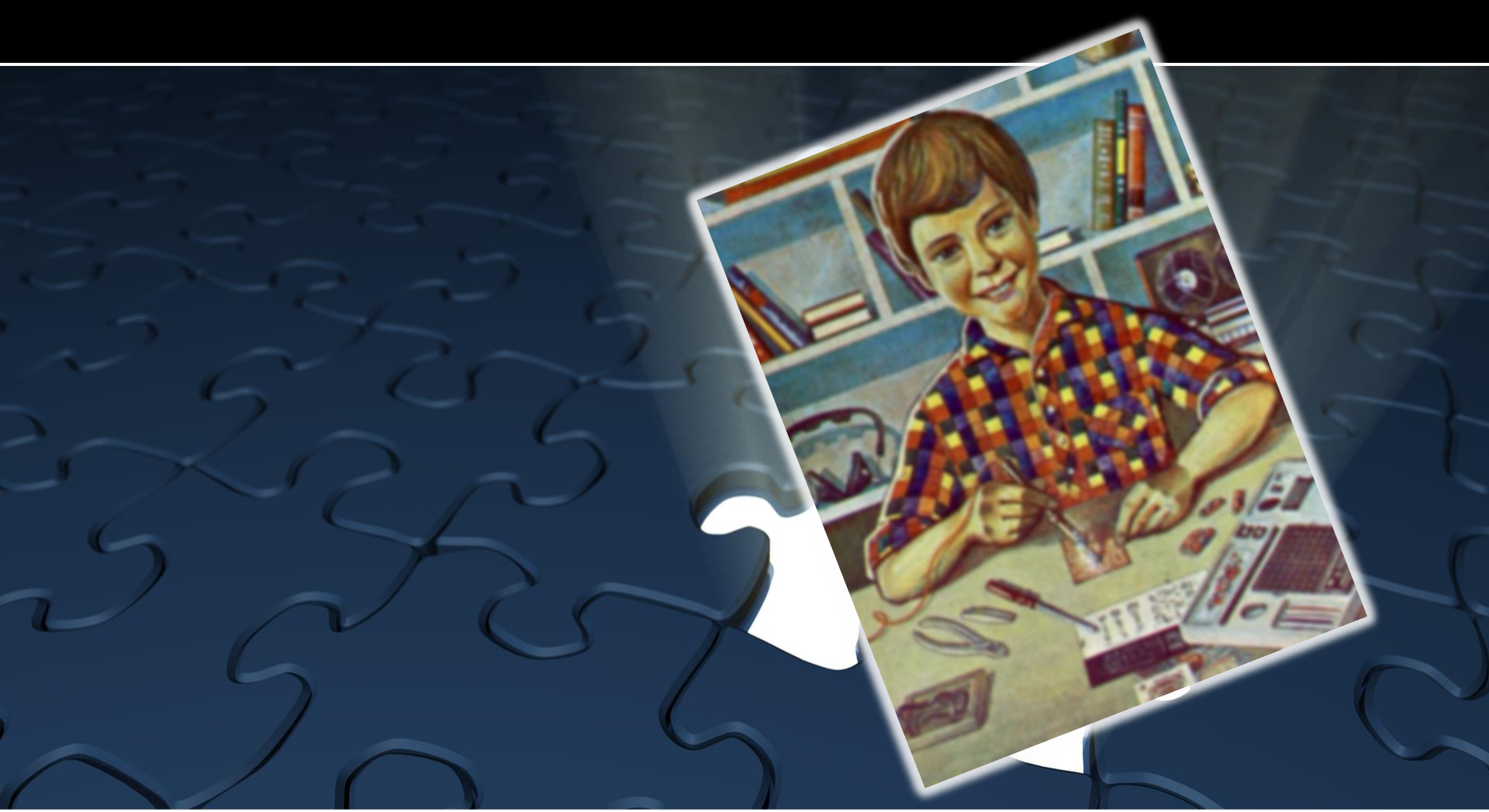


Warranty Voiding Techniques

This thing came with a warranty?

By: magikh0e

I never break things, I create things that do it for me.

Summary

A hacker will do it with all sorts of characters…

What and Why

What is hardware hacking – Why do it?
After all curiosity did kill the cat. Who does not like cats?

Tools to Void Warranties

Having fun while voiding warranties – Tools of the Trade
What to use and where to obtain

Interfaces and Attacking

Interfaces and Gaining Access – Exploring Attack Vectors

Interception	Modification	External Interfaces
Interruption	Fabrication	

Attacking Ninja Style

Mechanical, Enclosures and Electricals. Oh my!
A look into attack vectors..

Hardware Hacks

Hardware Hacks - Examples
Baby Monitor hacks, Keyboard, Raspberry Pi and Arduino.

Final Conclusions

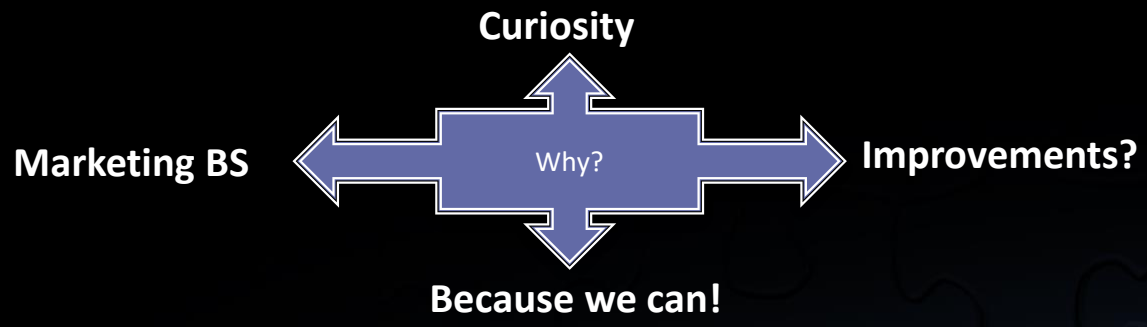
Final thoughts and Conclusions
Things we already know ;)

Questions?

Q and A time..
I like beer.

WTF is Hardware Hacking?

Pimping my *X* for hackers and geeks



- Create a new or modify an existing functionality.
- Recycle old junk into something bad ass..
- Personalization.
  - Creating something AWESOME
- **Defeating security or some sort of protection mechanism**.
  - Informational/Educational purposes only of course..

Tools of The Trade

Voiding warranties, made easy.. (hardware)

HARDWARE

- Safety Gear
- Soldering Iron (with accessories)
  - Solder sucker
  - Copper Braid
  - Tips
- Dremel
- Razors / X-Acto Blade
- Screwdrivers
  - Cruciform Types
    - Phillips
    - Frearson
  - Common Types
    - Square
    - Hex
    - Pentagon

HARDWARE CONT…

- Bus Pirate
- Sand Paper
- Heat Gun and Shrink tubing
- Adjustable Power Supply
  - DIY
- Digital and Analog multi-meters
- Tweezers and Wire Strippers
- Oscilloscope
- Logic Analyzers
- Solder-less Breadboards
- PCB Etching Supplies
  - Kits
- Chip Programmers
  - DIY
- Glue
- JTAG Gear
  - Software
  - Hardware

Tools of The Trade

Voiding warranties, made easy.. (software)

SOFTWARE

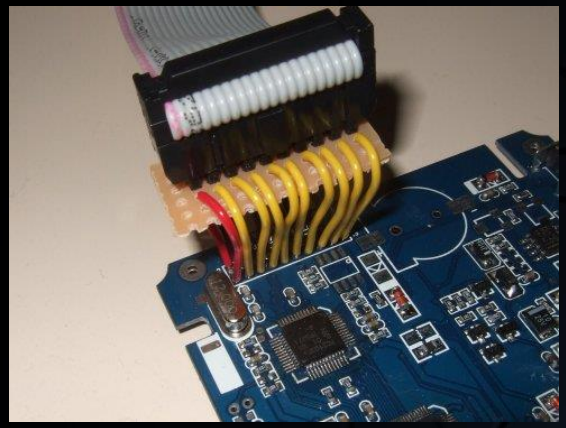
- **Protocol Analyzers**
  - USB
    - SnoopyPro - http://sourceforge.net/projects/usbsnoop/
  - RS232 & Parallel
    - PortMon - http://technet.microsoft.com/en-us/sysinternals/bb896644.aspx
- **JTAG Tools**
  - http://openwince.sourceforge.net/jtag

SOFTWARE CONT…

- BinWalk
- Strings
- SquashFS

Attacking - External Interfaces (JTAG)

Joint Test Action group



- **JTAG - IEEE 1149.1**
  - Provides a direct interface into the hardware.
  - Industry standard for testing and debugging hardware devices
    - System Level
    - Low Level testing of components
    - Boundary Scanning
- **JTAG Hardware**
  - Purchase
  - DIY – Google!

JTAG Connections

TDO = Data OUT

TDI = Data IN

TMS = Test Mode Select

TCK = Test Clock

/TRST = Test Reset (optional)

Attacking the Hardware – Attack Vectors

- Gaining stealth access to the device, ninja style.

Eaves Dropping or Interception

- Preventing a function from operating normally.

Fault Generation or Interruption

- Having your way with the device.

Modification or Fabrication

Attacking Ninja Style

Mechanical, Electrical, Enclosures and Tamper ~~Resistant~~

- **Mechanical and Electrical**
  - **External Interfaces**
    - JTAG
    - RS232 / Serial / UART
    - USB / Fire wire
    - Ethernet
    - Wireless / Blue Tooth
    - Unknown / Obfuscated / Proprietary
  - **Anti-tamper technologies**
- **Enclosures**
  - Opening Housings
  - Anti-tamper
  - Epoxy Encapsulation
  - Conformal Coating

Attacking Ninja Style - External Interfaces

Multi-meters and Oscilloscopes – Probing to Determining Functionality

Figuring out the logic state of the pins can help discovering what the purpose may be.

- **Monitoring Communications – Protocol Analyzers**
  - USB
  - RS232 and Parallel Ports
- **Causing Faults – Malformed / Bad signals**
  - Intentionally causing problems may cause the device to react in undesired ways, thus leaking information or triggering an unintended event useful for an attack

Enclosures and Anti-Tampering Tech

Accessing the hardware

- **The primary goal here is to access the internals**.
  - Most enclosures have no security in place and can simply be opened by loosening some screws or simply prying the device open or removing the glue holding it together.
  - Some devices will be sonically welded together, this process creates a solid piece outer shell. When done properly, destruction will be required for access…

- **Enclosures Sealed with Glue**
  - Some “secure-designs” use a glue with a high melting point. Thus making removing the glue harder. Chances are you will melt or deform the enclosure its self before the glue.
  - Other cases, are easily removed with a knife or by using a heat gun to soften the glue.

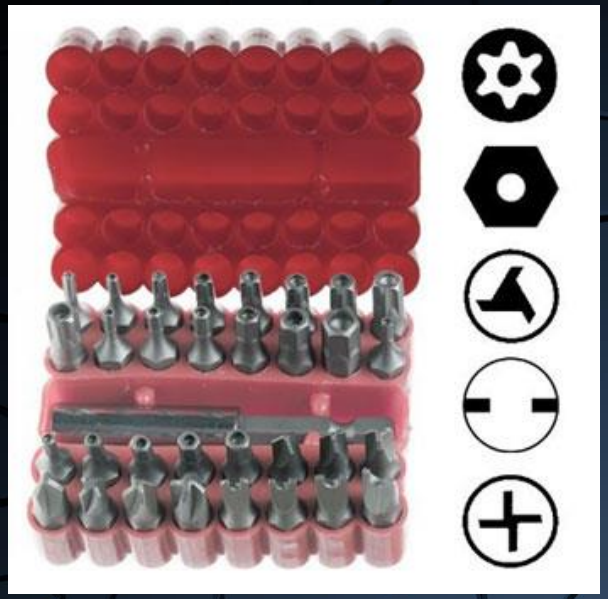
Security Bits and One way Screws

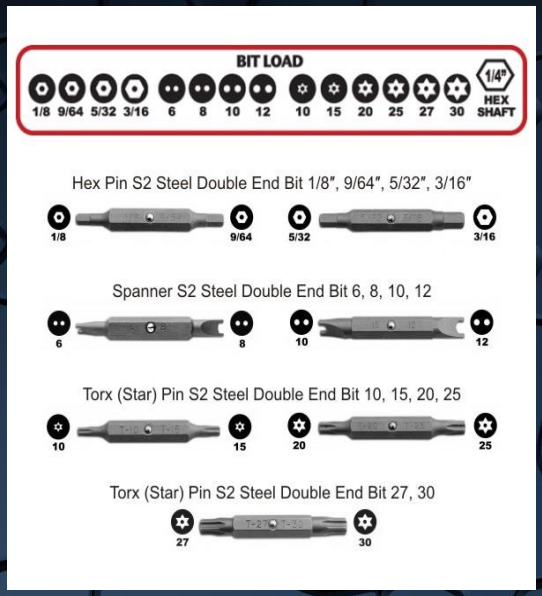
Accessing the hardware Cont..

- **One-Way Screws and Security Bits**
  - These methods are also employed in order to prevent tampering/unauthorized modification.
  - Some devices will be sonically welded together, this process creates a solid piece outer shell. When done properly, destruction will be required for access…

Removing One-Way Screws

- **Extraction Tools**
  - One way removal tool
- **Create a Slot in the Screw**
- **Locking Pliers**





Security Bits Cont..

Missing / Proprietary bit, no problem..

Using Silly putty and drywall compound or any other quick-drying spackle. You can easily make a mold for crafting your own bit Using a Dremel and some cheap Allen-wrench keys. 3D printers would make this process even simpler.

Anti-Tampering Tech

Physical Security… Is a myth?

- **Tamper Resistance**
  - One-Way Screws
  - Epoxy Encapsulation
  - Sealants
- **Tamper Detection**
  - Circuitry
  - Sensors
  - Switches
- **Tamper Evidence**
  - Seals, tapes, Glue
  - Special Enclosures
  - Unknown
- **Tamper Response**
  - Process?

Attempts to prevent unauthorized physical and/or electronic tampering.

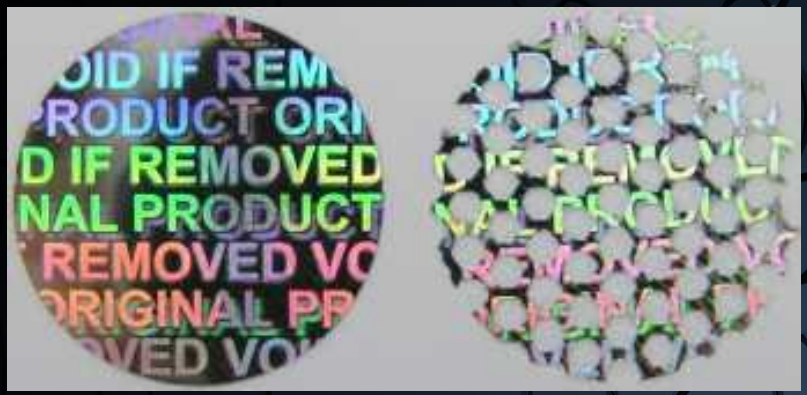
- Effective when used with “defense in depth” in mind
- Vulnerable to brute force attacks

Do NOT sacrifice the ONLY sheep!

Anti-Tampering Tech – Tamper Detection

Only works when a process for verification is in place…

- **Enables awareness of tampering**
  - **Switches**
    - Can detect that a device has been opened
  - **Sensors**
    - Can detect any operational and/or environmental changes.
  - **Circuitry**
    - Can detect a break-in or attempted modification.



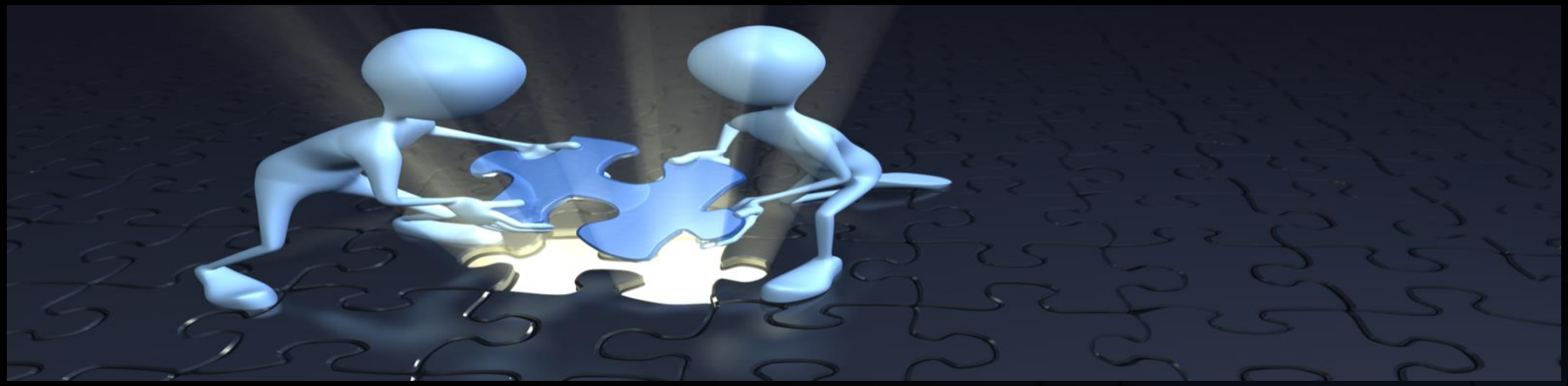
Anti-Tampering Tech – Tampering Evidence

Again, only works when a process for verification is in place…

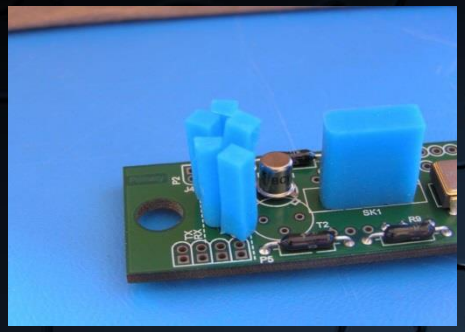
- **Always ensures that visible evidence is left behind.**
  - Passive Detectors are usually used
    - Seals / Labels
    - Tapes
    - Glues

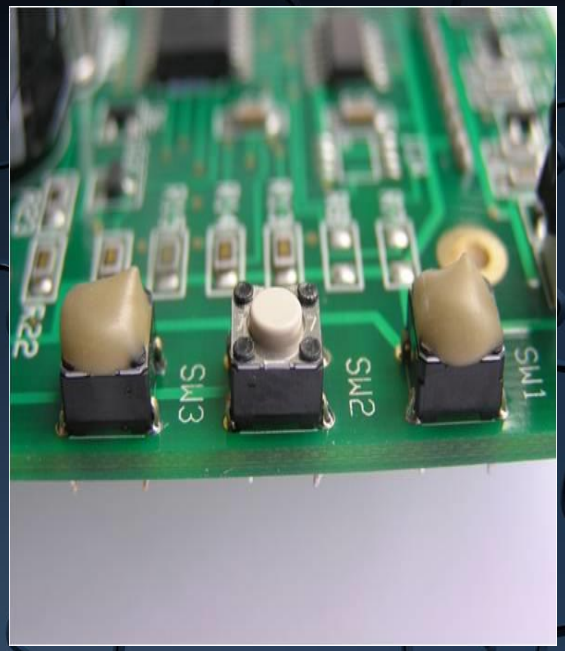
Epoxy and Conformal Coating Encapsulation

It’s a bitch, but keep calm. It can be removed!



- **Encapsulation**
  - Used to protect circuitry from:
    - Moisture
    - Dust , Mold
    - Corrosion
    - Arcing
  - Epoxy Encapsulation
  - Sealants





Conformal Coating Charts

Characteristics and Removal Methods

Table 1. Conformal Coating Characteristics courtesy of IPC

Characteristics	Conformal Coating Type				
	Epoxy	Acrylic	Polyure thane	Silicone Resin	Paraxy lylene
Hard	x		x		x
Medium Hard		x	X		
Soft			x	x	
Heat Reaction	x	x	X		
Surface Bond- Very Strong	x			x	x
Surface Bond Strong		x		X	
Surface Bond- Medium			x	x	
Surface Bond-Light				X	
Solvent Reaction		X			
Non-porous Surface	x	x	x		X
Glossy Surface	x	x	x		
Semi-Glossy Surface	X			x	
Dull Surface					X
Rubbery Surface				x	
Brittle	x	x			
Chips	x	x			
Peels and Flakes		x	x		X
Stretches			x	X	
Scratch, Dent, Bend, Tear			x	x	x

Table 2. Conformal Coating Removal Methods courtesy of IPC

Conformal Coating	Removal Method				
	Solvent	Peeling	Thermal	Grinding Scraping	Micro Blasting
Paraxylyene			1	2	3
Epoxy			1	2	3
Acrylic	1		2	3	4
Polyurethane	3		1	2	4
Silicone Thin	1		2	3	4
Silicone Thick		1		2	

Epoxy and Conformal Coating Encapsulation

Removal Methods

Method 1 – Chemicals / Solvents

- MG Chemicals 8310 – Conformal Coating Stripper
- Does not always work, as its coating dependent.

Method 2 – Brute Force

- Patience
- Dremel with a wooden skewer bit.
- Always works, when done with patience.

Other Options

- Thermal Degradation
- Excimer Laser
- Plasma

Attacking Ninja Style – Electrical Attacks

SMD – Surface Mount Devices

- Good luck de-soldering…

Side-Channel Attacks

- Cold Boot
- Clock and Timing
  - Changing or measuring timing traits of the system
  - Cryptographic systems and Timing Attacks
  - Invasive and Passive attacks
- Information Leaks
  - Differential Fault Analysis
  - Data Remanence
  - Power Analysis
    - Simple Power Analysis (SPA)
    - Differential Power Analysis (DPA)

Programmable Logic and Memory

- Bypassing fuses and boot-block protections.

Probing

- Test Point Discovery

Attacking Ninja Style – Side-Channel Attacks

- **Timing Attacks** involve watching data movement into and out of the CPU, or memory, on the hardware running the cryptosystem or algorithm. By observing variations in how long it takes to perform cryptographic operations, it might be possible to determine the entire secret key.

- **Power Analysis Attacks** These types of attack can provide loads of detailed information by observing the power consumption of a hardware device such as a CPU or cryptographic circuit. These types of attacks are categorized into *Simple Power Analysis* (SPA) and *Differential Power Analysis* (DPA). Fluctuations in current also generate radio waves, enabling attacks that analyze measurements of electromagnetic emanations.

    - **Simple Power Analysis (SPA)** involves visually interpreting power traces, or graphs of electrical activity over time.

    - **Differential Power Analysis (DPA)** is a more advanced form of power analysis which can allow an attacker to compute the intermediate values within cryptographic computations by statistically analyzing data collected from multiple cryptographic operations.

Power analysis attacks cannot generally be detected by a device, since the adversary's monitoring is normally passive.

Attacking Ninja Style – Side-Channel Attacks

SPA and **DPA** were introduced in the open cryptologic community in **1998** by Cryptography Research's **Paul Kocher, Joshua Jaffe and Benjamin Jun.**

FIPS 140-3: *Requires power analysis countermeasures for cryptographic devices bought to the U.S. government.*

- **Electromagnetic Attacks** are based on leaked electromagnetic radiation which can directly provide plaintexts and other information. Techniques equivalent to *power analysis* , it also can be used in combination with other attacks*; ie; TEMPEST*

- **Acoustic Cryptanalysis** Involve attacks which exploit sound produced during computation.

- **Power Analysis Attacks** These types of attack can provide loads of detailed information by observing the power consumption of a hardware device such as a CPU or cryptographic circuit. These types of attacks are categorized into *Simple Power Analysis* (SPA) and *Differential Power Analysis* (DPA).

Fluctuations in current also generate radio waves, enabling attacks that analyze measurements of electromagnetic emanations.

Attacking Ninja Style – Side-Channel Attacks

Timing Analysis Attacks

A timing attack is an example of an attack that exploits the data-dependent behavioral characteristics of the implementation of an algorithm rather than the mathematical properties of the algorithm itself.

Every logical operation in a computer takes time to execute, and the time can differ based on the input; with precise measurements of the time for each operation, an attacker can work backwards to the input.

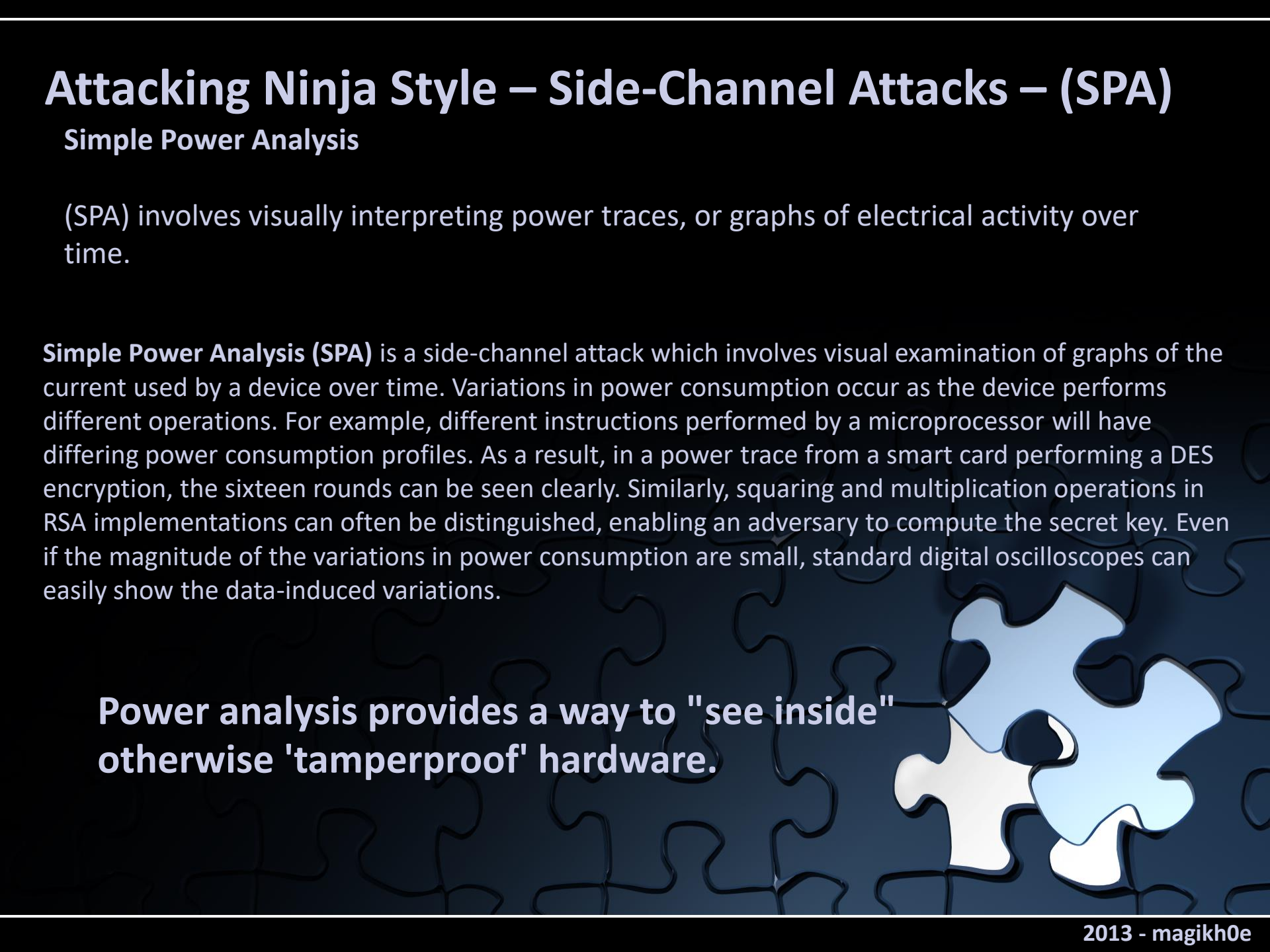
Timing attacks are often overlooked in the design phase because they are so dependent on the implementation. After all people design with security in mind... Right?

Attacking Ninja Style – Side-Channel Attacks – (SPA)

Simple Power Analysis

(SPA) involves visually interpreting power traces, or graphs of electrical activity over time.

Simple Power Analysis (SPA) is a side-channel attack which involves visual examination of graphs of the current used by a device over time. Variations in power consumption occur as the device performs different operations. For example, different instructions performed by a microprocessor will have differing power consumption profiles. As a result, in a power trace from a smart card performing a DES encryption, the sixteen rounds can be seen clearly. Similarly, squaring and multiplication operations in RSA implementations can often be distinguished, enabling an adversary to compute the secret key. Even if the magnitude of the variations in power consumption are small, standard digital oscilloscopes can easily show the data-induced variations.

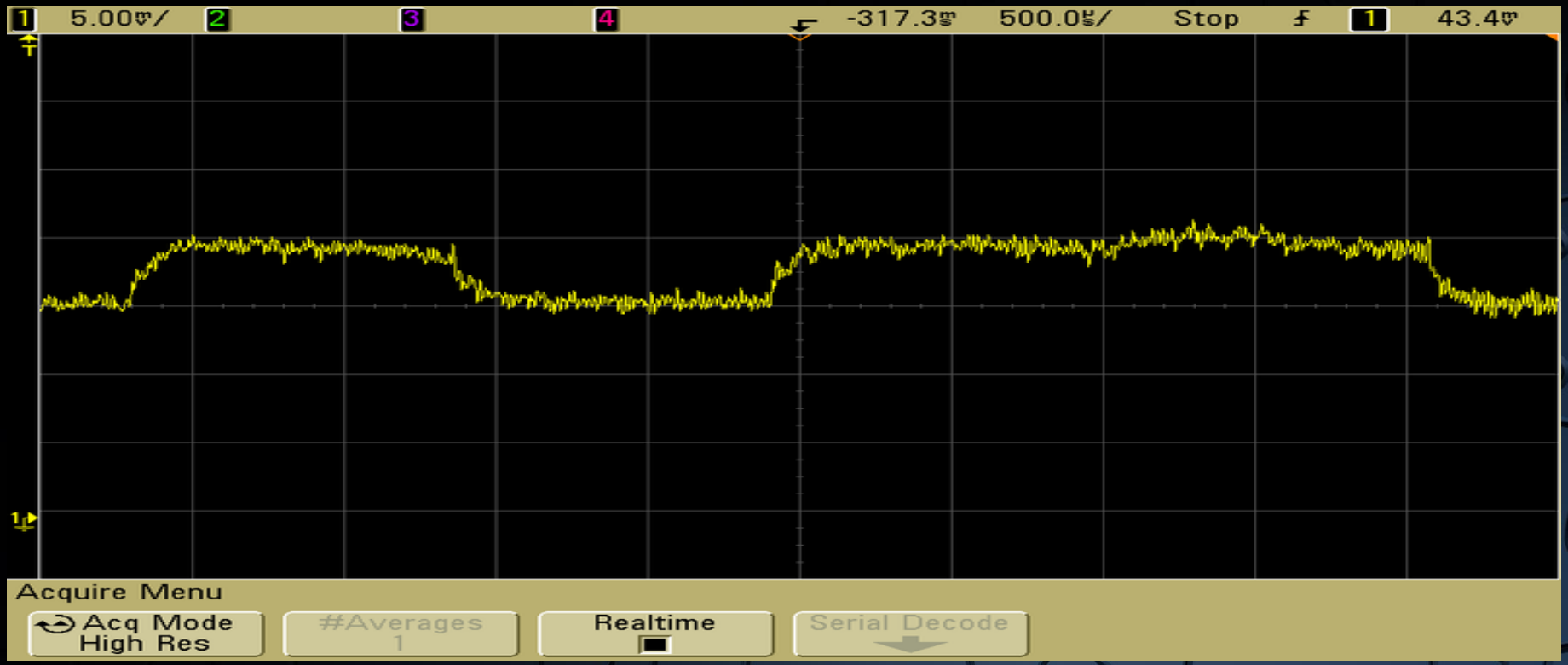


Power analysis provides a way to "see inside" otherwise 'tamperproof' hardware.

Attacking Ninja Style – Decoding RSA key bits

Using Simple Power Analysis

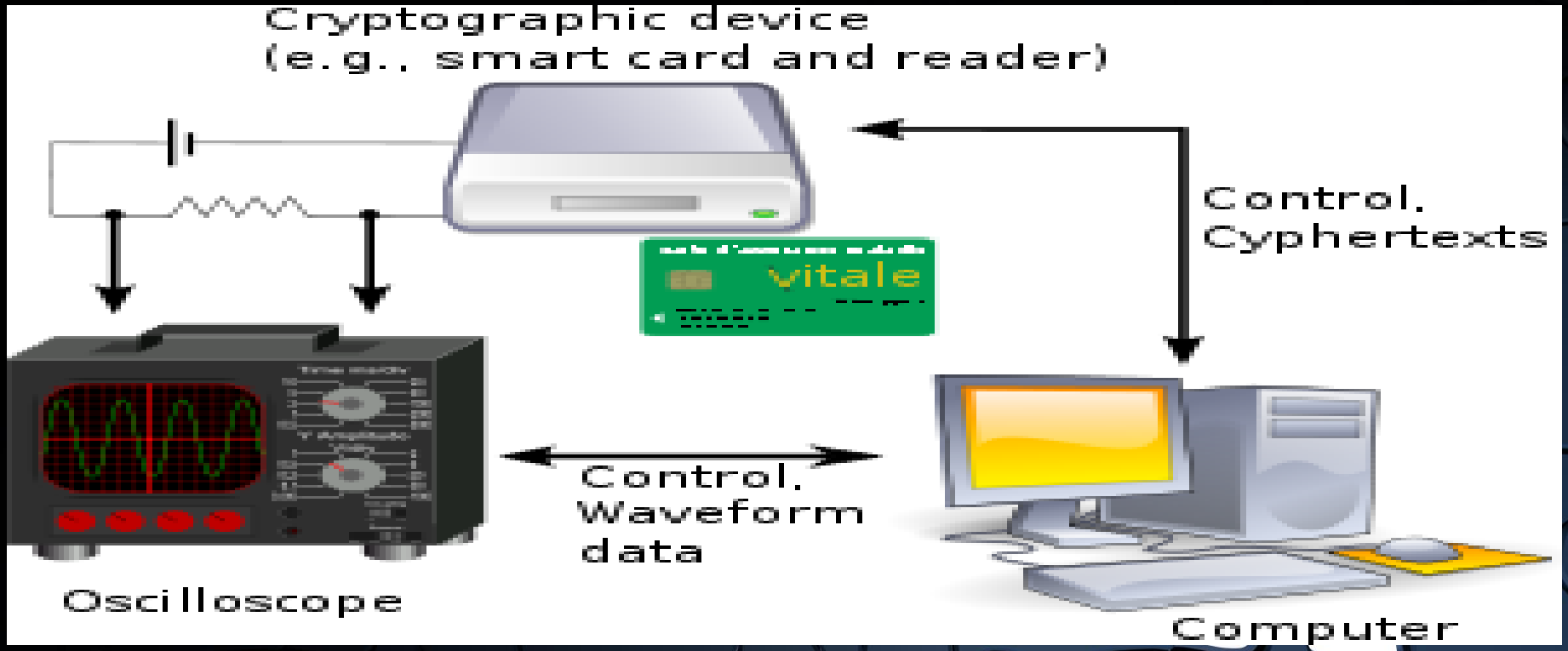
As a result, in a power trace from a smart card performing a DES encryption, the sixteen rounds can be seen clearly. Similarly, squaring and multiplication operations in RSA implementations can often be distinguished, enabling an adversary to compute the secret key. Even if the magnitude of the variations in power consumption are small, standard digital oscilloscopes can easily show the data-induced variations.



Attacking Ninja Style – Side-Channel Attacks – (DPA)

Differential Power Analysis

(DPA) is a more advanced form of power analysis which can allow an attacker to compute the intermediate values within cryptographic computations by statistically analyzing data collected from multiple cryptographic operations.



Attacking Ninja Style - Probing

Finding the way to grandmas house…

Finding test points and exposed traces, bus lines etc is only half the battle in hacking hardware. Most surface mounts and points are way to small to probe via manual methods.

Probing Boards with SMDs

- **Solder a probe wire/lead onto the board**
- **SMD Micro Grabbers**
- **Probe Adapters**
  - BGA, QFN, QFP, SOIC
- **Build your own probe**
  - Google DIY probe

Hardware Hacks – Stealth Baby Monitor/ Eaves Dropper

Modifying a simple 49 Mhz baby monitor to operate on a non-standard frequency.

49Mhz baby monitors commonly operate on these frequencies:

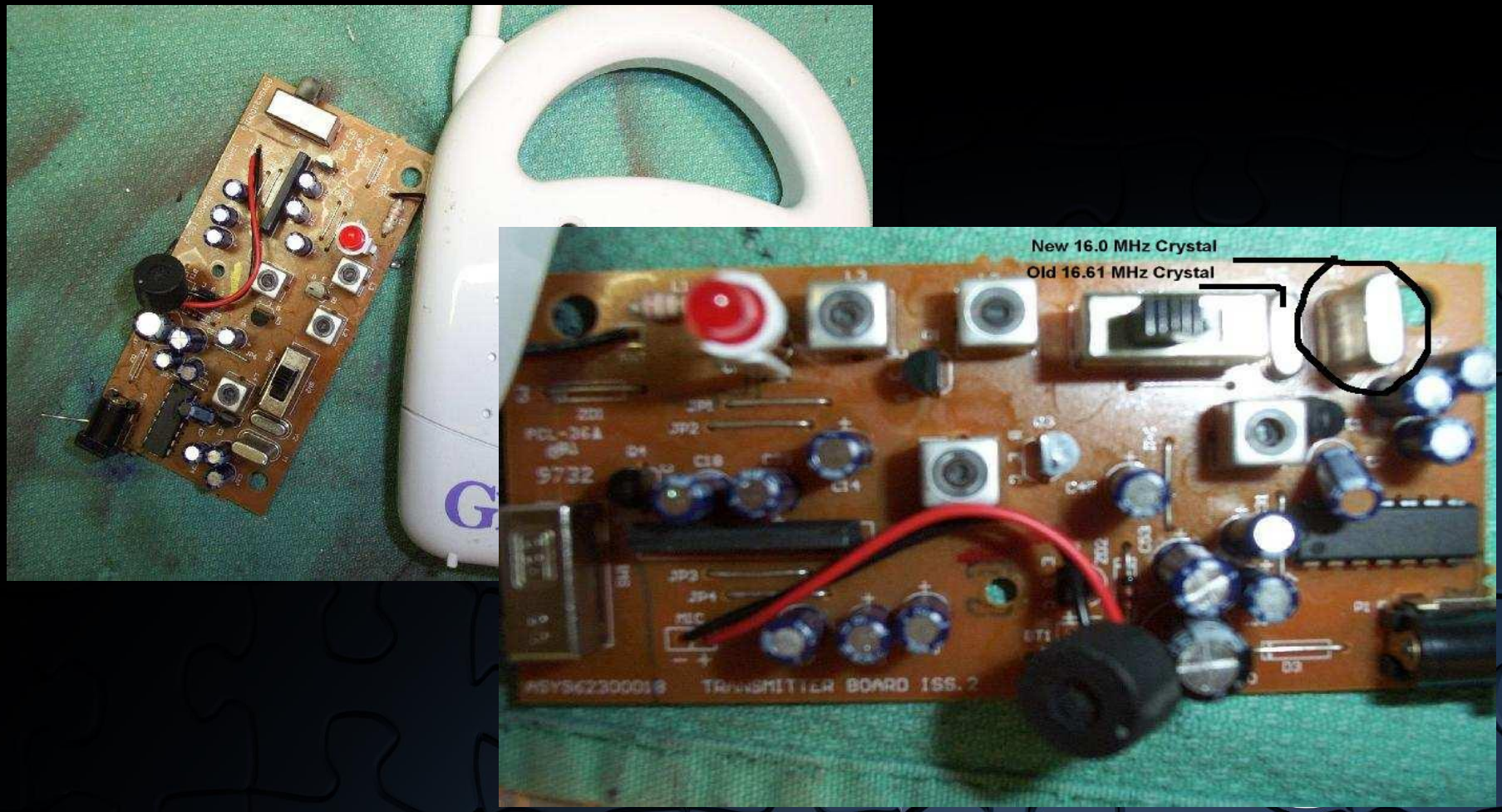
Channel A	49.83 MHz
Channel B	49.845 MHz
Channel C	49.86 MHz
Channel D	49.875 MHz
Channel E	49.89 MHz

The baby monitors transmitter uses a crystal within the 16 MHz range followed by a multiplication-by-3 buffer/amplifier circuit. A 16.61 MHz crystal is used to transmit at 49.83 MHz.

Replacing the 16.61 MHz crystal with a non-standard frequency of 16.0 MHz, the baby monitor will transmit on a frequency within 48 MHz, which can not be picked up by the other paired monitors. Allowing for the creation of a stealth eaves dropping device.

Hardware Hacks – Stealth Baby Monitor/ Eaves Dropper

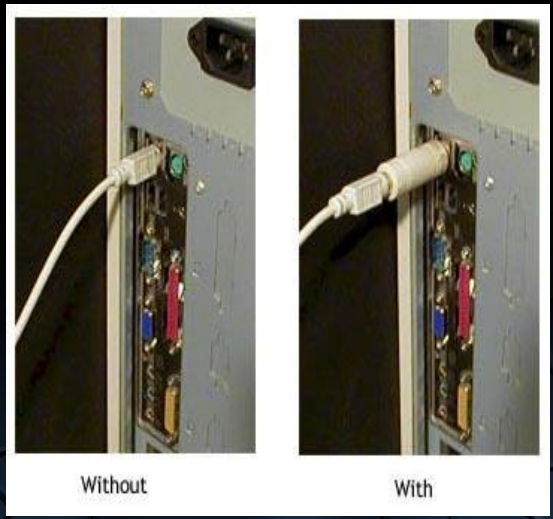
Modifying a simple 49 Mhz baby monitor to operate on a non-standard frequency.



Hardware Hacks – Defeating Hardware Key-loggers

A simple method to defeat inline hardware-based key-loggers.

You could always simply look, but where is the fun in that! Hardware key-loggers are easy to get and very simple to install. However the simplicity of operation with such devices is also the main weakness/flaw.



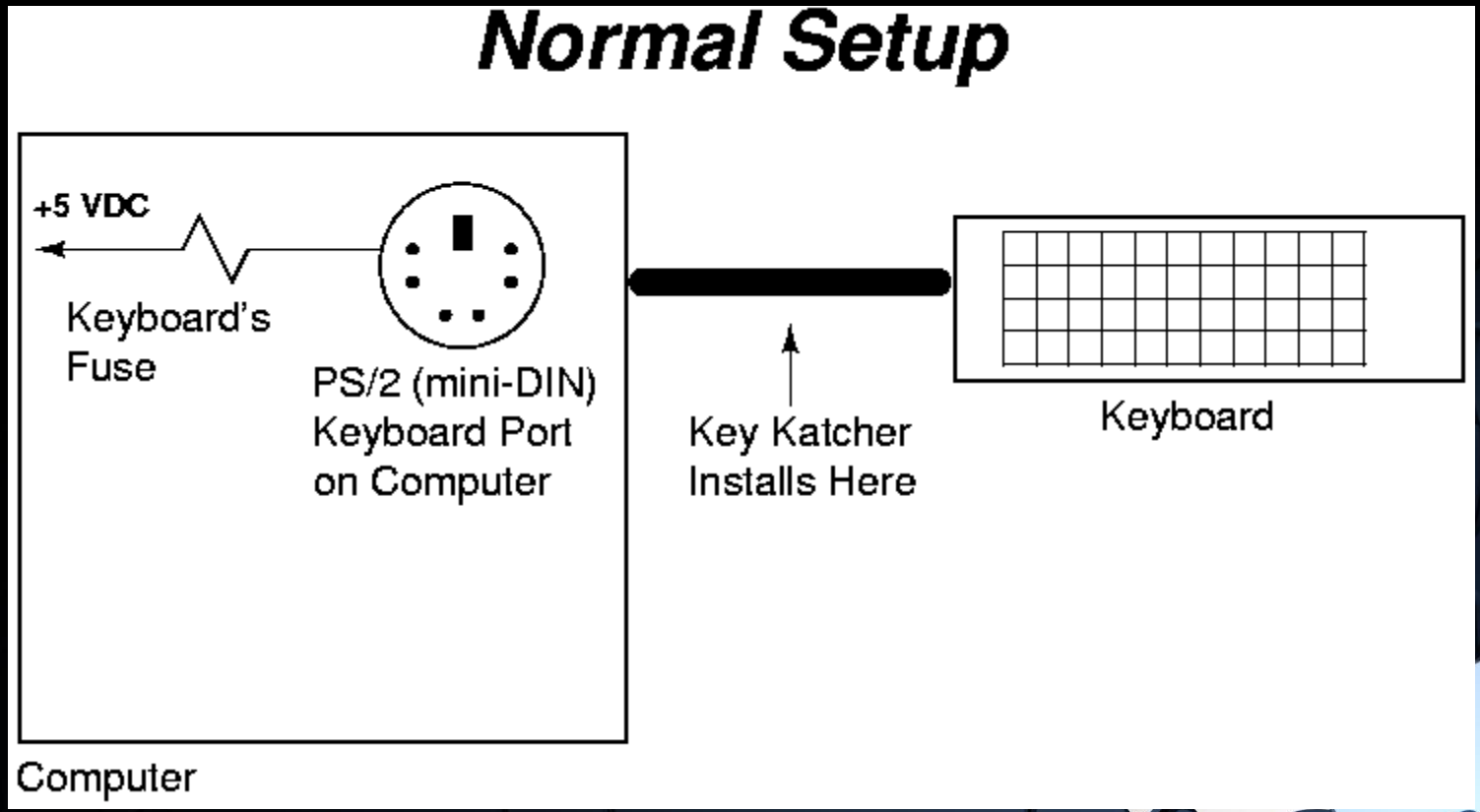
Most hardware Key-loggers draw the power required from the 5Vdc line on the keyboards internal circuit.

*On a PS/2 style connector, this will be **PIN 4**.*

By disabling the keyboards internal 5Vdc line, anything attempting to draw power from it will be unable to do so. This also includes the Keyboard it's self, so a new *EXTERNAL* 5 Vdc power source will be required.

Hardware Hacks – Defeating Hardware Key-loggers

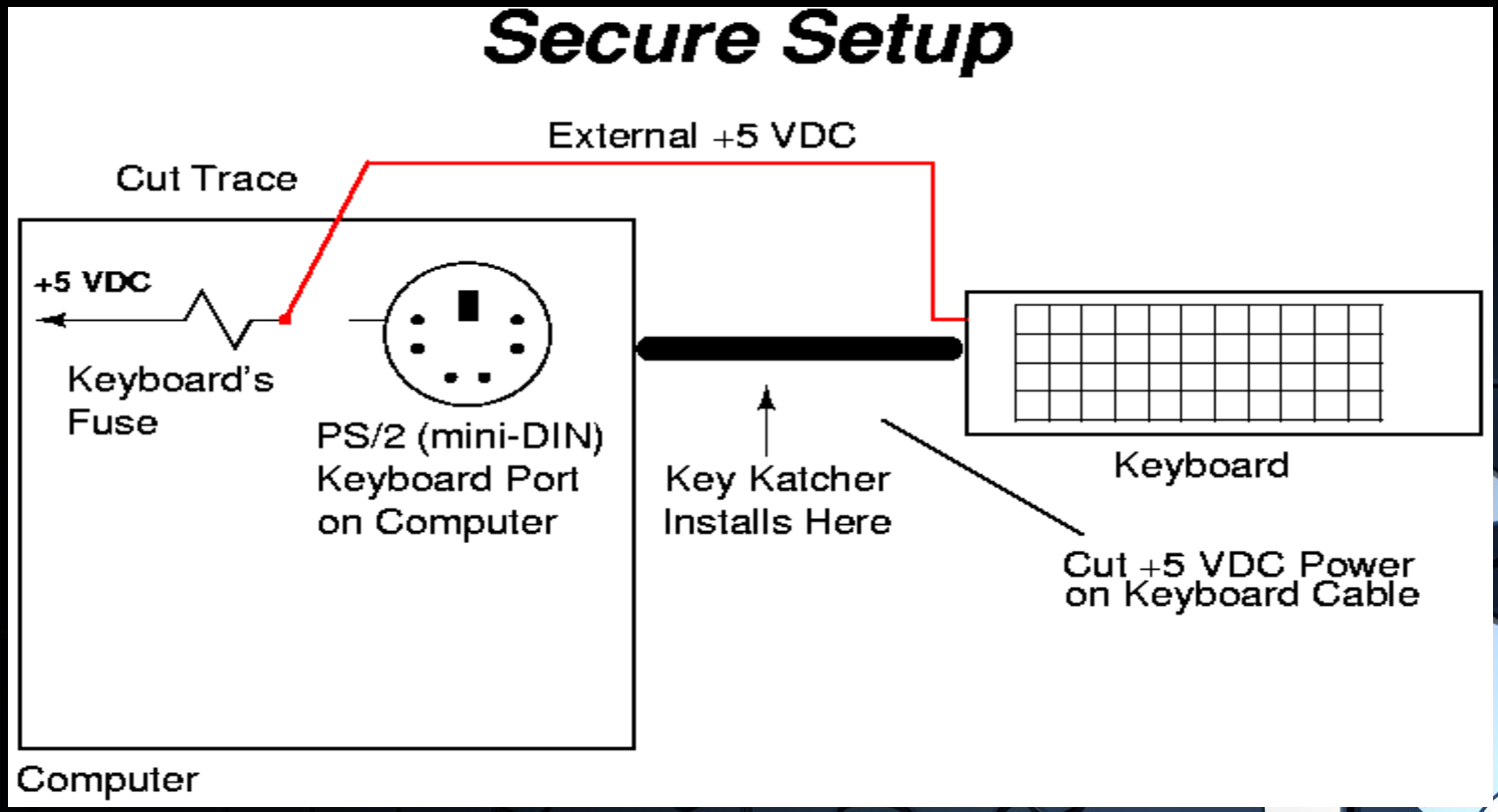
Normal Setup – PS/2



Hardware Hacks – Defeating Hardware Key-loggers

Secure Setup – PS/2

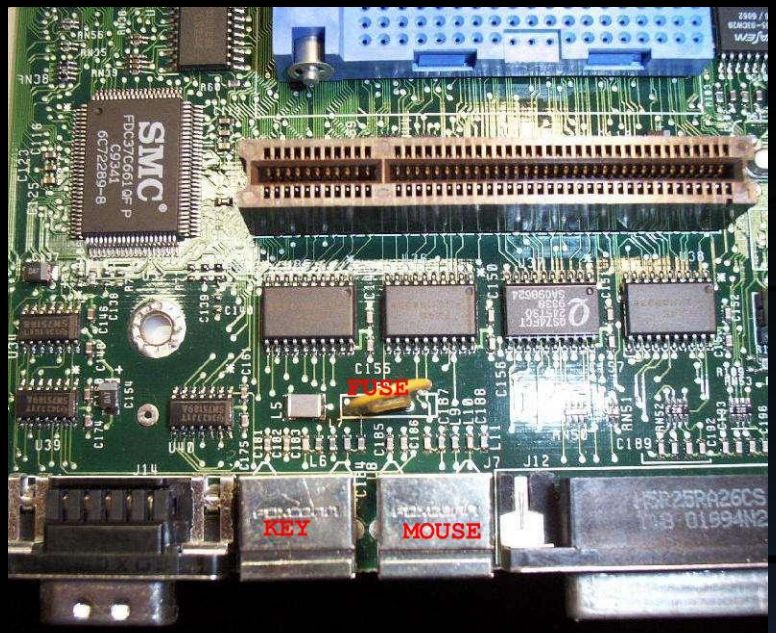
Another option would be to install a battery pack somewhere inside the keyboard

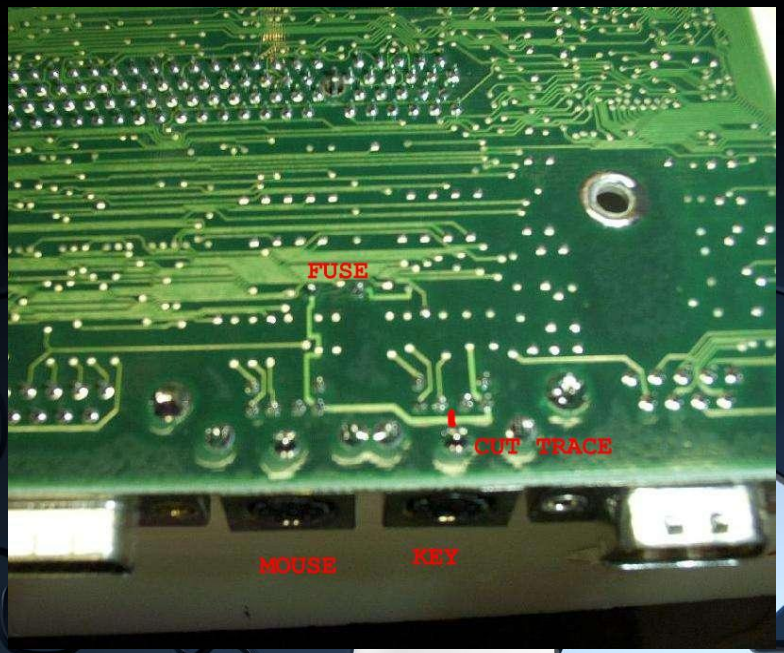


Hardware Hacks – Defeating Hardware Key-loggers

Example

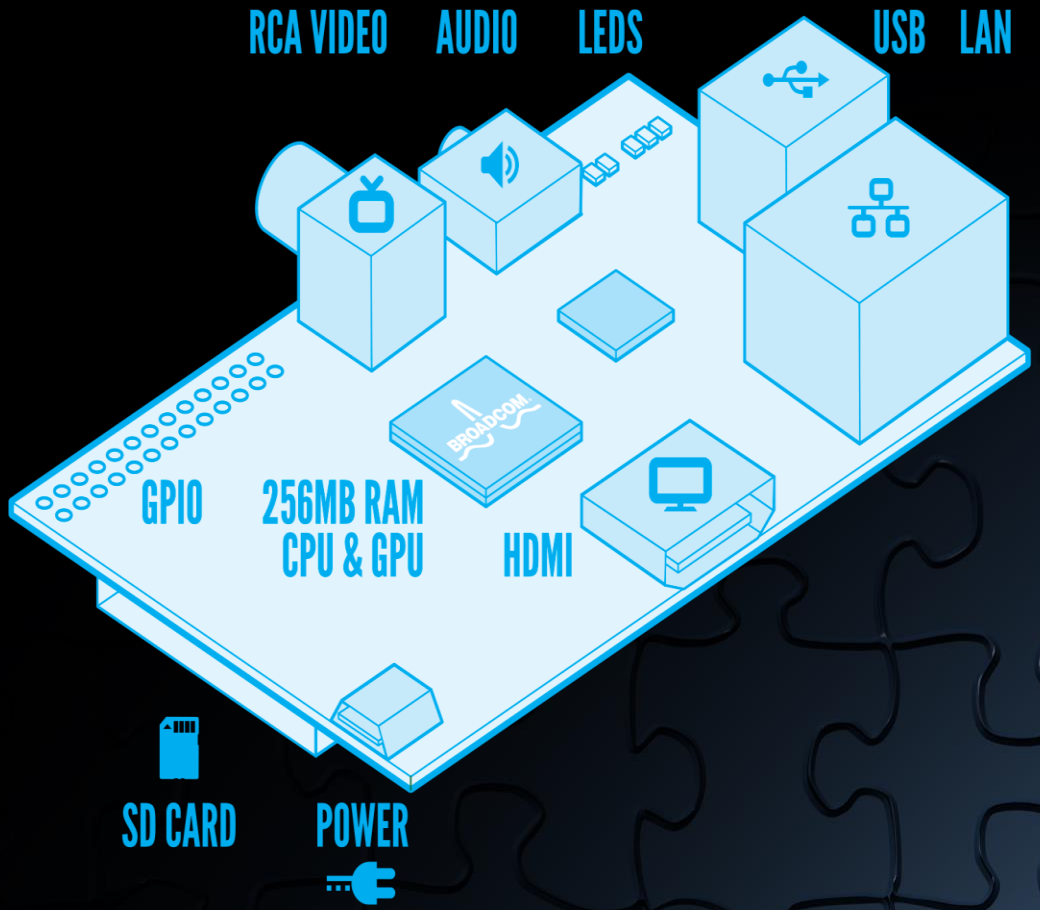
The yellow disk is a resettable fuse for the mouse and keyboard. Most boards fuses power both the mouse and the keyboard. On these types of boards, you will be required to cut a trace.

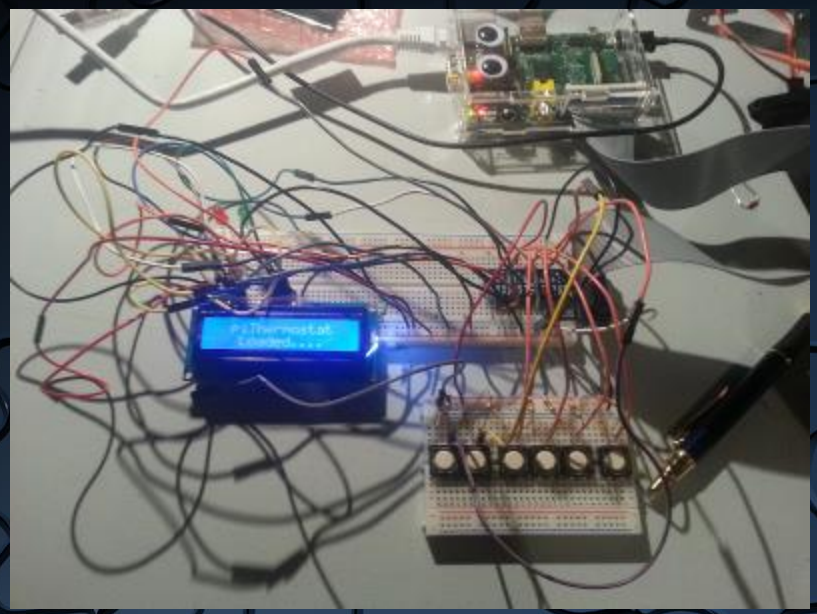




Hardware Hacks – Raspberry PI

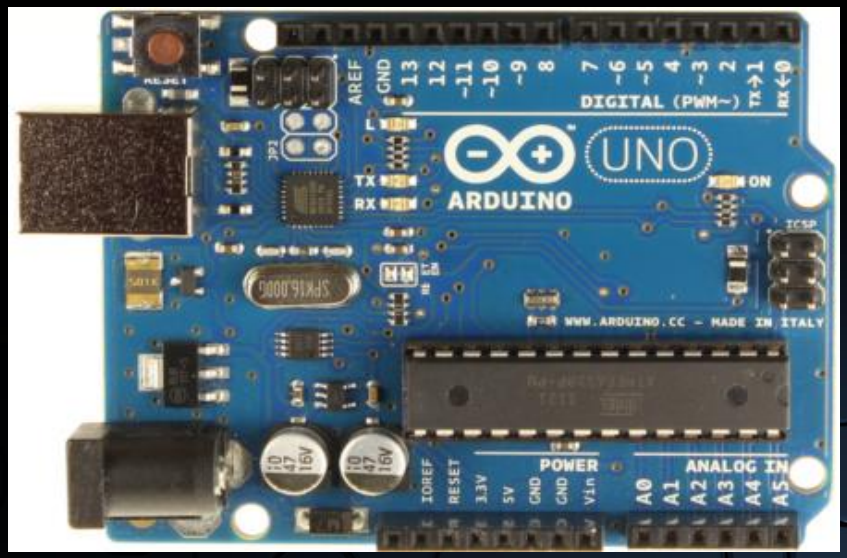
Raspberry PI, the 35$ mini computer.





Hardware Hacks – Arduino

Arduino is an open-source electronics prototyping platform based on flexible, easy-to-use hardware and software. It's intended for artists, designers, hobbyists and anyone interested in creating interactive objects or environments.



The boards can be built by hand or purchased preassembled;
The software can be downloaded for free.
The hardware reference designs (CAD files) are available under an open-source license, and you are free to adapt them to your needs.

Final Thoughts and Conclusions

……