Hardware Trojans

Infiltrating the Faraday Cage

Nick Waite, Researcher, CVORG, University of Delaware

Stephen Janansky, Researcher, CVORG, University of Delaware

Updated slides and papers

Please visit us at cvorg.ece.udel.edu for updated slides and papers that will be presented at the conference. As this topic is still under active research, these slides will most likely change.

Some Common Questions

- What is a hardware trojan?
- Why should I care about this?
- Doesn’t my anti-virus protect against this?
- Why bother with hardware when software is so easy?

Some Answers

- We define Hardware Trojans to be malicious alteration of hardware, that could, under specific conditions, result in functional changes to the system.
- Most products will go through multiple locations before it reaches the consumer (ie Design - US, HDL - Israel, Fab - China) and attacks can occur anywhere along this line
- Most security practices assume the hardware is secure or trusted
- Hardware can be easy to manipulate and disguise
- Active TEMPEST anyone?

Quick Scenario (or is it?)

- New “super secure” smart card comes out
- Banks adopt as main method of authentication, wide adoption takes place
  - DOD CAC, EZ-PASS, etc
- Device weak against 0-day attack
  - accidental? intentionally inserted? how did it get there?
- Banks confronted by bad guys
  - Admit flaw in chip - people lose faith in system, banks lose money
  - Deny flaw in chip – hope no one else finds out, banks lose money
  - Pay blackmail – fund/encourage further attacks, no guarantee of good faith

Hardware Trojans

- DC16 Demonstration of Hardware Trojans (Kiamilev/Hoover)
- Optical Trojan - Blink LED faster than human eye can see, optical to audio reads out key, data, password, etc
- Thermal Trojan - Heat up and cool component by running electricity to it, creating changing IR signature
- RF Trojan - Run current through a wire or pin creating EM waves that can be picked up by off the shelf radio

Our Power Trojans

- Use the power lines to leak data
- Similar to Barisani/Bianco's research but still unique
- Offers bidirectional communication
- Does anyone monitor power lines?
- Other examples of the concept: X10, PowerLine Ethernet, Broadband over Power, etc

Crash course in Electricity

- Voltage = Current * Resistance (Ohm's Law, V=IR)
- Power = Current * Voltage (Power Law, P=IV)
- AC is alternating current (60Hz US, 50Hz Europe)
- DC is direct current (think batteries)
- Power line uses AC, Power supply converts AC to DC

Getting Data Out - Part 1

- Consuming power means more power draw on AC line
- Increasing load on CPU increases power usage
- Modulate load on AC line by modulating CPU usage
- Measure power line and read in signal
- Data successfully exfiltrated

Getting Data In - Part 1

- PSU provides DC at: +12V,+5V,+3.3V,-12V,-5V
- Conversion: 120VAC=>12VDC=>5VDC=>3.3VDC
- 12V rail poorly regulated, used for motors on drives
- 5V and 3.3V rails highly regulated
- 12V rail effected by variations in 120VAC
- Modulate with VARIAC, read out 12V using motherboard sensors

Faraday's Cage - the horror!

- A Faraday Cage blocks out all external static electric fields
- Keeps out signals (ex: Wifi, Cellphones, Radio, GPS, etc)
- Used in Sensitive Compartmented Information Facility to make "TEMPEST" proof
- Forgot one thing...everything needs power
- Can't run off batteries forever ;)

Demo

Visit http://www.cvorg.ece.udel.edu for video demos created that will be conducted live during the talk. We will also post the demos we conduct during out talk.

Amplified Active TEMPESTs

- Coin new phrases: passive and active TEMPEST to describe their creation
- Passive TEMPEST: Traditional TEMPEST attack, accidental side effects of technology
- Active TEMPEST: Actively created through the modification of hardware to create TEMPEST conditions
- Think about all the TEMPEST attacks amplified...

Can we amplify ours?

Why yes, we can! How?

With a little help from a few discreet electronic bits

Getting Data Out - Part 2

- Modify Power Supply
- Attach microcontroller to the AC line
- Connect microcontroller to system

- Use 60Hz signal as carrier and do crazy modulation
- Make it appear as noise, truly disguising itself
- Pass data from PSU to CPU disguised as fan speed sensor or by modulating internal power rails

Getting Data In - Part 2

- Use same setup as described previously
- Add small circuit to demodulate signal (more capacitors and resistors? oh no! They might just fit in with the rest)
- Fan speed sensor right? Should connect back and report data somehow
- Connect microcontroller to the PSU's fan connector
- Data leaks in using sensors again by reporting varying RPMs to motherboard sensor

Demo

Visit http://www.cvorg.ece.udel.edu for video demos created that will be conducted live during the talk. We will also post the demos we conduct during out talk.

Do you get the not so hidden message?

- pay attention! don’t make us bring out tHe bIg guns!
- people should take a Look aT hardware, it’s not that scary
- trusted coMputIng, needs a serious looK
- IEt’s not live through a battleSTAr galactica scenario...
- More effort could help defeAT software attacks
- you can TRUST us, we’re professionals (just ask DOD)
- I just spot a fed! now can you? :)