Secure Processor

SECURE PROCESSOR

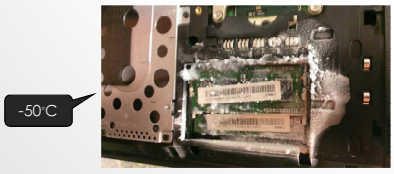
Hardware-supported security

THREAT MODEL 攻击模型

- Physical attack on:
  - Memory
  - Bus
- 方法：
  - **Cold-boot attack**
  - **DMA attack**
  - 探针监听
  - 温度、电磁攻击等

COLD-BOOT ATTACK

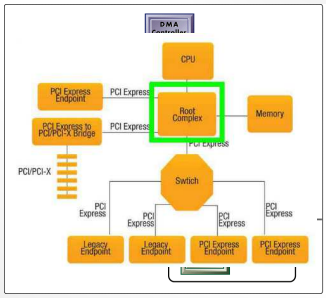
- Lest We Rember: COLD BOOT ATTACKS ON ENCRYPTION KEYS. 2008, Princeton University
- 年年初,普林斯顿大学电子前沿基金会和温瑞尔系统公司的研究人员联合发表了一篇题为《**鲜为人知的秘密：对密钥的冷启动攻击**》的文章，该文详解了从运行系统获取内存信息的一种新型攻击方式。



HOW TO：

DMA ATTACK

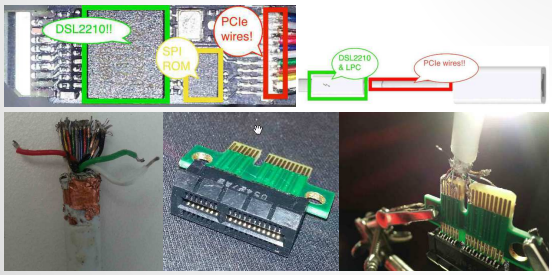
- **DMA**
  - **Direct Memory Access**
- 将传送到模块的信息复制到内存(RAM)，并允许已处理的信息自动从内存移到外部外围装置。所有这些工作皆独立于目前的CPU活动。



HOW TO:

- 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

Example：Russ Sevinsky's Thunderbolt DMA



DMA ATTACK

- Current DMA research
  - I/O attacks in Intel-PC architectures and countermeasures
  - Understanding DMA malware

After-class reading

- Current Thunderbolt attacks：
  - **Inception——Dump 4GB memory**
  - Daisy chaining Thunderbolt and Firewire
  - De Mysteriis Dom Jobsivs (Mac EFI Rootkits)

MEMORY DUMP ANALYSIS

- **Tool：AESKeyFind**
  - 在镜像中搜索并恢复AES密钥
  - 支持从不完整镜像中恢复密钥
- Paper：
  - **Lest We Remember: Cold Boot Attacks on Encryption Keys**, in *Proc. 17th USENIX Security Symposium* (Sec '08), San Jose, CA, July 2008.

MEMORY DUMP ANALYSIS

- **Tool：Volatility** http://code.google.com/p/volatility/
  - 开源内存取证分析框架，以灵活增补插件的方式工作
- 利用某些插件，渗透人员可以抽取出：
  - Windows的hashes
  - SAM（安全用户帐户信息数据库）
  - 注册表系统文件地址

ATTACKS ON HARDWARE:

- Hardware-targeting
- Purpose:
  - obtain the **critical data** storing/transmitting in the system

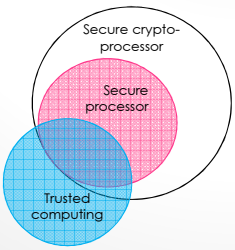
protect !

COUNTERMEASURES

- Hardware-support security mechanisms
  - Bus encryption
  - Memory encryption

1. Trusted computing
2. Secure processor
   - Secure processor
   - Secure cryptoprocessor

Root of security:
Complexity of CPU chips



A QUICK REVIEW ON MEMORY HIERARCHY

VON NEUMANN ARCHITECTURE

- Von Neumann model or the Princeton architecture
  - It describes a design architecture for an electronic digital computer with subdivisions of a **processing unit** consisting of **an arithmetic logic unit** and **processor registers**, **a control unit** containing an instruction register and program counter, **a memory** to store both data and instructions, **external mass storage**, and input and output mechanisms.

MEMORY HIERARCHY

- **Primary memory**
  - **Registers, Cache**
  - **Main memory**

- Secondary memory
  - Hard drives
  - Solid-state drives

- Off-line storage
  - BluRay-RW, ...

PROCESSOR REGISTERS

- Registers are the fastest of all forms of computer data storage.
- Location:
  - inside the processor
- Content:
  - Each register typically holds a word of data, often 32 or 64 bits

PROCESSOR CACHE

- Processor cache is an intermediate stage between ultra-fast registers and much slower main memory.
- Goal
  - **Increase performance**
  - Most actively used information in the main memory is just duplicated in the cache memory, which is faster, but of much lesser capacity.
  - Multi-level hierarchical cache setup is also commonly used—*primary cache* being smallest, fastest and located inside the processor; *secondary cache* being somewhat larger and slower.

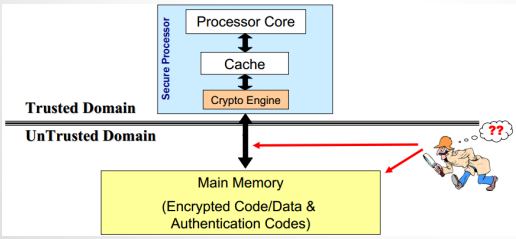
MAIN MEMORY

- Main memory is directly or indirectly connected to the central processing unit via a memory bus.
- How it's connected to CPU
  - It is actually two : an address bus and a data bus.
- How it works:
  - The CPU firstly sends a number through an address bus, a number called memory address, that indicates the desired location of data. Then it reads or writes the data itself using the data bus. Additionally, a memory management unit (MMU) is a small device between CPU and RAM recalculating the actual memory address, for example to provide an abstraction of virtual memory or other tasks.

VON NEUMANN BOTTLENECK

- 将CPU与内存分开的设计，导致了所谓的冯·诺伊曼瓶颈（von Neumann bottleneck）
- **原因：**在CPU与内存之间的数据传输率与内存的容量相比起来相当小。
- **性能下降体现在：**CPU将会在数据输入或输出内存时闲置。由于CPU速度远大于内存读写速率，因此瓶颈问题越来越严重。

- Architecture support for memory encryption and verification



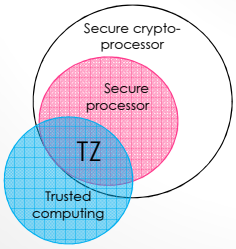
HOW TO IMPLEMENT

1. Hardware assist
   - Von Neumann bottleneck: performance loss
   - Security engine design
   - Modify the CPU
2. Software-stack support
   - Modify the OS
   - Application management: authorized and non-authorized

NEXT:
TRUSTED COMPUTING

TRUSTZONE

- ARM ® TrustZone ®

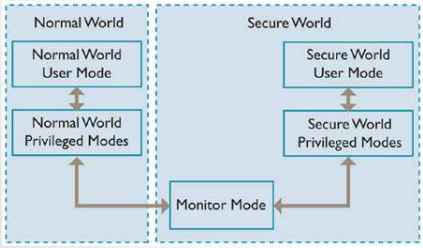


TRUSTZONE

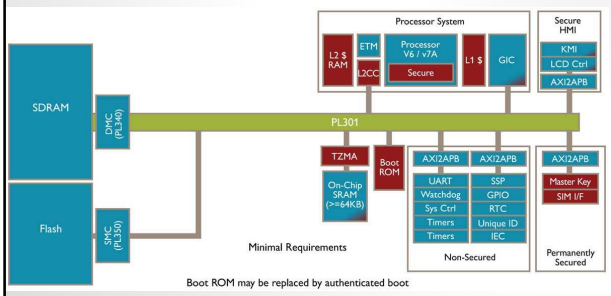
- ARM ® TrustZone ® technology is a system-wide approach to security for a wide array of client and server computing platforms, including handsets, tablets, wearable devices and enterprise systems. Applications enabled by the technology are extremely varied but include payment protection technology, digital rights management, BYOD, and a host of secured enterprise solutions.

http://www.arm.com/zh/products/processors/technologies/trustzone/index.php

TRUSTZONE ARCHITECTURE



TRUSTZONE HARDWARE ARCH



TRUSTZONE SOFTWARE STACK