SKEE - 针对ARM架构的轻量级Linux内核安全执行环境

作者：申文博（美国北卡州立大学计算机博士，现为Samsung Research America, Samsung Knox Linux内核组成员）

近年来，随着安卓设备的普及，针对其系统的攻击也愈发频繁。作为支持安卓系统的底层系统，Linux内核备受黑客关注，如何攻破内核获取其root权限也成为黑客们争相尝试的目标。而且Linux内核由于其代码量巨大，软件漏洞在所难免 [1]。这些漏洞往往会被黑客利用，开发恶意软件，盗取用户信息[2]。

与此同时，移动安全也越来越为学术界以及工业界所重视。为了保护Linux内核，人们提出各种内核保护机制，开发出多种内核安全工具，涵盖从最基本的越界访问保护到复杂的实时内核保护系统（RKP [3]）。这些内核安全工具不但要保护内核的完整性 （kernel integrity），而且要在内核完整性被破坏后通知上层以及远端系统。这就要求内核安全工具和Linux内核之间要有较强的隔离（isolation），以保证内核里的漏洞不会直接影响到这些内核安全工具。

在以前的研究中， 内核安全工具通常被放置到拥有比内核更高权限的系统构件中，例如Hypervisor, 或者硬件安全组件中， 例如ARM TrustZone，从而将安全工具和内核中潜在的可攻击的漏洞隔离开来。但是由于安全工具本身的代码量以及潜在的软件漏洞，将安全工具放置到更高权限的系统构件不但增加了运行维护的成本，而且会增加所在高权限的系统构件的代码量和可攻击点，反而使系统更易受到攻击。

NDSS 2016的一篇论文: SKEE - 针对ARM架构的轻量级Linux内核安全执行环境 [4]，致力于解决这些问题。该论文创新性的提出一个轻量级的内核安全执行环境SKEE （Secure Kernel level Execution Environment）。这个安全执行环境拥有和内核同等的权限级别，但却可以保证即使内核被攻破，攻击者依然不能突破SKEE和内核之间的隔离，从而保证其内部所放置的安全工具的安全。

SKEE的实现基于两套内存页表（kernel page table）- 内核的内存页表以及SKEE的内存页表。在内核的内存页表中，内存页表本身，以及SKEE的代码和数据页面没有被映射，这样内核便不能访问SKEE，也无法更新内核本身的内存页表。而SKEE的内存页表包含所有内存的映射。内核需要更新内存页表时，会陷入（trap）到SKEE中，SKEE会检查每一个内存页表更新操作，确保其不会破坏SKEE和内核之间的隔离。SKEE另一贡献是针对ARMv7和ARMv8平台的内核和SKEE切换逻辑的设计。该切换逻辑保证切换的原子性，确定性以及唯一性。这些的创新设计保证即使内核中存在漏洞导致内核被攻破，攻击者依然不能突破SKEE和内核之间的隔离，无法访问SKEE内部的代码和数据。

正是由于SKEE创新而且实用的系统设计，该论文获得NDSS 2016杰出论文奖（Distinguished Paper Award）。

作者简介：

申文博，现为Samsung Research America, Knox Linux内核组成员，研究方向为Linux内核安全。2015年于美国北卡州立大学获得计算机博士学位，师从Dr. Ning Peng和Dr. Huaiyu Dai，从事无线网络安全以及操作系统安全研究。本科2010年毕业于哈尔滨工业大学，师从张伟哲老师，曾代表信息安全国家工程重点实验室参加首届全国大学生信息安全竞赛，荣获一等奖。

参考文献：

[1] Linux内核漏洞统计，http://www.cvedetails.com/product/47/Linux-Linux-Kernel.html?vendor_id=33

[2] Android Security Advisory, https://source.android.com/security/advisory/2016-03-18.html

[3] Hypervision Across Worlds: Real-time Kernel Protection from the ARM TrustZone Secure World: Ahmed M. Azab, Peng Ning, Jitesh Shah, Quan Chen, Rohan Bhutkar, Guruprasad Ganesh, Jia Ma, and Wenbo Shen, In CCS, Scottsdale, AZ, 2014

[4] SKEE: A lightweight Secure Kernel-level Execution Environment for ARM

Ahmed Azab, Kirk Swidowski, Rohan Bhutkar, Jia Ma, Wenbo Shen, Ruowen Wang and Peng Ning, In NDSS, 2016