PHYSICAL TAMPER RESISTANCE
CHAPTER 16

DANNY MEDAN
What is Tampering?

“To meddle, especially for the purpose of altering, damaging, or misusing”
- Dictionary.com

• Read restricted data
• Change software
• Reverse engineering
• Piracy
TYPES OF TAMPER SECURITY

- Seals
- Stickers / Tape
- Traps
Make tampering your system not worthwhile

- Expensive
- Complicated
- Time consuming
- Special Tools
- Little reward

TYPES OF TAMPER SECURITY

- Tamper Evident
- Tamper Resistant
- Tamper detection
- Tamper Response
TYPES OF TAMPER SECURITY

- Tamper Evident
- Tamper Resistant
- Tamper detection
- Tamper Response
- Tamper Proof
TAMPER EVIDENT DEVICES

When the seal is cut the diagonal lines make it difficult to realign the seam of the package.
BYPASSING TAMPER EVIDENT DEVICES

https://youtu.be/80MM1guWnQk
HARDWARE SECURITY MODELS

“...microcomputers encased in robust metal enclosures, with encryption hardware and special key memory, static RAM which is zeroized if the enclosure is opened.” – Anderson (Security Engineering)

Used to provide crypto-processing and to safeguard and manage digital keys for strong authentication
HSM EVALUATION – ATTACKERS CLASSIFICATION

CLEVER OUTSIDERS
- Intelligent but may have little knowledge of the system
- Have access to moderately sophisticated equipment
- Will try to take advantage of an existing weakness in the system, rather than try to create new ones

KNOWLEDGEABLE INSIDERS
- Have substantial technical education and experience
- Varying degrees of understanding of parts of the system but potential access to most of it
- Often have very sophisticated tools and instruments for analysis

FUNDED ORGANIZATIONS
- Able to assemble teams of specialists
- Capable of in-depth analysis of the system, designing sophisticated attacks and using advanced analysis tools.
- May use knowledgeable insiders as part of the attack team
# HACKING THE HSM

<table>
<thead>
<tr>
<th>Hack</th>
<th>Solution</th>
<th>Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steal the keys</td>
<td>Shared control – split the master key</td>
<td>Senior managers thought typing was “women’s work” and just handed their keys to the engineer</td>
</tr>
<tr>
<td>Disable sensors on one visit and extract keys on the next</td>
<td>Separate all parts that need service from the core of the device which would force the engineer to drill/cut into the device – which would then alert the guard overseeing them</td>
<td>Although guards were often present during maintenance, they had no real way of differentiating between servicing and attacking</td>
</tr>
<tr>
<td>Memory remanence</td>
<td>Update your system and / or security keys</td>
<td>---</td>
</tr>
</tbody>
</table>
SMART CARDS
WHAT IS A SMART CARD?

A physical electronic authorization device, used to control access to a resource

• Contains microprocessor and memory
• Easily produced and replaced
• Has limited memory storage
SMART CARDS – EARLY HISTORY

- Earliest version developed in 1959 (!)
- Used as Subscriber Identity Module (SIM) cards during the late 1980’s
- Up to this point the small size and relative obscurity of the design were enough to ward off most attackers
- As long as smart cards were only used as SIMs, there was very little reward from hacking them
- Started being used as satellite TV subscriber cards in the late 80’s
- When satellite-dishes became cheaper to buy and install, satellite TV began broadcasting encrypted feeds, with the decryption keys stored on the subscriber smart cards
- European ‘pirates’ copied and sold other countries’ TV subscription cards to bypass geo-blocking
MODERN CARD TAMPERING

- EMV Cards are an obvious target to tampering, from harvesting cards information to stealing cards and bypassing PIN protection
- Rewriting terminals to present transaction value while charging a higher amount
- Man-in-the-middle devices charge stolen cards by returning True to any PIN entered in the authentication phase
- Overlay SIMs enable data roaming and bypassing network restrictions on mobile phones
- Can be used to attack EMV technology
- Market for lemons
SONY PLAYSTATION

• Sony PlayStation was released when home CD-ROM burning was starting to become mainstream

• Sony’s main concerns were DRM (Digital Rights Management) and region locking
SONY’S SECRET PROTECTION

https://youtu.be/2TnK8vyPUZI?t=62
“Wobble Groove” Protection

- CD readers can read “wobbly” disks without much difficulty
- CDs have a Lead-IN area, which holds information about the disk
- Sony’s CDs were burned using special hardware, which shifted while burning specific code words in the Lead-IN area.
- These code words indicated which region the game belongs to (Asia, Europe, North America)
- When the PlayStation starts playing a CD, it looks for the wobbly word in the Lead-IN area
- If the PlayStation did not detect the “wobble”, if the device’s region code did not match the CD’s code, or if the CD didn’t have a region code altogether, the PlayStation would not read the data on the disk
WHY THIS WORKED

• The information stored in the Lead-IN area isn’t copied when burning a disc

• Standard market CD burners could not be easily programmed to perform the “wobble groove”

• This also prevented imported games from playing, as they were treated the same as pirated copies
A simple ModChip could be added to the system which would detect the “wobble groove” scan. It would then block the failed authentication check and send out the relevant region’s codeword, enabling the PlayStation to run both pirated AND imported games.
THE SALVAGE ATTEMPT

• Sony implemented more hardware DRM checks on their later versions of the PlayStation – which the Modding community quickly bypassed.

• Game developers had to implement software DRM protection as well.

• Some had more clever approaches than others.
SPYRO — YEAR OF THE DRAGON

IF YOU CAN’T BEAT THEM, TRICK THEM

• PAL copies of the game will switch between English, French, German, Spanish and Italian.
• The ability to Pause will be removed.
• Collected items will disappear from the inventory.
BIBLIOGRAPHY

- Security Engineering, Ross Anderson (Third Edition)
- Wikipedia
- Ross Anderson Interview
- Introduction to Tamper Evident Devices, datagram
- Security Offense and Defense Strategies: Video-Game Consoles Architecture Under Microscope, Renard, Benadjila
- How the Sony PlayStation Was Hacked, Littrell