National Institute of Standards and Technology | NIST [EB/OL]. NIST. [2018-03-10].htt ps://www.nist.gov/

柯文浚, 董碧丹, 高洋. 基于Xen的虚拟化访问控制研究综述[J]. 计算机科学, 2017, 44 (s1): 24-28.

石源, 张焕国, 赵波, 等. 基于SGX的虚拟机动态迁移安全增强方法[J]. 通信学报, 2017, 38(9).

林闯, 苏文博, 孟坤, 等. 云计算安全: 架构、机制与模型评价[J]. 计算机学报, 2013, 09: 1765-1784.

俞能海, 郝卓, 徐甲甲, 等. 云安全研究进展综述[J]. 电子学报, 2013, 02: 371-381.

Ali M, Khan S U, Vasilakos A V.Security in cloud computing :opportunities and challe nges[J]. Information Science, 2015, 305: 357-383.

Zhao D, Mohamed M, Ludwig H. Locality-aware Scheduling for Containers in Cloud Computing[J]. IEEE Transactions on Cloud Computing, 2018, PP(99): 1-1.

Kumar P R, Raj P H, Jelciana P. Exploring Data Security Issues and Solutions in Clou d Computing[J]. Procedia Computer Science, 2018, 125:691-697.

沈昌祥, 张大伟, 刘吉强, 等. 可信3.0战略: 可信计算的革命性演变[J]. 中国工程科学, 2016, 18(6): 53-57.

余发江, 陈列, 张焕国. 虚拟可信平台模块动态信任扩展方法[J]. 软件学报, 2017, 28(10): 2782-2796.

谭良, 徐志伟. 基于可信计算平台的信任链传递研究进展[J]. 计算机科学, 2008, 10: 15-18.

中国信通院-研究成果-权威发布-专题报告[EB/OL]. [2017-07-10]. 中国信息通信研究院. http://www.caict.ac.cn/kxyj/qwfb/ztbg/201709/t20170919\_2208939.htm.

工业和信息化部关于印发《云计算发展三年行动计划（2017-2019年）》的通知[EB/OL].[2017-04-10]. 中华人民共和国工业和信息化部. http://www.miit.gov.cn/n1146295/n1146592/n3917132/n4062056/c5570298/content.html.

McAfee: 2017年全球云计算安全报告[EB/OL]. [2017]. 中国云计算社区. http://www.chinacloud.cn/show.aspx?id=25993&cid=29.

徐明迪, 张焕国, 张帆, 杨连嘉. 可信系统信任链研究综述[J]. 电子学报, 2014, 10: 2024-2031.

BERGER S, CACERES R, GOLDMAN K A, et al. VTPM: virtualiz-ing the trusted platform module[C]// Proc of the 15th USENIX Security Symposium. Berkeley, USA, 2006. 305-320.

Xensource, Xen Open-Source Hypervisor[EB/OL]. [2018-03-12]. Xensource. https://www.citrix.com/downloads/xenserver/.

Data Storage, Converged, Cloud Computing, Data Protection | Dell EMC US[2018-03-10]. Dell Inc. https://www.dellemc.com/en-us/index.htm.

Microsoft - Official Home Page [EB/OL]. [2018-03-10]. Microsoft 2018. https://www.microsoft.com/zh-cn/.

Garfinkel T, Pfaff B, Chow J, et al. Terra: a virtual machine-based platform for trusted computing[C]// Nineteenth ACM Symposium on Operating Systems Principles. ACM, 2003:193-206.

B. PFITZMANN, J. RIORDAN, C. STUBLE,et al. "The PERSEUS system architecture", Technical Report RZ 3335 (#93381), IBM Research Division, Zurich Laboratory, 2001.

CHRIS I D, DAVID P, WOLFGANG W, et al. Trusted virtual platforms: a key enabler for converged client devices[C]// Proc of the ACM SIGOPS Operating Systems Review. New York, USA, 2009. 36-43.

BERGER S, RAMON C, DIMITRIOS P, et al. TVDc: managing security in the trusted virtual datacenter[C]. Proc of ACM SIGOPS Operating Systems Review. New York, USA, 2008. 40-47.

KRAUTHEIM F J, DHANANJAV S P, ALAN T S. Introducing the trusted virtual environment module: a new mechanism for rooting trust in cloud computing[C]// Proc of the 3rd International Conference on Trust and Trustworthy Computing. 2010.211-227.

王丽娜, 高汉军, 余荣威, 等. 基于信任扩展的可信虚拟执行环境构建方法研究[J]. 通信学报, 2011, 32(9): 1-8.

Zhang Lei, Chen Xingshu, Liu Liang, Jin Xin.Trusted domain hierarchical model based on noninterference theory[J]. The Journal of China Universities of Posts and Telecommunications. August 2015, 22(4): 7-16.

常德显, 冯登国, 秦宇, 张倩颖. 基于扩展LS2的可信虚拟平台信任链分析[J]. 通信学报, 2013, 34(5): 31-41.

Yu, Z., Zhang, W. & Dai, H. J A Trusted Architecture for Virtual Machines on Cloud Servers with Trusted Platform Module and Certificate Authority[J]. Journal of Signal Processing Systems, 2017, Vol.86 (2-3), pp.327-336.

池亚平, 李欣, 王艳, 王慧丽. 基于KVM的可信虚拟化平台设计与实现[J]. 计算机工程与设计, 2016, (06): 1451-1455.

李海威, 范博, 李文锋. 一种可信虚拟平台构建方法的研究和改进[J]. 信息网络安全, 2015, (01): 1-5.

蔡谊, 左晓栋. 面向虚拟化技术的可信计算平台研究[J]. 信息安全与通信保密, 2013, (06): 77-79.

徐天琦, 刘淑芬, 韩璐. 基于KVM的可信虚拟化架构模型[J]. 吉林大学学报(理学版), 2014, (03): 531-534.

杨丽芳, 刘琳. 基于虚拟机的可信计算安全平台架构设计[J]. 煤炭技术, 2014, (02): 170-172.

陈亮, 曾荣仁, 李峰,等. 基于无干扰理论的信任链传递模型[J]. 计算机科学, 2016, 43(10): 141-144...

F. John Krautheim\*, Dhananjay S. Phatak, and Alan T. Sherman,Introducing the Trusted Virtual Environment Module:A New Mechanism for Rooting Trust in Cloud Computing[C]// TRUST 2010, LNCS 6101, 2010: 211–227.

朱智强. 混合云服务安全若干理论与关键技术研究[D].武汉大学,2011.

曲文涛. 虚拟机系统的可信检测与度量[D].上海交通大学,2010: 90-117.

CHEN S Y, WEN Y Y,ZHAO H. Formal analysis of secure bootstrap in trusted computing[C]// Proc of the 4th International Conference on Autonomic and Trusted Computing Berlin, Springer, 2007. 352-360.

张兴, 黄强, 沈昌祥. 一种基于无干扰模型的信任链传递分析方法[J]. 计算机学报, 2010, 33(1): 74-81.

Rushby J. Noninterference, transitivity, and channel-control security policies[M]// SRI International, Computer Science Laboratory, 1992: 01-50

Kai E, Meyden R V D, Zhang C. Intransitive noninterference in nondeterministic systems[C]// ACM Conference on Computer and Communications Security. ACM, 2012: 869-880.

Paolo Baldan, Alessandro Beggiato. Multilevel Transitive and Intransitive Non-interference, Causally[J]. Theoretical Computer Science, 2018, 706: 54-82.

张兴, 陈幼雷, 沈昌祥. 基于进程的无干扰可信模型[J]. 通信学报, 2009, 30(3): 6-11

赵佳, 沈昌祥, 刘吉强, 等. 基于无干扰理论的可信链模型[J]. 计算机研究与发展, 2008, 45(6): 974-980

刘威鹏, 张兴. 基于非传递元干扰理论的二元多级安全模型研究[J]. 通信学报, 2009, 30(2): 52-58

陈菊, 谭良. 一个基于进程保护的可信终端模型[J]. 计算机科学, 2011, 38(4): 115-117

徐甫. 支持进程代码修改的非传递元干扰可信模型[J]. 计算机工程, 2013, 39(11): 150-153, 168

秦晰, 常朝稳, 沈昌样, 等. 容忍非信任组件的可信终端模型研究[J]. 电子学报, 2011, 39(4): 934-939

Smith, Jim, Nair, et al. Virtual Machines: Versatile Platforms for Systems and Processes (The Morgan Kaufmann Series in Computer Architecture and Design)[J]. 2005.

Adams K, Agesen O. A comparison of software and hardware techniques for x86 virtualization[J]. Acm Sigops Operating Systems Review, 2006, 40(5): 2-13.

Get Docker | Docker [EB/OL]. [2018-03-10]. Docker. https://www.docker.com/get-docker.

KVM project[EB/OL], [2018-03-10]. KVM. http://www.linux-kvm.org/.

Goguen J A, Meseguer J. Security Policies and Security Models[C]// IEEE Symposium on Security & Privacy. DBLP, 1982: 11-20.

Datta A, Franklin J, Garg D, et al. A Logic of Secure Systems and its Application to Trusted Computing[J]. 2009: 221-236.

GILLES B, GUSTAVO B, JUAN D C, et al. Formally verifying isolation and availability in an idealized model of virtualization[C]// Proc of the 17th International Conference on Formal Methods. Berlin, Springer, 2011: 231-245.

WANG Zhi, JIANG Xu- xian. HyperSafe:a lightweight approach to provide lifetime hypervisor control- flow integrity[C]// Proc of IEEE Sym-posium on Security and Privacy. Washington DC:IEEE Computer Society, 2010: 380-395.

JONATHAN M M, NING Q, LI Y L, et al. TrustVisor: efficient TCB reduction and attestation[C]// Proc of the IEEE Symposium on Security and Privacy. Oakland, USA, 2010: 143-158.

Mozilla Firefox Ltd.[EB/OL]. [2018-03-10]. http://www.firefox.com.cn/download/.

CodeWeavers Inc.[EB/OL]. [2018-03-10]. https://www.winehq.org/.

Kingsoft Office Corporation.[EB/OL]. [2018-03-10]. http://linux.wps.cn/.

The Eclipse Foundation. [EB/OL]. [2018-03-10]. https://www.eclipse.org/downloads/.