

A detailed technical diagram of a telescope mechanism, likely from a historical document. The diagram shows a large circular structure with various components labeled in English. Labels include 'LOUVER', 'UPPER CURTAIN', 'UPPER POSITION OF MOUNT', 'SHUTTERS', 'LOWER CURTAIN', 'PARRY PLATFORM', 'SPECTROGRAPH BODY', 'ELEVATING PLATFORMS', 'OBSERVING FLOOR', 'STAIRS', 'TURNING CABLE GUARD', '30 FT. 3 IN. RADIUS OF BAIL', '62" TELESCOPE', 'RAIL', 'CABLES', 'TRACK', 'LOWER POSITION OF COUNTERWEIGHTS', and 'PARRY'. The diagram is a cross-section or side view of the telescope, showing its internal structure and mounting.

Computer System Security CS3312

计算机系统安全

2024年 春季学期

主讲教师：张媛媛 副教授

上海交通大学 计算机科学与技术系

第十四章

系统安全：硬件攻击

System Security: Physical Attacks



目录/CONTENTS

01. 物理攻击

Physical attacks

02. 冷冻攻击

Cold-boot attack

03. 总线攻击

DMA attack

04. 其他攻击

Other attacks

05. 硬件安全模块

Hardware security module (HSM)

●—————

物

01

理

攻

击

—————●

P h y s i c a l A t t a c k s



物理攻击的主要手段

- 侧信道攻击
 - A door with a highly secure lock does little good if the door can be removed by unscrewing its hinges.
 - 系统组件行为模式泄漏——Cache读取模式暴露数据访问行为
 - 物理信息泄露——智能卡执行密码算法时的能量、电磁辐射、时间等信息暴露内部计算行为
- Eavesdropping
 - Wiretapping
 - Hardware key loggers
- Counterfeiting （下一页视频）
 - Message injection
 - Radio jamming

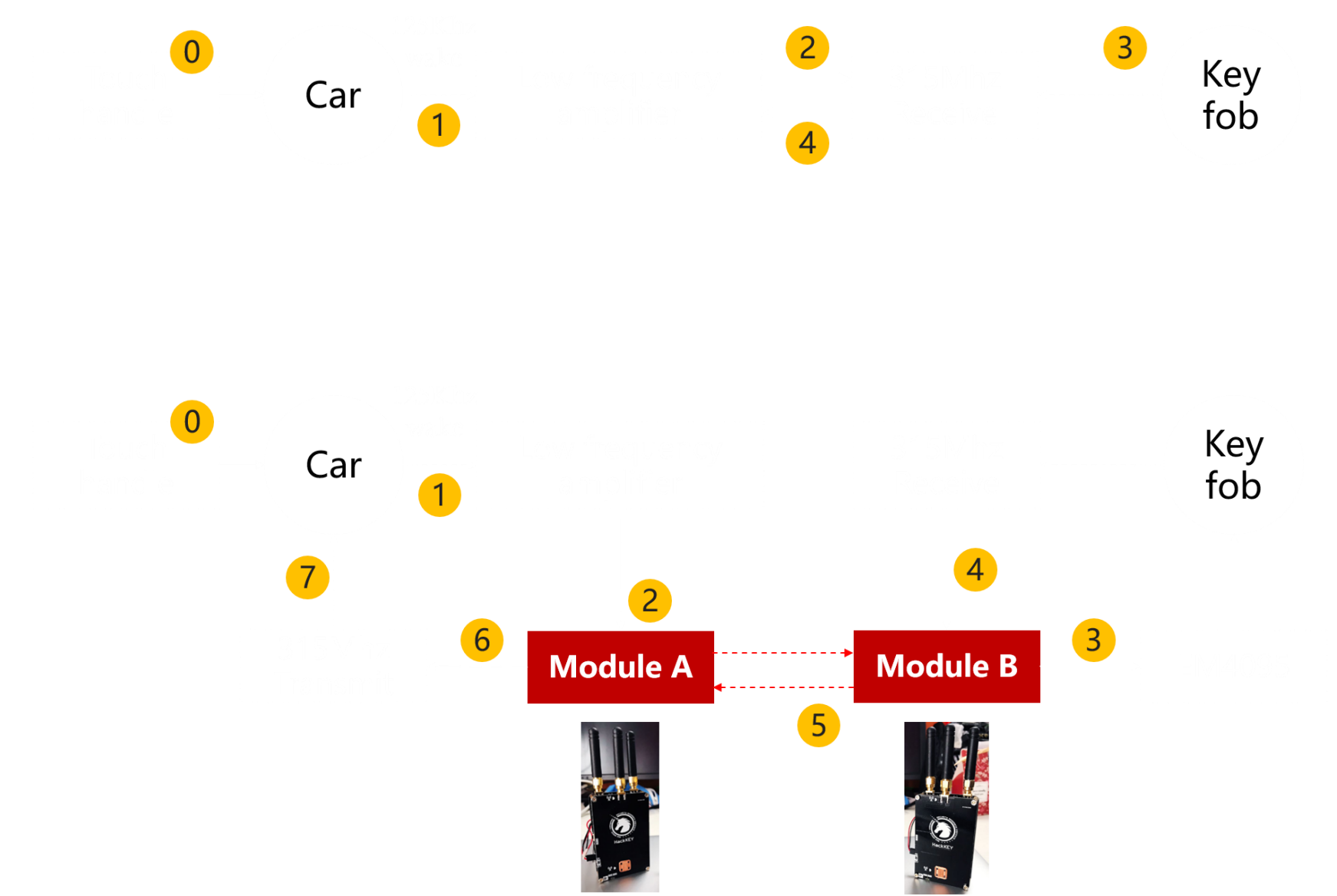
栗子: hacking a car key fob

JUST A PAIR OF THESE \$11
RADIO GADGETS CAN STEAL A
CAR



QIHOO 360 TEAM UNICORN





针对计算机系统的硬件攻击

攻击目标：计算机系统代码和数据

存放在哪里？

Memory (in which the data resides / data-at-rest)

Bus (through which the data transfers / data-in-transfer)

因此，针对计算机系统的硬件攻击主要有两个攻击客体：

against memory: Cold-boot attack

against bus: DMA attack

●—————●

冷

02

冻


攻

击

—————●

C o l d - b o o t A t t a c k

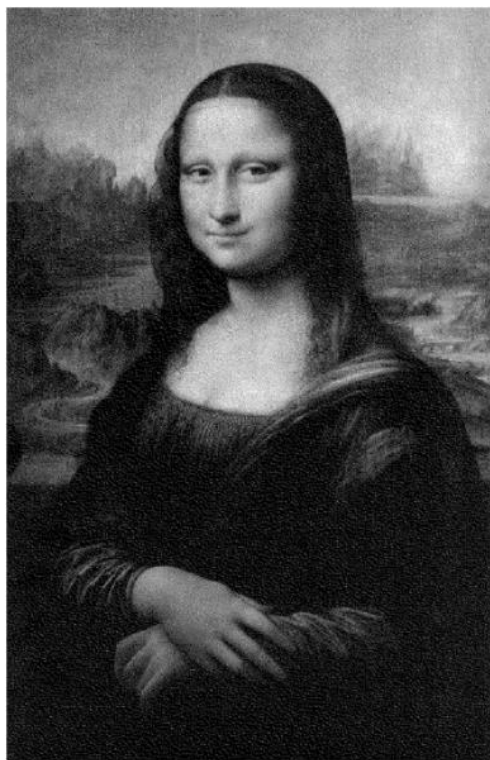




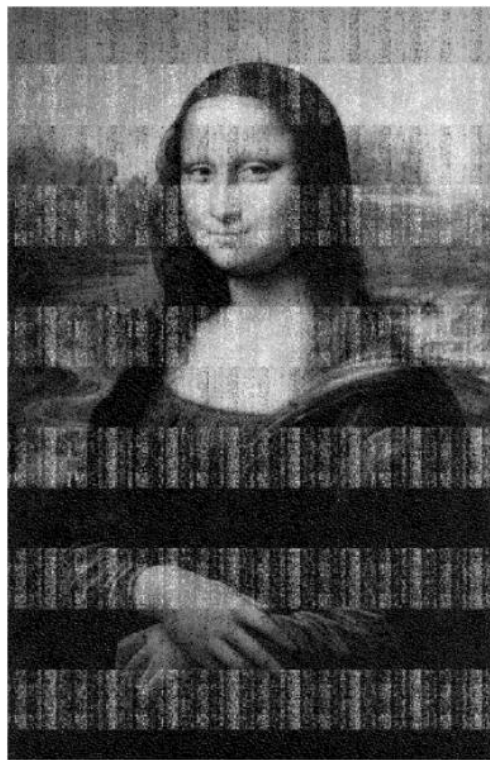
2008年初,普林斯顿大学电子前沿基金会和温瑞尔系统公司的研究人员联合发表了一篇题为《鲜为人知的秘密：对密钥的冷启动攻击》[\[1\]](#)的文章，该文详解了从运行系统获取内存信息的一种新型攻击方式。

[1] Lest We Remember: Cold Boot Attacks on Encryption Keys, in Proc. 17th USENIX Security Symposium (Sec '08), San Jose, CA, July 2008.

冷冻后内存数据残留



5s



30s



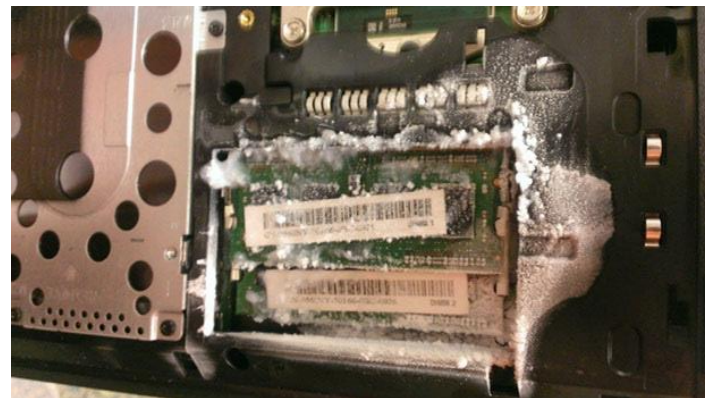
60s



5 mins

冷冻攻击原理

这种攻击利用了DRAM和SRAM内存部件中一个物理特性。数据在这些部件中有一个data remanence的特点（即，掉电几秒钟甚至几分钟内，memory栅格中的电平状态仍然存在，就是说数据还存在，利用硬件探针和使用一些技巧是可以拿出来的。）
这类攻击的着眼点是存储器硬件的器件特性，而非软件安全问题。



接入新系统中启动过程会覆盖部分代码，不能启动为原有操作系统状态，可使用专门工具将内存数据dump出来，进行分析



总

线

03

攻

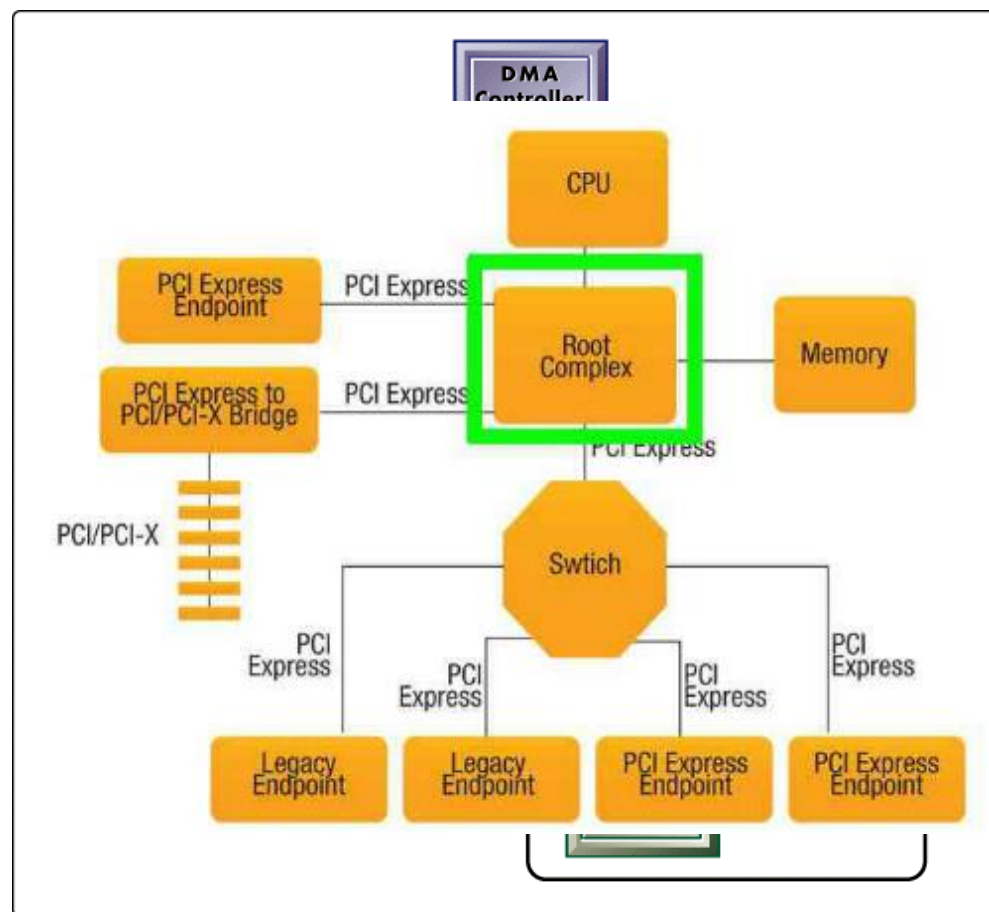
击





DMA

- DMA
 - Direct Memory Access
- 将传送到模块的信息复制到内存 (RAM), 并允许已处理的信息自动从内存移到外部外围装置。所有这些工作皆独立于目前的CPU活动。

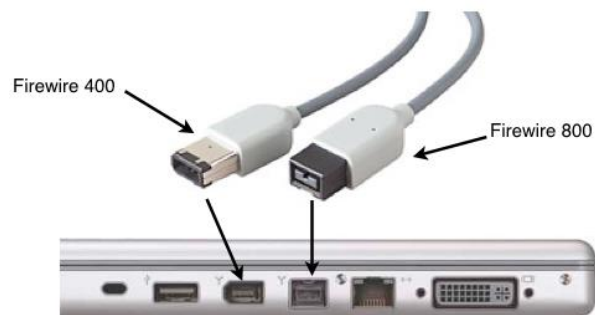


DMA攻击

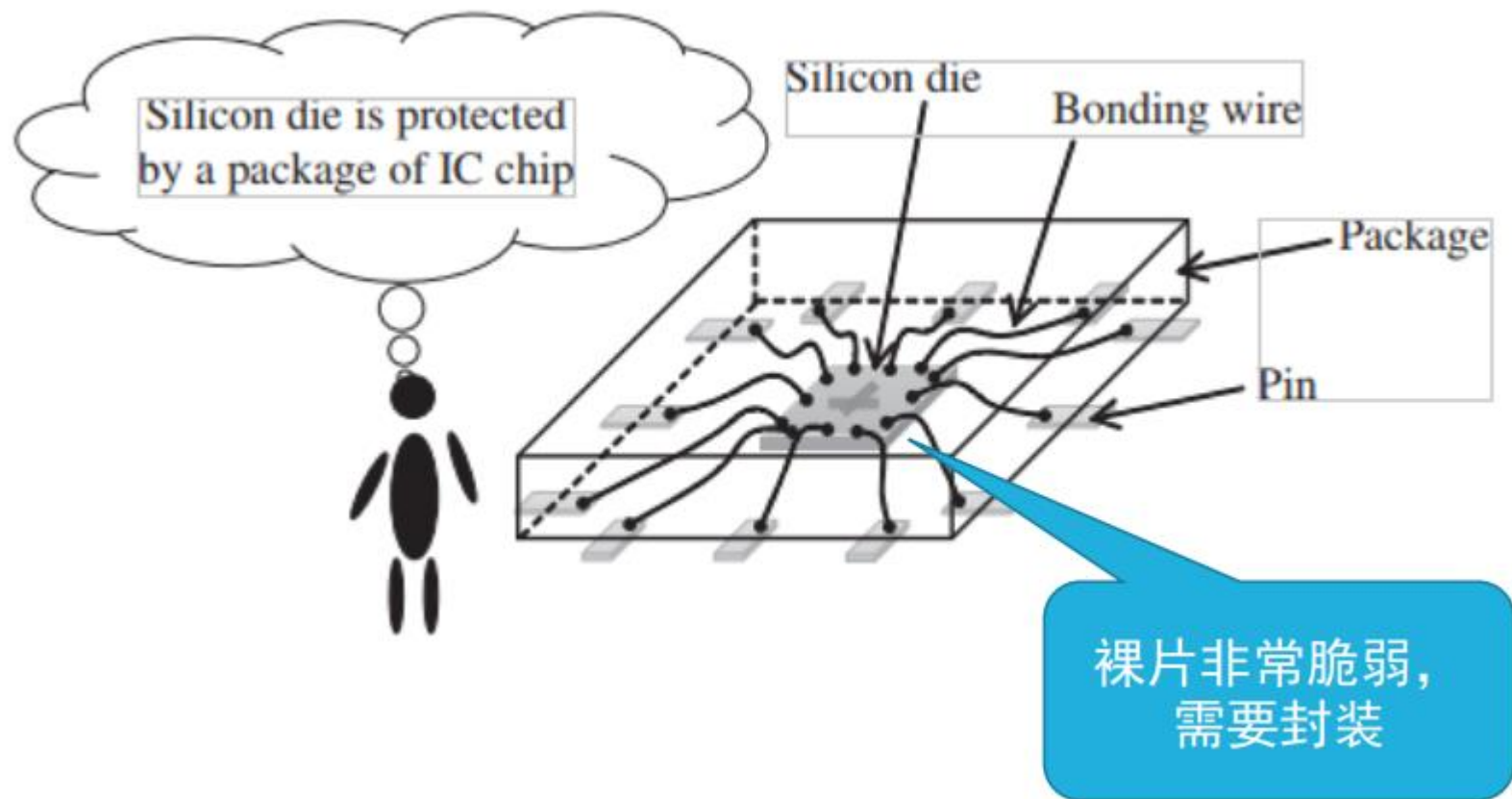
实施总线偷听攻击，攻击者可通过DMA通道直接访问小于4G物理内存（覆盖敏感数据的几率非常大）。

典型案例：

- 火线(Apple Firewire)攻击
- Thunderbolt攻击
- PCIe总线攻击



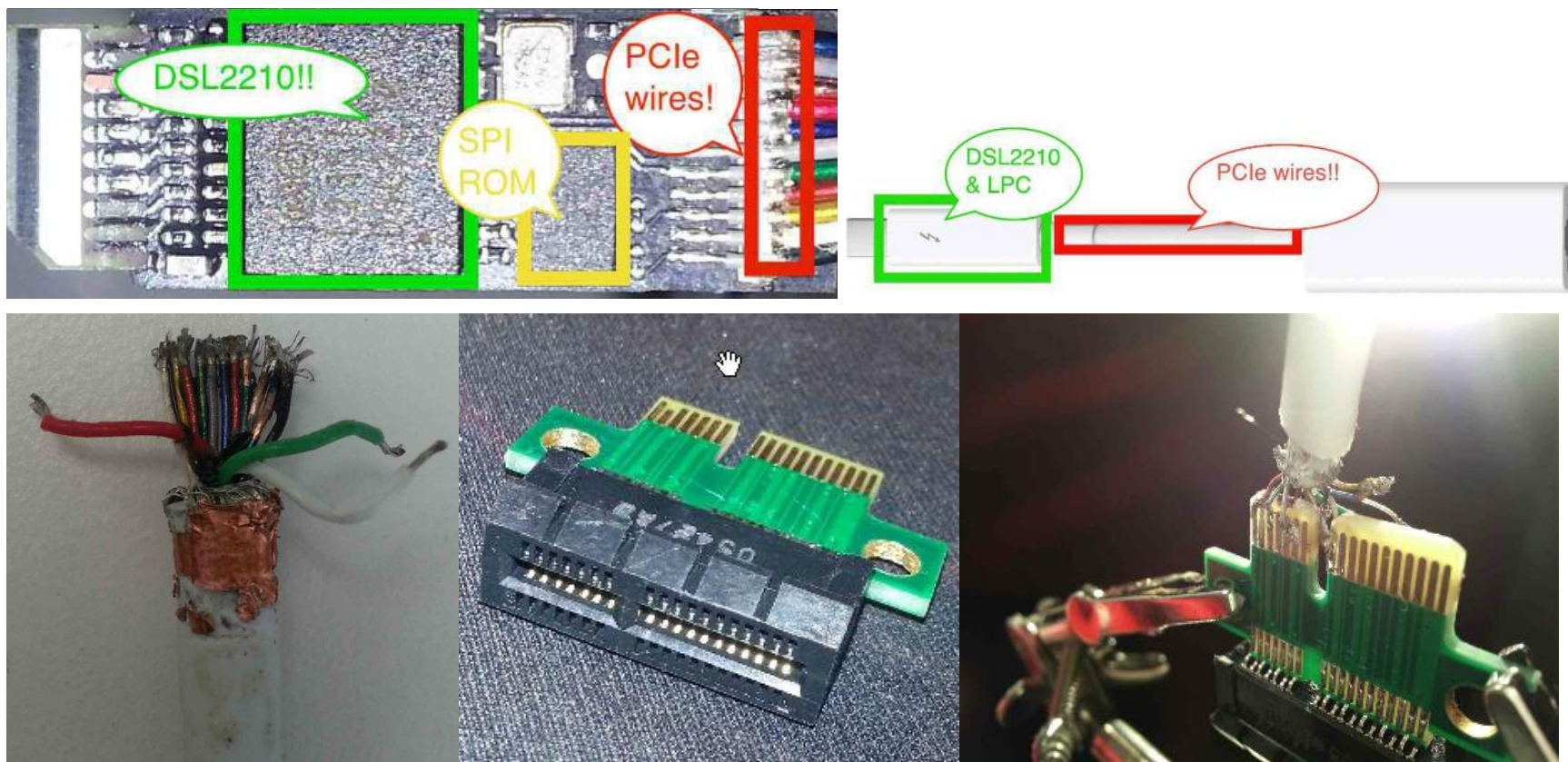
一个集成电路芯片



攻击分类

- 侵入式
 - 通过特殊工具对设备进行物理篡改，打开封装package直接访问芯片表面
 - 例如，解开智能卡保护层，直接在数据总线上搭线，观察数据传输
- 半侵入式
 - 打开封装package，访问表面，但不去改钝化层，也就是对金属表面不上电
- 非侵入式
 - 只利用暴露在外部的可用信息，如运行时间、电磁辐射、能量消耗等

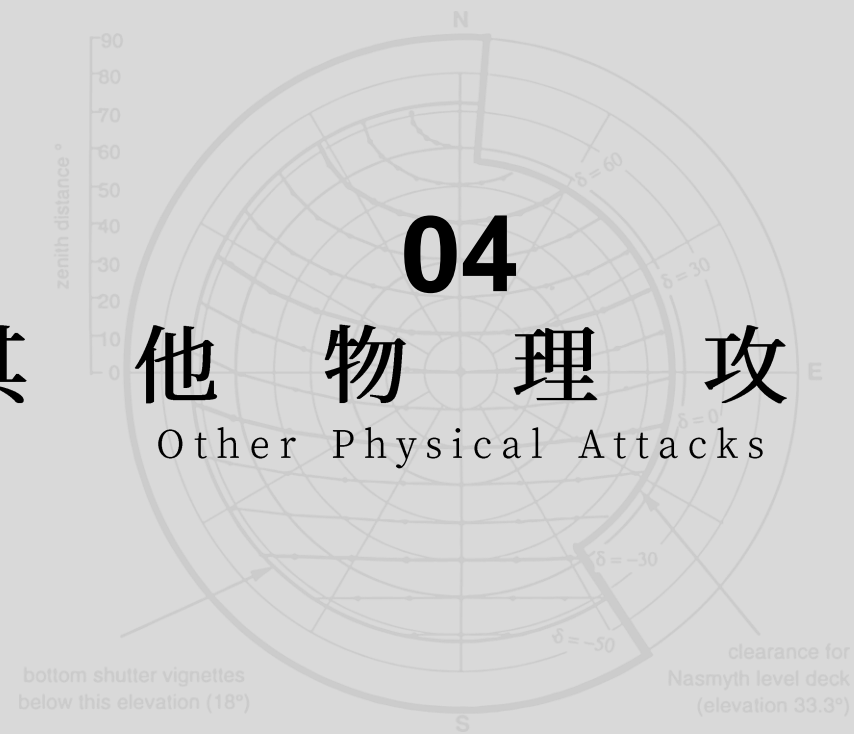
范例：Russ Sevinsky的攻击 Thunderbolt DMA



04

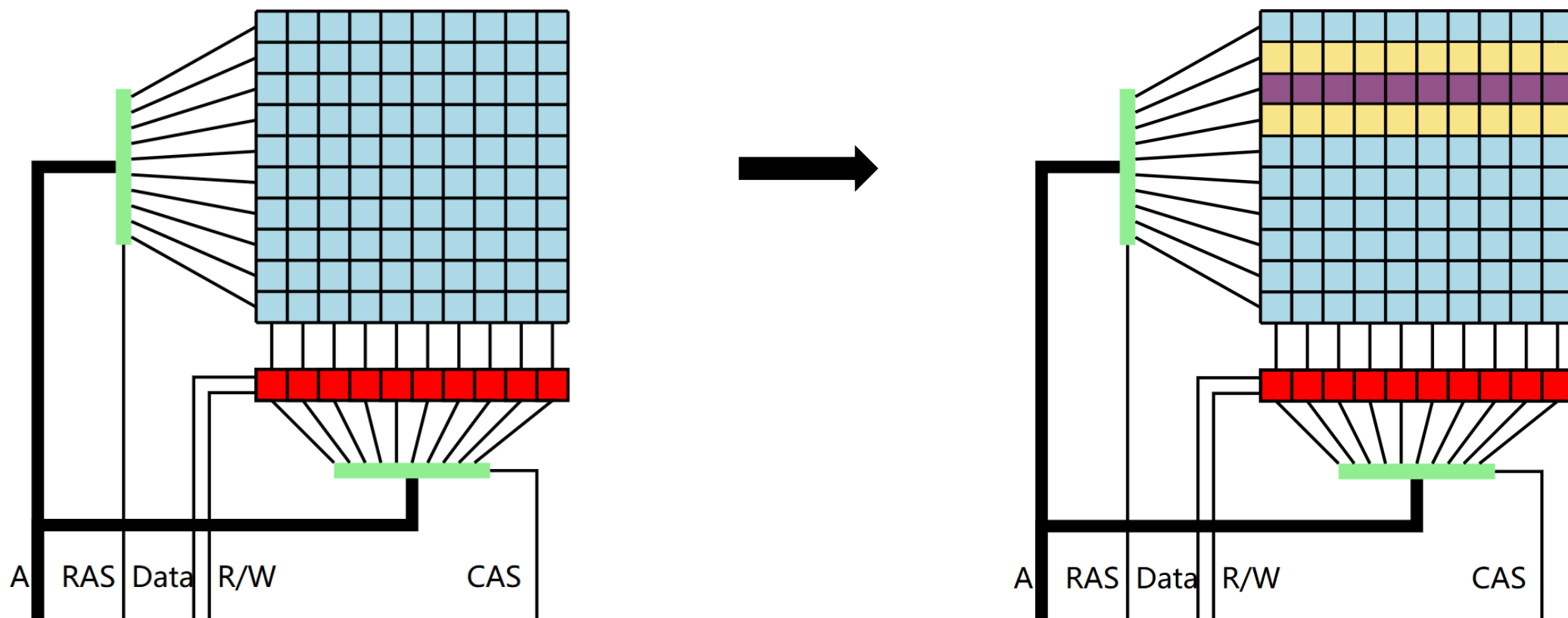
其他物理攻击

Other Physical Attacks



Rowhammer

今天的DRAM单元为了让内存容量更大，所以在物理密度上更紧凑，但这样很难阻止临近的内存单元之间的电子上的互相影响，在足够多的访问次数后可以让某个单元的值从1变成0，或者相反。



Rowhammer

Rowhammer Attack

Presented by: Google Project Zero, Mark Seaborn and Thomas Dullien

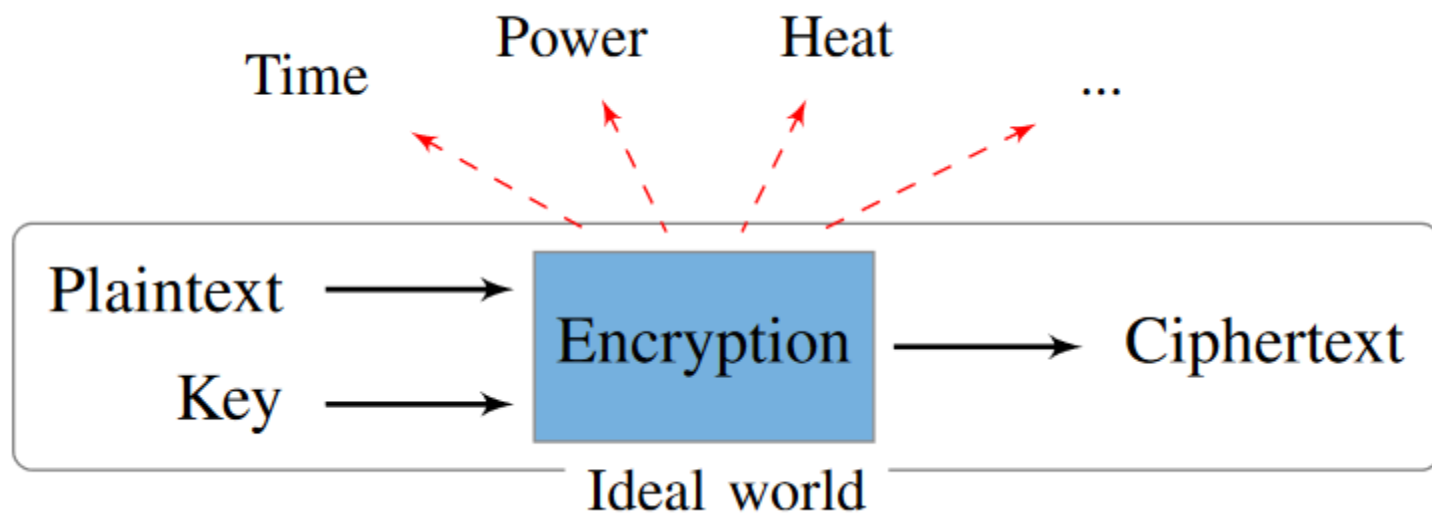
Bit-flip in physical memory

在x86-64的GNU/Linux平台上利用这个漏洞通过CLFLUSH指令和PET的某一位的变化(比如0到1)直接获得内核权限

研究人员认为在其他的硬件架构和操作系统上也有类似的方法可以达到这一目的，解决这个漏洞的修复可能需要BIOS更新针对内存控制器部分的操作。

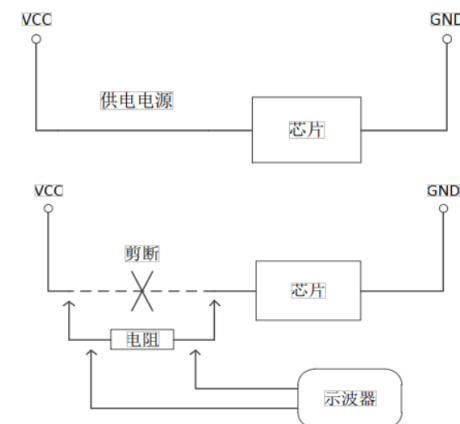
侧信道攻击

The implementation produces unintended output as a byproduct



侧信道攻击

- 侵入式
 - 通过特殊工具对设备进行物理篡改，打开封装package直接访问芯片表面
 - 例如，解开智能卡保护层，直接在数据总线上搭线，观察数据传输
- 半侵入式
 - 打开封装package，访问表面，但不去改钝化层，也就是对金属表面不上电
- 非侵入式——侧信道攻击
 - 只利用暴露在外部的可用信息，如运行时间、电磁辐射、能量消耗等
 - 计时攻击——操作数对运算执行的时间产生影响，如大数乘法耗时更久
 - 能量攻击——与计时攻击类似，复杂计算耗能更多
 - 故障攻击——在算法执行时注入错误
 - 电磁攻击——分析密码算法在运行时的电磁辐射
 - 声音攻击
 - 其他脑洞



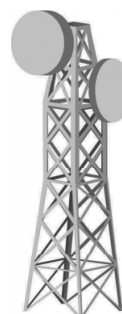
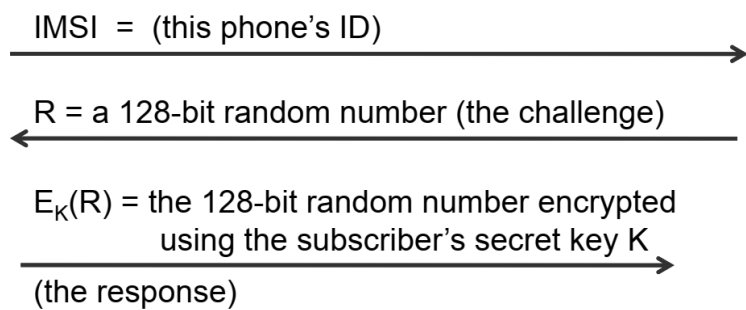
05

硬件安全模块

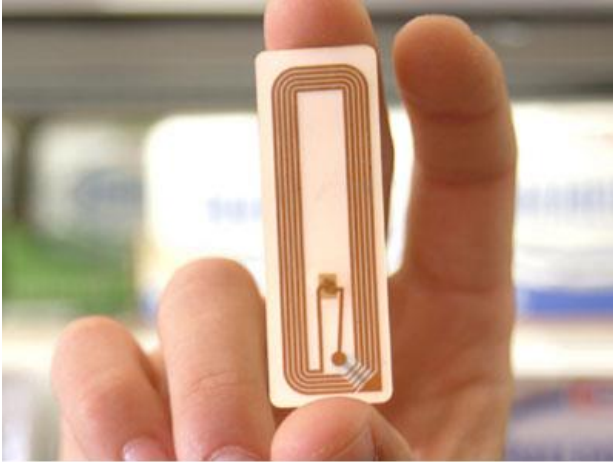
Hardware Security Module



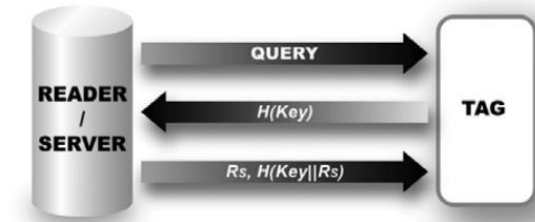
硬件安全模块：智能芯片 Smart Card



硬件安全模块：RFID



A RFID authentication protocol:



Authentication Type		Example
Implicit Authentication (IA)	IA ₀	$A : \text{APriKey}\{B\}$
	IA _F	$A \leftarrow B : r_B$ $A : \text{APriKey}\{B, r_B\}$
Origin Authentication (OA)	OA ₀	$A \rightarrow B : \text{APriKey}\{B\}$
	OA _S	$A \rightarrow B : TS_A, \text{APriKey}\{B, TS_A\}$
	OA _F	$A \leftarrow B : r_B$ $A \rightarrow B : \text{APriKey}\{B, r_B\}$
Destination Authentication (DA)	DA ₀	$A \leftarrow B : \text{APubKey}\{B\}$
	DA _{F, NoAck}	$A \leftarrow B : \text{APubKey}\{B, r_B\}$
	DA _{F, Ack}	$A \leftarrow B : \text{APubKey}\{B, r_B\}$ $A \rightarrow B : r_B$

- Reader sends Query to Tag.
- Tag sends MetaID ($= H(\text{Key})$) to Reader/Server.
- Server looks up *Key* using MetaID, generates a random number R_s , and checks whether $H(\text{Key} \oplus R_s)$ is unique among the other MetaIDs. If it is not unique, Server regenerates R_s until $H(\text{Key} \oplus R_s)$ becomes unique.
Server updates *Key* as follows.
If $H(\text{Key}_{\text{Curr}}) = \text{MetaID}$
 $\text{Key}_{\text{Prev}} \leftarrow \text{Key}_{\text{Curr}}, \text{Key}_{\text{Curr}} \leftarrow H(\text{Key}_{\text{Curr}} \oplus R_s)$
If $H(\text{Key}_{\text{Prev}}) = \text{MetaID}$
 $\text{Key}_{\text{Curr}} \leftarrow H(\text{Key}_{\text{Prev}} \oplus R_s)$
 $\text{Key} \leftarrow \text{Key}_{\text{Prev}}$
Server sends R_s and $H(\text{Key} \parallel R_s)$ to Tag through Reader.
- Tag checks whether $H(\text{Key} \parallel R_s)$ is correct.
If it is correct, Tag updates $\text{Key} \leftarrow H(\text{Key} \oplus R_s)$.

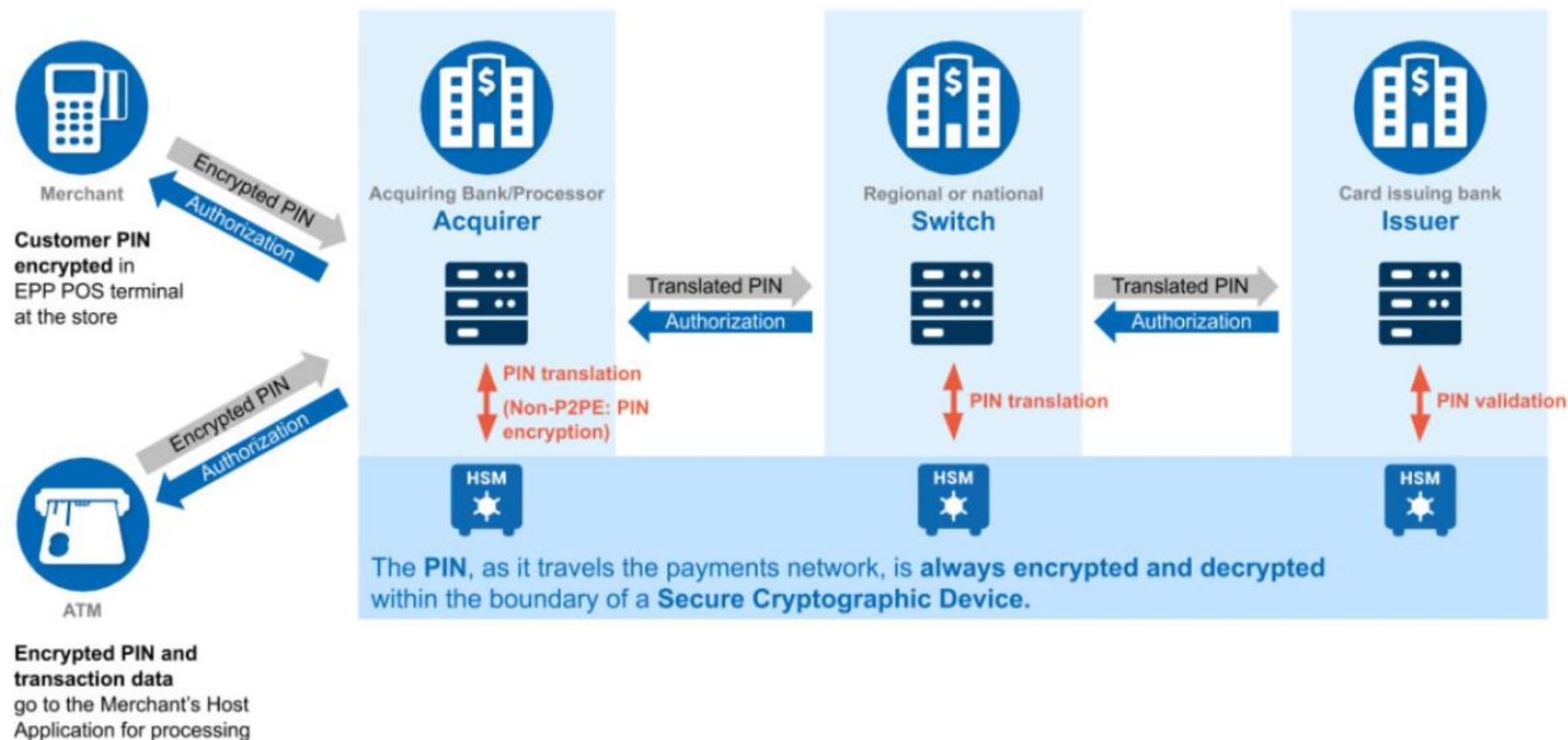
硬件安全模块：生物特征



不可复制的资源

隐私泄露风险

一个当代HSM（智能芯片卡）应用



用户的PIN码在网上支付过程中使用处于加密状态，仅在HSM中执行解密操作

HSM的优势

硬件安全模块（HSM）是一个物理计算设备，可以提供机密性、完整性和认证保护，以及对数字密钥的管理能力、密码计算的能力。

- 较好的安全性
 - 敏感数据存放在专用硬件中，保护更充分
 - 敏感数据：密钥、生物特征信息、专利算法代码等
 - 相比通用CPU，具有更好的抗侧信道能力
 - 相比通用OS，攻击面更小
 - 通常需要经过国际标准或规范的认定，例如Common Criteria或FIPS 140-2 等标准/机构认证
- 形态：
 - 有的直接焊在计算机主板，有的通过USB连接，也有的作为网络上一个可信服务节点
 - 例如，银行U盾、TPM芯片

防范物理攻击

- Protection Epoxy ——环氧树脂保护层，热保护，耐高低温、绝缘
- Wiring Mesh——构成输入输出电路网，通过检查输入输出一致性，检测物理攻击行为
- 温度传感器
- 光传感器
- 供电稳定性检查
- 清空数据的应急机制

HSM抗物理攻击能力分级：

- Tamper resistance
- Tamper evidence
- Tamper detection
- Tamper response

在物理攻击外，HSM 的逻辑防护思路：

- 限制/推迟尝试次数——口令
- 固件更新的完整性和认证—— 签名+ MAC
- 多用户之间的逻辑隔离——例如使用不同的物理内存区域
- 审计追踪——可以存取和记录所有用户的所有操作

本章要点

- 物理攻击概述
- 冷冻攻击——针对物理内存，直接获取内存器件
- 总线攻击——针对物理内存，搭载总线开展窃听
- 其他攻击
 - Rowhammer
 - 侧信道
- 硬件安全模块（HSM）简介