2019年月报

2019年工作主要是对原始系统进行细节研发。

2019年5月

上月完成了地址空间隔离功能，本月针对虚拟机上下文安全切换功能完成VMCS结构体的地址隔离功能。主要的方式是将VMCS结构体的创建和销毁函数放在隔离地址空间中运行，这样就保证了VMCS结构体是被存放在隔离地址空间中，避免恶意的Hypervisor进行访问。基本完成VMCS的地址隐藏后，需要对VMCS进行访问控制，因系统中存在一些关键指令可以访问VMCS，为了防止恶意的Hypervisor直接通过指令访问VMCS，下月计划对VMCS的一些访问指令进行隐藏处理，即访问控制功能。

2019年6月

上月完成了上下文安全切换功能中的VMCS地址隐藏功能，本月针对虚拟机上下文安全切换功能完成VMCS结构体的访问控制函数调研。因VMCS被隐藏在隔离地址空间中，那么Hypervisor本身无法在自己的地址空间中访问到VMCS，从而造成程序无法运行，系统终止的问题。为了使得系统能够正常地运行，HyperMI通过将VMCS访问的相关函数挂钩到安全执行环境中运行，这样就可以保证系统的正常运行。主要的方式是将访问VMCS地址的函数找到，并统计；通过对内核代码的阅读，发现访问VMCS结构体的函数，主要是创建、访问、销毁VMCS函数，位于mmu\_audit.c文件中。在代码实现的过程中，需要对这些函数进行挂钩处理，下月计划学习一下挂钩函数的主要技术，然后将这些VMCS访问函数一一进行挂钩。

2019年7月

上月完成了虚拟机上下文安全切换功能中VMCS结构体的访问控制函数调研，本月计划完成VMCS访问函数挂钩处理。主要方式是在于原代码中访问函数入口地址处写入两条汇编指令，使得当执行访问函数的时候，就可以直接跳转到切换门入口，随后再跳转到地址隔离空间中对应的访问函数（该函数是在隔离地址空间中被重新实现的）。基本完成了VMCS关键访问函数，由于虚拟机退出后仍会访问VMCS用来虚拟机退出函数处理，为了避免挂钩大量的虚拟机退出函数，需实现虚拟机退出重定向，下月计划实现虚拟机退出重定向实现。

2019年8月

上月完成了虚拟机上下文安全切换功能中VMCS访问函数挂钩处理，本月计划完成虚拟机退出重定向。根据虚拟机退出流程进行分析，不同的虚拟机退出原因会对应不同的虚拟机退出事件处理。一般包含EPT访问地址缺页处理、IO访问处理等，由于虚拟机退出事件处理代码和函数相对庞大，考虑实际的编程问题，不可能将所有的事件处理函数都通过挂钩的方式放在隔离地址空间中。于是针对虚拟机退出处理，通过在隔离地址空间中访问完VMCS后，控制流切换到普通地址空间中处理退出函数。虚拟机上下文安全切换基本处理完成，下月计划完成虚拟机地址映射监控和内存隔离。

2019年9月

上月完成了虚拟机上下文安全切换功能，本月针对虚拟机地址映射监控和内存隔离功能进行地址映射流程梳理。通过阅读内核源码发现，在支持硬件虚拟化的平台上，虚拟机的地址映射需要两套页表，一套虚拟机自身的页表，另一套是归Hypervisor管理的EPT（扩展页表）。虚拟机上的虚拟地址翻译过程是：通过自身页表将GVA（客户机虚拟地址）映射到GPA（客户机物理地址），通过EPT页表将GPA映射到HPA（宿主机物理地址）。通过分析，为了防止EPT被恶意攻击和篡改，需要对EPT进行监控保护，主要是两个方面，EPT地址隐藏和EPT 访问函数监控，下月计划完成EPT的地址隐藏。

2019年10月

上月完成了虚拟机地址映射中地址映射流程梳理，本月针对EPT地址隐藏进行实现。主要的方式是将EPT结构体的创建和销毁函数放在隔离地址空间中运行，这样就保证了EPT结构体是被存放在隔离地址空间中，避免恶意的Hypervisor进行访问。基本完成EPT的地址隐藏后，需要对EPT进行访问控制，因系统中存在一些函数是直接访问EPT，为了防止恶意的Hypervisor直接访问EPT的地址，下月计划对EPT的一些访问函数进行隐藏处理，即访问控制功能。

2019年11月

上月完成了虚拟机地址映射功能中的EPT地址隐藏功能，本月针对虚拟机地址映射功能完成EPT结构体的访问控制函数监控。因EPT被隐藏在隔离地址空间中，那么Hypervisor本身无法在自己的地址空间中访问到EPT，从而造成程序无法运行，系统终止的问题。为了使得系统能够正常地运行，通过将EPT访问的相关函数挂钩到安全执行环境中运行，这样就可以保证系统的正常运行。主要的方式是通过对内核代码的阅读，将访问EPT地址的函数找到，主要是创建、遍历、销毁函数。在代码实现的过程中，通过挂钩处理，跳转到安全门再跳转到已在隔离空间中写好的处理函数，实现基本功能。下月计划对虚拟机内存进行高强度隔离。

2019年12月

上月完成虚拟机地址映射功能中EPT访问函数监控，本月针对虚拟机内存高强度隔离实现内存标签标记，使得虚拟机之间无法相互访问物理内存。内存标记技术主要是通过对真实的物理内存，即虚拟机或者宿主机使用的物理内存进行标记，标记每一个物理内存页的使用属主。当内存被系统分配使用的时候，能够对内存的使用进行分辨，对当前正在被使用中的内存，不再给宿主机或者其余是虚拟机进行分配，可以防止内存双映射攻击；对于未被使用内存直接进行分配。下月计划完成虚拟机内存高强度隔离功能中内存页释放时内容删除功能。