test benches

4/22/03

Copyright © 2003 Xenatera LLC

13

Hardware Hacking Trends

- ◆ Cheap PCBs
- ◆ FPGAs
- ◆ Soldering Myths and Techniques
- ◆ Probing Boards
- ◆ IC Analysis Tools
- ◆ Backdoors and Manufacturability
- ◆ Turnkey mass-production
- ◆ Sideband signal attacks

4/22/03

Copyright © 2003 Xenatera LLC

14

Moore's Law Steps In...

- ◆ Increasingly, FPGAs are test vehicles for cutting-edge fabs
 - Repeated structure excellent for process validation
 - FPGA can even be configured for self-testing!
- ◆ As a result
 - FPGA performance is gaining ground on ASICs
 - FPGA price/gate is dropping
- ◆ FPGA architecture has been improved
 - Excellent high performance I/O support
 - Increasing number of embedded "hard cores"
 - ◆ After all, a PowerPC core is now about the size of a couple bond pads

4/22/03

Copyright © 2003 Xenatera LLC

15

Implication for Hardware Hackers

- ◆ Hackers can build system-on-a-chip
 - One \$10 FPGA can hold a custom 32-bit microprocessor and peripherals
 - The "\$10 ASIC"
- ◆ Hackers can build high performance custom test equipment
 - High-end FPGAs have multi-hundred MHz system performance
 - Native support for most I/O standards
 - Remarkably, FPGAs of this sort cost around \$50

4/22/03

Copyright © 2003 Xenatera LLC

16

Hardware Hacking Trends

- ◆ Cheap PCBs
- ◆ FPGAs
- ◆ Soldering Myths and Techniques
- ◆ Probing boards
- ◆ IC Analysis Tools
- ◆ Backdoors and Manufacturability
- ◆ Turnkey mass-production
- ◆ Sideband signal attacks

4/22/03

Copyright © 2003 Xenatera LLC

17

Trends in Board Assembly

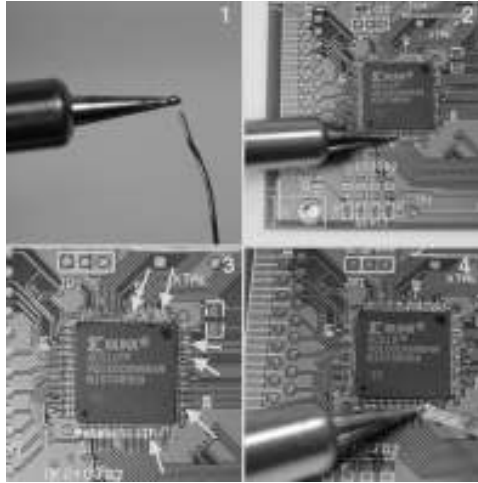
- ◆ Myth: SMD soldering is difficult
 - Fact: human hands have more resolution than the naked eye can resolve
 - A low-power microscope greatly aids soldering
- ◆ Myth: SMD soldering requires a fine-tipped soldering iron
 - Fact: solder does not like to stick to plastics
 - Fact: solder does like to stick to metal
 - Surface tension and bulk heat is all you need to solder fine-pitched visible pin components

4/22/03

Copyright © 2003 Xenatera LLC

18

SMD Soldering



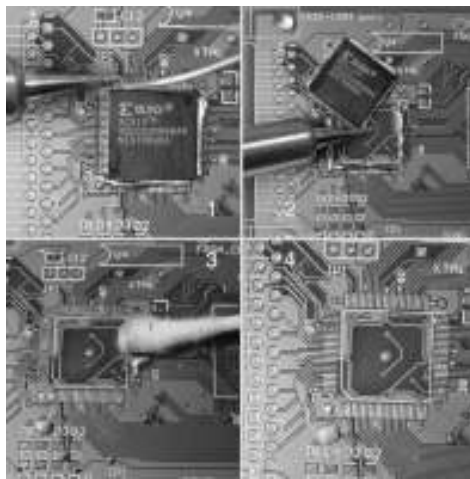
4/22/03

From "Hacking the Xbox" (www.hackingthexbox.com)

Copyright © 2003 Xenatera LLC

19

SMD Desoldering



4/22/03

From "Hacking the Xbox" (www.hackingthexbox.com)

Copyright © 2003 Xenatera LLC

20

Hardware Hacking Trends

- ◆ Cheap PCBs
- ◆ FPGAs
- ◆ Soldering Myths and Techniques
- ◆ Probing Boards
- ◆ IC Analysis Tools
- ◆ Backdoors and Manufacturability
- ◆ Turnkey mass-production
- ◆ Sideband signal attacks

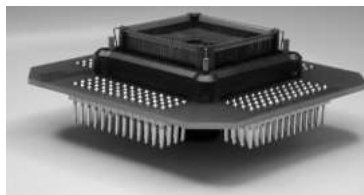
4/22/03

Copyright © 2003 Xenatera LLC

21

Probing Boards

- ◆ Problem: SMD leads are too small!
 - Solder on a probe wire using a microscope
 - Use a probe adapter (expensive)
(www.emulationtechnology.com)



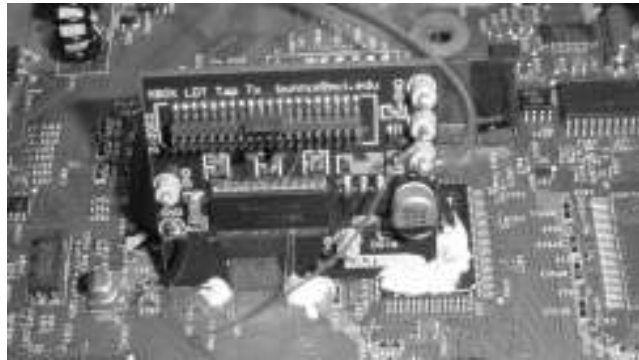
4/22/03

Copyright © 2003 Xenatera LLC

22

Build Your Own Probe

- ◆ A circuit board is cheaper than most custom probe assemblies



4/22/03

Copyright © 2003 Xenatera LLC

23

Hardware Hacking Trends

- ◆ Cheap PCBs
- ◆ FPGAs
- ◆ Soldering Myths and Techniques
- ◆ Probing Boards
- ◆ IC Analysis Tools
- ◆ Backdoors and Manufacturability
- ◆ Turnkey mass-production
- ◆ Sideband signal attacks

4/22/03

Copyright © 2003 Xenatera LLC

24

IC Analysis Trends

- ◆ ICs have long been the hardest thing for hardware hackers to crack
- ◆ ...but IC designers make mistakes
 - Need repair, inspection tools
 - How do *they* do this at sub-micron geometries?
 - ◆ Focused Ion Beams
 - ◆ Laser Ablation and Deposition
 - ◆ Voltage Contrast Microscopy

4/22/03

Copyright © 2003 Xenatera LLC

25

How Much Does IC Analysis Cost?

- ◆ A cut and jumper about \$1k-\$10k
 - Cost dependant upon complexity
 - Not within reach of the weekend hobbyist
 - Certainly in reach of corporations and motivated hackers
 - ◆ Helps assign a value to secrets protected by silicon structures
- ◆ Full analysis of a chip sector around \$10k-\$20k

4/22/03

Copyright © 2003 Xenatera LLC

26

Hardware Hacking Trends

- ◆ Cheap PCBs
- ◆ FPGAs
- ◆ Soldering Myths and Techniques
- ◆ Probing Boards
- ◆ IC Analysis Tools
- ◆ Backdoors and Manufacturability
- ◆ Turnkey mass-production
- ◆ Sideband signal attacks

4/22/03

Copyright © 2003 Xenatera LLC

27

Please, Come in my Back Door

- ◆ "Back doors" put in place by electronics manufacturers
 - Design-for-manufacturability
 - Design-for-test
- ◆ Hardware security and low manufacturing costs are at odds with each other
 - Ultimately, cost wins

4/22/03

Copyright © 2003 Xenatera LLC

28

Design-for-Manufacturability

- ◆ As a rule, manufacturers desire:
 - Full visibility into system state
 - Unhindered access to key signals
 - Visual inspectability
- ◆ This helps keep rework costs low, yield high, and failure analysis simple
 - It also helps hackers!

4/22/03

Copyright © 2003 Xenatera LLC

29

Design-for-Test

- ◆ Design in *test structures* that enable quick diagnostics
 - Proximity contact probe points on all key signals
 - JTAG boundary scan
 - Special test and debug ports

4/22/03

Copyright © 2003 Xenatera LLC

30

Hardware Hacking Trends

- ◆ Cheap PCBs
- ◆ FPGAs
- ◆ Soldering Myths and Techniques
- ◆ Probing Boards
- ◆ IC Analysis Tools
- ◆ Backdoors and Manufacturability
- ◆ Turnkey mass-production
- ◆ Sideband signal attacks

4/22/03

Copyright © 2003 Xenatera LLC

31

Mass-Producing Hardware

- ◆ Mass-producing a hardware hack
 - "Just add money" – not a lot of money either
 - ◆ Solder stencil costs ~\$400 each side of a board
 - ◆ Pick and place programming ~\$200
 - ◆ Machine time between \$0.25 - \$0.01 per component for low volumes, depending on vendor
 - Component and board costs scale well with volume
 - ◆ PCBs are <\$1/in² in moderate volumes
 - ◆ Volume discounts on chips can be fairly aggressive as well

4/22/03

Copyright © 2003 Xenatera LLC

32

Hardware Hacking Trends

- ◆ Cheap PCBs
- ◆ FPGAs
- ◆ Soldering Myths and Techniques
- ◆ Probing Boards
- ◆ IC Analysis Tools
- ◆ Backdoors and Manufacturability
- ◆ Turnkey mass-production
- ◆ Sideband signal attacks

4/22/03

Copyright © 2003 Xenatera LLC

33

A Note on Sideband Hardware Attacks

- ◆ Hardware leaks information
 - Emitted radiation from circuits, traces and wires
 - Power supply fluctuations
 - Emitted visible radiation from LEDs and CRTs
- ◆ Techniques exist to harvest this information
 - Collect many samples over time
 - Average them to build a stronger signal
 - Use a local copy of the hardware to develop a comparison reference
- ◆ Potentially low-cost way to extract secrets from chips

4/22/03

Copyright © 2003 Xenatera LLC

34

Potential Costs

◆ Power

- Ciphertext is a near-white noise signal, which is the most power-hungry signal in the digital domain
 - ◆ Negatively impacts portable applications

◆ Noise

- A/D converters are very sensitive to noise
- Encryption logic would be very noisy
- Increase design risk, costs (larger chips, more process steps needed for noise isolation)

4/22/03

Copyright © 2003 Xenatera LLC

35

Potential Costs

◆ Testability

- Production line chip testers cost \$10mm+
- Each extra second on a tester adds a quarter to the cost of a part, i.e., split the cost of \$10mm over a 5-year chip lifetime

4/22/03

Copyright © 2003 Xenatera LLC

36

Potential Costs

- ◆ Unique IDs (if used)
 - Requires a "burn" step in mfg.
 - Requires special mask steps for fuses, storage cells

4/22/03

Copyright © 2003 Xenatera LLC

37

The Cost of A/D Converters

- ◆ NTSC Video Bandwidth
 - ~ 5 MHz
 - ~ 14 MHz for HDTV-1160
- ◆ Video dynamic range
 - Professional-quality requires 10-12 bits
 - Acceptable quality as low as 5-6 bits/channel (about 30-35 dB)
- ◆ AD9283 from Analog Devices
 - ~\$5 in single quantities
 - 100 MSPS, 3.3V, 8-bit device

4/22/03

Copyright © 2003 Xenatera LLC

38

Build Your Own A/D?

- ◆ 6-bit, 10 MHz A/D converter—can a hobbyist at home build it using plans off the web?
 - YES!

4/22/03

Copyright © 2003 Xenatera LLC

39

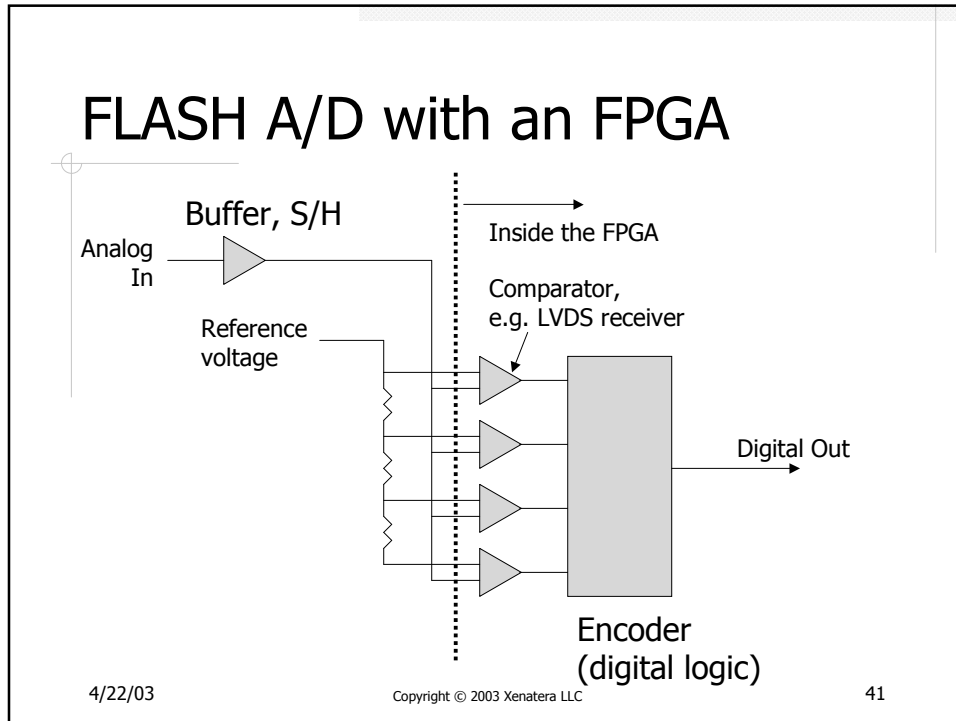
Proposal – FLASH A/D

- ◆ 6 bits = 64 levels
- ◆ Use 64 external resistors to set reference chain
- ◆ Use LVDS comparators inside the FPGA as the comparator bank
- ◆ Use FPGA logic to perform bit encodings
 - A/D converter has potentially many 10's of MHz conversion performance

4/22/03

Copyright © 2003 Xenatera LLC

40

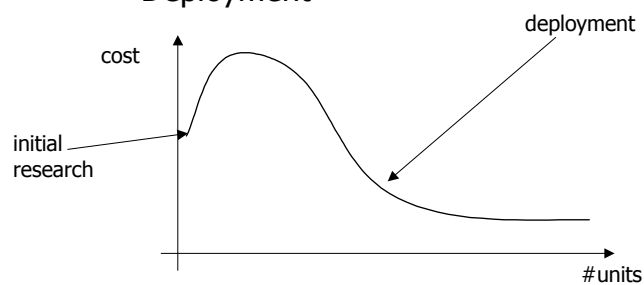


- ## Parts Cost of FLASH A/D
- ◆ Total Cost: \$25
 - 64 1% resistors: \$3
 - FPGA with LVDS inputs (Spartan II-e): \$20 in single quantities
 - Op-amp: \$2
 - ◆ Difficulty level: easy
 - All hand-solderable surface mount devices
 - FPGA bitfiles, verilog can be open-sourced and downloaded on-line
 - PCB could be downloaded as an electronic design file and fab'd for about \$40 to 60
- 4/22/03 Copyright © 2003 Xenatera LLC 42

Ramifications

◆ How secure is pure hardware security?

- Roughly two "phases" of costs
 - ◆ Initial research
 - ◆ Deployment



4/22/03

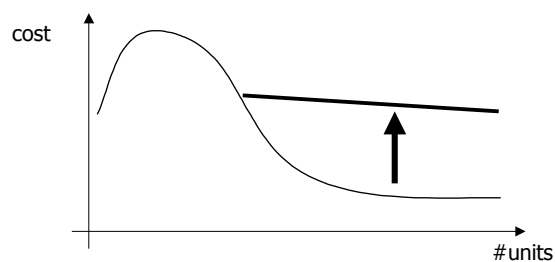
Copyright © 2003 Xenatera LLC

43

Ramifications

◆ Factors that affect shape of curve

- Robust hardware security complicates deployment
- Robust security is more **expensive!**



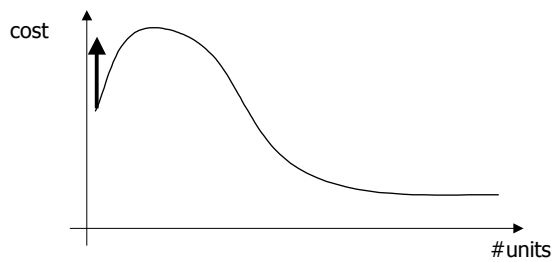
4/22/03

Copyright © 2003 Xenatera LLC

44

Ramifications

- ◆ Factors that affect shape of curve
 - Complicated hardware security complicates initial research
 - Less expensive, but once broken an entire population is insecure



4/22/03

Copyright © 2003 Xenatera LLC

45

Conclusion

- ◆ Hardware hacking technology is catching up with mainstream technology (again)

4/22/03

Copyright © 2003 Xenatera LLC

46

Conclusion

- ◆ Custom PCBs are getting cheap
- ◆ FPGAs are fine stand-ins for ASICs
- ◆ Board assembly and rework techniques accessible to weekend hobbyists
- ◆ Chip and PC board analysis becoming more economical with time
 - Hardware security is become less effective as the population starts to embrace new hacking technologies
- ◆ It is easy & cheap to build A/D converters out of standard parts

4/22/03

Copyright © 2003 Xenatera LLC

47

Thank you for your attention.

4/22/03

Copyright © 2003 Xenatera LLC

48

Cheap PCBs

◆ Where can I get them?

- www.sierraprotocircuits.com
- www.advancedcircuits.com
- www.datacircuitsystems.com
- www.apcircuits.com
- Typical line widths between 6 and 7 mil,
min holes around 12 mil
 - ◆ Much finer pitch available for only a little bit more

4/22/03

Copyright © 2003 Xenatera LLC

49

FPGAs

◆ FPGA = Field Programmable Gate Array

- Programmable logic and flip flops
embedded in a sea of programmable wires
- FPGAs in the early 90's were expensive
technology
 - ◆ \$100's for a few hundred gates!
 - ◆ Slow, low performance technology
 - ◆ Pathetic I/O performance
 - ◆ Extremely expensive design tools

4/22/03

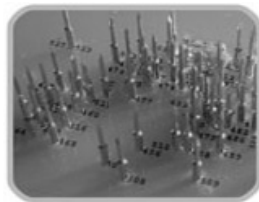
Copyright © 2003 Xenatera LLC

50

Probe Points

◆ "Bed of nails" testing

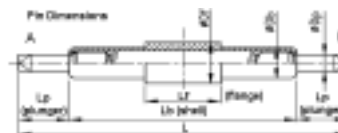
- Board has open contact points
- Spring-loaded pogo-pin structures are pressed into the board



<http://www.spea.net/pages/Eg/Easytesteng.html>

4/22/03

Spring-loaded pin example



<http://www.emulation.com/pogo/>

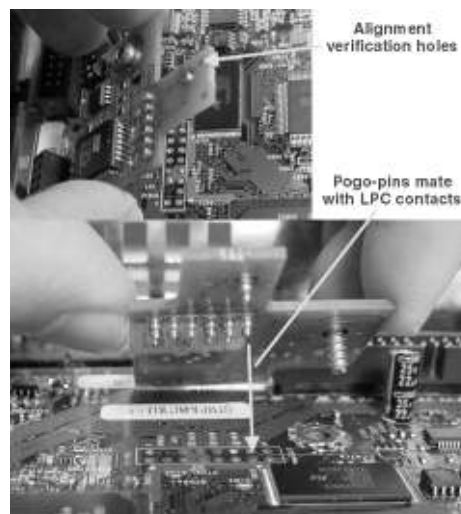
Copyright © 2003 Xenatera LLC

51

Probe Points

◆ Enables solderless mods for hackers

- Shown here: "the Matrix" modchip for the Xbox™



4/22/03

Copyright © 2003 Xenatera LLC

52

JTAG Boundary Scan

◆ Joint Test Action Group

- Serial "boundary scan chain"
 - ◆ Chip boundaries, i.e., I/O pads, contain a shift register controlled by a single serial bus
 - ◆ Shift in any desired pattern of bits on the I/O pads
 - ◆ Also, read out the state of I/O pads
 - ◆ Useful for testing both the inside and outside of a chip
- Open standard

4/22/03

Copyright © 2003 Xenatera LLC

53

Hacking with JTAG

◆ JTAG interface is fairly simple

- Many have built homebrew JTAG drivers
- Unfortunately, chips have implementation-specific opcodes and pin mappings
- Many manufacturers make this proprietary to discourage hacking with JTAG
 - ◆ Great if you can afford or borrow the turnkey JTAG tools (\$5k-\$50k)

◆ Board-level JTAG lockdown

- Manufacturers can disable JTAG mechanism by stripping out or modifying JTAG PCB resources

4/22/03

Copyright © 2003 Xenatera LLC

54

Special Test and Debug Ports

- ◆ Architecture-specific debug and test resources
 - PC: "LPC" ROM override
 - Diagnostic serial port
 - ◆ Frequently found on routers, networking equipment
 - Developer's back doors
 - ◆ Sega Dreamcast CD-ROM boot back door
 - ◆ Networking equipment, phone switches, servers have been found with developer's back doors

4/22/03

Copyright © 2003 Xenatera LLC

55

Ramifications

- ◆ Recall that many security systems are based on a secret
 - Gotta hide that secret somewhere
- ◆ "Pure hardware" attacks include
 - Secret recovery
 - Bypassing cryptographic checks involving the secret

4/22/03

Copyright © 2003 Xenatera LLC

56

Ramifications: Assigning Real Costs

◆ Initial research costs

- Assume an adversary with access to common lab equipment (o-scope, DLA)
- For PCB security \ll \$1000
 - ◆ Assuming system can be defeated with PCB-only modifications
 - ◆ Any system that transmits secrets between chips is vulnerable to PCB-based attacks
- For IC-based security \sim \$10k-\$100k
 - ◆ Assuming hardware-fuse or hardwired code/key style security
 - ◆ More if the IC incorporates true-tamper resistant features

4/22/03

Copyright © 2003 Xenatera LLC

57

Ramifications: Assigning Real Costs

◆ Some classes of IC attacks are very cheap to research and deploy

- "Photoflash" attacks
- Power modulation attacks
- Probe-point attacks

4/22/03

Copyright © 2003 Xenatera LLC

58

Ramifications

◆ Deployment Costs

- For PCB-based security, ~\$10 per unit
- For IC-based security, ~\$1k per unit
 - ◆ Assumes simple security, e.g. fuse based