虚拟化软件栈安全研究（计算机学报-中科院信工所-朱民）

至彤

2020 年 7 月 10 日

1 摘要

在虚拟化软件栈，虚拟机监控器具有最高权限和较小的可信计算基，故而能为虚拟化系统提供安全监控和保护．但同时也引入了新的软件层，增加了脆弱性，增大了攻击面．另外，多租户模式以及软硬件平台资源共享，更加剧了新软件栈的安全威胁。

* 分析虚拟化软件栈的安全威胁、攻击方式和威胁机理

* 比较了国内外相关安全方案和技术，并指出了当前仍然存在的安全问题．

* 对未来的研究方向进行了探讨和分析，给出了虚拟化软件栈的安全增强方案。

2 引言

* 虚拟化扩增了传统服务器的软件栈．软件栈越大、越复杂，攻击面和脆弱性就越多，安全性则更难以保障。
* 虚拟化技术提供的隔离性并不强
* 软件漏洞，攻击者利用侧信道攻击也可窃取其它虚拟机的敏感数据
* 当前虚拟化的研究主要集中在对Hypervisor的保护、对虚拟机的隔离以及对VM的内部系统、应用的保护，甚至将虚拟化从可信计算基中剔除，以此来增强虚拟化软件栈的安全．