Anti-Tamper Techniques

Elena Dubrova
Royal Institute of Technology, Stockholm, Sweden
Overview

• Anti-tamper techniques
  • Tamper prevention
  • Tamper detection
  • Tamper response
  • Tamper evidence
• Hardware Security Modules
I. Tamper Prevention
Tamper prevention mechanisms

• Making housing difficult to open
• Encapsulation/Coating
• Using security fuses to prevent unauthorized access
• Layout and data bus scrambling
Tamper prevention I: Making housing difficult to open

Make housing difficult to open by using:

- Security bits
- Adhesives
- Ultrasonic welding
Security bits

• Security bits are intended to protect outer shells from being open
• Often rubber feet or labels are used to hide them

source: http://justinpaulin.com/tag/security-bits/

source: [1]

source: https://www.ifixit.com/Teardown/Xbox+One+Teardown/19718/

source: http://www.androidcentral.com/how-upgrade-ram-your-hp-chromebox/
Defeating security bits

- Screwdriver sets for opening security bits are easy to purchase
- The head of a security bit can be drilled out
- 3D printer can be used to create a required screwdriver

source: toolguyd.com/cheap-security-bit-sets/
Adhesives

• High strength glue is used to hold the housing together

source: www.ifixit.com/Teardown/iPad+4+Wi-Fi+Teardown/11462
Defeating adhesives

- Unless the glue is high-temperature, it will soften when heat is applied
- Use a heat gun to soften the adhesive
- Run a sharp knife/plastic opening tool ($3) around the edge to separate the adhesive

source: www.ifixit.com
Ultrasonic welding

• Applies high-frequency ultrasonic vibrations to pieces pressed together to create a one-piece outer shell
  • There are no connective bolts, nails, soldering materials, or adhesives
  • Outer shell is difficult to open without a noticeable damage
    – Cooling with liquid nitrogen and filling with compressed air may crack the weld in some cases

source: http://www.ebay.com/gds/How-to-Repair-a-USB-Stick-/
Tamper prevention II: Encapsulation/Coating

Encapsulation/coating is used to protect integrated circuits or boards from:

- Dust, moisture, corrosion, etc.
- Tampering, reverse engineering, cloning
Encapsulation

Types of encapsulation include:

**Fully Closed:**
- **Flattened:** Packages are fully encapsulated with filled epoxy
- **Glob Top:** Packages are fully encapsulated with filled epoxy and have a domed surface
- **Clear Encapsulant:** Packages are fully encapsulated with non-filled epoxy (for bonding verification, visual samples and optical applications)

**Partially Closed:**
- **Partial Encapsulation:** Packages are encapsulated with filled epoxy in selected areas (i.e. around leads only.)

http://www.icproto.com/capabilities-services/ic-assembly/encapsulation-options/
Coatings

Common coating types are [2]:

- **Acrylic**
  - Good resistance to chemicals, moisture, and abrasion (surface wear caused by rubbing), temperature resistance 150°C
  - Very easy to rework

- **Epoxy**
  - Excellent resistance to chemicals and abrasion, fair resistance to moisture, temperature resistance 150°C, hard to rework

- **Silicone**
  - Good resistance to chemicals, excellent resistance to moisture, fair resistance to abrasion, temperature resistance 200°C
  - Easy to rework

source: http://electronics.stackexchange.com/questions/56649/what-is-a-die-package
Removing coating by abrasion

A protective layer can be often removed by rubbing the surface with knife, sand paper, using dremel tools or milling machine.

source: http://www.kevtris.org/Projects/votraxpss/unpot.html
Removing coating by chemicals

Hot fuming nitric acid dissolves the smartcard package without affecting the chip [3]

The de-packaged smartcard is glued into a test package, whose pins are connected to the contact pads of the chip with fine aluminum wires in a manual bonding machine [3]
Defeating encapsulation by X-ray or acoustic microscopy

- X-ray or acoustic microscopy can be used to get images of a chip
- Helps to find out component location, hidden sensors, etc.

source: www.multigame.com/pacplus.html
Tamper prevention III: Using security fuses to prevent non-authorized access

- Security fuses can be used to protect on-chip memories from non-authorized access
- ID authentication is performed when an access is attempted; if the authentication fails, the access is not allowed
- Modification or readback of certain regions of memory is prevented

http://www.bunniestudios.com/blog/?page_id=40
Defeating security fuses

- Security fuses can be erased with UV light [4]
  - Metal shields over the security fuses can be surpassed by placing the chip at an angle
- To prevent the erasure of data from the Flash memory, a piece of electrical tape can be placed over the Flash
- With fuses disabled, the code stored in the Flash can be read out

PIC 18F1320 microcontroller

http://www.bunniestudios.com/blog/?page_id=40
Countermeasures to the attack in [4]

The attack presented in [4] can be mitigated using more secure methods for key storage, including

- Encode a key in a Finite State Machine (FSM) and implement the FSM on-chip by a sequential circuit [5]
- Reverse-engineering of the chip netlist will be required to defeat this method
- Store a key using a Physical Unclonable Function [6]

source: http://rijndael.ece.vt.edu/puf/main.html
Using security fuses to disable debug interfaces

- Debug interfaces, such as JTAG, are created for chip-level testing
- Can be used to [7]:
  - Access all pins via boundary scan
  - Extract program code
  - Modify memory content
- Security fuses can be used to temporary disable or destroy debug interfaces

Focused ion beam image of a blown polysilicon fuse next to a test pad (interrupted white line at the bottom of the cavity) [3]
Defeating JTAG security fuses

- However, destroying JTAG removes debugging capabilities, which is undesirable
- Usually JTAG is disabled rather than destroyed
  - can be enabled again

The WRT120N JTAG header

source: http://www.devttys0.com/2014/02/re-enabling-jtag-and-debugging-the-wrt120n/
JTAG is disabled by removing jumper R356  A solder blob enables JTAG back

source: http://www.devttys0.com/2014/02/re-enabling-jtag-and-debugging-the-wrt120n/
Tamper prevention V: Layout and data bus scrambling

Layout and data bus scrambling can be used to confuse an attacker

STMicroelectronics ST16601 smartcard MCU

Motorola SC27/28 smartcard MCU

source: [8]

source: [9]
II. Tamper Detection
Tamper detection mechanisms

- Anti-tamper switches
- Anti-tamper sensors
- Anti-tamper circuitry
Tamper detection I: Anti-tamper switches

Various switches can be used to detect tampering when a cover is removed, some component is moved, or a physical security barrier is breached

- Microswitches
- Magnetic switches
- Pressure contacts
Tamper detection II: Anti-tamper sensors

- **Temperature** sensors can detect changes in operating temperature (cold boot attack)
- **Voltage** sensors can detect changes in operating voltage (glitch attacks)
- **Radiation** sensors can detect for X-rays and ion beams

source: https://wisense.wordpress.com/2013/12/02/lm75b-temperature-sensor/
Tamper detection III: Anti-tamper circuitry

- Intrusion detection meshes such as
  - Wire meshes
  - Piezo-electric sheets
  - Fiber optics
  can be wrapped around critical hardware areas to detect an attempted intrusion
- Sensors monitoring these meshes recognize small changes in mesh’s capacitance or resistance


http://zch5584.buy.reelisor.com/pz5084ee1-pvdf-piezo-film-pvdf-piezo-sensor.html
Defeating anti-tamper circuitry

The ST16SF48A data bus extends several micrometers beyond the protected mesh area, providing easy probing access [3].
Defeating anti-tamper circuitry, cont.

A FIB was used here to drill a fine hole to a bus line through the gap between two wires [3]
III. Tamper Response
Tamper response

Tamper response is the actions taken upon the detection of tampering with a device
Possible responses include:
• Shut down or disable the device
• Erase critical parts of memory
• Physically destroy the device
Tamper response I: Memory zeroization

• Erasing critical parts of memory in response to tampering is called zeroization
• However, zeroization mechanisms often require a continuous power supply
  – the attacker can disable them before powering up a chip
• Another problem is data remanence – residuals of data remain after erasure
Data remanence in volatile memories

Contrary to conventional belief, volatile memories (SRAM, DRAM) do not entirely lose their contents when power is turned off [11]

– for SRAM, at room temperature the data retention time varies from 0.1 to 10 sec
– cooling SRAM to -20ºC increases the retention time to 1 sec to 17 min
– at -50ºC the retention time is 10 sec to 10 hours

source: revision3.com
Data remanence in non-volatile memories

It may take many cycles to erase data from a non-volatile memory (EEPROM, Flash, etc.)

Data was successfully recovered from the Flash memory PIC16F84 after 10 erase cycles [12]

To overcome this problem, it is recommended to erase data by writing all-0, all-1, and random data in the memory
Tamper response II: Physical destruction

- Devices requiring very high security can be physically destroyed using, e.g. a small explosive charge
- But this option is not practical for consumer electronics
  - a chip on the left is destroyed in response to tamper detection [13]
  - $1500 hard drive, 128GB

source: www.alphr.com
Chip made of tempered glass can be triggered remotely to self destruct. The silicon computer wafers is attached to a piece of tempered glass that breaks when heated in one spot [14]
IV. Tamper Evidence
Tamper Evidence

The goal is to ensure that visible evidence is left behind when tampering occurs

- Tamper evidence may be provided by:
  - Tamper-evident housing, e.g. ultrasonic welding creates a housing which is difficult to open without a noticeable damage

Tamper Evidence

- Enclosures with tamper-evident seals or locks
- Tamper-evident encapsulating materials or coatings
- "Bleeding" paint - paint of one color is mixed with micro-balloons containing paint of a contrasting color. If the painted surface is damaged, the colors blend and tampering is easy to identify [15]
Tamper Evidence, cont.

- Logging the type of detected attack and its time
  
  • For example, tamper detection mechanisms in electricity meters can record a tamper event in the memory and report it during the next meter reading by an authorized personnel. A tamper LED is enabled and date is recorded [16]

source: [17]
Trusted Platform Modules/
Hardware Security Modules
What about Trusted Platform Modules?

Trustable Platform Module installed on a motherboard

source: en.wikipedia.org/wiki/Trusted_Platform_Module
Hardware-security enabled embedded system architecture

source: [20]
10 February 2010, 17:41

Hacker extracts crypto key from TPM chip

An American hacker has, with a great deal of effort, managed to crack a Trusted Platform Module (TPM) by Infineon. He was able to read the data stored on the TPM chip, for instance cryptographic keys (RSA, DES) such as those also used by Microsoft's BitLocker on appropriate motherboards.
Conclusions

- Do not assume hardware to be trustworthy
  - Instead, design a system to be tamper-resistant
- Use a combination of anti-tamper techniques
  - A hacker will search for the weakest link and exploit it

source: rocketgirlolutions.com
References

References, cont.

Acknowledgement

To Joe Grand for his course “Hands-on Hardware Hacking and Reverse Engineering” at Black Hat Europe 2015