可信系统信任链研究综述

徐明迪[1],张焕国[2],张 帆[3],杨连嘉[1]
(1. 武汉数字工程研究所,湖北武汉 430205; 2. 空天信息安全与可信计算教育部重点实验室,湖北武汉 430072;
3. 杭州电子科技大学通信工程学院,浙江杭州 310018)

摘 要: 信任链是实施可信系统的关键技术之一,本文从信任链理论和应用系统出发,介绍了研究信任链理论的典型模型及近年来的研究进展,包括基于无干扰理论的信任链传递模型和基于组合安全理论的信任链模型,详细阐述了这两种信任链理论模型的优势和不足. 介绍了基于静态信任根和动态信任根的信任链应用系统的研究状况,介绍了信任链远程证明技术,介绍了云计算环境下的信任链应用系统,对信任链应用系统存在的安全缺陷以及一致性和安全性测评方法进行了分析论述,并展望了该领域未来的发展趋势.

关键词: 可信计算; 信任链理论; 无干扰理论; 组合安全理论; 静态信任链; 动态信任链; 信任链应用系统安全
中图分类号: TP309.1 **文献标识码:** A **文章编号:** 0372-2112 (2014) 10-2024-08
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2014.10.024

Survey on Chain of Trust of Trusted System

XU Ming-di[1], ZHANG Huan-guo[2], ZHANG Fan[3], YANG Lian-jia[1]
(1. *Wuhan Digital and Engineering Institute, Wuhan, Hubei* 430205, *China*;
2. *The Key Laboratory of Aerospace Information Security and Trust Computing, Ministry of Education, Wuhan, Hubei* 430072, *China*;
3. *Communication Engineering School, Hanzhou Dianzi University, Hangzhou, Zhejiang* 310018, *China*)

Abstract: Chain of trust (CoT) is one of the key technologies for constructing trusted system. As viewed from theories and application systems of CoT, this paper introduced several representative models and the latest investigations including noninterference-based CoT theory and composition security-based CoT theory firstly. Afterward, this paper expatiated advantage and shortage of two CoT theories in detail. Secondly, this paper introduced the development of application systems comprising static CoT and dynamic CoT, and analyzed the remote attestation technology of chain of trust, and presented the CoT systems in cloud computing environment, and analyzed the security deficiency of those systems, and then discussed the conformance testing and security evaluation for CoT application system. Finally, this paper put forward the research and development trend for CoT.

Key words: trusted computing; theory of CoT (chain of trust); noninterference theory; composition security theory; static CoT; dynamic CoT; security of CoT application systems

1 引言

自 2003 年可信计算组织(Trusted Computing Group, TCG)成立以来,可信计算取得了长足的发展[1]. 目前,可信计算已经成为信息系统安全的支撑技术之一,具有重要的地位. 例如,在云计算等新型计算环境中,将可信计算技术融入其中,以可信赖的方式提供安全服务已经成为构建云安全基础设施的重要方法[2].

可信计算具有度量、存储和报告三大基本功能. 其中,度量功能又是上述三大功能的基础. 实现度量功能的关键理论和技术是 TCG 所定义的信任链[1]. 因此,信任链在可信计算中具有核心基础地位. 信任链的建立与传递涉及到三个基本概念[3]:信任根、信任传递和可信度量. 其中,信任根是系统可信的锚节点(Anchor Node),从信任根开始,通过完整性度量和完整性存储技术对代码的可信赖性进行度量和记录,实现信任的链式传递,并最终将从信任根扩大到整个系统. 之后,利用完整性报告技术实现信任从终端到网络的传递.

鉴于信任链的重要地位,近年来,国内外学术界和工业界对其展开了广泛而深入的研究. 大量的工作发

收稿日期: 2013-07-25; 修回日期: 2014-03-21; 责任编辑: 孙瑶
基金项目: 国防预研基金(No. 9140A15040211CB3901); 国家自然科学基金(No. 61003268); 浙江省教育厅基金(No. Y201224055)

表在 Oakland、CCS、USENIX Security 等顶级会议上[4~14]. 在已有的工作中,研究人员在信任链传递模型[3,15,16]、信任链构建技术[17,18]、信任链远程证明[17,19]、信任链系统测评[16,20]等方面取得了丰硕的成果. 其中,信任链理论模型逐步从传递无干扰理论[21]向非传递无干扰理论[22]的方向发展,信任链无干扰信息流分析逐渐从特定无干扰属性的建模验证[23]向广义非传递无干扰属性的自动化验证[24]方向发展. 信任链构建技术从静态信任链[3]向动态信任链[25]、虚拟平台信任链[26]、云计算平台信任链[27]等新型计算环境下的信任链构建技术方向发展. 信任链远程证明技术从二进制远程证明[3]向基于属性的远程证明[28]、基于语义和特定应用场景的远程证明[17,19]方向发展. 信任链系统测评从对信任链规范一致性测评[29]向抽象协议验证、信任链关键运行机制逻辑分析[12,30,31]的方向发展等.

在信任链的产业实现与应用方面: TCG 陆续发布了 PC、服务器、移动平台、虚拟化的信任链规范. 我国制定了一系列具有创新结构的可信计算标准和信任链规范[1]. 微软的 Win8 操作系统全面支持可信计算,全磁盘加密技术 BitLocker 运用信任链技术实现对卷主密钥的保护. AMD、Intel 先后发布了支持动态可信度量根的处理器产品. 可信计算开源项目 tgrub、tboot 分别实现了代表性的可信计算静态和动态信任链系统. 完整性度量架构(Integrity Measurement Architecture,IMA) 作为目前最为实用的完整性度量方案,已经集成到 Linux 内核中. 华为、中标软、Intel 也先后推出了可信云系统,通过全信任链确保云计算基础设施安全.

根据 TCG 信任链理论与技术的十余年发展,本文对信任链的无干扰理论和组合安全理论进行了论述和总结,对静态信任链系统和动态信任链系统的优点和不足进行了分析,对信任链应用系统的安全缺陷和安全测评进行了探讨,力求对信任链理论与技术的研究发展进行客观和全面的介绍.

2　基于无干扰理论的信任链模型

根据可信计算组织 TCG 对于可信的行为学定义,可信的判定问题本质上可以归结为实体的真实行为与实体的预期行为之间的无干扰分析的问题,因此无干扰模型[32]成为目前信任链中信任传递分析的重要工具之一.

2.1　基于传递和非传递无干扰的信任链模型

近年来,无干扰模型在可信计算领域得到了广泛的应用. 沈昌祥院士领导的研究团队[21,22,33,34]利用无干扰模型来分析进程和信任链组件传递的安全性. 赵佳[33]建立了基于传递无干扰理论的可信链模型,并给出了系统 M 可信的基本条件. 张兴则提出了基于进程的无干扰可信模型[21],利用传递无干扰研究进程动态运行时的可信性. 张兴还指出[22]: 信息流在组成信任链系统的各个安全域之间传递的时候必须是受限的,并提出了一种基于非传递无干扰模型的信任链安全性分析方法. 秦晰提出了一种容忍非信任组件的可信终端模型[34],通过域间无干扰给出了可信终端应满足的充分条件,尝试解决可信系统中应用非可信组件的问题.

围绕信任链完整性度量的有效性问题,邱罡提出了一种基于操作无干扰的完整性度量模型[35],从动态的角度对系统的运行完整性进行度量. 针对可信系统应满足的完整性无干扰条件,张帆给出了完整性条件下的无干扰模型[36],将软件动态行为视为原子行为的时序序列,给出软件动态行为在传递和非传递安全策略控制下可信性分析的判定条件. 石文昌[37]认为 TCG 描述的信任链是粗粒度的,提出了对 TCG 信任链进行细粒度划分的思路.

如表 1 所示,NTCM 模型(Noninterference-based Trusted Chain Model) 以 Rushby 无干扰模型中的输出隔离性质和单步隔离性质为基础,描述了可信进程、可信状态和可信传递性质,将 Rushby 无干扰模型的域映射到进程. NITM 模型(NonInterference Trusted Model) 则强调了进程间切换时可信验证的重要性,通过 Rushby 的状态机模型对操作完整性和系统完整性传递进行了严格定义,与 NTCM 模型在本质上是相同的,都是从传递无干扰的角度给出了系统 M 运行可信的条件. Rushby 曾指出: 传递无干扰只是非传递无干扰的一个特例[32]. 基于传递无干扰的信任链理论在实际使用中是受限的. 文献[22]则给出了信任链非传递无干扰的条件,更加清楚地体现了 TCG 信任链只能逐层传递,而不能跨层传递的思想.

表 1　基于无干扰理论的信任链传递模型

NTCM 模型[33]	NITM 模型[21]	文献[22]提出的模型	TUC 模型[34]
①系统 M 从可信根开始运行 ②系统 M 中的进程满足单步隔离性和输出隔离性 ③系统 M 满足可信传递性质	①进程 p 满足单步隔离性和输出隔离性 ②进程满足可信验证,验证函数 verify (p,q) = ture	①视图隔离系统 M 满足输出一致性,弱单步一致性和局部干扰性 ②系统域间满足非传递无干扰	①可信域 D_T 是运行可信的 ②$(N_{IO} \subset N_T) \wedge (N_{IO} \not\subset N_N)$ ③ $N_T \cap$ write $(D_N) = \varnothing$

2.2　基于无干扰理论研究信任链模型的进一步探讨

利用无干扰理论研究信任链安全性具有固有的优点,但也存在一些开放问题需要进一步研究.

(1) 无干扰属性难以进行验证

Rushby 给出了非传递无干扰的形式系统及其验证

定理,但是该验证定理在实践中却是难以应用的. 其最主要的原因是 Rushby 的形式系统中的弱单步一致性和局部无干扰性并不是递归的形式,这使得难以构造相应的验证算法[32]. Eggert 指出,相对于传递无干扰,非传递无干扰的自动化验证工作[38]相当少见. 近年来,研究人员也在尝试解决上述问题. 国内的周从华分别采用量化布尔公式求解[24]和 Petri 网可达图求解[39]作为工具,对广义非传递无干扰的验证问题进行了研究. 但这些工作仍然存在改进的空间,如文献[24]在特殊的情况下计算量过大,且不能应用于半建模的系统等. 寻求有效的无干扰属性验证方法将促进无干扰模型在实际中的应用.

(2) 物理意义不明显

Rushby 所给出的非传递无干扰形式系统基于三条基本属性. 但是,三条基本属性的物理意义并不明显. 以弱单步一致性为例,弱单步一致性要求 $s \overset{\mathrm{dom}(a)}{\sim} t \wedge s \overset{u}{\sim} t \wedge \mathrm{dom}(a) \rightarrow u$,在这种情况下才会有 $\mathrm{step}(s,a) \overset{u}{\sim} \mathrm{step}(t,a)$. 那么上述式子中状态 s 和 t 的含义是什么? 与传递无干扰相比,非传递无干扰与传递无干扰的差别仅仅是 $s \overset{\mathrm{dom}(a)}{\sim} t$,那么 $s \overset{\mathrm{dom}(a)}{\sim} t$ 的含义是什么? 为什么 $s \overset{\mathrm{dom}(a)}{\sim} t$ 会造成两者根本的区别? 经研究发现,对上述问题的研究有助于寻求有效的无干扰属性验证方法,且促进无干扰在信任链模型实践当中的应用[20].

3 基于组合安全理论的信任链模型

信任链是多个子系统组成的组合系统,Deepak 指出[31],在单个子系统满足安全属性的前提下,多个子系统组合而成的复合系统是否仍然满足给定的安全属性? 研究人员对 SRTM/DRTM 信任链构建机制、PCR(Platform Configuration Register)扩展机制、远程证明机制的安全性质开展了研究.

3.1 基于可组合安全理论的信任链模型

从保护数据机密性的角度出发,组合安全问题被认为是可信计算的另外一个主要科学问题[24]. 可组合安全性最早被 McCullough 在分析组合系统安全性时提出[40]. 单个组件是安全的,组合之后的系统也会出现不满足既定的端到端的安全属性的情况[31].

文献[16,29]指出:信任链组合系统不应出现直接或间接的信息泄露. 要获得一个组合安全系统的构成需要对组合算子进行扩展,以便将两个系统通过并行方式进行语义操作,并同步内部互补动作. Focardi[41]提出使用并行算子和限制算子来实现安全进程代数中组合算子的功能.

针对静态可信度量根(Static Root of Trust for Measurement,SRTM)和动态可信度量根(Dynamic Root of Trust for Measurement,DRTM)的信任链形式化建模和证明问题,Deepak[4,30]提出了基于协议组合逻辑和线性时序逻辑的形式化框架(Logic of Secure System,LS^2),用于对可信系统的架构层和实现层进行建模和分析,LS^2 包括标准的进程演算原语和强制性构造语句,对可信系统的描述更加接近实际系统. 针对可信计算信任链系统接口层的抽象问题,Deepak 还对 rely-guarantee 推理进行扩展并提出了 assume-guarantee 推理[31],基于并发编程逻辑和迹语义对可信系统的机密性、完整性和认证性等安全属性进行了描述和推理. 常德显给出了基于扩展 LS^2 的可信虚拟平台信任传递模型[42]. Delaune 则针对 PCR 的扩展机制进行了理论分析[12].

如表 2 所示,策略不可推断模型(Non Deducibility on Strategies,NDS)[43]是一类很强的可组合安全性质. NDS 本质上强调了低安全级进程无法从视图中推断出高安全级进程的运行策略. 文献[23]提出的可组合的强互模拟不可推断模型(Strong Bisimulation Non Deducibility on Composition,SBNDC)表示从低安全级进程的观察中得不到任何高安全级的信息. NDS 和 SBNDC 都是无干扰理论的扩展和延伸,属于模型检验方法. 文献[4,30]从安全协议的角度对 SRTM 和 DRTM 的正确性进行证明,通过 LS^2 系统进行建模,从严格时序约束和谓词约束的角度对 SRTM/DRTM 协议参与者应满足的条件进行限定,通过定理证明的方式给出了几种攻击下 SRTM 和 DRTM 依然保持正确性属性的条件. 与 NDS 和 SBNDC 模型相比,LS^2 模型更侧重系统的严格时序性建模,但缺乏对信息流安全属性的定义.

3.2 基于组合安全理论研究信任链模型的进一步探讨

对信任链组合系统进行安全性分析的难点在于对组合系统以及安全属性的形式化定义. Schneider 认为,属性和系统都是迹集合,属性对于系统是可保持的当且仅当系统是属性的一个细化[44]. Abadi 和 Lamport 在此框架之上加入了规范的概念,遵从规范预期行为的迹集合和违反系统输入约束的迹集合. 但是,基于迹语义对于安全属性是难以表达的. NDS 和 SBNDC 模型从安全语义的角度给出了低安全级进程不会推断出高安全级进程行为的充要条件. 信任链组合系统还包含了点积、串行和反馈等动作,这些为信任链复合系统的安全属性研究提供了一个新的视角.

在信任链系统的定理证明类方法方面,文献[17]指出:相比模型检验方法,基于定理证明的可信计算安全机制分析还处于起步阶段,对现有可信计算技术实际运用中的一些具体问题,包括信任链远程证明协议、

表 2　组合安全理论下的信任链传递模型

NDS 模型[43]	SBNDC 模型[23]	SRTM LS² 模型[30]	DRTM LS² 模型[4]
对于任意长度为 n 的低安全级视图 λ 与高安全级进程长度为 n 的策略保持一致.	①基于迹语义的组合安全属性: $E/\mathrm{Act}_H \approx_T (E\mid H)\setminus H)/\mathrm{Act}_H$ ②基于互模拟语义的组合安全属性: $E/\mathrm{Act}_H \approx_B (E\mid H)\setminus \mathrm{Act}_H$ ③信任链组合系统 E 的 Act_H 集合中的元素对偶和 S_y 集合满足双射关系: $E \xrightarrow{\mu} E', E' \xrightarrow{h} E'' \Rightarrow E'\setminus \mathrm{Act}_H \approx_B E''\setminus \mathrm{Act}_H$	①Reset(m, t_R, X) ②∃TPM(m). Read(TPM(m), t_{Re}, m. PCR(s), seq(0, BL, OS)) ③Call($X, t_{BL}, BL(m)$) ④$\forall t \forall Y.(t_R < t < t_{Re}) \supset \neg$Reset($t, m, Y$)	$[\mathrm{Verifier}(m)]_V^{t_b, t_e}$ $\exists J, t_X, t_E, t_N, t_L, t_C, n.$ $\wedge(t_L < t_C < t_E < t_X < t_e) \wedge (t_b < t_N < t_E)$ $\wedge(\mathrm{New}(V, n)@t_N) \wedge (\mathrm{LateLaunch}(m, J)@t_L)$ $\wedge(\neg\mathrm{LateLaunch}(m)\ \mathrm{on}\ (t_L, t_X])$ $\wedge(\neg\mathrm{Reset}(m)\ \mathrm{on}\ (t_L, t_X])$ $\wedge(\mathrm{Jump}(J, P(m))@t_C)$ $\wedge(\neg\mathrm{Jump}(J)@(t_L, t_C]) \wedge (\mathrm{Eval}(J, f)@t_E)$ $\wedge(\mathrm{Extend}(J, m, \mathrm{dpcr}.k, \mathrm{EOL})@t_X)$ $\wedge(\neg\mathrm{Eval}(J, f)@(t_C, t_E)) \wedge (\neg\mathrm{Eval}(J, f)@(t_E, t_X])$ $\wedge(\neg\mathrm{IsLocked}(m, \mathrm{dpcr}.k, J)\ \mathrm{on}\ (t_L, t_X])$

直接匿名证明(Direct Anonymous Attestation,DAA)协议等,尚未出现令人信服的研究成果. 对 DAA 协议、可信虚拟平台等较为复杂的分析对象,现有的形式化描述方法与安全属性定义[45]还不够完善,对定理证明类方法在可信计算领域的运用还有待探讨.

4　信任链应用系统

信任链应用系统从实现上分为静态信任链系统和动态信任链系统,后者更多地被用于构建可信云计算平台. 基于平台架构的攻击对信任链系统具有较大破坏作用. 现有的信任链应用系统在具体实现与规范说明之间存在较大差异.

4.1　基于静态信任根的信任链应用系统

国内外众多学者在信任链应用系统方面进行了不懈努力,出现了一些具有代表性的基于静态信任根的信任链应用系统,如 Trusted GRUB 系统、完整性度量架构 IMA[9]、Daoli 云计算基础设施安全系统[11]、ISCAS 信任链系统[17]等. 表 3 给出了三种静态信任链应用系统的对比说明.

表 3　三种静态信任链应用系统对比

静态信任链系统	先进性	局限性
Trusted GRUB	①支持第一代 GRUB 信任链传递的系统 ②支持对用户指定的任意文件进行完整性度量	①不支持第二代 GRUB ②过于依赖 INT 1A 中断提供的可信计算服务,存在着 BIOS 攻击安全问题
IMA	①Linux 下的完整性度量架构,将信任链扩展至操作系统和应用程序 ②支持对 Linux 内核模块、可执行程序、动态链接库和脚本文件的完整性度量	①加载时刻度量,不能精确反映程序的运行时刻行为 ②需要完全信任软件度量列表,缺少可信第三方验证
Daoli	①支持第一代 GRUB 全信任链度量的系统,可创建软件层的 SML ②信任链可传递至 Xen 和 VM	①对 GRUB 的全信任链度量存在着和 Trusted GRUB 系统类似的安全隐患

除上述系统外,也出现了其它信任链应用系统. 如文献[1]提出的并在移动终端中得到实际应用的星型信任链系统,IBM 研究人员设计实现的 TPod 可信引导、GNU 组织实现的可信启动补丁. Zhen 提出使用 U-Key 来保证普通计算机启动的可信性[5]等,李晓勇[46]提出了 Windows 平台下的动态多路径信任链.

4.2　基于动态信任根的信任链应用系统

Kauer 针对 SRTM 存在的安全问题,提出了使用 DRTM 来缩短信任链并简化 TCB[10],通过增加 SKINIT 指令来实现对启动过程进行认证,使用 SKINIT 指令来创建 DRTM,替代了基于 BIOS 的 SRTM 和信任链. Kauer 还开发出了针对 AMD 处理器的原型系统,对多重引导器中的所有引导模块进行度量,并通过 $\mathrm{locality}_2$ 将度量结果存储到 PCR_{19}. McCune 提出了 Flicker 保护框架[25],该框架不需要信任 BIOS、OS 以及支持 DMA 的设备,TCB 仅包含了可信平台模块(Trusted Platform Module,TPM)、芯片组、CPU 和安全敏感代码(Piece of Application Logic,PAL),并保证 PAL 被执行在一个完全隔离的环境,提供细粒度的代码执行证明. Intel 开发了可信启动系统 tboot,与普通的 Linux 度量过程不同的

是,tboot 在度量 Linux 内核之前度量 Xen 的完整性. 这 三种动态信任链应用系统之间的对比见表 4.

表 4 三种动态信任链应用系统对比

动态信任链系统	先进性	局限性
OSLO	①实现动态完整性度量的系统,支持 AMD 平台,简化后的 TCB 不需要包含 BIOS 和 bootloader ②可防范 BootLoader 攻击、TPM 重启攻击和 BIOS 攻击 ③支持 DMA 保护和创建 ACPI event-log	①仅用于对 Linux 多重引导器的认证启动
Flicker	①在 BIOS、OS 和 DMA 设备都不可信的情况下,仍然可以保证敏感代码执行的隔离安全 ②相比 OSLO 的 TCB,Flicker 实现了最小化 TCB	①需要应用开发人员提供 PAL,并定义 PAL 与应用之间的接口 ②需要在 Linux 内核中增加额外的 flicker module
Trusted Boot	①通过 Intel TXT 技术度量内核或虚拟机监控器,比传统 GRUB 启动更加安全	①预存在 chipset 中的公钥杂凑值难以更换,认证代码模块只能在特定硬件平台上运行

4.3 信任链远程证明技术

远程证明是信任链从终端到网络的延伸[17]. 远程证明按照证明目标可分为平台完整性证明和平台身份证明[17]. 信任链是平台完整性证明的重要基础. 根据信任根的不同,平台完整性证明可分为基于静态信任根的平台完整性证明[3]和基于动态信任根的平台完整性证明[13,25]. 根据证明方法的不同,平台完整性证明又可分为二进制证明[3]、基于属性的证明[28]、基于语义的证明[11]、基于策略模型的证明[47]等. 具体关于信任链远程证明理论、系统和应用参见文献[1,17,19].

4.4 云计算环境下的信任链应用系统

信任链在云计算等新型计算环境下的保护对象主要是数据安全和隐私保护. Sadeghi 指出[48],可信计算技术为云计算提供了可信的软件和硬件以及证明自身行为可信的机制,可以解决外包数据的机密性和完整性问题.

在可信云计算环境构建研究方面,金海提出了在 Xen 中实现虚拟 DRTM 和虚拟 LPC(Low Pin Count)总线的可信执行环境 TEE(Trusted Execution Environment)[7],用户可通过 TEE 在不可信的 Guest OS 中执行上下文敏感的应用程序. 怀进鹏提出了一种基于虚拟机的动态完整性度量方案[49]. Juan 提出了运行态数据完整性验证框架 RunTest[8],能够实时地对服务提供者的输入和输出数据的完整性进行一致性监控. Santos 提出了可信云计算平台(Trusted Cloud Computing Platform,TCCP)[27],TCCP 通过提供一个密封的计算环境以阻止对虚拟机的破坏、篡改和非法访问.

在云计算可信服务研究方面,Schiffman 实现了虚拟机验证器[50],能够对虚拟机及其内部的应用程序进行动态完整性度量. 陈海波实现了 CHAOS 系统[51],该系统使得云用户能够确认云服务中虚拟机监控器的版本以及完整性. 张逢喆 提出了 Dissolver 系统[52],进一步完善了用户数据在云端的全生命周期的隐私性保护协议. Intel 公司推出了 SGX(Software Guard eXtensions)技术,能够给用户态程序提供一个可信执行环境,为云计算环境下的信任链构建提供了更加明确的技术框架和解决思路.

4.5 信任链应用系统安全缺陷

TCG 提出的 SRTM 和 DRTM 已经成为提升现有计算机体系结构安全性的主要技术. 但是可信计算技术也成为了许多攻击者的攻击目标.

SRTM 难以防范 TOCTOU(Time of Check,Time of Use)攻击. Bear 系统[53]、IMA 和 Trusted GRUB 在度量操作与加载操作之间都存在着时间窗口问题. 利用 Intel 处理器的系统管理模式(System Management Mode,SMM)和系统管理中断(System Management Interrupt,SMI)对 SRTM 和 DRTM 的攻击也较为普遍,Wojtczuk 给出了对 TXT 技术的攻击方法和针对 tboot 的演示系统[54].

4.6 信任链应用系统安全测评

文献[20,29]对信任链系统展开了一致性测评,发现了国内外大部分可信计算产品并不符合规范说明,存在着可信度量根核(Core Root of Trust for Measurement,CRTM)内部没有平台证书的严重安全问题. 文献[1]认为 TCG 的信任链结构存在的安全问题有:(1)根证书的缺失导致 CRTM 的安全性无法得到保障;(2)TCG 信任链模型中存在信息流安全问题;(3)TCG 信任链并没有从真正意义上实现安全度量和信任链恢复机制.

5 总结与展望

可信计算经过了十余年的发展,已经在构建基础性安全方面体现了其技术优势. 信任链技术是实现可信系统的关键技术之一,受时代和技术发展的影响,其技术特点也在不断变化着,从上世纪侧重保护敏感信息的机密性,到本世纪 TCG 提出的以保护静态信息的完整性实现系统行为的可预期,再到虚拟化计算、云计算等新型计算环境下多种安全需求和应用模式对信任

链技术提出的新挑战: 软件动态可信度量和用户数据的隐私保护. 同时,信任链也随着 SRTM、DRTM、vTPM、TPM 2.0 等新技术和新产品的出现而不断完善着.

TCG 的信任链对于增强信息系统安全起着关键作用,但是基于信任链构建的可信系统还存在着一些开放问题尚待解决: 可信计算理论模型研究发展相对缓慢; 缺少信任链的可信度量数学模型; 缺少云计算环境下的信任链组合安全模型; 信任链规范的安全性尚未得到充分验证; 信任链体系结构存在安全缺陷等. 这些问题制约着着可信计算信任链系统的应用、推广和普及,需要研究人员对其展开深入研究. 特别地,伴随着云计算、物联网等新型计算模式和计算环境的出现,提炼信任链系统在新的情况下所出现的科学问题,并对其进行研究,具有更加迫切的意义.

参考文献

[1] 张焕国,赵波. 可信计算 [M]. 武汉: 武汉大学出版社, 2011. 184 - 193.
Zhang Huan-guo, Zhao Bo. Trusted Computing [M]. Wuhan: Wuhan University Press, 2011. 184 - 193. (in Chinese)

[2] 冯登国,张敏,张妍. 云计算安全研究 [J]. 软件学报, 2011, 22(1): 71 - 83.
Feng Deng-guo, Zhang Min, Zhang Yan. Study on cloud computing security [J]. Journal of Software, 2011, 22(1): 71 - 83. (in Chinese)

[3] 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, 35(10): 15 - 18.
Tan Liang, Xu Zhi-wei. Development of the transitive trusted chain based on TPM [J]. Computer Science, 2008, 35(10): 15 - 18. (in Chinese)

[4] Anupam D, Jason F, Deepak G, et al. A logic of secure systems and its application to trusted computing [A]. Proceedings of the 30th IEEE Symposium on Security and Privacy [C]. Washington, DC: IEEE Press, 2009. 221 - 236.

[5] Shuanghe P, Zhen H. Enhancing PCsecurity with a U-key [A]. Proceedings of the IEEE Symposium on Security and Privacy [C]. Washington, DC: IEEE Press, 2006. 34 - 39.

[6] Wang Z, Jiang X. HyperSafe: a lightweight approach to provide lifetime hypervisor control-flow integrity [A]. Proceedings of the 31th IEEE Symposium on Security and Privacy [C]. Washington, DC: IEEE Press, 2010. 380 - 395.

[7] Weiqi D, Hai J, Deqing Z, et al. TEE: A virtual DRTM based execution environment for secure cloud-end computing [A]. Proceedings of the 17th ACM Conference on Computer and Communications Security [C]. New York: ACM Press, 2010. 663 - 665.

[8] Juan D, Wei W, Xiaohui G, et al. RunTest: assuring integrity of dataflow processing in cloud computing infrastructures [A]. Proceedings of the ACM Symposium on Information, Computer and Communications Security [C]. Washington, DC: IEEE Press, 2010. 293 - 304.

[9] Sailer R, Zhang X L, Jaeger T, et al. Design and implementation of an tcg-based integrity measurement architecture [A]. Proceedings of the 13th USENIX Security Symposium [C]. Oakland: USENIX Press, 2004. 223 - 238.

[10] Kauer B. OSLO: Improving thesecurity of trusted computing [A]. Proceedings of the 16th USENIX Security Symposium [C]. Oakland: USENIX Press, 2007. 229 - 237.

[11] Haldar V, Chandra D, Franz M. Semantic remote attestation: A virtual machine directed approach to trusted computing [A]. Proceedings of USENIX Virtual Machine Research and Technology Symposium [C]. Oakland: USENIX Press, 2004. 3 - 20.

[12] Delaune S, Kremer S, Ryan M, et al. Formal analysis of protocols based on TPM state register [A]. Proceedings of the 24th IEEE Computer Security Foundations Symposium [C]. Washington, DC: IEEE Press, 2011. 66 - 82.

[13] Jun H H, Hyoungshick K, John L, et al. Achieving attestation with less effort: An indirect and configurable approach to integrity reporting [A]. Proceedings of the Sixth ACM Workshop on Scalable Trusted Computing [C]. New York: ACM Press, 2011. 31 - 36.

[14] Sadeghi A R, Selhorst M, Stüble C, et al. TCG inside? A note on TPM specification compliance [A]. Proceedings of the First ACM Workshop on Scalable Trusted Computing [C]. New York: ACM Press, 2006. 47 - 56.

[15] Shen Chang-xiang, Zhang Huan-guo, Wang Huai-min, et al. Research on trusted computing and its development [J]. Science China: Information Sciences, 2010, 53(3): 405 - 433.

[16] Zhang Huan-guo, Yan Fei, Fu Jian-min, et al. Research on theory and key technology of trusted computing platform security testing and evaluation [J]. Science China: Information Sciences, 2010, 53(3): 434 - 453.

[17] 冯登国. 可信计算—理论与实践 [M]. 北京: 清华大学出版社, 2013. 135 - 138.
Feng Deng-guo. Trusted Computing: Theory and Practice [M]. Beijing: Tsinghua University Press, 2013. 135 - 138. (in Chinese)

[18] 邹德清,羌卫中,金海. 可信计算技术原理与应用 [M]. 北京: 科学出版社, 2011. 61 - 72.
Zou De-qing, Qiang Wei-zhong, Jing Hai. Trusted Computing: Technology, Principle and Application [M]. Beijing: Science Press, 2011. 61 - 72. (in Chinese)

[19] 谭良,刘震,周明天. TCG 架构下的证明问题研究及进展 [J]. 电子学报, 2010, 38(5): 1105 - 1112.
Tan Liang, Liu Zhen, Zhou Ming-tian. Development of attestation in TCG [J]. Acta Electronica Sinica, 2010, 38

(5):1105 – 1112. (in Chinese)

[20] 张帆,徐明迪,杨飏. 可信链度量与测评 [M]. 西安: 西安电子科技大学出版社,2011. 69 – 104.
Zhang Fan,Xu Ming-di,Yang Yan. Trusted Chain: Measurement and Evaluation [M]. Xi'an: Xidian University Press,2011. 69 – 104. (in Chinese)

[21] 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.
Zhang Xing,Chen You-lei,Shen Chang-xiang. Non-interference trusted model based on processes [J]. Journal on Communications,2009,30(3):6 – 11. (in Chinese)

[22] 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.
Zhang Xing,Huang Qiang,Shen Chang-xiang. A formal method based on noninterference for analyzing trust chain of trusted computing platform [J]. Chinese Journal of Computers,2010,33(1):74 – 81. (in Chinese)

[23] 徐明迪,张焕国,赵恒. 可信计算平台信任链安全性分析 [J]. 计算机学报,2010,33(7):1165 – 1176.
Xu Ming-di,Zhang Huan-guo,Zhao Heng,et al. Security analysis on trust chain of trusted computing platform [J]. Chinese Journal of Computers,2010,33(7):1165 – 1176. (in Chinese)

[24] Zhou Cong-hua,Liu Zhi-feng,Wu Hai-ling,et al. Symbolic algorithm verification of intransitive generalized noninterference [J]. Science China: Information Sciences,2011,41(11):1310 – 1327.

[25] McCune J M,Bryan P,Adrian P,et al. Flicker: an execution infrastructure for TCB minimization [A]. Proceedings of the 3rd ACM European Conference on Computer Systems [C]. New York: ACM Press,2008. 315 – 328.

[26] Azab A M,Ning P,Wang Z,et al. HyperSentry: enabling stealthy in-context measurement of hypervisor integrity [A]. Proceedings of the 17th ACM Conference on Computer and Communication Security [C]. New York: ACM Press,2010. 38 – 49.

[27] Santos N,Gummadi K P,Rodrigues R. Towards trusted cloud computing [A]. Proceedings of the Workshop on Hot Topics in Cloud Computing [C]. San Diego: ACM Press,2009.

[28] 秦宇,冯登国. 基于组件属性的远程证明 [J]. 软件学报,2009,20(6):1625 – 1640.
Qin Yu,Feng Deng-guo. Component property based remote attestation [J]. Journal of Software,2009,20(6):1625 – 1640. (in Chinese)

[29] 徐明迪,张焕国,严飞. 基于标记变迁系统的可信计算平台信任链测试 [J]. 计算机学报,2009,32(4):635 – 645.
Xu Ming-di,Zhang Huan-guo,Yan Fei. Testing on trust chain of trusted computing platform based on labeled transition system [J]. Chinese Journal of Computers,2009,32(4):635 – 645. (in Chinese)

[30] Deepak G,Jason F,Dilsun K,et al. Towards a Theory of Secure Systems [R]. Pittsburgh: Carnegie Mellon University,2008. 1 – 17.

[31] Deepak G,Jason F,Dilsun K,et al. Compositional system security in the presence of interface-confined adversaries [A]. Proceedings of the 26th Conference on the Mathematical Foundations of Programming Semantics [C]. Amsterdam: Elsevier press,2010. 49 – 71.

[32] Rushby J. Noninterference,Transitivity,and Channel-Control Security Policies [R]. Menlo Park: SRI International,2005. 1 – 50.

[33] 赵佳,沈昌祥,刘吉强. 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.
Zhao Jia,Shen Chang-xiang,Liu Ji-qiang,et al. A noninterference-based trusted chain model [J]. Journal of Computer Research and Development,2008,45(6):974 – 980. (in Chinese)

[34] 秦晰,常朝稳,沈昌祥. 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.
Qin Xi,Chang Chao-wen,Shen Chang-xiang,et al. Research on trusted terminal computer model tolerating untrusted components [J]. Acta Electronica Sinica,2011,39(4):934 – 939. (in Chinese)

[35] 邱罡,王玉磊,周利华. 基于无干扰理论的完整性度量模型 [J]. 四川大学学报(工程科学版),2010,38(4):117 – 120.
Qiu Gang,Wang Yu-lei,Zhou Li-hua. Noninterference-based integrity measurement model [J]. Journal of Sichuan University (Engineering Science Edition),2010,38(4):117 – 120. (in Chinese)

[36] 张帆,陈曙,桑永宣. 完整性条件下无干扰模型 [J]. 通信学报,2011,32(10):78 – 85.
Zhang Fan,Chen Shu,Sang Yong-xuan,et al. Noninterference model for integrity [J]. Journal on Communications,2011,32(10):78 – 85. (in Chinese)

[37] 石文昌,单智勇,梁彬. 细粒度信任链研究方法 [J]. 计算机科学,2008,35(9):1 – 4.
Shi Wen-chang,Shan Zhi-yong,Liang Bin,et al. Approach for research on fine-grained chain of trust [J]. Computer Science,2008,35(9):1 – 4. (in Chinese)

[38] Eggert S,Meyden R,Schnoor H,et al. The complexity of intransitive noninterference [A]. Proceedings of the 32th IEEE Symposium on Security and Privacy [C]. Washington,DC: IEEE Press,2011. 196 – 211.

[39] 周从华,鞠时光. 一种基于 Petri 网的隐蔽信息流分析方法 [J]. 计算机学报,2012,35(8):1688 – 1699.
Zhou Cong-hua,Ju Shi-guang. A petri net based approach

to covert information flow analysis [J]. Chinese Journal of Computers, 2012, 35(8): 1688 – 1699. (in Chinese)

[40] McCullough D. Noninterference and the composibility of security properties [A]. Proceedings of the IEEE Symposium on Security and Privacy [C]. Washington, DC: IEEE Press, 1998. 177 – 186.

[41] Focardi R, Gorrieri R. Classification of security properties [A]. Proceedings of Foundations of Security Analysis and Design [C]. Berlin: Springer-Verlag Press, 2001. 331 – 396.

[42] 常德显,冯登国,秦宇. 基于扩展 LS^2 的可信虚拟平台信任链分析 [J]. 通信学报, 2013, 34(5): 31 – 41.
Chang De-xian, Feng Deng-guo, Qin Yu, et al. Analyzing the trust chain of trusted virtualization platform based on the extended LS^2 [J]. Journal on Communications, 2013, 34(5): 31 – 41. (in Chinese)

[43] Wittbold J T, Johnson D M. Information flow in nondeterministic systems [A]. Proceedings of the IEEE Symposium on Security and Privacy [C]. Washington, DC: IEEE Press, 1990. 144 – 161.

[44] Ryan P, Schneider S. Process algebra and noninterference [J]. Journal of Computer Security, 2001, 9(1): 75 – 103.

[45] 马卓. 无线网络可信接入理论及其应用研究 [D]. 西安: 西安电子科技大学, 2010.
Ma Zhuo. TrustedAccess in Wireless Networks Theory and Applications [D]. Xi'an: Xidian University, 2010. (in Chinese)

[46] 李晓勇,韩臻,沈昌祥. Windows 环境下信任链传递及其性能分析 [J]. 计算机研究与发展, 2007, 44(11): 1889 – 1895.
Li Xiao-yong, Han Zhen, Shen Chang-xiang. Transitive trust and performance analysis in windows environment [J]. Journal of Computer Research and Development, 2007, 44(11): 1889 – 1895. (in Chinese)

[47] Xu Wen-juan., Zhang xin-wen., Hu Hong-xin., et al. Remote attestation with domain-based integrity model and policy analysis [J]. IEEE Transactions on Dependable and Secure Computing, 2012, 9(3): 429 – 442.

[48] Sadeghi A R, Schneider T, Winandy M. Token-Based cloud computing: Secure outsourcing of data and arbitrary computations with lower latency [A]. Proceedings of the 3rd International Conference on Trust and Trustworthy Computing [C]. Berlin: Springer-Verlag Press, 2010. 417 – 429.

[49] 李博,李健欣,胡春明. 基于 VMM 层系统调用分析的软件完整性验证 [J]. 计算机研究与发展, 2011, 48(8): 1438 – 1446.
Li Bo, Li Jian-xin, Hu Chun-ming, et al. Software integrity verification based on VMM-level system call analysis technique [J]. Journal of Computer Research and Development, 2011, 48(8): 1438 – 1446. (in Chinese)

[50] Schiffman J, Moyer T, Shal C, et al. Justifying integrity using a virtual machine verifier [A]. Proceedings of the IEEE Annual Computer Security Applications Conference [C]. Washington, DC: IEEE Press, 2009. 83 – 92.

[51] 陈海波. 云计算平台可信性增强技术的研究 [D]. 上海: 复旦大学, 2008.
Chen Hai-bo. Improving the Dependability of Cloud Computing Systems [D]. Shanghai: Fudan University, 2008. (in Chinese)

[52] 张逢喆,陈进,陈海波. 云计算中的数据隐私性保护与自我销毁 [J]. 计算机研究与发展, 2011, 48(7): 1155 – 1167.
Zhang Feng-zhe, Chen Jin, Chen Hai-bo, et al. Lifetime privacy and self-destruction of data in the cloud [J]. Journal of Computer Research and Development, 2011, 48(7): 1155 – 1167. (in Chinese)

[53] MacDonald R, Smith S W, Marchesini J, et al. Bear: An Open-Source Virtual Secure Coprocessor Based on TCPA [R]. Hanover: Dartmouth College, 2003. 1 – 15.

[54] Wojtczuk R, Rutkowska J. Attacking Intel trusted execution technology [A]. Proceedings of Black Hat DC [C]. Washington, DC: Light Point Security. 2009. 1 – 6.

作者简介

徐明迪　男, 1980 年 11 月生, 湖北武汉人. 2009 年毕业于武汉大学计算机学院, 获得工学博士学位. 现为武汉数字工程研究所副研究员, 硕士生导师, 学术带头人, 主要研究方向为信息系统安全、可信计算、可信软件等.
E-mail: siemendy@whu.edu.cn

张焕国　男, 1945 年 6 月生, 河北蓟县人. 武汉大学计算机学院教授、博士生导师, 空天信息安全与可信计算教育部重点实验室名誉主任、首席科学家, 主要研究方向为容错计算、可信计算、抗量子密码安全等.
E-mail: liss@whu.edu.cn

张　帆(通信作者)　男, 1977 年 10 月生, 湖北当阳人. 2009 年毕业于武汉大学计算机学院, 获工学博士学位. 现为杭州电子科技大学讲师. 主要研究方向为信息系统安全、软件安全等.
E-mail: hdzf@hdu.edu.cn