Chapter 6 系统硬件安全

赵晨阳 2020012363

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

Meltdown 和 Spectre 是两种基于 CPU 漏洞的侧信道攻击，可以窃取用户的敏感信息，例如密码、密钥等。

Meltdown 攻击利用了 CPU 的乱序执行机制，在特定的条件下，攻击者可以访问系统内存中的敏感数据，即使这些数据本应该被保护。攻击者可以通过构造恶意代码，在用户空间中访问内核空间的数据，甚至可以窃取其他进程的数据。

Spectre 攻击主要指攻击者获取计算机中所有的内存信息，导致敏感信息泄露。Spectre 漏洞的根源在于 CPU 的分支预测机制，分支预测技术是为了提高 CPU 的计算性能，如果处理器执行一个分支指令，而这个分支指令需要一个不在缓存中的数据时，CPU 就需要等待很长一段时间（相较于处理器时钟来说）去内存中获取这个数据。而在等待期间，分支预测技术允许处理器根据历史情况预测控制流的跳转方向，先执行预测路径下的指令，如果预测正确则处理器性能提升，如果预测失败则处理器将寄存器恢复到检查点，分支预测技术模块看上去很完美，即使执行了错误代码也能回到正确状态，并且似乎不会造成任何负面影响。

共同点：

1. 都是基于 CPU 漏洞的侧信道攻击，可以窃取用户的敏感信息。
2. 都是利用了 CPU 的一些特殊机制来实现攻击，即乱序执行机制和分支预测机制。
3. 都属于“跨进程攻击”，可以在不同的进程之间窃取数据。

区别：

1. Meltdown 攻击主要针对 Intel 和 ARM Cortex-A75 CPU，而 Spectre 攻击对所有 CPU 都有效。
2. Meltdown 攻击可以访问内核空间的数据，而 Spectre 攻击只能访问用户空间的数据。
3. Meltdown 攻击是通过直接访问系统内存来实现攻击，而 Spectre 攻击是通过构造恶意代码来诱使 CPU 执行本不应该被执行的代码来实现攻击。
4. Meltdown 攻击的修复可能会导致性能下降，而 Spectre 攻击的修复不一定会影响性能。

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?

侧信道分析是一种利用电磁辐射、功耗、时间等“侧信道”泄露的信息来推断计算机系统内部信息的攻击方法。这种攻击方法通常不需要直接攻击计算机系统内部的安全机制，而是通过分析系统的侧信道，来推断出系统内部的机密信息。

侧信道分析可以通过分析硬件设备的功耗、电磁辐射等侧信道信息，来推断出硬件设备内部的信息，从而检测是否存在硬件木马。例如，对于一块恶意添加的硬件设备，其功耗、电磁辐射等侧信道信息可能与正常设备不同，因此可以通过侧信道分析来检测是否存在硬件木马。

侧信道分析在硬件木马检测上具有一定的优势，因为侧信道分析不需要直接访问被检测的硬件设备，而是通过分析其周围的环境信息来推断出内部信息，因此可以避免对硬件设备的损坏，同时也具有一定的隐蔽性。