网络空间安全导论 · Ch6

计01　容逸朗　2020010869

Q1.

请简要描述 Meltdown 与 Spectre 的攻击原理，并比较其共同点和区别。

- **攻击原理:**
  - Meltdown 利用了处理器的乱序执行时的漏洞。攻击者可以通过一些特殊的指令来访问未授权的内存数据，由此获取操作系统内核的敏感信息。
  - Spectre 利用了处理器的分支预测时的漏洞。攻击者可以通过一些特殊的代码来让处理器预测错误的分支，这样就可以在未经授权的情况下访问受保护的内存数据。
- **共同点:** Meltdown 和 Spectre 都是利用计算机处理器中的漏洞来进行攻击的。它们都可以让攻击者在未经授权的情况下访问受保护的内存数据，从而获取敏感信息。
- **区别:** Meltdown 攻击利用的是处理器中的乱序执行技术，而 Spectre 攻击则是利用分支预测技术攻击。需要注意的是，Meltdown 攻击只能在受影响的处理器上执行，而 Spectre 攻击可以在几乎所有处理器上执行。

Q2.

请简要描述侧信道分析的原理，并简述其用于硬件木马检测的原理?

- **分析原理:** 基于从密码系统的物理实现中获取的信息，例如时间信息、功率消耗、缓存使用等旁路信息，来推断系统中正在执行的操作或者正在处理的数据，从而获取敏感信息。
- **木马检测原理:** 利用硬件木马在系统中的非正常行为所产生的侧信道特征来进行检测。
  - 一般而言，硬件木马会在目标系统中插入一些额外的电路或者芯片，从而窃取关键信息或者影响系统的正常功能。这些额外的电路或者芯片通常会导致系统中的电源消耗、电磁辐射、时间延迟等方面的变化，从而产生了硬件木马的侧信道特征。
  - 基于这些侧信道特征，可以使用电源分析技术来分析系统中的电源消耗波形，从而检测出系统中的额外电路；也可以使用时序分析技术来分析系统中的信号延迟和时序关系，从而检测出硬件木马对系统时序的影响。