
PHYSICAL SECURITY FOR COMPUTING SYSTEMS, A LOOK AT DESIGN, ATTACKS AND DEFENSES

Steve Weingart



Outline

- **What is Physical Security**
- **What is a Secure Processor**
- **Relevant Standards**
- **Physical Security Descriptions and Methods**
- **Attacks**
- **Physical Security Design Examples and Hacks**
- **Demo**
- **Q & A**

What is Physical Security? (for computing systems)

Physical security is a barrier placed around a computing system to deter unauthorized physical access to the computing system itself.

This concept is complementary to logical security, the mechanisms by which operating systems and other software prevent unauthorized access to data.

Both physical and logical security are complementary to environmental security.

Definition (Kinds Of Physical Security)

Physical Security should resist access (tamper resistant), detect tampering attempts and respond (tamper responding), and/or provide evidence of attempted tampering at a later audit (tamper evident).

A combination of tamper evidence, resistance and response or can be used to create sufficiently strong level of protection to thwart many attacks.

SECURE PROCESSORS

aruba
a Hewlett Packard
Enterprise company

What is A Secure Processor?

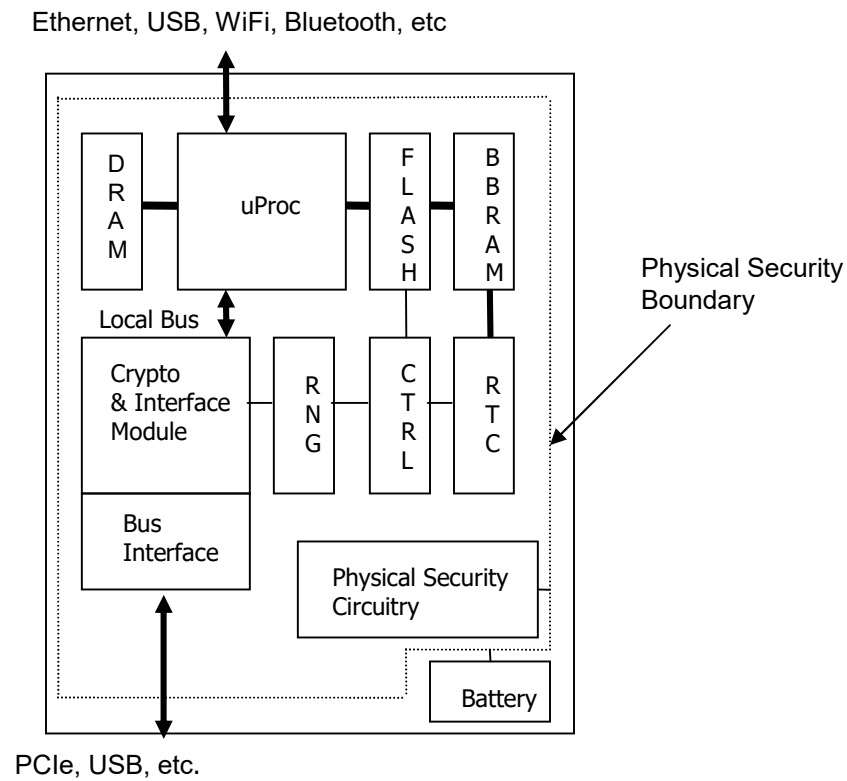
A computing device, maybe general purpose, maybe fixed or special function; generally housed in a package that is physically secure. They are used for performing high integrity operations (controlling your house, car, or bank account) and/or computations using secrets (such as cryptography or proprietary algorithms).

These used to be uncommon, generally these devices were designed and tested as a cryptographic modules under the FIPS 140 Standard from NIST. But with all of the new payment methods, IoT and home/car automation, they are everywhere now.

What Are Secure Processors Used For?

- IP protection - DRM
- Credit card personalization
- Certification authorities
- Electronic currency dispensers
- Electronic payments
- Electronic benefits transfer - SS
- Electronic securities trading
- Banking transactions
- Home banking
- Personal Firewall
- Master key protection
- e-postage meters
- Secret/proprietary algorithms
- Secure timestamps
- Software usage metering
- VPN
- Hotel room gaming
- Secure Database Access Control
- Pay TV
- Electronic Voting
- Automotive Controllers
- Home Automation
- Home Monitoring/Alarms
- Process Control (SCADA)
- Door Locks

A Typical Secure Processor



Secure Processor: Typical Features

- Standard Programming Environment inside, Bus and/or Network Attachment to the Outside
- Secure
 - Tamper Evident
 - Tamper Resistant
 - Tamper Detecting
 - Tamper Responding
- Crypto Support
 - Algorithms (RSA, EC, AES, RC4, ECDSA, etc)
 - Protocols (TLS, SSL, PKCS, etc)
 - HW Random Number Generator, RTC, etc.
- Special Functions
 - Data visualization or manipulation, Hardware Interface

Secure Processors

They Are Supposed To.....

Create a 'Trusted Agent' in the Hostile Field

- The 'Real Thing' Doing the 'Right Thing'

Create a Platform to Build High Security Applications.

- Programmable, to Support Arbitrary Applications that Need Crypto, Privacy and/or Integrity

Obviously There Have Been Some problems.....

...Welcome to Def Con!

STANDARDS

aruba
a Hewlett Packard
Enterprise company

Standards

FIPS 140-2

- Required For All Crypto Used By The US Government
- Complimentary To Common Criteria (May Need Both)
- Accepted/Endorsed By Several Industries (Digital Cinema Initiative, Banking In General)

FIPS 201/GSA PIV

- From Above, All Require FIPS 140-2 For Cards/Apps That Do Crypto

Common Criteria

- Not Specifically Part Of The Standard, But Some Protection Profiles, Notably, Smartcards And Financial Have Very Specific Requirements

PCI (Payment Card Industry)/EMV (Europay, Mastercard And Visa)

- Requirements For POS, HSM And Cards In Place

PHYSICAL SECURITY

aruba
a Hewlett Packard
Enterprise company

Physical Security

So, What it is it?

Let's Start With The Most Common Items and Requirements.....

- **Tamper Evidence**
 - Attempts at tampering leave evidence and can be detected by audit
- **Tamper Resistance**
 - It will be very likely to damage the device opening it.

Physical Security

- **Tamper Detection**
 - Detects entry into the secure zone
- **Tamper Response**
 - Must Reliably clear all sensitive data when an attack or dangerous condition is detected

Physical Security

- **Environmental Failure Protection/Testing**
 - Power
 - All Supplies (High & Low)
 - Battery too
 - Temperature (High & Low)
 - Radiation (optional)
- EFP/T Is Generally Used at the Highest Levels

NOW FOR SOME DETAILS

aruba
a Hewlett Packard
Enterprise company

Tamper Evidence

This is almost always a basic requirement at all levels of security

- **Any attempt to penetrate the package must leave evidence that can be audited.**
- **There are many ways to achieve tamper evidence**
 - The classic are seals/stickers, they were not very successful anymore due to new solvents.
 - But new techniques are making them useful again
 - Try clear substrates and colored adhesives
 - Paints and smooth shiny surfaces tend to work well.
 - Also, optical techniques, like crazing (fingerprinting), work very well, but need the reference to be stored.
 - Most wire seals are useless

Tamper Resistance

- **This Is The Bank Vault Approach**
- **The Goal Is To Prevent Access, Or Make It So Difficult The Module Will Be Damaged In The Attempt**
- **There Are Two Major Types Of Tamper Resistant Packaging**
 - Potted Or Filled
 - Strong Enclosure

Tamper Detection

Tamper detection must detect unauthorized entrance

- At the simplest, it is just a cover switch
- At higher levels the undetected hole size should get smaller
- At the highest levels, holes as small as 50 μm should be detected

Tamper Response

Need To Erase Secret Data When Tamper Is Detected

- It Has To Be Reliable And Fast

The Most Effective Methods Are Not Obvious

- And They Are Not Permanent Or Violent (I Know, Awwwww)

The Design Has To Make Sure That Erasure Is Possible

- Several Things Can Prevent Erasure
 - The Circuit May Not Be Fast Enough If The Processor Has To Wake Up
 - Backpowering (Powering The Chip Through Other Pins Than The Power Pins)
 - Imprinting (Making a RAM a ROM)

ATTACKS

aruba
a Hewlett Packard
Enterprise company

Attacks

- **Low Tech Attacks**
 - Mechanical
- **Disruptive and Energy Attacks**
 - Simple, Like Heat and Cold
 - Slightly more complicated
- **High Tech Attacks**

Examples – Mechanical Attacks

- **Machining: Drilling, Milling, Cutting; Using Conventional Manual, Mechanical, Or Exotic Methods (Water, Sandblasting, Laser, Chemical, Shaped Charge)**
- **Manual Methods Are Surprisingly Effective!**
 - But It Does Take Some Skill & Practice
- **Simple Versions Of Exotic Methods Can Be Even More Effective**
 - 'Water Torture' Version Of Water Machining Is Very Effective
 - Conventional Sandblasting Techniques Can Remove Microns Of Material At A Time
 - Drano Can Be Used On Epoxies
 - Orange Oil Based Solvents (Goo Gone) Can Remove Almost Any Label
- **Visualization**
 - Fiber Optic Cameras Are Now So Inexpensive And Available, They Can Be Used To Guide The Attack Inside An Area Where They Attacker Can't Normally See To Enable Attacks

Basic Tools



Examples – Energy (simple)

- **Temperature based disruption**
 - Often the simplest attack (hairdryer or freeze spray)
- **Direct connection disruption**
 - Voltage (High or Low voltage)
 - Can be used in conjunction with temperature
- **Clock Glitching**
 - Very effective
 - For best results use with a trigger
 - Variation: 'Four corners' attacks

Examples – Energy (high tech)

Imaging

- Penetrating energy (X-Ray, Ultrasound, etc) can be used to visualize internals and support an attack

Radiation

- Memory Imprinting (temperature, voltage spiking)
 - Princeton paper, this is well known and it works
- Circuit Disruption (full Electromagnetic spectrum)
 - Even a microwave oven can be used, but results can be unpredictable
- Electron or Ion beam (directly on active surface)
- Infra Red (on surface or through bulk silicon, laser or focused beam)
 - Lots of options, not a lot of work here, and it is very powerful
- Laser (various frequencies) can disrupt or ‘modify’ data or circuit
 - Same as IR above, very powerful
 - Biology lab tools (lasers) can be used for drilling, etc.

Passive Attacks, Sensed Energy (very high tech)

Power Analysis (SPA & DPA, lcc based)

- Supply current is sensed and analyzed to extract information
- This has become a well known technique, commercial systems are common.

Electromagnetic Analysis

- EM emanations are detected and analyzed to extract information (like SPA/DPA just using EM emanations).
- Tends to be more resistant to SW obfuscation mechanisms
- Some commercial systems are available

TEMPEST

- The wider variety of EM based passive attacks including EMA (above), plus screen grabbing, communications detection, etc). This was ALL classified, but now some details are available (<http://www.jammed.com/~jwa/tempest.html>)

EXAMPLE DESIGN AND HACKS

Example: Designs and Hacks

**This Is A High Security Design, But It Illustrates Many
Tamper Detection And Response Techniques**

- **Tamper Evidence**
- **Tamper Detection**
- **Tamper Response**
- **Environmental Failure Protection**
- **Operating Envelope**

Tamper Evidence

- The classic is the tamper evidence label (TEL)
 - They typically show 'VOID' when peeled to allow an audit of a tamper event.
 - To have the highest likelihood of success, test labels with the material they are going to be used on, prep the surface and let them cure for at least 24 hours before deployment
- Use multi-color adhesives if possible to ensure the label is ruined if solvents are used
- Smooth, shiny surfaces like epoxy, high gloss paint and polished metal also are very good tamper evident surfaces.
- The high tech approach is to use a unique surface coverage and store a picture of the 'fingerprint.' These techniques use crazed or surface shattered materials to produce unique surfaces.

Tamper Evidence

- Removing Tamper Evidence Labels Without Leaving Evidence
 - Use An Orange Oil Based Solvent (Goo Gone, Goof Off), And Razor Blades, Syringes, Q-tips, A Little Heat And Smooth Jawed Tweezers To Remove Without Damage (Go To The Tamper Evidence Village!)
- Smooth, Shiny Surfaces Like Epoxy, High Gloss Paint And Polished Metal Can be repaired and Repainted/Epoxied/Polished/Etc, take Photos for matching (at oblique angles to see ripples and shine).
- Crazed Or Surface Shattered Materials Are Virtually Impossible to Reproduce (like Fingerprints), try Substituting the Reference.

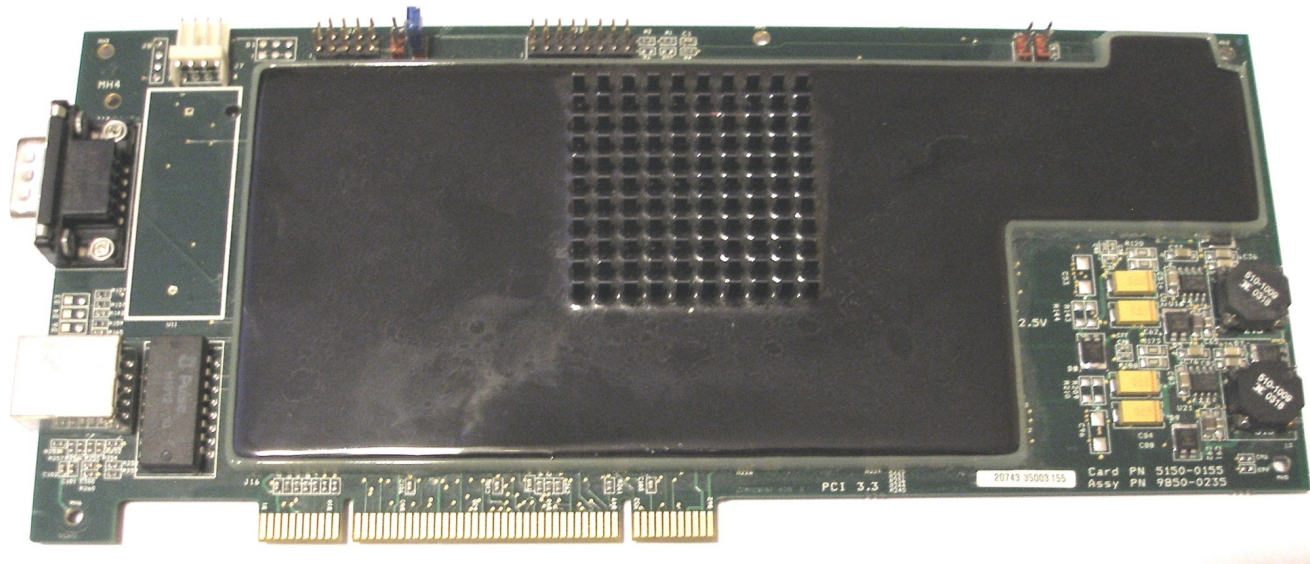
Tamper Resistance – Potted or Filled

- This is the best approach for small packages such as USB tokens or modules on cards that do not require maintenance or cooling (but there are ways to manage cooling)
- It is relatively easy to fill a package so that it is difficult or impossible to open the package without damage, at a low to medium tech level.
- Fillers may be added to make mechanical opening more difficult (both for strength and abrasion)
- The devices on the card, may need to be protected mechanically by preventing the potting from getting underneath them.

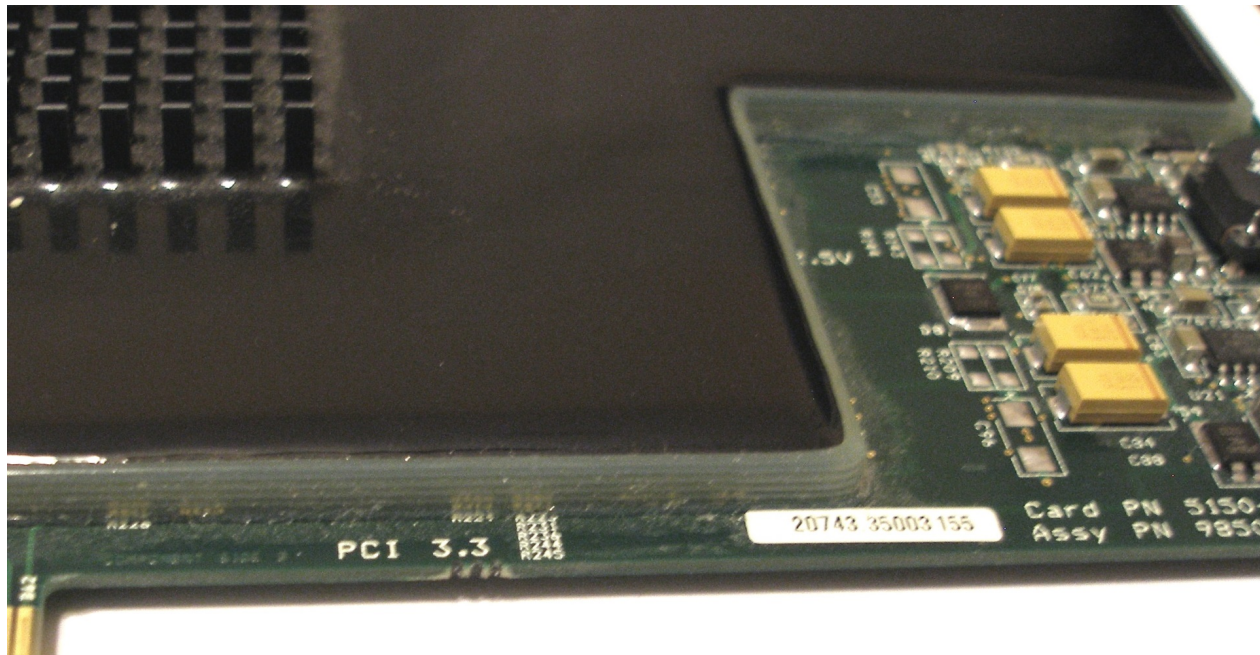
Tamper Resistance – Potted or Filled

- The potting may be poured directly into the outer case, an RF shield 'can' or a wall may be placed around a portion of a card and the area inside the wall can be filled.
- A potted package can be augmented by adding tamper detecting elements within the potting. The simplest is to loosely wrap the card in a tamper sensing wire before potting so that the wire floats freely within the potting material. The randomness of the wire placement improves security.

Tamper Resistance – Potted or Filled



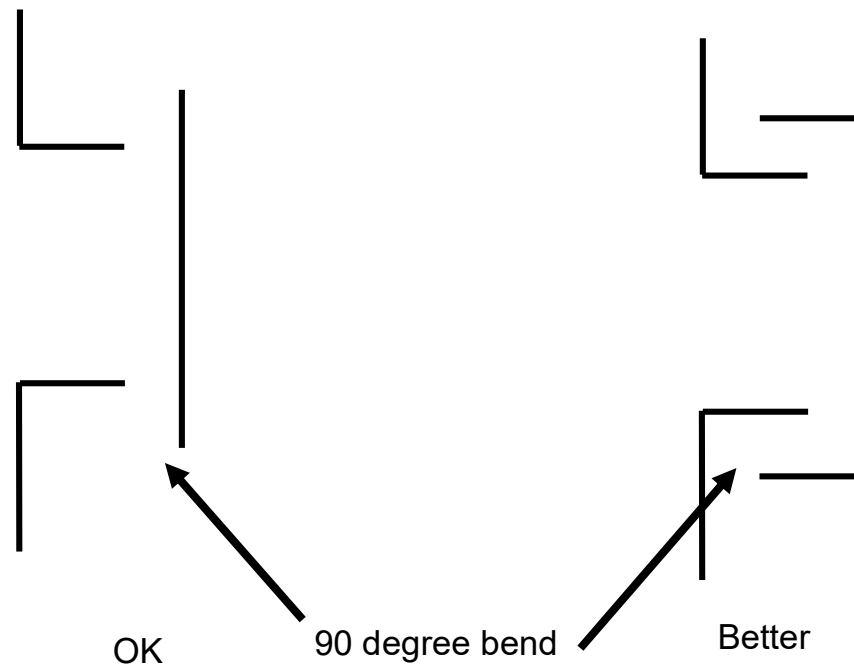
Tamper Resistance – Potted or Filled



Tamper Resistance – Strong Enclosure

- This type of enclosure may be an improved computer case, or a custom case. It may be metal or plastic, or any other material that meets the rest of the requirements
- This type is most appropriate for larger and higher power systems.
- At Moderate Levels, air vented cooling is relatively easy (must have at least one 90 degree bend in the path)
- The case may be openable (but opening must be detected. Cover open detection switches and such are important, it must not be easy to trick them – More on this in Tamper Detection)

Tamper Resistance – Strong Enclosure Ventilation



Tamper Detection

There are many different methods and technologies available

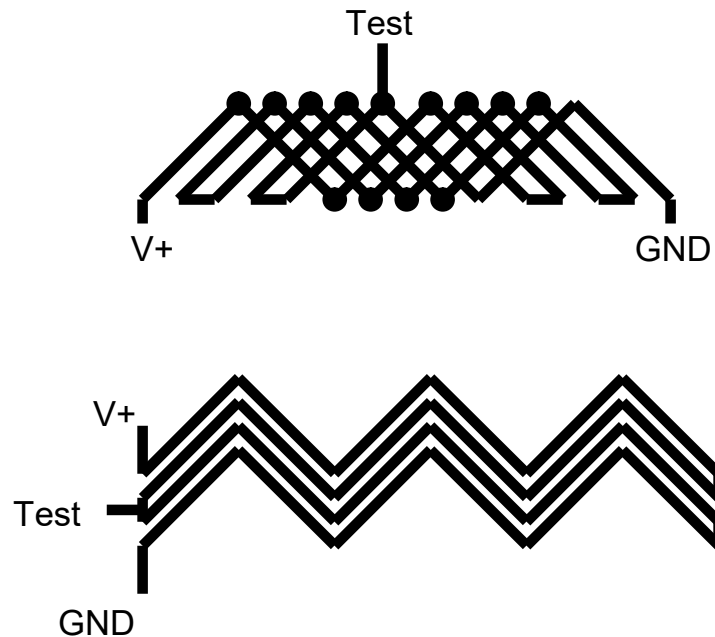
- At the basic level a simple door switches and sometimes wire loops are common
- At moderate levels the same techniques are used with additional protection.
 - Cover switches are guarded against tampering
 - Vents are blocked
 - Area penetration sensors are used (maybe even on the entire case), along with light and vibration.
- At the highest level, there is no limit on the attack, all known attacks must be defended against.
 - The most common design is to use a detector that is wrapped around and glued to the package.
 - It is activated in the factory and stays active for the product life

Tamper Detection

- **Should Detect Very Small Holes (50 μ M Lower Size Target)**
- Detector Is A Grid Of Printed Conductors On A Flexible Substrate
 - We Can Use Multiple Layers
 - One Pattern On Each Side Of Each Layer
 - This Can Also Be Done With A One Sided Grid, But The Outside Must Be Difficult To Access Without Damaging It.
- The Detector Is Wrapped Around And Glued To The Package
- Winding The Package In Wire, Like A Cocoon Can Work Too
- It Is Activated In The Factory And Stays Active For The Product Life
- Very Few To No False Positives Or Negatives.

Tamper Detection (example design)

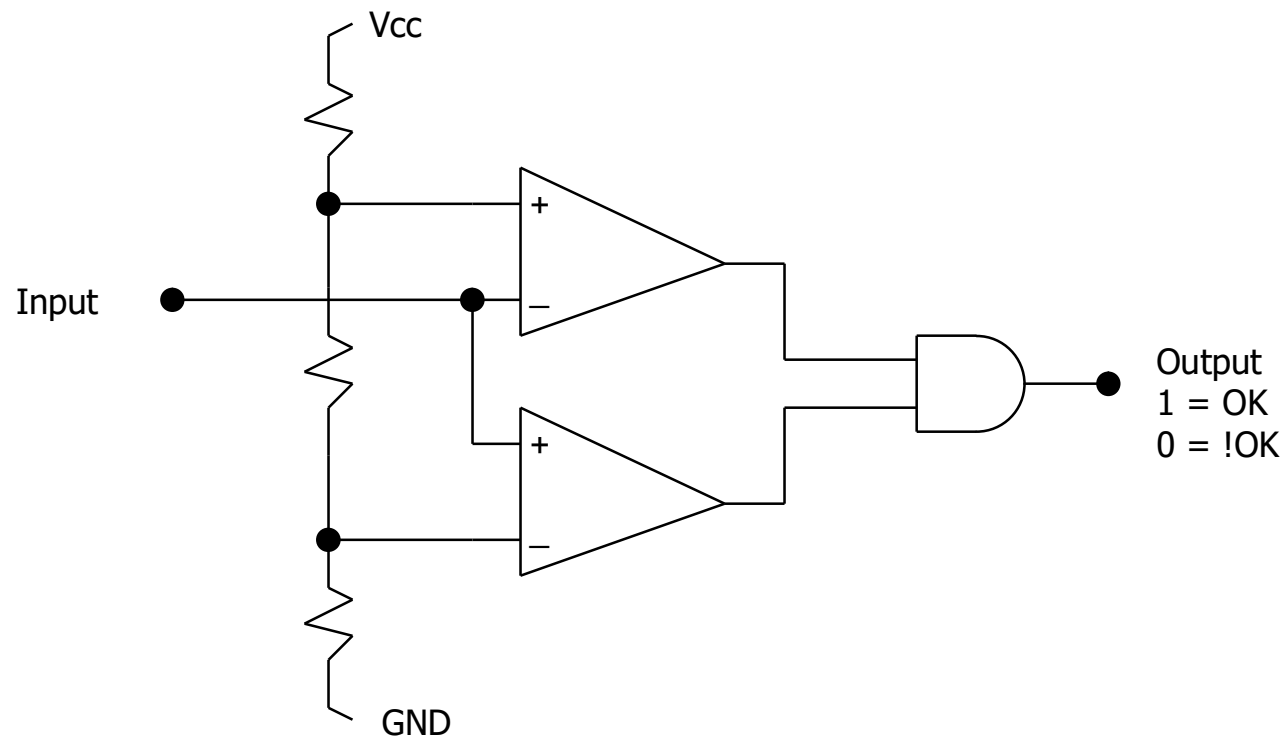
- ✓ Lines on Top
- ✓ Lines on Bottom
- This line requires ink 'vias' and covers both sides



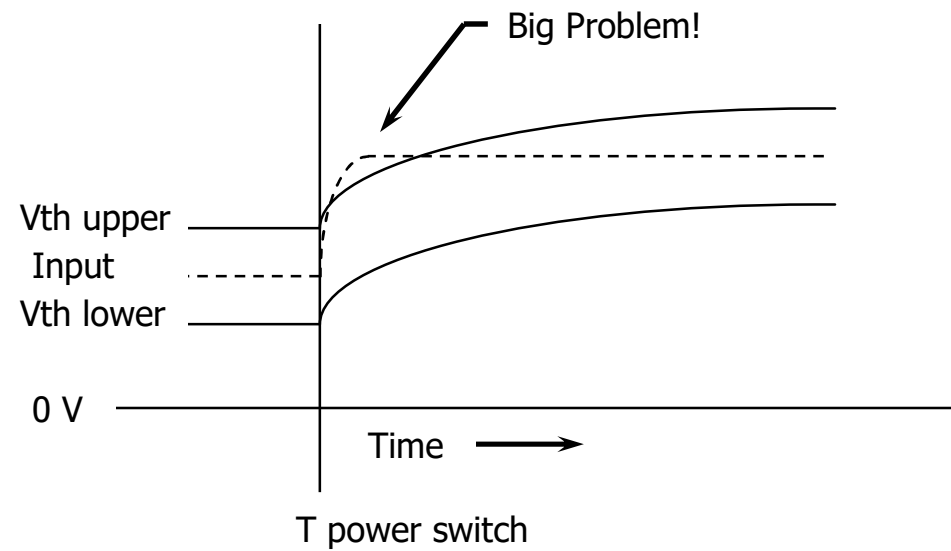
Same pattern printed on top and bottom
This is a single sided pattern

- Lots of materials to try:
 - Conductive Ink
 - Flex Printed Circuit
 - Indium Tin Oxide
- Connectors can be
 - Glued
 - Clamped
 - Applied Metal and Plastic

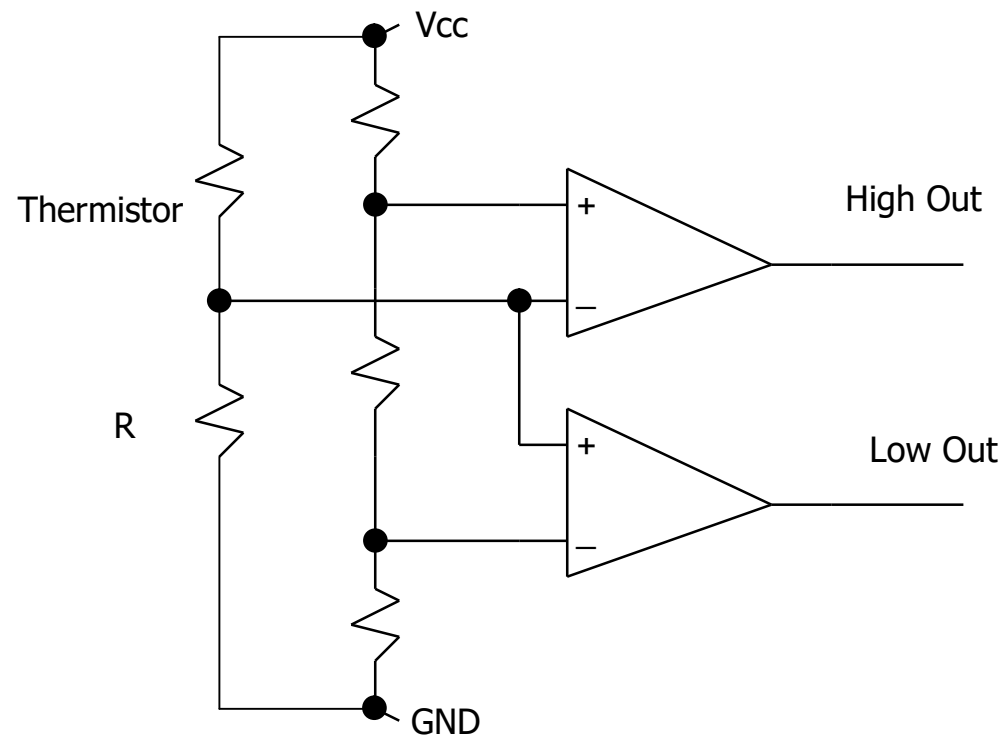
Basic Detection Circuit (Window Comparator)



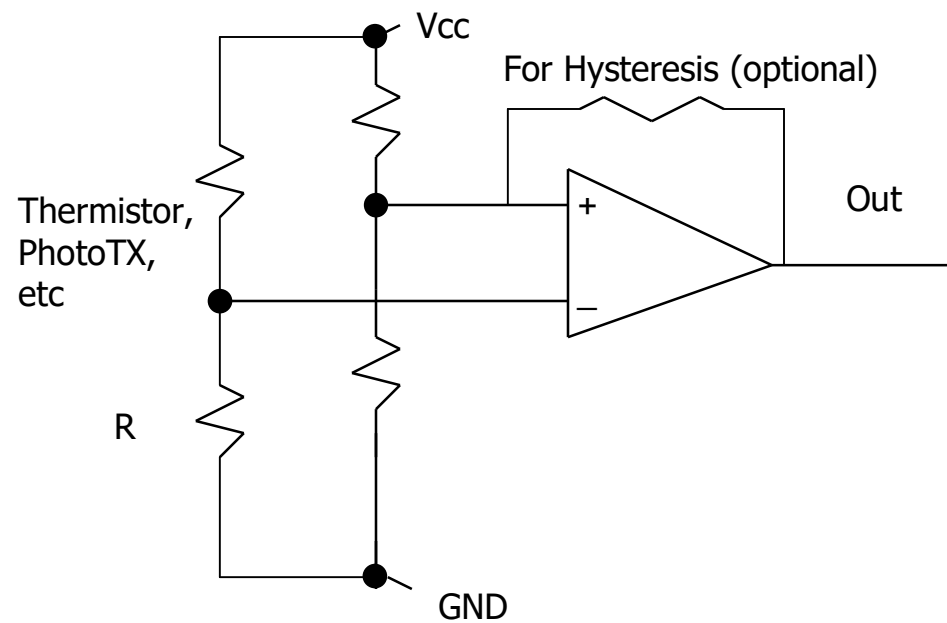
The Power Transient Problem



Basic Detection Circuit (temp)



Basic Detection Circuit (temp, radiation, etc)



Tamper Detection Notes

- **To save power use micro-power comparators with open drain**
- **Wire OR all the sensors together to one pull-up**
- **A low on the node is TAMPER**
- **It is possible to have a complete tamper detection and response system running on ~ 25 uA at 3V making a multi-year life on an AA Li battery easy**

Tamper Detection Notes

- **For best reliability, latch the TAMPER signal**
- **Use an RC (or some time delay on power up) on CLR to make sure it comes up in not tampered state**
- **Make sure TAMPER activates RESET to ensure all lines from the processor(s) are TRI-STATE or Hi-Z**
- **Arrange wires or mesh to minimize EMI effects (try to achieve a bifilar geometry)**

Tamper Detection

- A Well Designed Tamper Detection System Is The Hardest Thing To Crack
 - You Must Work Slowly And Carefully To Reach The Sensor Without Tripping It
 - For Cover Switch Type Sensors, Consider Piping Super Glue Through A Small Tube. Pry Up An Edge Of The Case (Be Careful Not To Lift The Switch), Or Drill A Small Hole (If No Area Sensor) And Glue The Switch Then Open The Case
 - A Thin Flat Piece Of Metal Or Plastic (Is Conductivity An Advantage Or Drawback?) Can Also Be Used To Hold The Switch As The Case Is Opened.
 - Plastic Gun Cleaning Tools Or Model Airplane Props Are Good Non-conductive Tools
 - For Area Sensors, You Need To Understand The Circuit. You May Be Able To Intentionally Short Or Open Some Lines To Allow Removal Of An Area. The Hard Approach Is To 'Jump Out' Enough Segments To Allow Penetration. Use Conductive Epoxy Or Ink To Make Bypass Connections Then Remove Lines.

Tamper Detection

- To Get Down To The Sensor's Active Elements (Assuming Potting)
 - You Must Work Slowly And Carefully To Reach The Sensor Without Tripping It (Yeah This Is A Repeat, I'm Serious, One F*^% Up And You're Done...)
 - You Can Use Gross Methods To Get Close...
 - Mechanical Machining
 - Chemical 'Machining' (Solvents, Water Machining, Sandblasting)
 - Then Use Fine Methods To Get The Last Distance
 - 'Lean' Sandblasting
 - 'Light' Chemical Machining
 - Manual Material Removal (Surprisingly Effective)
- For Area Sensors, You Need To Understand The Circuit. You May Be Able To Intentionally Short Or Open Some Lines To Allow Removal Of An Area. The Hard Approach Is To 'Jump Out' Enough Segments To Allow Penetration. Use Conductive Epoxy Or Ink To Make Bypass Connections Then Remove Lines.

Tamper Response

Need to Erase Secret Data When a Tamper Is Detected

- Permanent or Violent Actions are Not Allowed
- But it Still Has to be reliable and fast

Removing Power and Shorting the Power Pin Works Well

- Reasonably Fast
- Reasonably Sure
- Not Permanent or Violent

Overwriting the secrets is often not a good idea

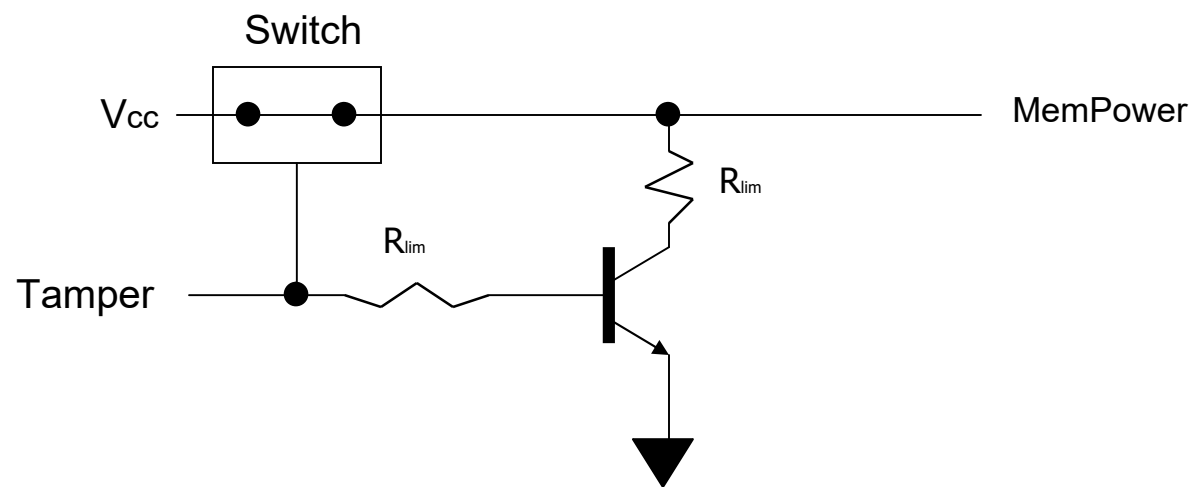
- No Guarantee that there is enough power available
- Maybe not be fast enough if the processor has to wake up
- However, some new security processors have this feature built in

Tamper Response

Tamper Response Works.... Provided.....

- There are No Imprinting Conditions
 - The Temperature has to be High Enough
 - The Unit has Not Been Irradiated
 - The Power Supply has Been Smooth
 - The Memory has Not Been Constant for Too Long
- No Back Powering !!!!!

Typical Zeroization Circuit (Crowbar)



Back Powering

- Back Powering is when a device is powered by energy from data or control lines with the power removed.
- A single control line pulled up on a low power SRAM can prevent power-down erasure (like the WR\ line)
- It is essential to make sure everything goes tri-state or off (including pull-ups) when the Tamper Response is triggered. Usually holding reset Tri-States most lines.

Imprinting

Imprinting is the process that can make a RAM a ROM.

- **It can be temporary**
 - Low Temperature (may start as high as -15 C)
 - Leaving contents unchanged for too long
- **It can be permanent**
 - Irradiation (low X-Ray band is often the most effective, in the 30 KeV range).
 - Other energy (power glitching, etc.)

Tamper Response

- The hard part about defeating a Tamper Response circuit is getting past the tamper detection Sensor first.
- So, if you can prevent the tamper response from being effective, then you don't have to worry about being detected
 - If any pins are exposed that can be used for back powering (JTAG?) that helps
 - If you can cause imprinting (cold?) you are also ahead of the game
 - Can you find a fault in the design that
- Needless to say, the more you know about the circuit and the components, the better
- If you can't manage a slow, deliberate attack, there are 'fast attacks.'
 - These are all pretty crazy, trying to beat the circuit with speed
 - Proposed methods include tiny shaped charges and even a bullet to cut a critical line inside the secure area to prevent the erasure

Environmental Failure Protection

- These are Really Assurance Issues
- The goal is to keep the module in its correct and safe operating range at all times
- Prevent Clock Glitching With PLLs, Protect I/O Lines With Diodes Up and Down To VCC and GND
- If the module is outside of its operating range, but in a safe zone, keep it in reset
- If the module is outside of its operating range and in a potentially unsafe zone, then all secrets must be permanently erased as quickly as possible

Environmental Failure Protection

Uses Basic Detection Circuit to Measure Parameters

- Non-damaging Conditions: Cause Reset
 - Low Voltage
 - High Temperature (Above Operating, Below Storage Limit)
- Damaging and/or Security Risk Conditions: Cause Erasure
 - High Voltage (Above Storage)
 - High Temperature
 - Low Temperature
 - High Battery Voltage
 - Ionizing Radiation (optional)

Environment Failure Protection

- This is the one that is supposed to beat you!
- If properly designed the EFP circuitry prevents any glitching, power supply attacks or any transient attacks
- To beat it try to find the places that it might miss
 - Power up or down crossover
 - Temperature crossover points (operation to storage, etc)
 - Clock or communication timing.

The Operating Envelope Concept

Manufacturers define the operating range of the components that they make, but often the specification is incomplete. It can be incomplete because no one ever intended the part to be used in some particular way, and the manufacturer, justifiably, doesn't want to deal with the problem. In general, designers can design circuits that stay within prescribed limits and the circuit functions properly.

For example, if the circuit is run at too high a temperature while at too low a supply voltage, the condition is undefined. This may open the system to attack.

This is essentially a more encompassing view of environmental failure protection.

Interactive Considerations

Must do All of the Above on Power Supply or Battery (& During Transition)

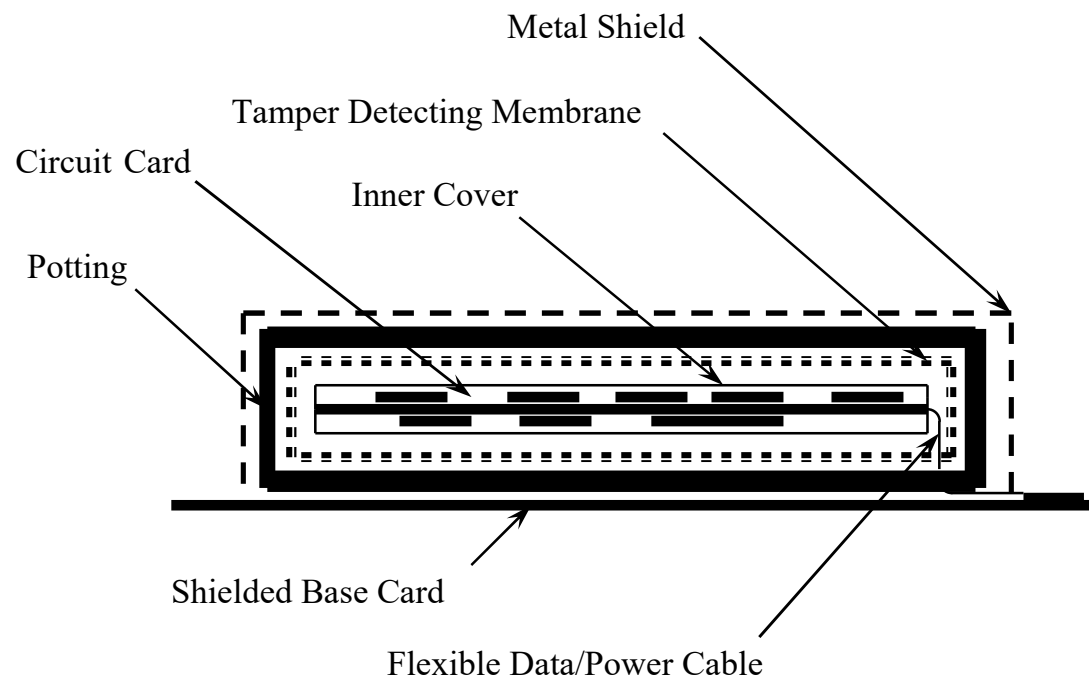
- Protection circuitry is Activated at Factory
- Stays Active for the Life of the Product
- Must Have Reasonable Battery Life
 - Can You Change The Battery, Without Powering Down Or Bricking The Unit?
- Must Have Sufficient Power to Respond to Tamper

Interactive Considerations (cont)

Defenses have to 'Cover Each Other'

- I.E. Unusual Considerations for Tamper Response
 - Temperature
 - Back Powering
- **Transients During Power Up/Down are “Normal Conditions” (For These Designs, Not For “Normal” Devices)**
- **No False Positives or False Negatives**
- **It has to be Manufacturable too**

Tamper Resistant-Detecting-Responding Package



A FEW OTHER HACKS

Now for a Few Other Hacks

- **Most Physical Attacks are Just Too Hard, so the Software Hacks are Smarter**
 - Just Look At The Rest Of The Conference...
 - FIB Might Just Be Changing That
 - Repair of Debug/Run Fuse is Still a threat, But Less So Now
- **But There ARE Good, Doable Physical Hacks**
- **Clocking**
 - AES Short Loop
 - Clock Glitching can Cause Unexpected Actions
- **Reset**
 - Incomplete Reset
 - Reset Glitching can Cause Unexpected Actions

Now for a Few Other Hacks (cont)

- **Power Glitching**
 - Power Glitching Can Cause Unexpected Actions
 - It Can Also Cause Imprinting Of RAM Contents (But Not As Easily With Newer Components)
- **Side Channel Analysis/Power Analysis (SPA/DPA/EMA)**
 - Determine Data/Secret Parameters By Analysis Of Icc EM Analysis Can Do The Same Via Radiated Output
 - This Is A Huge Thing! Google It. Commercial Systems Are \$100K, But You Can Piece It Together For Almost Nothing.

Lock Picking

- Popular Hobby In Security (As Are Other Puzzles :-)
- Especially Here At Defcon!
- Gets A Vacationing Office Mate's Desk Open Quickly
- Often The First Step In An Attack
- Google "***The MIT Guide to Lock Picking***" for a Great Reference.
- Metal Street Sweeper Bristles Make Great Lock Pick Material and are Available Everywhere, Free and No One Knows You Have Them
- See the Lockpicking Village and the vendor area too!
- Have Fun

DEMO

aruba
a Hewlett Packard
Enterprise company

THANK YOU!

???????

THANKS FOR LISTENING!

STEVE WEINGART

STEVE.WEINGART@HPE.COM

aruba
a Hewlett Packard
Enterprise company