Physical Tamper Resistance
Chapter 16
Ziv Klein
Crypto-Processors

- Processors designed to perform cryptographic operations.
- By nature, such processors contain sensitive information.
- If an attacker gains direct physical access to a processor while it is working, or a memory component it uses, he can easily read its contents.
Why We Need Tamper Resistance

• Many applications require the processor to be in the hands of a possible attacker.
  • Accessory Control
  • Smartcards
• Even in less exposed system, such as a bank server in a secure room, the sensitive data must be protected from the maintenance crew.
• For these reasons, cryptoprocessors need some kind of built-in defense mechanism.
Tamper Resistance - Definition

• Tamper resistance is protecting a product or device from anyone with physical access to it against:
  • Being altered or modified,
  • Being studied or reverse-engineered,
  • Extraction of information from it.

• This includes actual resistance, as well as detection, response and evidence.
A Naïve Approach

- The simplest technique is to prevent physical access to the whole circuit by some kind of casting.
- When the device is opened for maintenance, it automatically zeroes the key memory.
- This solution is only applicable in a system such as a bank server, where the keys can be kept somewhere else and loaded back after maintenance.
  - As we’ll see, it does not matter since this approach has many flaws.
How To Hack a Cryptoprocessor

• A maintenance engineer can disable the zeroing mechanism after opening the device. Then, on the next visit, he can open the processor and read the key right from the memory.
• To prevent this, the core of the processor is potted into a solid block. The secrets (usually cryptographic keys) are stored in a special key memory in the core.
  • This prevents accessing the key memory as well as putting probes on the BUS lines.
• However, the potting can usually be scraped or cut off.
• The answer is to make the potting itself tamper-detecting. The secrets will be erased when penetrated.
• A harder metal shield can be added outside, so that breaking the shield would also break the tamper-sensing layer and zero the memory.
Memory Remanence

• When the same data is stored in memory for a long time, it can sometimes be recovered even after being erased.
  • Good devices have “RAM savers” that move the data around so it will not be burned in.
• Memory can also be frozen by low temperatures. So an attacker can freeze the device, cut through the tamper-sensing material and extract the RAM.
  • Temperature sensors can be installed to prevent this.
  • Some memory components have worse remanence, even in room temperature.
  • Also, shipping such devices is complicated since they can not be exposed to cold temperatures.
Side Channel Attacks

- Side channel attacks can also be used, as was discussed in a previous lecture.
- Devices sometimes have aluminium shielding to block radiation.
- Other forms of side channel attacks are a significant threat but will not be discussed.
Evaluation

• IBM proposed the following classification of attackers:
  • Class 1 – clever outsiders
  • Class 2 – knowledgeable insiders
  • Class 3 – funded organizations
• This classification is becoming a bit outdated as class 1 attackers gain access to expensive class 3 tools.
• Device manufacturers should decide what threats they intend to protect their product against.
Evaluation (2)

• The US government develops security standards (FIPS 140), so that devices could be evaluated by certified labs.

• The standard has 4 evaluation levels, with a large gap between levels 3 and 4 – level 3 devices can sometimes be broken by class 1 attackers while level 4 is expected to keep out class 3 attackers.

• The evaluation does not cover every attack vector, only physical tamper, and a certified device could still be vulnerable to API attacks, etc.
Dallas 5000

- A medium security (and price) processor.
- Has a unique feature – *bus encryption*. It can use an external, unsecure memory and encrypts all data it stores on it on the fly.
- It’s early version could be attacked a *cipher instruction search attack*.
- This is a good example of an unexpected problem that comes up when implementing a new concept.
Smartcard

• A self-contained microcontroller, with a microprocessor and memory integrated in a single chip.
• Used in pay-tv and mobile phones.
• Can be easily and cheaply replaced, without replacing the whole product.
• Has a very limited memory.
Until around 1995, there was no demand for security, and everyone relied on their small size and rarity of tools for security.

Satellite TV changed this – as it broadcasted across large areas, and sold large amounts of card with the keys to decipher the channels.

As soon as the broadcasts of ‘Star Trek’, which people around Europe picked up from UK satellites, has been encrypted – a black market of TV-cards was created.
How To Hack a Smartcard

• The easiest attacks were on the protocols being used – blocking messages from going into the card to cancel the subscription when it is over.
  • This was also a problem with phone cards.
• Another attack is to slow the card’s execution, since the card gets a clock from the outside. Then the memory can be read using an electron microscope.
  • It can be prevented by detecting low frequencies and reset the card
  • This can result in false alarms (especially with cheap card readers) and so OEMs would sometimes disable this feature.
How To Hack a Smartcard (2)

- Another attack was probing the bus lines with second-hand testing equipment. This way, the operations being processed are discovered and with it the key.
  - A defense was loading the cards with multiple keys, and changing the key used as soon as pirates found the current one.
  - Probing became harder as the device’s size shrank.

- Power analysis is also possible.
Designing a Smartcard-Based System

• Defense in Depth – used by TV companies, this method is based on using non-standard processors with custom instruction sets and algorithms.

• This makes hacking the system expensive and time consuming, and combined with other methods and legal actions, unprofitable.

• Stop Loss – making sure that a successful attack on one card will not result in a great loss.
• Trusted Interface – a tamper resistance processor does no good if you can’t trust the machine it’s installed in.
  • This is a problem with systems that need authentication.
• The Market for Lemons in evaluation – firms looking to evaluate their product have no incentive to seek trustworthy evaluation rather than an easy one.
Problem (2)

- Security by Obscurity – companies tend to rely on the secrecy of the design.
- Politics – can affect the market unexpectedly.
  - Using smartcard for signing instead of PDAs.
- Function Creep – added functionality undermine the initial design assumptions.
Summary

• Tamper resistance is a relatively successful field.
• There are many solutions, at a variety of prices.
• Tamper resistance often fails because of API related issues, or side channel attacks.
• Politics and bad incentives are a big problem.