

Physical Tamper Resistance

(Ross Anderson's book "Security Engineering" - Chapter 16)

Tamper: VERB

(tamper with)

Interfere with (something) in order to cause damage or make unauthorized alterations.

someone tampered with the brakes of my ~~car~~ biometric database.

-Oxford Dictionary

Computer Security Seminar

Presenter: Asaf Shamir

19/04/2016

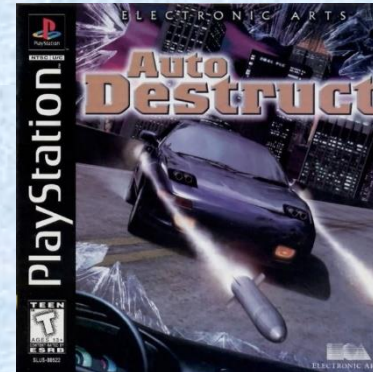
What is “Physical Tamper Resistance”?

The resistance to tampering (intentional malfunction or sabotage) by either normal users of a product or others with physical access to it.

Physical access is unavoidable – **When thinking about computer security always keep in mind that hardware security is a serious issue.**

Once an attacker gains physical access, they can

- modify the product.
- reverse-engineer the product.
- extract information from the product.



A brief history

The use of tamper resistance dates back before modern computers:



Problems:

- Those mechanisms depended on the vigilance of the operator.
- Surprise attacks and espionage often resulted in capturing key material before it was destroyed.
- Due to their valuable nature, products were sometimes sold to attackers.

A brief history

(The sequel)

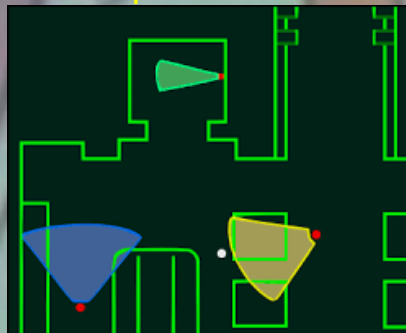
To prevent those problems, engineers paid more attention to protecting keys in transit, and reducing the value of key material.

This led to a more general view on tamper resistant devices:

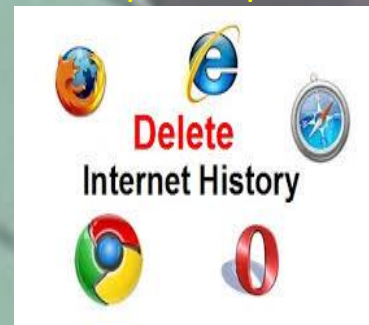
Tamper resistance



Tamper detection



Tamper response



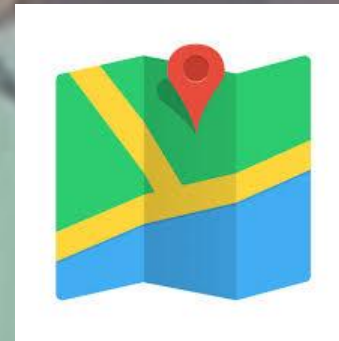
Tamper evidence



A brief history

(It's a trilogy)

The spread of multi-user OS and the regularity with which bugs were found in their protection mechanisms meant that large numbers of people might potentially have access to the data being processed.



The general approach in the early 1980s was that the level of protection available from commercial OS was likely to remain insufficient.

The attackers

Serious tamper resistance emerged out of an arms race between firms that wanted to lock down their products, and others who wanted to unlock them.

There are several different types of attackers that use physical tampering methods:

Lawyers



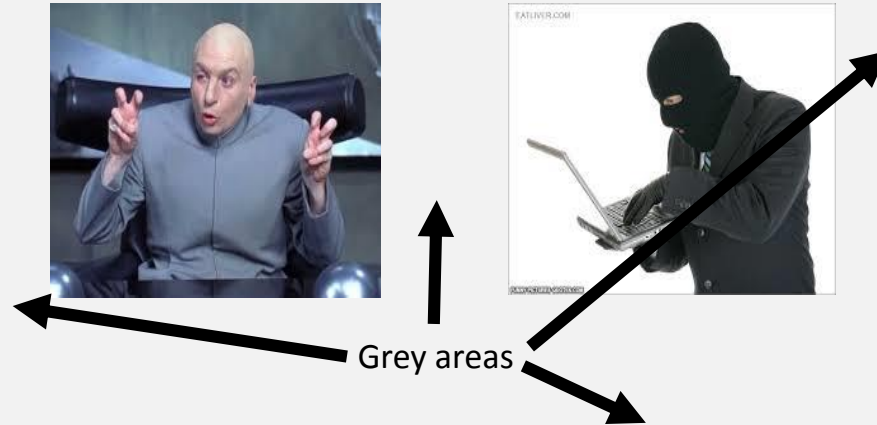
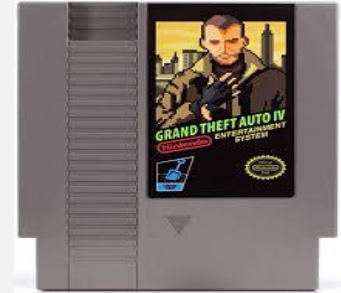
Academics



Criminals



Big companies

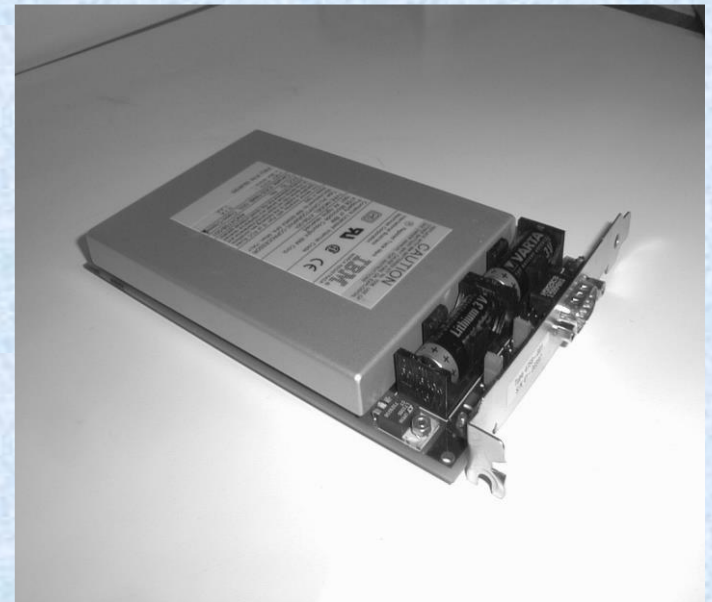


Crypto-processors

Processors that contain sensitive information and are designed to perform cryptographic operations.

The IBM 4758

- The first commercially available processor to have been successfully evaluated the highest level of tamper resistance.
- There is extensive literature about it.
- It was the highest profile target in the world of tamper resistance.



IBM 4758

The IBM 4758 was basically a closed metal box with a micro-computer with encryption hardware with static RAM designed to be zeroized when the enclosure was opened



והם חיו באושר ועושר, עד עצם היום הזה.

Hacking a crypto-processor (1)

There are many methods to hacking a crypto-processor, such as:

1. **Steal the keys** – In early banking security models, the keys were on PROMs or in plaintext, both can easily be stolen.

A possible solution is to have shared control, multiple keys kept in different places under different departments.

2. **Cutting through the casing** – Early devices were vulnerable to attackers cutting the casing.

A possible solution is adding more sensors (tilt, light, etc...) or, even better, separating the different components of the system (such as batteries) from the core.

3. **Planting a probe** – With access to the core, an attacker can plant a probe and monitor the information directly.

A possible solution is adding more sensors to the core.

Hacking a crypto-processor (2)

- 4. **Memory remanence** – Many types of memories leave tracks of the information they held, even after deletion.



A possible solution is using memory components that move the data around.

- 5. **Freezing** – Cold temperatures can prevent the degradation of the information on static RAM.

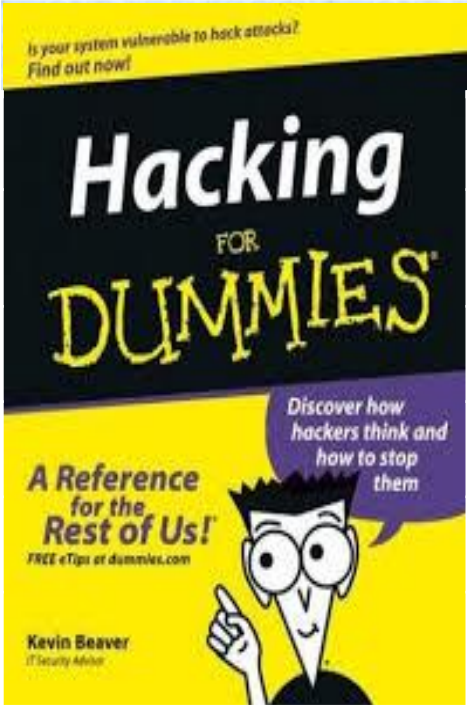
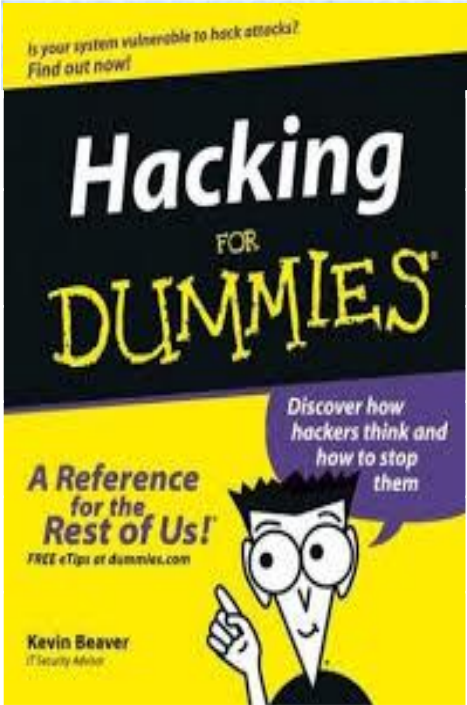
A possible solution is adding a cooling system to the processor.

- 6. **Monitoring** – The signals emitted by the device can be monitored, and signals can be injected into the device.
- A possible solution is plating the device with aluminum and using conductors to change the emission pattern.



The signals emitted by the device can be monitored, and signals can be injected into the device. A possible solution is plating the device with aluminum and using conductors to change the emission pattern.

Hacking a crypto-processor (3)

<u>Hacking method</u>		<u>Proposed solution</u>
Steal the keys.		Shared control
Cutting through the casing.		More sensors/separating components
Planting a probe		Sensors on the core
Memory remanence		Move the data around
freezing		More sensors
Monitoring/injecting signals		Aluminum shielding

The majority of these solutions might work only if a professional, alert, and trustworthy employee is in charge of any physical access to the device.

Evaluation (1)

IBM evaluated the level of tamper resistance in a device by classifying the level of the attacks it can withstand.

According to the proposed scale, there are 3 types of attackers:

Clever outsiders



Knowledgeable insiders



Funded organizations



Evaluation (2)

- The classification became a bit outdated, as the classes' properties are merging.
- There is a new classification scheme, licensed by the U.S. government – the FIPS 140 (Federal Information Processing Standards).
- FIPS 140 have 4 levels of security.
- **It's best to check the threats that each specific device have and evaluate accordingly (Common Criteria).**

Medium Security Processors

The crypto-processor is a strong machine, but it is relatively large and expensive (~60,500,000 ريال).

Not all services require the high security levels that the crypto-processor provides, but rather put more emphasis on cost, size and speed.

We will briefly speak of two available small-medium security processors that meet these requirements:

- The iButton
- The smartcard

iButton

The iButton was designed to be a minimal, self-contained cryptographic processor for a variety of applications.

It contains:

- A microcontroller
- Static RAM for keys and software
- A clock
- Tamper sensors
- A lithium battery

Early applications included:



Smart cards

- The most common secure processors.
- Used in various applications.
- Have a wide range of capabilities.
- Very cheap (~1\$).

The smart cards were hacked mostly thanks to the efforts of Kirk & Spock.



Smart cards (2)

(The hack awakens)

1. Earliest hacking methods targeted the protocol the cards used.
2. Physical or optical probing.
3. There are other methods.



Don't forget the protective mesh



Things aren't perfect (yet) (1)

The Trusted Interface Problem:

A tamper resistant processor can be compromised by the environment.



Conflicts:

We have to consider what happens in a situation where different parties try to attack each-other.



Things aren't perfect (yet) (2)

The Lemon Market:

- A growing market for smaller security products.
- The evaluation problem.
- Responsibility dumping.



Security-By-Obscurity:

Most companies are still reluctant to give their products a hard challenge and “risk” the need to improve the product.



Things aren't perfect (yet) (3)

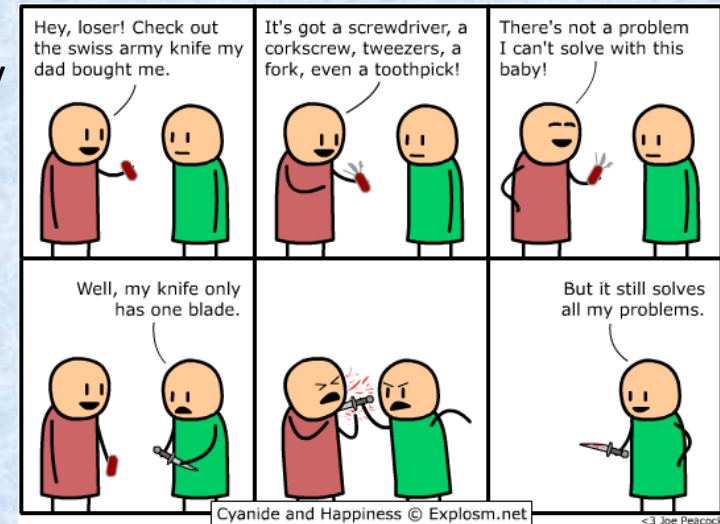
Interaction With Policy:

Regional laws and politics affect the industry in various ways, not all are for the best.



Function Creep:

A change in the environment and functionality might reduce the level of physical tamper resistance of existing products.



Summary

- The field of physical tamper resistance is one that keeps evolving as end-users get increasingly more access to different crypto-based devices.
- It is very important to remember the physical vulnerability of the device, and not to rely only on software level protection.
- Even in regards to the more secure devices, the main obstacle on the way to a better physical tamper resistance remains the human factor.
- The subject of physical tamper resistance still receives less public attention than others in the field of computer security, and until it will, most of the manufacturers will probably choose to produce devices that are more vulnerable to physical tampering.

Questions?

