授权约束下的平台配置证明研究

徐明迪[1],张焕国[2],张 帆[3],任正伟[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. 武汉轻工大学数学与计算机学院,湖北武汉 430023)

摘 要: 针对完整性报告协议中平台配置证明存在的安全问题,本文提出了一种基于授权策略的平台配置证明过程,在协议应答者与平台配置证明信息之间建立授权约束,解决应答者提交平台配置信息前存在的篡改攻击,以及提交平台配置信息后存在的中间人攻击. 增强后的协议保持对应性属性,可有效解决平台配置证明存在的全局攻击和局部攻击问题,提高完整性报告协议的安全性.

关键词: 平台配置证明; 对应性属性; 授权约束
中图分类号: TP309. 1 **文献标识码:** A **文章编号:** 0372-2112 (2017)06-1389-07
电子学报 URL: http://www. ejournal. org. cn **DOI:** 10. 3969/j. issn. 0372-2112. 2017. 06. 016

Authorization Restriction-Based Platform Configuration Attestation

XU Ming-di[1], ZHANG Huan-guo[2], ZHANG Fan[3], REN Zheng-wei[1]
(1. *Wuhan Digital and Engineering Institute, Wuhan, Hubei* 430205, *China*;
2. *Key Laboratory of Aerospace Information Security and Trusted Computing Ministry of Education, Wuhan, Hubei* 430205, *China*;
3. *School of Mathematics and Computer Science, Wuhan Polytechnic University, Wuhan, Hubei* 430023, *China*)

Abstract: Aiming at the security problem existing in platform configuration attestation (PCA) of integrity report protocol (IRP), this paper puts forward a PCA based on authorization policy by establishing an authorization restriction between respondent and platform configuration information. The authorization-based PCA prevents the tampering attack before the information of PCA is submitted to the respondent and the middle-man attack after the information of PCA is sent to requester. The proposed PCA holds the correspondence properties and solves the security problems about local and global attacks, which enhances the security of IRP.

Key words: platform configuration attestation; correspondence property; authorization restriction

1 引言

目前,将可信计算技术融入到云计算等新型计算环境,并以可信赖方式提供安全服务已成为云计算安全基础设施研究领域的重要方法[1]. 远程证明是可信计算提供的核心功能之一,能够为云计算应用提供可信的计算环境. 然而,远程证明过程中的完整性度量、完整性存储和完整性报告,都存在着不同程度的安全缺陷[2].

国内外众多学者对完整性报告协议 IRP(Integrity Report Protocol)的安全性问题进行了广泛研究,发现该协议在抵御重放攻击、篡改攻击和假冒攻击上存在安全缺陷[3]. IRP 协议包含了平台身份证明和平台配置证明. 在对 IRP 协议的平台身份证明研究方面,Goldman 等人使用 TLS(Transport Layer Security)为远程证明建立了端到端的安全通道,保证了 IRP 协议中与挑战者通信的实体与应答者是同一个实体,可有效防止中间人攻击[4],但该方法不能解决合谋假冒攻击的问题. Stumpf 等人[5]认为 TPM 内部的 AIK(Attestation Identity Key)既不能为完整性报告协议建立安全信道,也不能对协议参与者进行认证,为此采用了 Diffie-Hellman 密钥协商[6]提出了一种健壮性的 IRP 协议[4]. 张焕国等人提出了 IRP 协议的平台配置证明过程存在着平台配置寄存器 PCR(Platform Configuration Register)可被任意读写操作,以及存储度量日志 SML(Stored Measurement Log)可被任意修改的问题[7,8]. 在 IRP 协议形式化建模与验证

收稿日期:2015-10-15;修回日期:2016-03-10;责任编辑:覃怀银
基金项目:国家自然科学基金(No. 61502438, No. 61272452, No. 61403350)

方面,Xu 等人开发出了基于信息流完整性模型的远程证明系统 DR@ FT[9],在 CW-Lite 模型的完整性度量框架基础上,DR@ FT 将系统的可信性归结为系统状态变化的可信性. Ryan 等人用 Horn 子句对 TPM 的内部状态寄存器 PCR 进行建模[10],并分析了 PCR 状态的变化对 BitLocker 协议带来的攻击. Datta 等人用 LS^2 系统对静态和动态完整性度量协议进行了形式化建模和证明[11].

IRP 协议的参与方包括挑战者和应答者,本文根据攻击者所在位置的不同,将攻击者分为全局攻击者和局部攻击者. 全局攻击者通过截获、篡改、重放等攻击手段对挑战者或应答者进行中间人攻击、伪装攻击和平台配置隐私窃取等. 局部攻击者通过对应答者本地平台的完整性度量架构 IMA(Integrity Measurement Architecture)以及可信平台模块 TPM(Trusted Platform Module)的攻击,包括度量与加载时间差(Time of Check Time of Use,TOCTOU)攻击、信任链攻击和 TPM 硬件攻击等[12]. 针对 IRP 协议中的平台配置证明存在的安全问题,本文解决以下四类攻击带来的安全隐患:

(I) 应答者提供的正确 SML 被全局/局部攻击后,使得挑战者认为远程平台配置信息中的 SML 错误.

(II) 应答者提供的正确 PCR 被局部攻击后,使得挑战者认为平台配置信息中的 PCR 不满足安全预期.

(III) 应答者的正确 PCR 和 SML 同时被局部攻击后,使得局部攻击者构造出能通过 IRP 协议验证过程的 PCR′和 SML′.

(IV) 攻击者绕过应答者构造出可通过验证的 PCR′和 SML′,使得挑战者认为平台配置信息正确.

2 平台配置证明安全分析

在 IRP 协议中,平台配置证明涉及到图 1 中步骤 3b、3c 以及 5b、5c. 步骤 3b 和 3c 用于获取应答者 PB 的 PCR 和 SML,步骤 5b 和 5c 用于对应答者 PB 的 PCR 和 SML 进行安全验证,在应答者 PB 获得本地平台 PCR 和 SML 的过程中,国际可信计算规范没有对 PCR 和 SML 的访问或操作进行安全约束. 这使得应答者 PB 中的局部攻击者 attacker_l 可直接进行恶意修改或破坏,造成应

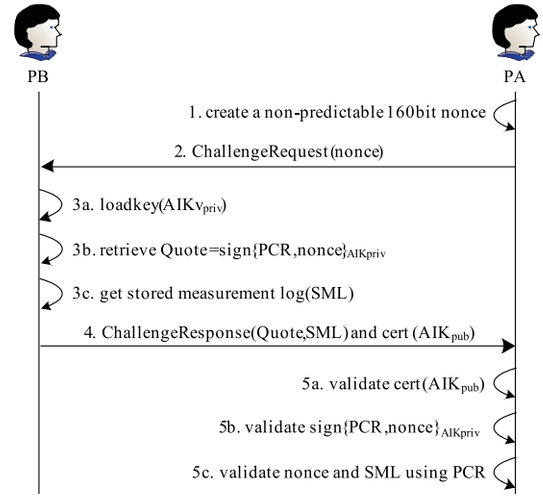


图1 完整性报告协议

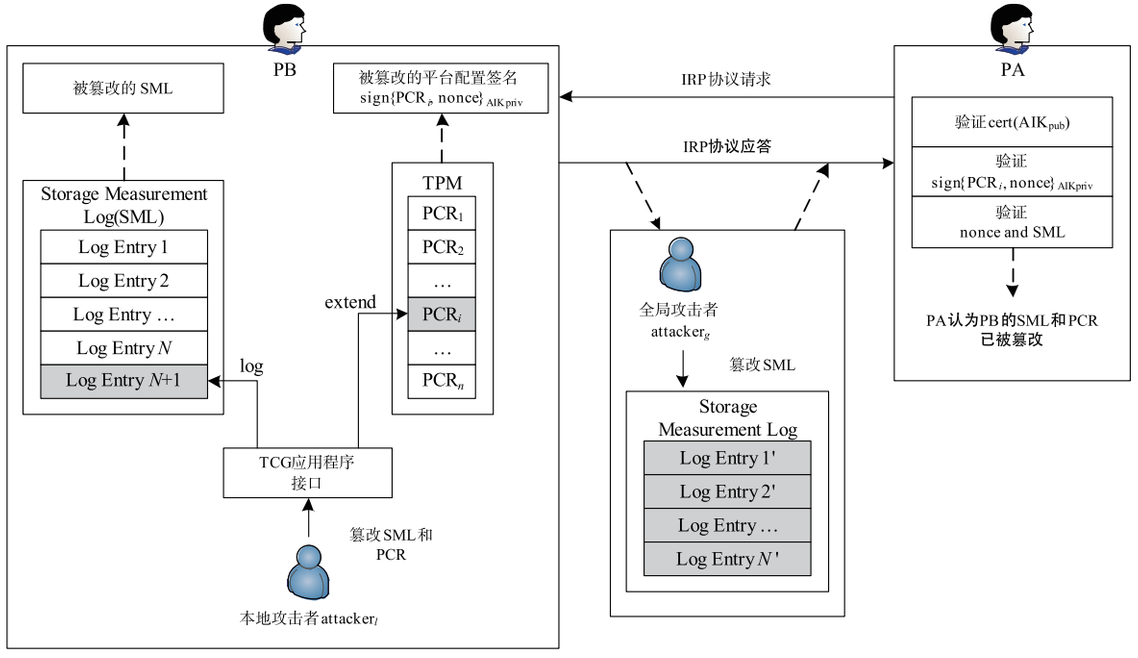


图2 平台配置证明存在的局部攻击和全局攻击

答者 PB 获取的 PCR 和 SML 的可信状态不可控. 同时,全局攻击者 $attacker_g$ 能够直接对明文 SML 进行替换攻击,导致挑战者 PA 对 PCR 和 SML 的验证结果与应答者 PB 的本地实际状态并不一致.

图 2 给出了平台配置证明存在的局部攻击和全局攻击. 局部攻击者(local attacker)位于应答者 PB 平台,在应答者 PB 执行完整性度量协议之前,局部攻击者 $attacker_l$ 分别篡改 PCR 和 SML,造成应答者 PB 发送给挑战者 PA 的平台配置信息与实际值不一致,在没有可信第三方提供 PCR 参考值的情况下,挑战者 PA 难以对 PCR 的真实性进行验证,同时,应答者 PB 可根据平台配置证明的验证规则保持 PCR 和 SML 之间的验证正确性,这也使得挑战者 PA 难以对 SML 的真实性进行判别. 因此,局部攻击能够让不可信运行环境的平台通过验证,也可以让可信运行环境的平台不能通过验证. 全局攻击者(global attacker)对应答者 PB 发送的明文 SML 进行篡改,使得挑战者 PA 认为 PCR 与 SML 之间不一致,在应答者 PB 的运行环境是可信的情况下,全局攻击可造成应答者 PB 不能通过挑战者 PA 的认证.

3　平台配置证明安全增强

3.1　基于授权约束的平台配置证明安全增强

攻击者对平台配置证明进行攻击的前提在于对 PCR 和 SML 访问操作的任意性,为确保应答者在进行完整性度量协议过程的平台配置证明信息的真实性,本文引入授权策略(authPolicy)实现对 PCR 和 SML 访问过程进行安全约束,authPolicy 定义了使用命令接口的断言,包括会话 nonce,共享秘密,失效时间和满足特定值的对象等. 这里的策略可以是单条策略,也可以是多个策略的组合,不同的 authPolicy 通过策略摘要(policyDigest)进行区分.

以平台配置证明中的应答者 PB 收集完整性信息为例,应答者 PB 为防止对 PCR 和 SML 等命令的非授权调用,首先生成授权策略,即:预期的 pcr 值,预期的 locality 值和用户现场物理授权,然后生成不同授权策略下的策略摘要,并对涉及到修改 PCR 和 SML 的所有命令接口进行策略更新. 图 3 给出了增加授权策略后的平台配置证明过程.

$$
\begin{aligned}
&\mathrm{PB} := c(n).\nu x.\nu y.\nu k.\\
&\quad \text{let policyDigest}_{pcrs} =\\
&\quad\ H_{policyAlg}(\text{policyDigest}_{pcrs} \parallel \text{TPM\_CC\_PolicyPCR} \parallel \text{pcrs} \parallel \text{digestTPM}) \text{ in}\\
&\quad \text{let policyDigest}_{locality} =\\
&\quad\ H_{policyAlg}(\text{policyDigest}_{locality} \parallel \text{TPM\_CC\_PolicyLocality} \parallel \text{locality}) \text{ in}\\
&\quad \text{let policyDigest}_{pp} =\\
&\quad\ H_{policyAlg}(\text{policyDigest}_{pp} \parallel \text{TPM\_CC\_PhysicalPresence}) \text{ in}\\
&\quad \text{let policyDigest}_{new} =\\
&\quad\ H_{policyAlg}(\text{policyDigest}_{pcrs} \parallel \text{policyDigest}_{locality} \parallel \text{policyDigest}_{event} \parallel \text{policyDigest}_{pp}) \text{ in}\\
&\quad \text{PolicyUpdate(commandcode, policyDigest}_{new})\\
&\quad \text{let pcr}_x = \text{readpcr}(x, \text{policyDigest}) \text{ in}\\
&\quad \text{let sml}_y = \text{readsml}(y, \text{policyDigest}) \text{ in}\\
&\quad \text{let aik}_k = \text{loadkey}(k, \text{policyDigest}) \text{ in}\\
&\quad \overline{\text{startedB}}\langle n, \text{pcr}_x, \text{sml}_y \rangle\\
&\quad \bar{c}\langle \text{sign}(\text{pair}(\text{pcr}_x, n), \text{aik}_k, \text{policyDigest}) \rangle . \bar{c}\langle \text{sml}_y \rangle . \bar{c}\langle \text{pk}(\text{aik}_k) \rangle .\\
&\quad \overline{\text{completedB}}\langle \text{pair}(\text{sign}(\text{pair}(\text{pcr}_x, n), \text{aik}_k), \text{sml}_y) \rangle
\end{aligned}
$$

$$
\begin{aligned}
&\mathrm{P}_C^l := \nu x.\nu y.\nu z.\nu d.\\
&\quad \text{let } x_h = \text{hash}(x) \text{ in}\\
&\quad \text{let } y_p = \text{readpcr}(y, d) \text{ in}\\
&\quad \text{let } z_s = \text{eventlog}(z, d) \text{ in}\\
&\quad \overline{\text{startedC}_l}\langle x_h, y_p, z_s \rangle\\
&\quad \text{let rc}_0 = \text{extendpcr}(y, y_p | x_h, d) \text{ in}\\
&\quad \text{let rc}_1 = \text{logsml}(z_s, d).\\
&\quad \overline{\text{completedC}_l}\langle \text{pair}(rc_0, 0), \text{pair}(rc_1, 0) \rangle
\end{aligned}
$$

$$
\begin{aligned}
&\mathrm{P}_C^g := c(n).\nu x_1.\nu x_2.\nu y_1.\nu y_2.\nu z.\\
&\quad \overline{\text{startedC}_g}\langle n \rangle\\
&\quad \text{let } x = \text{eventlog}(x_1, x_2, y_1, y_2, z) \text{ in}\\
&\quad \text{let } n' = n + x \text{ in}\\
&\quad \overline{\text{completedC}_g}\langle n' \rangle\\
&\quad \bar{c}(n').
\end{aligned}
$$

图3　增加授权策略后的平台配置证明

3.2　平台配置证明安全增强的完整性报告协议

与图 1 所示的原始 IRP 协议相比,本文提出了安全增强的完整性报告协议(Secure IRP,SIRP),针对 SML 存在的全局和局部替换攻击,篡改攻击,以及 PCR 存在的局部篡改攻击,对 IRP 中的平台配置证明部分进行了安全增强,消除中描述的全局攻击和局部攻击. 如图 4 所示,修改的或增加的协议步骤用方框注明. 下面将分别对平台配置证明全局可靠和局部可靠进行详细描述.

3.3　基于 DH 密钥交换的平台配置证明全局可靠

为防止全局攻击者对明文 SML 进行任意篡改攻击,应答者 PB 通过 Diffie-Hellman 密钥交换对明文 SML 进行加密处理. 在图 4 的步骤 1b 中,挑战者 PA 选择秘密 $a = \mathrm{K}_{\mathrm{priv}}^{\mathrm{PA}}$ 得到 $\mathrm{K}_{\mathrm{pub}}^{\mathrm{PA}} = g^a \bmod q$. 接下来在步骤 3b 中,应

0. PB	: create policy and update policyDigest ' =H(policyDigest ‖ PolicyAssertion)
1a. PA	: create a non -predictable 160bit nonce
1b. PA	: GenerateKey(K^{PA}_{pub},K^{PA}_{priv})
2. PA→PB	: ChallengeRequest(nonce, K^{PA}_{pub})
3a. PB	: Enhanced authorization commands with PolicyCommandCode
3b. PB	: GenerateKey(K^{PB}_{pub},K^{PB}_{priv})
3c. PB	: ComputeSessionKey(K^{PAB})
3d. PB	: loadkey(AIK_{priv})
3e. PB	: retrieve PCR and SML with authorization session
3f. PB	: validate pd with policyDigest '
3g. PB	: retrieve Quote = sign{PCR,SHA1(nonce, K^{PAB}_{pub})}$_{AIK_{priv}}$
3h. PB	: get stored measurement log (SML)
4. PB→PA	: ChallengeResponse(Quote, K^{PAB}_{pub},enc{SML}$_{K^{PAB}}$) and cert(AIK_{pub})
5a. PA	: validate cert (AIK_{pub})
5b. PA	: validate sign {PCR,SHA1(nonce, K^{PAB}_{pub})}$_{AIK_{priv}}$
5c. PA	: ComputeSessionKey(K^{PAB})
5d. PA	: compute sml = dec{enc{SML}$_{K^{PAB}}$}$_{K^{PAB}}$
5e. PA	: validate nonce and sml using PCR
6. PA	: create a non -predictable 160bit nonce$_1$
7. PA→PB	: ChallengeRequest(nonce$_1$)
8. PB	: compute res = enc{nonce$_1$}$_{K^{PAB}}$
9. PB→PA	: ChallengeResponse(res)
10. PA	: validate nonce$_1$

图4 安全增强后的完整性报告协议

答者 PB 选择秘密 $b = K^{PB}_{priv}$ 得到 $K^{PB}_{pub} = g^b \bmod q$. 在图 4 的步骤 3c 和 5c 中,应答者 PB 和挑战者 PA 分别计算得到会话密钥 $K^{PAB} = (K^{PA}_{pub})^b \bmod q = (K^{PB}_{pub})^a \bmod q$,应答者 PB 在图4 的步骤4 中用会话密钥 K^{PAB}对明文 SML 加密,防止全局攻击者对明文 SML 的篡改攻击. 对于 DH 密钥交换的中间人攻击,图 4 的步骤 3g,步骤 4,步骤 5b 都把 K^{PB}_{pub}作为参数进行运算,能够对 K^{PB}_{pub}所在的参与方 PB 进行认证. 图 4 的步骤 6 ~ 10 继续完成 DH 密钥交换过程.

在描述的全局攻击中,全局攻击者 P^g_C 为达到对 SML 攻击的目的,首先必须获得项 enc{SML}$_{K^{PAB}}$中的 SML,也就是要获得 K^{PAB}. 全局攻击者 P^g_C 虽然可以进行替换攻击:即用 K^{PC}_{pub}去替换挑战者 PA 的公钥 K^{PA}_{pub},使得应答者 PB 使用了会话密钥 K^{PAC}对 SML 进行加密并得到 enc{SML}$_{K^{PAC}}$,但由于在步骤 3g 中应答者 PB 加入了对自身公钥 K^{PB}_{pub}的认证,使得全局攻击者 P^g_C 不能将 ChallengeResponse(Quote K^{PB}_{pub}, enc{SML}$_{K^{PAC}}$ and cert(AIK_{pub}))中的 K^{PB}_{pub}替换为 K^{PC}_{pub},因此挑战者 PA 计算的会话密钥是 K^{PAB},在步骤 5d 中挑战者 PA 计算 dec{enc{SML}$_{K^{PAC}}$}$_{K^{PAB}}$将发现 SML 已经受到攻击,因此本文的方案可保证平台配置证明全局可靠,同时,通过会话密钥 K^{PAB}对平台配置完整性进行加密保护,在一定程度上解决了 IRP 协议存在的隐私泄露问题.

3.4 基于授权策略的平台配置证明局部可靠

为防止局部攻击者 P^l_C 通过命令接口对 PCR 和 SML 进行恶意修改,在图 4 的步骤 0 中,应答者 PB 首先根据授权策略类型生成授权断言 PolicyAssertion,并计算授权摘要 policyDigest′ = H(policyDigest‖PolicyAssertion),进一步的,在图 4 的步骤 3a 中,应答者 PB 通过授权策略 PolicyCommandCode 防止局部攻击者实现 attacker(extendpcr())和 attacker(logsml()),并在图 4 的步骤 3e 和步骤 3f 中对授权摘要进行验证,由于授权摘要的更新使得对命令接口的调用必须包含授权会话过程,使得局部攻击者通过命令接口对 PCR 和 SML 进行篡改攻击是不可行的.

进一步的,在描述的局部攻击中,局部攻击者 P^l_C 需要构造出 pcr_x 和 sml_y,使其通过挑战者 PA 的验证,那么局部攻击者 P^l_C 需要获得知识 attacker(extendpcr(x,y))和 attacker(logsml(x)),增强后的 IRP 协议要求所有的命令接口加入授权策略,即 H(policyDigest‖PolicyAssertion),使得局部攻击者 P^l_C 需要获得知识 pd = H(policyDigest‖PolicyAssertion),才能获得知识 attacker(extendpcr(x,y))和 attacker(logsml(x)),其中哈希函数 H 基于 SHA-1 密码算法,因此攻击者获得 policyDigest′的计算复杂度为 $O(2^{160})$,在计算上获得授权策略是不可行的,因此本文的方案可保证平台配置证明局部可靠.

4 安全实验系统

4.1 平台配置证明攻击系统

根据 IRP 协议中的平台配置证明过程,实验系统分为对平台配置证明的攻击系统以及安全增强后的平台配置证明系统. 应答者平台采用 HP NC6400 可信笔记本,可信平台模块为 IFX1.2,可信度量根核 CRTM 支持 MA/MP 驱动,操作系统加载器对开源软件 tgrub1.5 进行定制开发,操作系统为 Ubuntu12.10,可信软件栈为 trousers0.3.7,可信网络连接采用 TNC@ FHH0.8.3. 如图 5 所示,网络攻击者 P^g_C 通过构造 AttackerEventStruc 攻击序列对 SML 进行全局攻击造成第 I 类攻击.

本地攻击者 P_C^l 通过在应答者平台中通过局部攻击 PCR 造成第 II 类攻击;通过构造满足迭代验证的 AttackerEventStruc 攻击序列,并分别对 PCR 和 SML 进行局部攻击,造成第 III 类和第 IV 类攻击. 下面分别对这四类攻击的实验系统进行描述.

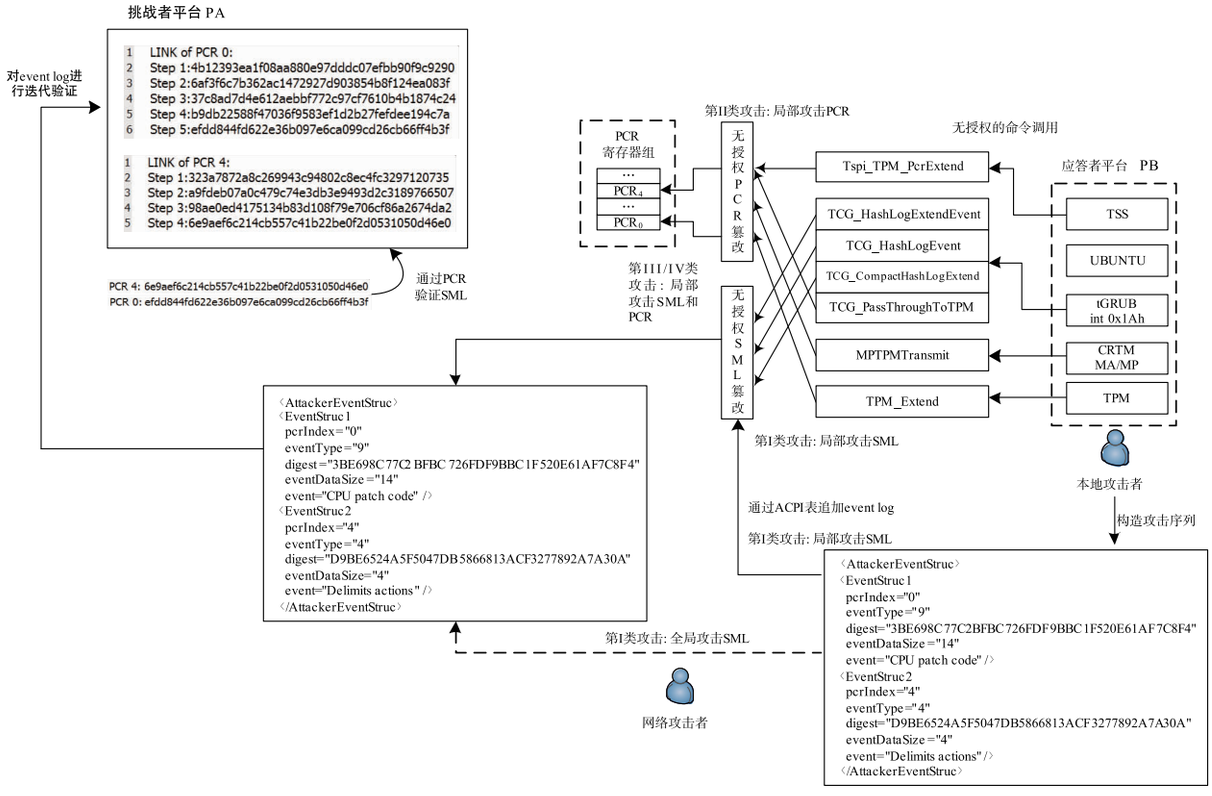


图5　对平台配置证明进行攻击的实验系统

对应前文所述的第 I 类攻击,对于全局攻击 SML 而言,在 Dolev-Yao 攻击模型下,网络攻击者 P_C^g 通过网络窃听方式对 IRP 协议中的 SML 明文进行截获,并对 EventStruc 列表中的五元组 eventlog(x_1,x_2,y_1,y_2,z) 进行修改后转发;或通过构造子构建出新的 EventStruc 结构对原始 SML 进行替换后转发. 挑战者 PA 收到挑战应答后,在图 1 的步骤 5c 进行验证时将发现 SML 错误.

对于局部攻击 SML 而言,本地攻击者 P_C^l 在 CRTM 的 POST 阶段,通过 TCG_HashLogEvent、TCG_HashLogExtendEvent 或 TCG_CompactHashLogExtendEvent 将 AttackerEventStruc 追加至 SML,实现 attacker(logsml(x)),挑战者 PA 收到挑战应答后,在步骤 5c(图 1)进行验证时将发现 SML 错误.

(2) 局部攻击 PCR

本地攻击者 P_C^l 可选择在 CRTM 的 POST 阶段,tgrub1.5 的 Stage2 阶段,或在 Ubuntu12.10 中,分别通过二进制命令流 TPM_Extend、TCG_PassThroughToTPM 或应用层接口 Tspi_TPM_PcrExtend 实现 attacker(extendpcr(x,y)),造成 IRP 协议发送的 PCR 与应答者平台的平台配置不一致,并造成挑战者 PA 收到挑战应答后,在图 1 的步骤 5c 进行验证时将发现 SML 错误.

(3) 局部攻击 SML 和 PCR

第 III 类和第 IV 类攻击结合了前两类攻击,都可归结为局部攻击 SML 和 PCR. 本地攻击者 P_C^l 相继进行局部攻击 PCR 和局部攻击 SML. 首先在 AttackerEventStruc 中的 EventStruc1 和 EventStruc2 构造出与 PCR_0,PCR_4 关联的事件结构,通过局部攻击 SML 将 AttackerEventStruc 追加至 SML,然后通过局部攻击 PCR 分别对 PCR_0,PCR_4 实现 attacker(extendpcr(p,d)). 使得挑战者在图 1 的步骤 5c 进行验证时始终认为平台配置信息正确.

4.2　安全增强后的平台配置证明系统

为防止本地攻击者 P_C^l 进行局部攻击 SML 和 PCR,需对 TPM 的命令接口进行授权访问. 本文对开源软件 tpm_emulator0.7.4 进行授权策略安全增强,在每个命令的输入参数结构中增加授权结构,主要包括会话句柄 sessionHandle,随机数 nonce,会话属性 sessionAttributes 和授权值 authorization 等信息,用于对 PCR 的

reset 和 extend 操作,以及对 SML 的 logevent 操作进行授权检查. 授权策略 authPolicy 包含了图 6 列出的 8 种情况,硬件环境如 PCR,locality,NV,PhysicalPresence 都被作为硬件授权断言,软件环境如 signed,secret,ticket,CpHash 都被作为软件授权断言. 应答者在系统完成了完整性度量后可通过 TPM_PolicyCommandCode 对有特定安全要求的命令接口增加授权策略,本文对 TPM_PCR_Extend,TPM_PCR_Event 和 TPM_EventSequence 增加了不同的授权策略,下面将对如何防范上节所描述的四类攻击进行描述.

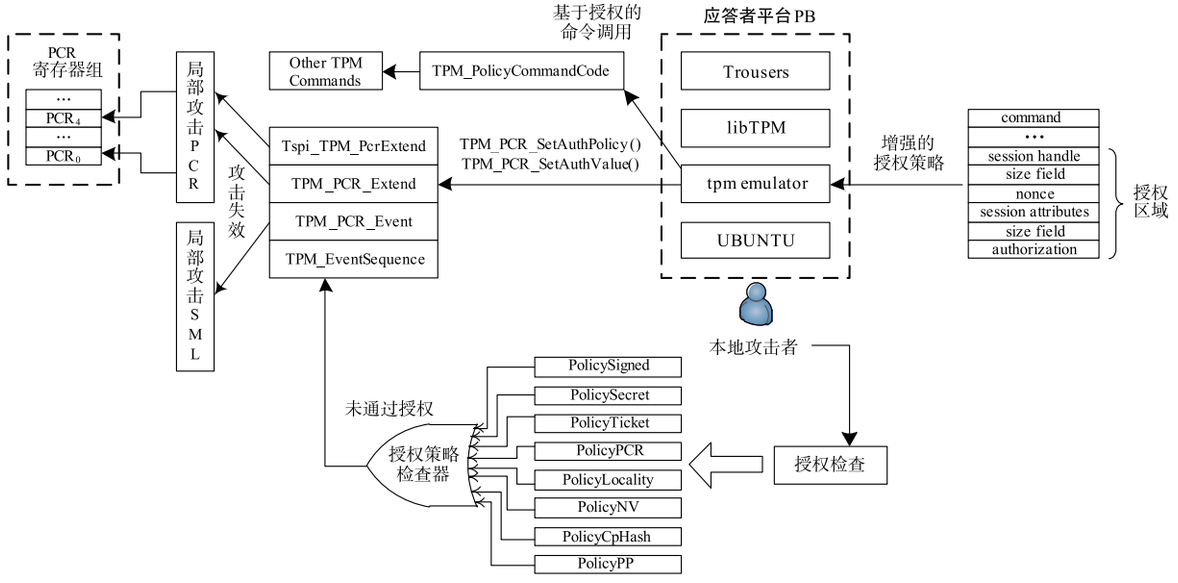


图6 对平台配置证明进行攻击的实验系统

(1) 防范全局/局部攻击 SML

对于全局攻击 SML 而言,由于明文 SML 在应答者平台已经被加密为 $\mathrm{enc}\{\mathrm{SML}\}_{K^{PAB}}$,网络攻击者 P_C^g 攻击 SML 需要获得 K^{PAB},因此该攻击方式在计算上是不可行的.

对于局部攻击 SML 而言,虽然本地攻击者 P_C^l 可构造出 AttackerEventStruc,但在调用命令接口 TPM_EventSequence()时触发了授权策略检查器,需通过 8 种授权策略组合的检查,由于本地攻击者 P_C^l 不能获得知识 H(policyDigest||PolicyAssertion),进而 attacker(logsml())总是不成立的.

(2) 防范局部攻击 PCR

对于局部攻击 PCR 而言,应答者通过 TPM_PCR_SetAuthPolicy()将对单个 PCR 或一组 PCR 的操作与授权策略关联,与局部攻击 SML 相同,attacker(extendpcr())也是不成立的.

(3) 防范局部攻击 SML 和 PCR

由于局部攻击 SML 和局部攻击 PCR 都不成立,即使本地攻击者 P_C^l 构造出与 PCR_0,PCR_4 关联的事件结构,但通过局部攻击 SML 将 AttackerEventStruc 追加至 SML 是不成立的,通过局部攻击 PCR 分别对 PCR_0,PCR_4 实现 attacker(extendpcr(p,d))也是不成立的,因此第 III 类攻击和第 IV 类攻击都是不成立的.

安全增强后的平台配置证明系统对原有 IRP 协议增加了额外的计算和通信开销. 如图 4 所示,为了防范全局攻击 SML,步骤 1b 至步骤 3c 在挑战者平台 PA 和应答者平台 PB 之间增加了 DH 密钥交换过程,用于生成会话密钥 K^{PAB};为了防止局部攻击 SML 和局部攻击 PCR,步骤 3e 至步骤 3g 通过授权会话对 PCR 和 SML 命令接口的授权策略进行检查;步骤 5b 至步骤 5d 用于对加密后的 SML 进行解密操作.

5 总结

平台配置证明是完整性报告协议的一部分,也是保障云计算外包计算的重要手段之一,PCR 和 SML 是平台配置证明的重要部件,由于缺乏必要的授权约束,使得存在对 SML 的全局攻击,以及对 PCR 和 SML 的局部攻击. 这四类攻击出现的原因在于协议应答者提供的平台配置信息与本地实际状态不一致,为解决该问题,本文提出了一种基于授权策略的平台配置证明过程,给出了安全增强后的完整性报告协议,在协议应答者与平台配置证明信息之间建立授权约束,解决了应答者提交平台配置信息前存在的命令接口攻击,以及提交平台配置信息后存在的中间人攻击,提高完整性报告协议的安全性. 下一步将结合云平台进行实际测试和应用.

致谢　感谢匿名审稿专家给本文提出的宝贵意见.

参考文献

[1] 冯登国,张敏,张妍,等. 云计算安全研究[J]. 软件学报,2011,22(1):71 -83.
Feng D G,Zhang M,Zhang Y,et al. Study on cloud computing security [J]. Journal of Software,2011,22(1):71 -83. (in Chinese)

[2] 徐明迪,张焕国,张帆,等. 可信系统信任链研究综述[J]. 电子学报,2014,42(10):2024 -2031.
Xu M D,Zhang H G,Zhang F,et al. Survey on chain of trust of trusted system [J]. Acta Electronica Sinica,2014,42(10):2024 -2031. (in Chinese)

[3] 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 Z. Trusted Access in Wireless Networks Theory and Applications [D]. Xi'an:Xidian University,2010.

[4] Goldman K,Perez R,Sailer R. Linking remote attestation to secure tunnel endpoints [A]. Proceedings of the first ACM Workshop on Scalable Trusted Computing [C]. New York:ACM Press,2006. 21 -24.

[5] Stumpf F,Tafreschi O,Röder P,et al. A robust integrity reporting protocol for remote attestation [A]. Proceedings of the Second Workshop on Advances in Trusted Computing [C]. Berlin:Springer-Verlag Press,2006. 25 -36.

[6] Whitfield D,Martin H. New directions in cryptography [J]. IEEE Transactions on Information Theory,1976,22(6):644 -654.

[7] 徐明迪,张焕国,赵恒,等. 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 M D,Zhang H G,Zhao H,et al. Security analysis on trust chain of trusted computing platform [J]. Chinese Journal of Computers,2010,33(7):1165 -1176. (in Chinese)

[8] Zhang H G,Yan F,Fu J M,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.

[9] Xu W J,Zhang X W,Hu H X,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.

[10] Arapinis M,Ritter E,Ryan M. StatVerif:verification of stateful processes [A]. Proceedings of the 24th IEEE Computer Security Foundations Symposium [C]. Washington,DC:IEEE Press,2011. 33 -47.

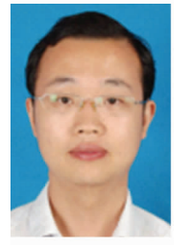
[11] Datta A,Franklin J,Garg D,et al. A logic of secure systems and its application to trusted computing [A]. Proceedings of the 30th IEEE Symposium on Security and Privacy [C]. Washington,DC:IEEE Press,2009. 221 -236.

[12] Jain L,Vyas J. Security Analysis of Remote Attestation [R]. Palo Alto:Stanford University,2008.

作者简介

徐明迪　男,1980 年 11 月出生,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 月出生,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. 现为武汉轻工大学数学与计算机学院讲师. 主要研究方向为信息系统安全、软件安全等.
E-mail:hdzf@hdu.edu.cn

任正伟　男,1986 年 4 月生,湖北新洲人. 2014 年毕业于武汉大学计算机学院,获工学博士学位. 现为武汉数字工程研究所助理研究员. 主要研究方向为应用密码学、云计算安全等.
E-mail:zhengwei_ren@163.com