



基于 VTCM 的分布式可信度量方法

何旺宇^{1,2}, 王中华^{1,2}, 李亚晖^{1,2}

(1. 中国航空工业集团公司西安航空计算技术研究所, 西安 710065; 2. 机载弹载计算机航空科技重点实验室, 西安 710068)

摘 要: 为实现多台协同工作的嵌入式计算机安全启动, 需在每台计算机内嵌入可信计算模块, 但会给资源受限的嵌入式系统带来较大的能耗与管理开销。为此, 提出一种结合可信密码模块(TCM)和虚拟可信密码模块(VTCM)的分布式可信度量方法。将已安装 TCM 模块的嵌入式计算机作为可信基础, 在其他计算机上运行 VTCM 与 TCM 模块验证配置信息以完成分布式可信度量, 从而实现工作域内可信扩展。实验结果表明, 该方法满足嵌入式计算机可信启动过程中的机密性和完整性要求, 在嵌入式环境下具有安全并行启动的可行性。

关键词: 可信计算; 嵌入式计算机; 可信密码模块; 虚拟可信密码模块; 分布式可信度量

开放科学(资源服务)标志码(OSID):



中文引用格式: 何旺宇, 王中华, 李亚晖. 基于 VTCM 的分布式可信度量方法[J]. 计算机工程, 2020, 46(8): 223-227, 234.

英文引用格式: HE Wangyu, WANG Zhonghua, LI Yahui. Distributed trusted measurement method based on VTCM[J]. Computer Engineering, 2020, 46(8): 223-227, 234.

Distributed Trusted Measurement Method Based on VTCM

HE Wangyu^{1,2}, WANG Zhonghua^{1,2}, LI Yahui^{1,2}

(1. Xi'an Aeronautics Computing Technique Research Institute, Aviation Industry Corporation of China, Xi'an 710065, China;

2. Key Laboratory of Aviation Science and Technology on Airborne and Missile-borne Computer, Xi'an 710068, China)

[Abstract] In order to realize the safe start-up of multiple cooperative embedded computers, it is necessary to embed trusted computing module in each computer, but this will bring large energy consumption and management overhead to resource-constrained embedded system. To address the problem, this paper proposes a distributed trusted measurement method combining Trusted Cryptography Module (TCM) and Virtual Trusted Cryptography Module (VTCM). The embedded computer with TCM module installed is used as the trusted base, and the VTCM and TCM module are run on other computers to verify the configuration information to complete the distributed trusted measurement, so as to realize the trusted extension in the work domain. Experimental results show that the method meets the requirements of confidentiality and integrity in the trusted start-up process of embedded computer, and has the feasibility of secure parallel start-up in embedded environment.

[Key words] trusted computing; embedded computer; Trusted Cryptography Module (TCM); Virtual Trusted Cryptography Module (VTCM); distributed trusted measurement

DOI: 10.19678/j.issn.1000-3428.0056142

0 概述

随着信息技术的高速发展, 嵌入式系统被广泛应用于工业、交通、军事以及航天等领域^[1], 成为国家基础设施与武器装备的重要组成部分。嵌入式计算机作为执行命令的重要单元, 容易受到信息攻击, 面临着病毒入侵、木马注入、内部人员非法操作等多种安全问题^[2-4], 因此, 需要在平台内嵌入可信平台

模块(Trusted Platform Module, TPM)或可信密码模块(Trusted Cryptography Module, TCM)^[5-6]以保证其底层硬件环境和平台运行安全可信, 从而实现可信启动^[7-8]。然而对于多个协同工作的嵌入式计算机而言, 如果在其内部使用 TCM 芯片, 则会造成能耗和技术管理上的问题。TCM 嵌入会导致计算机安全防护产生较大的时间与能耗开销^[6,9], 模块更新升级与后期维护也会造成人力和物力方面的负担。

基金项目: 国家部委基金。

作者简介: 何旺宇(1996—), 男, 硕士研究生, 主研方向为嵌入式系统安全; 王中华(通信作者), 高级工程师; 李亚晖, 研究员。

收稿日期: 2019-09-27 **修回日期:** 2019-10-30 **E-mail:** 1131710634@qq.com

此外,由于每个 TCM 模块对应多个证书和密钥类型,因此配置多个 TCM 模块会带来证书与密钥的生成、更新和撤销等管理问题^[10]。

本文通过引入 TCM 和虚拟可信密码模块(Virtual Trusted Cryptography Module, VTCM),提出一种分布式可信度量方法。将多台协同工作的嵌入式计算机构建为工作域,将每台嵌入式计算机作为计算节点,选取计算节点嵌入 TCM 完成可信启动,其他计算节点利用 VTCM 和 TCM 验证配置信息进行分布式可信度量,从而实现域内所有嵌入式平台的可信启动。

1 相关研究

近年来,针对嵌入式系统平台的可信启动问题,国内外学者进行大量研究并取得一定成果。文献[11]指出独立 TPM 芯片不适用于资源受限的嵌入式系统,将基于软件的 TPM 放置在受保护执行区域更合适。文献[12]提出一种基于嵌入式可信模块的嵌入式设备可信启动方法,在 Bootloader 启动前对通信设备进行初始化,建立与嵌入式可信计算模块的连接与认证,用可信计算模块度量 Bootloader,再用其度量操作系统内核。文献[13]设计基于 Vxworks 嵌入式操作系统的可信平台,通过 TPM 完成对该系统可信的完整性度量,增强了嵌入式平台安全性。文献[14]采用双内核架构建立无额外硬件的嵌入式信任根模型,在 VTCM 基础上实现了 FLASH + PMON + 可信内核的软件信任根,为构建嵌入式系统信任根提供可行的低成本方法。文献[15]建立基于国产处理器的嵌入式可信平台,在不增加额外硬件的情况下,大幅提高系统性能。文献[16]提出用于多个嵌入式系统完整性验证的架构,在数据中心等服务器站点获取嵌入式系统代码,通过用户应用程序在远程站点对其进行检查,使用计算得到的散列值验证系统完整性,并显示系统是否被更改,然而该方法不能保证系统可信启动。文献[17]针对 PDA 等手持计算机系统提出一种安全平台体系结构 PERSEUS,该结构采用虚拟机实现不同安全级别应用程序之间的隔离。与此类似,文献[18-19]提出嵌入式 Xen 平台,在 TPM 嵌入式硬件平台上运行多个 VTCM 虚拟机实例,但基于虚拟机的体系结构对系统资源要求较高,不适用于资源受限、强实时性的嵌入式系统^[9]。

在上述研究中,无论用硬件还是软件构建嵌入式系统环境,均主要针对单个嵌入式系统平台。关于多个协同工作的嵌入式系统平台分布式可信度量,目前国内外研究较少。因此,本文针对工作域内多个嵌入式计算机的可信启动问题,提出一种基于 VTCM 的分布式可信度量方法,在域内 1 个可信计算节点嵌入 TCM 模块,在其他非可信计算节点利用 VTCM 插件实现分布式可信度量,从而保证域内所有嵌入式计算机安全可信。

2 设计思路

本文利用 TCM 和 VTCM 插件完成对系统各计算节点分布式可信度量和域内管理密钥生成,基于 VTCM 的分布式可信度量过程如图 1 所示。嵌入式平台上电后,首先通过启动网络交换机加载以太网驱动,为实现分布式可信度量提供数据传输通道,然后在嵌入 TCM 的计算节点完成本地系统平台可信度量,同时其他非可信计算节点运行 VTCM 插件计算操作系统镜像和应用镜像等本地平台操作系统(OS)资源的哈希运算消息认证码(Hash-based Message Authentication Code, HMAC),并通过以太网将其发送给可信计算节点验证。在进行可信度量过程中,TCM 和每个 VTCM 通过信息交互生成域内管理密钥 GK,并用于域内不同计算节点管理组件之间数据传输,以保证域内传输数据安全。

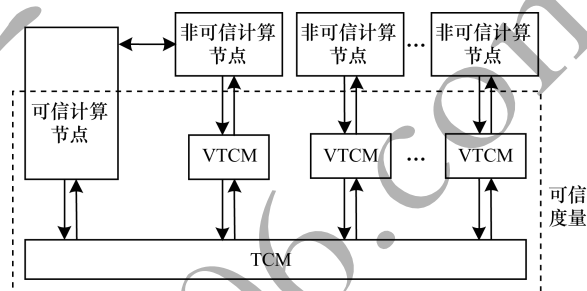


图 1 基于 VTCM 的分布式可信度量过程

Fig. 1 Distributed trusted measurement process based on VTCM

3 分布式可信度量方法

工作域内嵌入式系统上电后,嵌入 TCM 的可信计算节点先完成本地系统可信度量,同时非可信计算节点运行 VTCM 插件,计算得到本地系统资源 HMAC 并发送给 TCM,由 TCM 将该 HMAC 与预先存储的 HMAC 进行对比,若验证成功则启动系统,否则将中断系统启动并在可信计算节点打印错误信息。

在上述流程中,VTCM 作为插件嵌入到 Boot 引导程序(存放在 ROM 中以防止被篡改),VTCM 插件主要包括网卡驱动程序以及 HMAC 和通信 3 个模块。网卡驱动程序主要由初始化程序、关闭网络设备程序、发送数据包程序以及接收数据包程序等组成;HMAC 模块用于系统和应用镜像的签名值计算;通信模块负责与 TCM 保持通信并监听上层应用请求。与 TPM^[20-21]相比,VTCM 没有加密算法引擎、密钥生成器以及随机数生成器等模块,功能较单一,可考虑在后续应用中对其功能进行扩展。VTCM 和 TCM 分布式可信度量过程如图 2 所示,具体如下:

1) TCM 和每个 VTCM 分别预置身份标识(Identification, ID)和秘密信息,同时 TCM 存储每个 VTCM 预置的 ID_i 、秘密值 S_i 以及正确的系统资源值 $HMAC_{S_i}(OS_i)'$,TCM 的预置秘密信息为 S_0 。其中, $S_i(0 \leq i \leq n)$ 为 32 位的随机数, $S_1 \sim S_n$ 为 n 个

VTCM 预置的秘密信息,其分别存储在 TCM 和 VTCM 的安全空间区域内, H 为哈希函数。

2) 启动具有嵌入 TCM 硬件模块的计算节点并完成本地系统平台的可信度量。

3) 非可信计算节点运行 VTCM 插件,VTCM 发送 ID_i 到 TCM。

4) TCM 生成随机数 k ,利用秘密值 S_0 和对称加密算法 $E(x)$ 对 k 进行加密得到 $E_{S_0}(k)$,发送 $E_{S_0}(k)$ 到各 VTCM。

5) VTCM 对收到的 $E_{S_0}(k)$ 解密后得到随机数 k ,利用本地系统资源值和秘密信息 S_i 计算 $V_i = H(k \oplus \text{HMAC}_{S_i}(\text{OS}_i)) (1 \leq i \leq n)$,并发送 V_i 到 TCM。

6) TCM 计算 $V'_i = (k \oplus \text{HMAC}_{S_i}(\text{OS}_i))' (1 \leq i \leq n)$,再与 V_i 进行异或运算,由结果是否为 0 判断 V_i 与 V'_i 是否相等。若两者不相等则返回 VTCM,度量结果验证失败,终止相应非可信计算节点操作系统启动运行;若两者相等则 TCM 生成 1 个随机数 r ,计算 $\text{SK} = \text{HMAC}_r(S_0)$ 和 $E_{S_0}(r)$,然后发送 ID_0 、 ID_i 和 $E_{S_0}(r)$ 到 VTCM。

7) VTCM 对收到的 $E_{S_0}(r)$ 进行解密后得到随机数 r ,计算 $\text{SK} = \text{HMAC}_r(S_0)$ 和 $Z_i = H(\text{ID}_0 \parallel \text{ID}_i \parallel r \parallel S_i)$,发送 ID_i 和 Z_i 到 TCM。

8) TCM 计算 $Z'_i = H(\text{ID}_0 \parallel \text{ID}_i \parallel r \parallel S_i)$,通过异或运算,由结果是否为 0 判断 Z_i 与 Z'_i 是否相等,若两者相等则表示 VTCM 已成功收到 r 。

TCM 通过对每个 VTCM 进行完整性度量判断其是否可信。VTCM 根据 TCM 度量结果判断是否可以安全启动系统。此外,通过 TCM 分发过程,VTCM 安全获得域内管理密钥 $\text{GK} = \text{HMAC}_r(S_0)$ 。

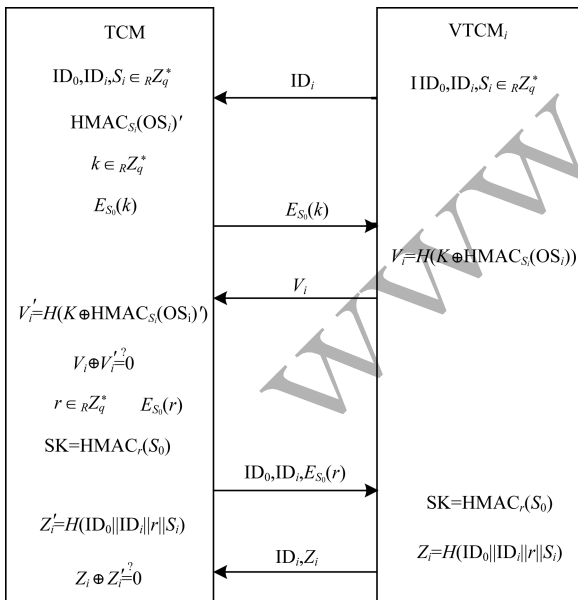


图 2 TCM 和 VTCM 分布式可信度量过程

Fig. 2 TCM and VTCM distributed trusted measurement process

4 方法分析

4.1 基于 BAN 逻辑的方法形式化证明

本文采用 BAN 逻辑分析对分布式可信度量方法进行形式化证明。假设 TCM 是主体 A, VTCM 是主体 B, 证明过程如下:

1) 协议形式化

消息 1: $A \triangleleft ID_i$ 。

消息 2: $B \triangleleft E_{S_0}(k)$ 。

消息 3: $A \triangleleft V_i = H(k \oplus \text{HMAC}_{S_i}(\text{OS}_i))$ 。

消息 4: $B \triangleleft ID_0, ID_i, E_{S_0}(r)$ 。

消息 5: $A \triangleleft ID_i, Z_i = H(\text{ID}_0 \parallel \text{ID}_i \parallel r \parallel S_i)$ 。

2) 安全目标

目标 1: $A \models \text{HMAC}_{S_i}(\text{OS}_i)$ 。

目标 2: $A \models Z_i$ 。

3) 初始假设

假设 1: $A \models A \leftrightarrow_{k,r} B$ 。

假设 2: $B \models A \leftrightarrow_{k,r} B$ 。

假设 3: $A \models \#(k, r)$ 。

假设 4: $A \models B \models \Rightarrow ID_i, S_i, \text{HMAC}_{S_i}(\text{OS}_i) (1 \leq i \leq n)$ 。

假设 5: $B \models A \models \Rightarrow ID_i, S_i, \text{HMAC}_{S_i}(\text{OS}_i)' (1 \leq i \leq n)$ 。

4) 分析推理及结论

(1) 证明 $A \models \text{HMAC}_{S_i}(\text{OS}_i)$

由假设 1 和消息 3 以及 BAN 逻辑消息含义规则式^[22]可以推导出:

$$A \models B \models \sim V_i \quad (1)$$

由假设 3 和新鲜规则式^[22]推导出:

$$A \models \#(V_i), \text{ 即 } A \models \#(\text{HMAC}_{S_i}(\text{OS}_i)) \quad (2)$$

由随机数验证规则式^[22]推导出:

$$A \models B \models \text{HMAC}_{S_i}(\text{OS}_i) \quad (3)$$

由假设 5 和仲裁规则式^[22]推导出:

$$A \models \text{HMAC}_{S_i}(\text{OS}_i) \quad (4)$$

(2) 证明 $A \models Z_i$

由假设 1、消息 5 以及 BAN 逻辑消息含义规则式推导出:

$$A \models B \models \sim Z_i \quad (5)$$

由假设 3 和新鲜规则式推导出:

$$A \models \#(Z_i) \quad (6)$$

由随机数验证规则式推导出:

$$A \models B \models Z_i \quad (7)$$

由假设 5 和仲裁规则式推导出:

$$A \models Z_i \quad (8)$$

经过 BAN 逻辑形式化分析,协议预期目标得到证明,即 TCM 相信其收到的配置信息 $\text{HMAC}_{S_i}(\text{OS}_i)$ 和需要验证的信息 Z_i 均为 VTCM 发送。

4.2 安全性分析

对上述 TCM 和 VTCM 分布式可信度量方法的安全性分析如下:

1) 防窃听和非法读取

由于哈希函数的单向性以及随机数 k, r 的可变性, 因此即使攻击者得到通信信息也无法从中得到 ID_i 对应的秘密信息 S_i 以及用其加密的信息。

2) 防假冒攻击

TCM 发送到 VTCM 的信息经过加密算法加密, 且加密内容为随机数, 攻击者无法伪造 TCM 发送的信息 $E_{s_0}(k)$ 和 $E_{s_0}(r)$ 。

VTCM 在第 1 次发送 ID 后, 其与 TCM 的每次会话都会计算哈希函数值并进行认证, 且每次认证时会更新随机数 k 和 r , 因此, 攻击者假冒 VTCM 发送的伪造信息无法通过验证。

3) 防重放攻击

由于协议目的是在嵌入 TCM 的可信计算节点验证 VTCM 所在计算节点的系统资源 HMAC 是否正确, 因此应确保攻击者无法获取 HMAC。本文协议 VTCM 计算 $V_i = H(k \oplus \text{HMAC}_{S_i}(\text{OS}_i))$ ($1 \leq i \leq n$), 发送 V_i 给 TCM, 从而攻击者就不会获取到 VTCM 所计算的本地系统资源 $\text{HMAC}_{S_i}(\text{OS}_i)$, 且由于每次所用 k 为随机数, 因而即使攻击者得到之前发送的 V_i , 也无法在 TCM 端通过验证, 有效防止了重放攻击。

4) 防中间人攻击

当 TCM 和 VTCM 之间存在中间人时, 中间人能窃听 TCM 和 VTCM 之间通信, 还可将信息进行篡改后发送给另外两方。而采用本文方法即使中间人得到通信信息, 也无法从中得到 ID_i 对应的秘密信息 S_i 以及用其加密的信息。即使中间人篡改 TCM 发送的 $E_{s_0}(k)$ 、 $E_{s_0}(r)$ 或者 VTCM 发送的 V_i 、 Z_i , 也无法在 TCM 端通过验证。

4.3 可信度量功能和性能实验

在 11 台嵌入式开发板上对本文提出的分布式可信度量方法进行可行性验证。开发板搭载 P2020 子卡和 TPM 子卡, P2020 子卡包括 P2020 处理器、100 MHz 以太网等对外接口, TPM 子卡以 Xilinx 公司 FPGA XC7K325TFBG676 芯片为控制核心。开发板外围包括时钟、电源、复位、JTAG、PROM、Flash、CCM3310S 电路及两路 RS232 串行通信接口。TPM 子卡通过 SPI 总线与 CPU 模块进行通信。所有开发板固化相同镜像, 镜像大小为 783 280 Byte。

在 11 台嵌入式开发板中, 10 台为客户端 (非可信计算节点), 1 台为服务器 (可信计算节点), 非可信计算节点运行 VTCM 应用, 可信计算节点运行 TCM 应用, 在应用层对分布式可信度量的时间开销进行测试。测试过程如下:

1) 系统启动后, VTCM 和 TCM 建立通信连接, VTCM 发送 ID 到 TCM。

2) TCM 接收到 ID 后生成随机数 k , 对其进行 AES 加密得到 $E(k)$, 将 $E(k)$ 发送到 VTCM。

3) VTCM 对收到的 $E(k)$ 进行解密后得到随机数 k , 利用本地系统资源值计算得到 $V_i = H(k \oplus \text{HMAC}_{S_i}(\text{OS}_i))$

($1 \leq i \leq 10$), 并发送 V_i 到 TCM。

4) TCM 计算 $V'_i = (k \oplus \text{HMAC}_{S_i}(\text{OS}_i))'$ ($1 \leq i \leq 10$), 然后再与 V_i 进行异或运算, 若运算结果为 0, 则在可信计算节点输出 VTCM 验证成功, 计算从可信计算节点和非可信计算节点开始建立通信连接到 TCM 验证成功所用时间。

经多次测试, 单个 VTCM 分布式可信度量平均时间开销为 574 ms, 其中加解密以及通信传输数据时间为 56 ms, 计算客户端系统资源 HMAC 时间为 518 ms。将系统资源值大小修改为 10 个不同的值进行系统资源值大小对分布式可信度量与 VTCM 计算 HMAC 时间开销的影响测试, 结果如图 3 所示。

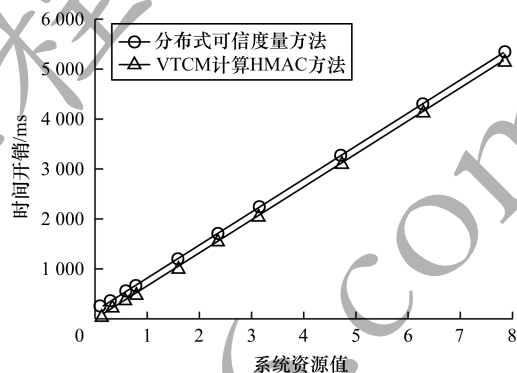


图 3 系统资源值大小对 2 种方法的影响

Fig. 3 Influence of system resource value on two kinds of methods

由图 3 可以看出, 系统分布式可信度量时间开销与 VTCM 计算得到 HMAC 的时间开销均随系统资源值增大而呈线性增长, 其中, 打印信息、加解密以及通信传输数据的时间开销保持不变。

为测试分布式度量方法的有效性, 现修改操作系统代码中网卡配置信息, 构建项目后将可执行文件固化进开发板, 重复上述测试步骤, 得到客户端系统资源 HMAC 如表 1 所示。

表 1 网卡配置修改前后的客户端系统资源 HMAC 对比
Table 1 Comparison of HMAC of client system resources before and after network card configuration modification

时间	客户端系统资源 HMAC
修改前	ee67c4692bf1f07b5b6c3c496793afad
	6ca7808da34306981382dfbb4eaf3e01
修改后	5a4431e8d34f4533f171c6ff0587c84d
	5815113f67f0c9fc4d6bae3ce5f828f7

由表 1 可以看出, 由于修改前后客户端系统资源 HMAC 发生变化, 因此修改后可信计算节点验证配置信息失败, 证明分布式度量方法具备有效性。

通过逐渐增加非可信计算节点数量, 进行非可信计算节点数量对分布式可信度量时间开销的影响测试, 结果如图 4 所示。可以看出, 随着非可信计算节点数量的增加, 系统分布式可信度量时间开销逐渐增加。所有非可信计算节点固化相同系统镜像并在启动过程中同步运行, 可信计算节点循环接收非可信计

算节点连接请求,建立连接后开辟新线程,并与相应非可信计算节点进行通信,相较单个VTCM增加了线程调度、通信以及TCM端打印输出信息的时间开销。在嵌入式系统中,通常5个~6个计算节点构成1个可信的安全域。将其中1个作为可信计算节点,其他作为非可信计算节点,非可信计算节点并行通过可信度量验证并启动,TCM端验证1个非可信计算节点系统资源值时间约为30 ms,完成整个分布式可信度量过程时间开销为707 ms。因此,本文提出的分布式可信度量方法具有嵌入式系统环境下多个计算节点安全启动的可行性。

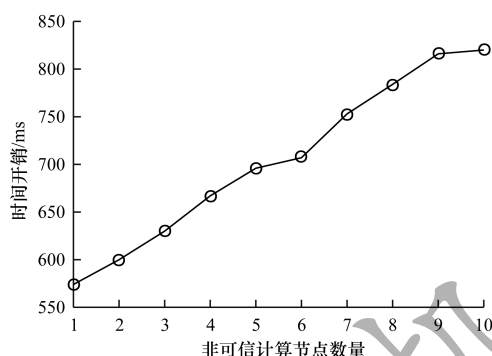


图4 非可信计算节点数量对分布式可信度量时间开销的影响
Fig.4 Influence of the number of non trusted computing nodes on the time cost of distributed trusted measurement

5 结束语

本文提出一种基于VTCM的分布式可信度量方法。对已安装TCM的嵌入式计算机进行可信度量,在非可信计算机上运行VTCM计算得到HMAC并发送给TCM,由TCM将该HMAC与预先存储的相应HMAC进行对比,若验证成功则启动操作系统,否则中断系统启动。实验结果表明,该方法满足嵌入式计算机可信启动过程中的机密性和安全性要求。后续将在机载嵌入式平台上设计和实现VTCM插件功能,进一步对本文提出的分布式可信度量方法进行研究,以实现单个TCM下多台嵌入式计算机的可信启动。

参考文献

- [1] CHEN Shijie. Embedded system security design based on trusted computing technology [D]. Chengdu: University of Electronic Science and Technology of China, 2018. (in Chinese)
陈世杰. 基于可信计算技术的嵌入式系统安全性设计[D]. 成都:电子科技大学, 2018.
- [2] YANG Ziyi, LI Yahui, WANG Zhonghua. High security protection system based on airborne embedded trusted computing platform [J]. Aeronautical Computing Technique, 2018, 48(5): 174-177. (in Chinese)
杨子怡, 李亚晖, 王中华. 基于机载嵌入式可信计算平台的高安全防护系统[J]. 航空计算技术, 2018, 48(5): 174-177.
- [3] MAENE P, GOTZFRIED J, CLERCQ R D, et al. Hardware-based trusted computing architectures for isolation and attestation [J]. IEEE Transactions on Computers, 2018, 67(3): 361-374.
- [4] HAN Lei, LIU Jiqiang, HAN Zhen, et al. Design and implementation of a portable TPM scheme for general purpose trusted computing based on EFI [J]. Frontiers of Computer Science in China, 2011, 5(2): 169-180.
- [5] SHEN Changxiang, ZHANG Huanguo, WANG Huaimin, et al. Research and development of trusted computing [J]. Scientia Sinica Informationis, 2010, 2(2): 139-166. (in Chinese)
沈昌祥, 张焕国, 王怀民, 等. 可信计算的研究与发展[J]. 中国科学: 信息科学, 2010, 2(2): 139-166.
- [6] ZHANG Huanguo, LI Jing, PAN Danling, et al. Trusted platform module in embedded system [J]. Journal of Computer Research and Development, 2011, 48(7): 1269-1278. (in Chinese)
张焕国, 李晶, 潘丹铃, 等. 嵌入式系统可信平台模块研究[J]. 计算机研究与发展, 2011, 48(7): 1269-1278.
- [7] WANG Bo, LI Bo, GAO Zhenjie, et al. Embedded trusted computing platform based on TPM [J]. Microcontrollers and Embedded Systems, 2011, 11(1): 13-16. (in Chinese)
王博, 李波, 高振铁, 等. 基于TPM的嵌入式可信计算平台设计[J]. 单片机与嵌入式系统应用, 2011, 11(1): 13-16.
- [8] KHALID O, ROLFES C, IBING A. On implementing trusted boot for embedded systems [C]//Proceedings of 2013 IEEE International Symposium on Hardware Oriented Security and Trust. Washington D. C., USA: IEEE Press, 2013: 75-80.
- [9] XU Mingdi, YANG Lianjia. Research on trusted computing technology in embedded real-time operation system [J]. Computer Engineering, 2014, 40(1): 130-133. (in Chinese)
徐明迪, 杨连嘉. 嵌入式实时操作系统可信计算技术研究[J]. 计算机工程, 2014, 40(1): 130-133.
- [10] GUO Yu. AIK management in TPM [J]. China Information Security, 2006, 28(4): 76-78. (in Chinese)
郭煜. TPM中身份证明密钥的管理[J]. 信息安全与通信保密, 2006, 28(4): 76-78.
- [11] AARAJ N, RAGHUNATHAN A, JHA N K. Analysis and design of a hardware/software trusted platform module for embedded systems [J]. ACM Transactions on Embedded Computing Systems, 2008, 8(1): 1-31.
- [12] WANG Tianshu, ZHANG Gongxuan, YANG Xichen, et al. Design and implementation of embedded systems trusted initiated mechanism [J]. Computer Measurement and Control, 2015, 23(4): 1364-1370. (in Chinese)
王天舒, 张功萱, 杨曦晨, 等. 嵌入式系统可信启动机制设计与实现[J]. 计算机测量与控制, 2015, 23(4): 1364-1370.
- [13] YANG Xuejiao, RUAN Junzhou, CUI Lizhen. Design and implementation of trusted computing platform based on VxWorks embedded operating system [J]. Radio Engineering of China, 2015, 45(12): 6-9. (in Chinese)
杨雪娇, 阮军洲, 崔丽珍. VxWorks嵌入式系统可信平台的设计与实现[J]. 无线电工程, 2015, 45(12): 6-9.
- [14] KONG Xiangying. Key technology research of trusted computing environment for embedded system [D]. Nanjing: Nanjing University of Aeronautics and Astronautics, 2015. (in Chinese)
孔祥营. 嵌入式系统可信计算环境构建关键技术研究[D]. 南京: 南京航空航天大学, 2015.

(上接第 227 页)

- [15] YI Ping, ZHUANG Yi. Design and implementation of embedded trusted platform based on Loongson processor[J]. Computer Technology and Development, 2018, 28(5): 112-116. (in Chinese)
易平, 庄毅. 基于龙芯处理器的嵌入式可信解决方法[J]. 计算机技术与发展, 2018, 28(5): 112-116.
- [16] ALWOSABI A, SHUKUR Z. Proposed system architecture for integrity verification of embedded systems[J]. Journal of Engineering and Applied Sciences, 2017, 12(9): 2371-2376.
- [17] SADEGHI A R, STÜBLE C. Towards multilaterally secure computing platforms with open source and trusted computing[J]. Information Security Technical Report, 2005, 10(2): 83-95.
- [18] WANG Yinchuan, YANG Lin, SUN Weifeng. Research on Xen implementation of IBM vTPM [J]. Journal of Military Communications Technology, 2010, 31(3): 69-73. (in Chinese)
王因传, 杨林, 孙伟峰. IBM vTPM 的 Xen 实现研究[J]. 军事通信技术, 2010, 31(3): 69-73.
- [19] PAN Wangyang. Research on dynamic integrity measurement model of Xen virtual machine based on vTPM[D]. Baoding: Hebei University, 2017. (in Chinese)
潘汪洋. 基于 vTPM 的 Xen 虚拟机动态完整性度量模型研究[D]. 保定: 河北大学, 2017.
- [20] TRUSTED COMPUTING GROUP. TPM main part 1 design specification[EB/OL]. [2019-08-12]. <https://trustedcomputinggroup.org/resource/tpm-main-specification/>.
- [21] ZHANG Xun. Research of embedded trusted platform module[D]. Xi'an: Xidian University, 2014. (in Chinese)
张询. 可信嵌入式 TPM 技术研究[D]. 西安: 西安电子科技大学, 2014.
- [22] WANG Huifang, GUO Jingeng. BAN logic analysis of SSL3.0 protocol[J]. Computer Engineering, 2001, 27(11): 147-149. (in Chinese)
王惠芳, 郭金庚. 用 BAN 逻辑方法分析 SSL3.0 协议[J]. 计算机工程, 2001, 27(11): 147-149.

编辑 宋 圆