Chapter 6 系统硬件安全

沙之洲 2020012408

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 利用 CPU 的指令乱序执行。乱序执行会使得 CPU 提前执行一些后边的指令来提高 CPU 利用率。具体来说，攻击者处于用户态，CPU 乱序执行会导致一些对于内核态数据操作的指令先于执行权限检查指令完成，虽然这些对于内核态数据操作的指令会因为访问违例而放弃其对寄存器的更改，但是执行这些指令导致 cache 中的改变并不会消除。攻击者可以通过观察缓存中改变的内容，来推测内核地址的内容。

Spectre 利用 CPU 的分支预测机制。分支预测会使 CPU 在得知是否要跳转之前，先执行预测路径下的指令。尽管预测失败会将寄存器恢复到之前的状态，但是并不会恢复 cache 的状态。攻击者可以通过训练 CPU 的分支预测单元，使其在运行时进行特定的预测。分支预测的越权访问会将敏感数据映射到缓存。攻击者可以通过分析缓存侧信道，知道哪一个缓存刚刚被访问过，从而得到敏感数据的信息。

相同点在于两者都利用了缓存侧信道进行攻击。利用了 CPU 撤销指令的时候只会恢复寄存器的状态而不会恢复 cache 的状态，来推断出敏感内容。

不同点在于 Meltdown 利用的是 CPU 的指令乱序执行，而 Spectre 利用的是 CPU 的分支预测，来达到缓存侧信道的攻击。

2 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?

侧信道分析是指利用算法在硬件实现过程中泄露的信息。攻击者利用这些信息进行密码破解或者敏感信息窃取。常见的侧信道分析涉及 时间侧信道，功耗侧信道，电磁侧信道，声学侧信道

硬件木马指的是在芯片电路中恶意添加或者修改的特殊模块。侧信道用于硬件木马检测的原理是，分析硬件的侧信道信息（如静态电流，最高频率和处理延时等）与标准参数进行对比，因为木马的存在会影响到这些标准参数。因此可以基于侧信道的信息来对硬件木马进行检测。