

---

# Hardware Security

*The (slightly) more tactile side of security*

---

## Overview of Today's Lecture:

- Hardware vs. Software Security
- Attacks, Threats and Attackers
- Security Categories
- Examples

---

## Hardware Security vs. Security So Far:

- Different Landscape
  - Threats
  - Attackers
  - Attacks
- As important as software/network security

---

## Threat Vectors:

- *Interception*
  - Gain access to information without interfering with system
- *Interruption*
  - Prevention of system functionality
- *Modification*
  - Invasive tampering
- *Fabrication*
  - Counterfeiting

## Attackers:

*Class 0 – Script Kiddies*

*Class I – Clever Outsider*

- Intelligent, limited knowledge of target
- Usually through a known weakness

*Class II – Knowledgeable Insider*

- High-tech expertise
- Advanced tools and instruments

*Class III – Funded Organisation*

- Specialists with lots of funding
- Most advanced tools and analysis

---

## Attacks:

- *Insider Attack*
  - e.g. Laid-off employee
- *Lunchtime Attack*
  - Performed during a small window of opportunity
  - e.g. during coffee break
- *Focused Attack*
  - Plenty of time, money and resources

## Attacks:

- *Invasive Attacks*
  - e.g. Hardware reverse engineering
- *Semi-invasive Attacks*
  - e.g. Heating
- *Non-Invasive Attacks*
  - e.g. EM radiation observation



---

## Security Categories:

- Physical
- Logical
- Environmental
- Operational



---

## Physical Security:

### Tampering

*“An (physical) interference of a harmful nature”*

### Tamper Mechanisms:

- Strive to prevent an attempt by an attacker to perform unauthorised physical or electronic action



---

## Tamper Mechanisms:

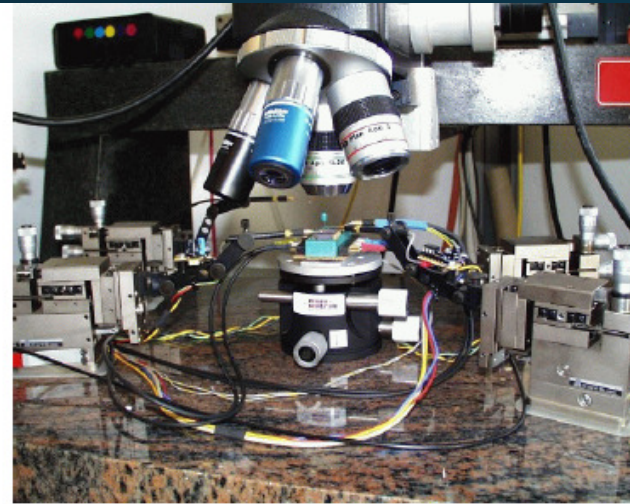
- *Tamper Resistance*
  - Special materials
- *Tamper Evidence*
  - Visible evidence left behind after tampering
- *Tamper Detection*
  - Hardware is aware of tampering
- *Tamper Response*
  - Countermeasures upon detection

## Physical Attacks:

- *Invasive*
  - Direct access to embedded components (e.g. cpu)
  - Micro probing, reverse engineering, memory readout techniques (e.g. freezing)
  - Require lot of time, knowledge and resources
- *Semi-invasive (integrated chip cards)*
  - UV lights, x-rays, laser, EM field, heating
  - Optical fault induction (SRAM illumination)
  - Low cost, easy reproduction on same target

## Physical Attacks:

Micro-probing station:



Modified Circuit:



*Source: Cambridge Security Lab*

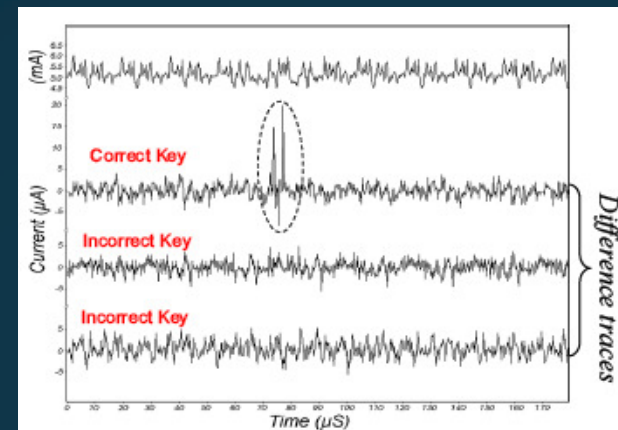
---

## Logical Security:

- Access Control
- Cryptographic Algorithms
- Cryptographic Protocols

## Logical Attacks:

- Non-Invasive
- No Physical Damage
- *Monitoring/Eavesdropping*
  - TEMPEST attacks
  - Side Channel Attacks
    - Timing Analysis
    - Power Analysis
    - Fault Analysis



---

## Logical Attacks:

- *Software Attacks – API*
  - No specialised equipment needed
  - Very fast

### Issues:

- Integrity of keys
- Function parameter checking
- Security policy enforcement

## Environmental Security:

- Device itself is the asset
- Goal – limit attacker’s possibilities by creating layers of hindrance (e.g. access)
- Administrative controls should be part of security policy



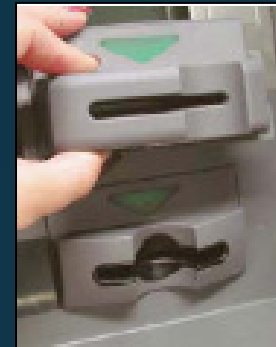


## Operational Security:

- Security risks related to operation of hardware
- Closely related to last week's lecture
- Example: ATMs

User's knowledge of:

- Real vs. Fake card reader
- Keypad operation
- PIN Safeguarding
- Latest attacks



## Hardware Security Modules:

- For secure generation and storage of crypto information
- Often physically tamper resistant
- Sometimes have H/W cryptographic acceleration
- Sometimes have special “trusted” peripherals  
(e.g. card readers, key pads, etc..)

### Example: Banks

- ATMs
- Pre-payment electricity meters



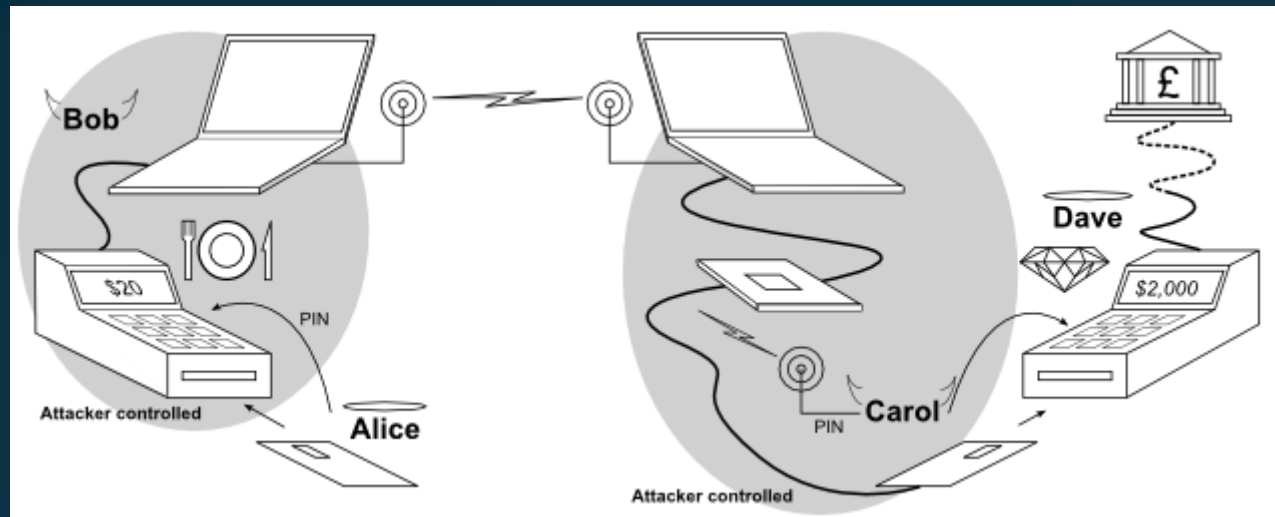
## Examples:



- Credit Cards
  - Magnetic Stripes
  - Chip & PIN
  - RFID (Radio Frequency Identification)

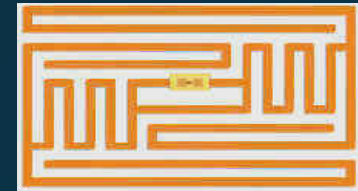
## Examples:

### Chip & PIN relay attack:



Source: Cambridge Security Lab

## Examples:



### *RFID – Radio Frequency Identification*

- Originally developed as the “Barcode of the future”
- Now used as
  - Inventory control
  - Logistics and supply chain management
  - Physical access cards
  - Payment
    - Motorway charges
    - Gas stations
    - Small items in shop

---

## Examples:

### Future:

- Embedded in all kinds of devices
  - From clothing, to all products we buy
- e.g. Milk that will tell fridge when it is expired

### Issues:

- Privacy
- Security – RFID was not designed with security in mind!!

## Examples:

- Susceptible to Power Analysis attacks
- Can be susceptible to Cloning attacks
- Susceptible to Relay attacks

“Is your cat infected with a computer virus?”



---

## Remember:

- H/W security as important as other security aspects
- H/W security devices do not solve security
- Many attacks exist
- Many more problems are on the way
- Because – Security added as an afterthought