[92] Sasy S, Gorbunov S, Fletcher CW. ZeroTrace: Oblivious memory primitives from Intel SGX. In: Proc. of the Symp. on Network and Distributed System Security (NDSS). 2018.

附中文参考文献:

[1] 王进文,江勇,李琦,杨芫.SGX 技术应用研究综述.网络新媒体技术,2017,6(5):3–9.

[58] GB/T 29827-2013.信息安全技术可信计算规范可信平台主板功能接口.2013.

[59] GB/T 29828-2013.信息安全技术可信计算规范可信连接架构.2013.

[60] GB/T 29829-2013.信息安全技术可信计算密码支撑平台功能与接口规范.2013.

[62] 石磊,邹德清,金海.Xen 虚拟化技术.武汉:华中科技大学出版社,2009.

[63] 沈晴霓.虚拟可信平台技术现状与发展趋势.信息网络安全,2010,(4):34–36.

[66] 张英骏,冯登国,秦宇,杨波.基于 Trustzone 的强安全需求环境下可信代码执行方案.计算机研究与发展,2015,52(10):2224–2238.

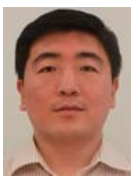
[68] 杨波,冯登国,秦宇,张倩颖,奚璨,郑昌文.基于可信移动平台的直接匿名证明方案研究.计算机研究与发展,2014,51(7):1436–1445.

[78] 沈昌祥,张焕国,王怀民,王戟,赵波,严飞,余发江,张立强,徐明迪.可信计算的研究与发展.中国科学:信息科学,2010,40(2):139–166.

[86] 范伟,孔斌,张珠君,王婷婷,张杰,黄伟庆.KVM 虚拟化动态迁移技术的安全防护模型.软件学报,2016,27(6):1402–1416. http://www.jos.org.cn/1000-9825/5009.htm [doi: 10.13328/j.cnki.jos.005009]

王鹃(1976－),女,博士,副教授, CCF 专业会员,主要研究领域为系统和网络安全,可信计算,云计算,物联网安全.

樊成阳(1994－),男,硕士生,主要研究领域为可信计算,云计算.



程越强(1984－),男,博士,研究员,主要研究领域为系统安全,云安全,可信计算,软件安全.

赵波(1972－),男,博士,教授,博士生导师, CCF 高级会员,主要研究领域为可信计算,系统安全.

韦韬(1975－),男,博士,主要研究领域为安全架构,编程语言,人工智能.

严飞(1980－),男,博士,副教授,CCF 专业会员,主要研究领域为系统安全.

张焕国(1945－),男,教授,博士生导师,CCF 高级会员,主要研究领域为信息安全,可信计算,密码学.

马婧(1982－),女,工程师,主要研究领域为信息安全.