支持验证代理方的远程证明模型及其安全协议

张志勇[1,2]，裴庆祺[1]，杨 林[3]，马建峰[1]

(1. 西安电子科技大学 计算机网络与信息安全教育部重点实验室，陕西 西安 710071；2. 河南科技大学 电子信息工程学院，河南 洛阳 471003；3. 中国电子设备系统工程公司 研究所，北京 100039)

摘要：针对现有的远程证明模型中存在的终端平台基本配置细节与安全属性特征等隐私的保护问题，提出了一种具有委托模式的支持验证代理方的远程证明模型(AP²RA)及其安全协议. 引入可信第 3 方接受验证方的委托，实施终端软硬件的完整性和安全性证明，并可信地报告平台当前状态的布尔值，改进了基于验证双方的远程证明模式，有效地保护了被验证方的平台隐私. 与已有的方案相比，该方案能够抵抗被验证方消息重放攻击和共谋攻击，以及追踪对验证代理方(APP)发起攻击的终端平台，适用于可信网络中的资源分发与信息共享等环境.

关键词：可信计算；远程证明；隐私保护；安全协议

中图分类号：TP309 **文献标识码**：A **文章编号**：1001-2400(2009)01-0058-06

Attestation proxy party-supported remote attestation model and its secure protocol

ZHANG Zhi-yong[1,2], *PEI Qing-qi*[1], *YANG Lin*[3], *MA Jian-feng*[1]

(1. Ministry of Education Key Lab. of Computer Network and Information Security, Xidian Univ., Xi'an 710071, China; 2. Electron. Inf. Eng. Coll., Henan Univ. of Sci. & Technol., Luoyang 471003, China; 3. The Research Inst., China Electron. Equ. & Sys. Eng. Corp, Beijing 100039, China)

Abstract: Since existing remote attestation models lead to an issue of privacy protection of basic configuration details and security attribute features of the terminal platform, an Attestation Proxy Party-supported Remote Attestation (abbr. AP²RA) model and its secure protocol, which have a delegation mode, are presented. The Trusted Third Party is introduced to accept an attestion delegation from the Attestor Party, implements integrity and security attestation of hardware and software on the terminal, and further trustworthily reports the boolean value of the current platform status, thus improving the remote attestation model based on two parties, as well as effectivly protecting the platform privacy of the Attested Party. Moreover, compared with other approaches, the proposed approach is capable of resisting against the message replay attack and collusion attack from the Attested Party together with the tracing terminal platform sponsoring attack on APP, so that it is suitable for resource dissemination and information sharing in the trusted network.

Key Words: trusted computing; remote attestation; privacy protection; secure protocol

远程证明(RA)[1]作为可信计算中的关键技术，旨在实现终端平台依赖可信芯片模块，通过本地度量忠实地向外界报告自身的完整性状态，使得远程实体能够确信平台的软硬件组件在按照预期的方式运行，没有被篡改和攻陷. 目前，RA 国内外研究主要集中在度量方式和验证机制上，如基于二进制代码度量的 TCG 方案[1]、基于平台属性[2-3]、软件语义或行为[4-6]的远程证明等，以及设计高安全性的 RA 相关协议[3,7]. 然而，这些仅支持验证双方参与的 RA 必然会导致平台隐私的暴露问题，其中包括平台身份隐私和基本配置隐私两

收稿日期：2007-11-09

基金项目：国家自然科学基金项目资助(60803150，60573036)；国家自然科学基金重点项目资助(60633020)；高等学校学科创新引智计划项目资助(B08038)

作者简介：张志勇(1975-)，男，河南科技大学副教授，西安电子科技大学博士研究生，E-mail：xidianzzy@126.com.

个方面,前者 TCG 已通过可信第 3 方 Privacy CA 和 DAA 协议[7]加以解决,而后者使得敌手能够结合平台软硬件配置细节、安全属性以及上层应用运行时的软件行为特征,发起更广泛、更具有针对性的攻击[2-3,8].文献[8]综述性地提出了几种 RA 模型,如基于验证双方的 RA,基于 3 方的"拉"模式,"推"模式和委托模式等,其中后两种模式能够有效地保护平台配置隐私,但文中并未深入探讨一个具有委托模式的 RA 模型及其安全协议,而是基于 Web 验证服务采用"推"模式和扩展平台配置寄存器机制保护平台隐私.笔者提出了具有委托模式的支持可信第 3 方验证的 AP²RA 模型与安全协议,并给出了与其他方案在机制和功能性方面的分析对比.

1　形式化的远程证明模型

1.1　AP²RA 模型基本框架

针对现有的 RA 模型存在着平台配置信息和安全属性等隐私的暴露问题,AP²RA 通过引入可信第 3 方——验证代理方(APP)改进现有的远程证明模式,由验证方(AtorP)发起验证请求,与被验证方(AtedP)协商认可一个 APP,然后 APP 和 AtedP 之间对被验证对象(AO)进行 RA 质询-应答,最后由 APP 验证组件来验证平台的完整性和安全性,并将平台(或 AO)状态的布尔值结果,即是否完整性保持和安全属性满足基本策略等,作为 RA 报告传递给 AtorP.这里 AtorP 并没有得到被验证方的平台配置细节和安全属性特征,有效地解决了被验证方的平台隐私保护问题,同时也提高了验证系统的可生存性.一旦验证方被攻陷,APP 仍然可以有效地提供远程证明服务,并安全地保持验证的结果.AP²RA 模型如图 1 所示.

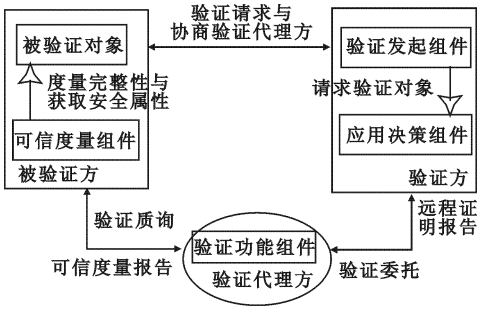

图 1　支持验证代理方的远程证明模型

1.2　基本实体与组件

AP²RA 模型主要由 AtedP,AtorP 和 APP 等 3 个基本实体构成,它们的功能性定义如下:

被验证方　RA 过程的受动者,在可信计算环境下,它通常为终端平台本身及其内部软硬件组件、固件等,利用可信芯片模块及上层软件栈完成可信度量,然后向外界实体可信地报告度量值.

验证方　RA 过程的发起者,通常为远端的验证平台.AtorP 根据应用需求发起验证请求,并借助于 APP 的 RA 报告及应用策略进行访问决策.

验证代理方　RA 过程的施动者,是验证双方认可的可信第 3 方.APP 接受 AtedP 发送的可信度量值,并依据完整性参考值和基本安全策略验证当前终端平台或 AO 的完整性和安全性,并向 AtorP 提供平台状态报告.

3 个实体中涉及以下基本组件,它们属于逻辑上的功能性组件,具体可实现为一个或多个硬件组件、软件代码或服务程序等.

被验证对象　RA 中被验证的固件、硬件组件、软件代码或进程(组)等,它们构成终端平台的软硬件环境,例如 BIOS,OS Loader,OS Kernel 及应用程序等.

可信度量组件(TMC)　AtedP 平台中提供可信度量机制的软件代码或硬件芯片.这里的可信度量模式采用基于二进制代码的完整性度量和获取安全属性相结合机制,前者利用散列算法来实施,后者对于软件代码及应用程序可通过访问平台特征数据、基于安全漏洞扫描、基于软件语义的对象属性检测[4]等机制获取安全属性.在 OS Kernel 加载前,即 BIOS-OS Loader-OS Kernel 信任链建立的安全启动过程中,TMC 主要功能为完整性度量,由 BIOS 中的 CRTM 和可信芯片模块完成;在 OS Kernel 加载之后,TMC 的功能为对 OS 服务程序和应用程序的完整性度量和安全评估.

验证功能组件(AFC)　RA 中提供可信验证机制的软硬件组件或程序等,通过访问完整性参考值和基本安全策略数据库,与 AtedP 提供的可信度量值进行校验,判定系统当前状态,并将验证结果作为 RA 报告发送给 AtorP.

验证发起组件(ASC)　RA 中发起证明请求的组件,通常为位于 AtorP 端的一段应用代码,根据应用需

求来激活 RA 会话.

应用决策组件(ADC) AtorP 中提供应用决策机制的软硬件组件,结合 APP 的 RA 报告和其他应用级安全策略判定 AtedP 是否通过平台或 AO 的远程证明,进行访问控制.

1.3 证明模式形式化定义

基于 BNF 形式化定义 AP²RA 证明模式中的主要操作如下:

$<\text{Action}>::=<\text{ActionName}>\text{“}\triangleq\text{”“}[\![\text{”}<\{\text{Actor}\}>\text{“}]\!]\text{”}<\text{ActionOperator}>[\text{“}\Rightarrow\text{”}][<\text{Result}>]$,

$<\text{Actor}>::=\{<\text{Entity}|\text{Component}|\text{Function}>\}$,

$<\text{ActionOperator}>::=\perp\ |\ \mapsto\ |\Delta|\ \wedge\ |\frac{\Delta}{\wedge}|\xleftrightarrow[\text{AC}]{\text{MR}}|\ \nabla\ |\ \vee\ |\frac{\nabla}{\vee}|\xleftrightarrow[\text{AR}]{\text{platformStatus}}|\ \Diamond$,

$<\text{ActionResult}>::=\{<\text{Function}>|<\text{Attributes}>|<\text{BooleanValue}>\}$.

定义 1(APP 协商) AtedP 和 AtorP 通过消息交互共同认可第 3 方 APP,信任它所实施的平台验证与报告,以及对平台隐私的保护. 记“$\perp$”为协商操作符.

$$\text{NegotiationAPP}\triangleq[\![\text{AtedP},\text{AtorP},\text{APP}]\!]\perp\Rightarrow<\text{Success}|\text{Fail}>\ .$$

定义 2(RA 会话) 一次完整的远程证明过程称为 RA 会话,包括从 AtorP 发起证明委托请求到 AtorP 基于 RA 报告作出应用决策的所有步骤与操作,即验证委托 AtorP_AttestDelegation、可信度量 AtedP_TrustedMeasure、度量报告 AtedP_MeasureReport、平台验证 APP_PlatformAttest、RA 报告 APP_RAReport,应用决策 AtorP_ApplicatonDecision 等.

定义 3(验证委托) AtorP 向验证双方可信的 APP 发出委托验证请求,由 APP 执行平台或 AO 的验证并可信地报告当前状态. 具体委托过程参见 2.2 节协议,记“$\mapsto$”为委托操作符.

$$\text{AtorP\_AttestDelegation}\triangleq[\![\text{AtorP},\ \ \text{APP}]\!]\mapsto\Rightarrow<\text{Success}|\text{Fail}>\ .$$

定义 4(可信度量) AtedP 利用可信度量组件所提供的完整性度量和安全属性获取功能,将 AO 的二进制代码度量值采用迭代哈希的方式存放于平台配置寄存器(PCR),同时保存获取的安全属性值,如软件补丁版本,病毒库数据版本、对象安全级、是否采用进程隔离机制等,并将度量过程写入平台的可信度量日志(TML). 记“$\frac{\Delta}{\wedge}$”为可信度量操作符,其中“Δ”和“$\wedge$”分别为完整性度量和获取安全属性操作符,$\text{PCR}_j[\text{n}]=\{\text{hashFunction}\ (\text{PCR}[n-1]||\ \text{hashFunction}\ (\text{AO}_i)\}$.

$$\text{AtedP\_IntegrityMeasure}\triangleq[\![\text{AtedP.TMC},\ \ \text{AO}_i\ ]\!]\Delta\Rightarrow<\text{hashFunction}(\text{AO}_i)><\text{PCR}_j>\quad(i=1,2,\cdots,m,\ \ j=1,2,\cdots,n)\ ,$$

$$\text{AtedP\_AcquiringSecureAttributes}\triangleq[\![\text{AtedP.TMC},\ \ \text{AO}_i\ ]\!]\wedge\Rightarrow<\text{secureAttributes}(\text{AO}_i)>\ ,$$

$$\text{AtedP\_TrustedMeasure}\triangleq[\![\text{AtedP.TMC},\ \ \text{AO}_i\ ]\!]\frac{\Delta}{\wedge}\Rightarrow<\text{measureMetrics}><\text{TML}(\text{AO}_i)>\ .$$

定义 5(度量报告) 对于 APP 的验证质询,AtedP 在完成可信度量后,将所得 AO 完整性度量值和安全属性特征值作为消息通过安全信道发送给 APP. 记“$\xleftrightarrow[\text{AC}]{\text{MR}}$”为度量报告操作符.

$$\text{AtedP\_MeasureReport}\triangleq[\![\text{AtedP},\text{APP}]\!]\xleftrightarrow[\text{AC}]{\text{MR}}\Rightarrow<\text{signedPCR}_j>|$$

$$<\text{singedSecureAttributes}(\text{AO}_i)>|<\text{TML}(\text{AO}_i)>\ .$$

定义 6(平台证明) APP 中的验证功能组件通过访问可信度量参考值数据库,获取由软硬件生产厂商提供、权威机构发布的完整性参考值 integrityReferences 和基本安全策略 securityPolicies,然后依据完整性参考值和 TML 对 PCR_j 进行一致性验证,判定 AO 的完整性,即是否被攻击或篡改过;此外依据基本安全策略和 secureAttributes 验证两者的一致性,判定 AO 是否存在安全漏洞;并综合给出 AO 是否完整性保持以及安全属性是否符合策略等平台状态 AtedP_platformStatus 的两个布尔值 integrityFlag 和 securityFlag. 记“$\frac{\nabla}{\vee}$”为平台验证操作符,其中“∇”和“$\vee$”分别为完整性度量验证和安全属性验证操作符.

$APP\_IntegrityAttest \triangleq [\![APP.AFC, PCR_j, integrityReferences \}]\!] \bigtriangledown \Rightarrow < compliance \mid nonCompliance >$,

$APP\_SecurityAttest \triangleq [\![APP.AFC, secureAttributes, securityPolicies]\!] \vee \Rightarrow < compliance \mid nonCompliance >$,

$APP\_PlatformAttest \triangleq [\![APP.AFC, measureMetrics, integrityReferences, securityPolicies]\!] \frac{\bigtriangledown}{\vee} \Rightarrow < platformStatus >$.

定义 7(RA 报告) 对于 AtorP 的验证委托,APP 向 AtorP 报告 AtedP 当前平台或 AO 状态,而不提供平台的基本配置细节和安全属性. 记"$\xleftarrow[AR]{platformStatus}$"为 RA 报告操作符.

$$APP\_RAReport \triangleq [\![APP, \quad AtorP]\!] \xleftarrow[AR]{platformStatus} < platformStatus > .$$

定义 8(应用决策) AtorP 收到 RA 报告后,结合其他应用级的安全策略,进行面向应用的访问决策,接受或拒绝 AtedP 访问操作等. 记"◇"为应用决策操作符.

$AtorP\_ApplicatonDecision \triangleq [\![AtorP.ADC, \quad AtedP\_PlatformStatus, \quad AtorP\_ApplicationPoliciy]\!] \diamond \Rightarrow < Accept \mid Refuse >$.

2　AP²RA 安全协议设计

2.1　攻击模型

对笔者所提出的 AP²RA 方案的攻击模型主要有以下 3 种模式:

(1) 对 APP 证明服务的攻击:敌手通过攻陷 APP,使其无法向验证方提供 RA 报告或提供虚假错误的平台当前状态,从而影响整个应用系统的消息交互,直至系统瘫痪. 所采用的攻击方式主要为 DoS 攻击、欺骗攻击等.

(2) AtedP 共谋攻击:被验证方控制有至少两个终端系统,其中一个是可信平台,另一个为非可信平台. 通过将可信平台的度量值发送给 APP 接受验证,骗取 APP 和验证方的信任,从而获取共享信息或接入网络.

(3) AtedP 消息重放攻击:利用截获的包含有可信度量信息的消息,重新发起验证过程,借助于已有的符合验证的平台配置和安全属性消息通过不可信平台的 APP 验证.

2.2　AP²RA 安全协议

基于 1.3 节定义的一次完整 RA 会话过程,AP²RA 安全协议主要涉及 AtorP 验证委托与 APP 远程证明等步骤,这里着重给出其中的消息交互过程. 协议中所涉及到的签名算法可采用基于公钥密码体制的 RSA,ECC 算法等,散列算法可采用 SHA-1,MD5 算法等.

在 AtorP 和 AtedP 通过协商 APP,确定了可信第 3 方的验证代理后,AtorP 向 APP 发出平台或应用组件的验证委托请求,包括 AIK 签名的验证对象 AO,待 APP 验证通过后,给出委托请求的许可结果,此后 APP 发出对 AtedP 平台上 AO 的 RA 质询;AtedP 在本地进行相关度量和安全评估,其中包括已有平台安全启动过程中的度量值和当前应用组件的完整性度量值,一起存放在相应的 PCR 中;并将签名后的 PCR 和安全属性值、AIK 证书和 PCR 值等消息发送给 APP; APP 先后验证签名和 PCR 值,是否来自被质询的平台并和标准度量值一致,以及安全属性值是否符合安全策略; APP 将向 AtorP 发出已签名的平台验证报告. 该协议具体消息交互如图 2 所示,其中第(2)~(5)步基于"⊢→"定义属于 AtorP 委托过程,第(4)~(7)步是 APP 远程证明过程.

(1) 协议预备过程:基于"⊥"定义,AtedP 在接受 AtorP 的平台验证请求后,双方进行可信第 3 方代理 APP 的协商,最终确定一个进行平台验证的代理服务,并且由它保护 AtedP 平台的隐私; 若协商失败,则该协议终止. 在开始 RA 会话前,这里假定 AtedP,AtorP 及 APP 等实体已从 Privacy CA 获得了 AIK 证书,$K^{AtorP\text{-}APP}$ 和 $K^{AtedP\text{-}APP}$ 分别为 APP 和 AtorP,AtedP 之间在 RA 会话开始前产生的共享秘密密钥;

(2) AtorP 向 APP 发出一个委托请求消息 $Message_D$,其中包含 AIK 私钥签名的被验证对象名称

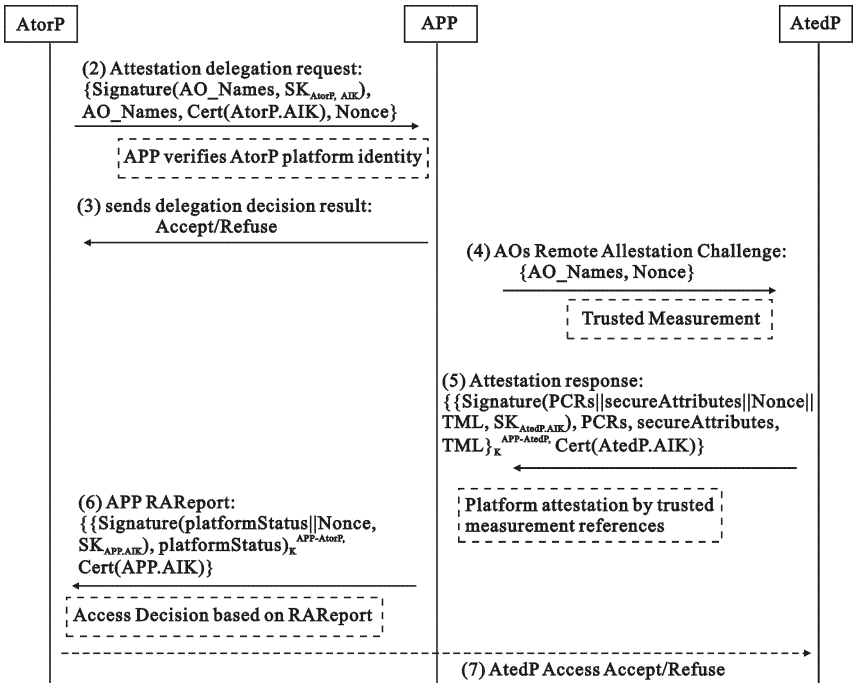

图 2 支持验证代理方的远程证明协议

Signature(AO_Name, $SK_{AtorP.AIK}$)和 AIK 证书 Cert(AtorP.AIK),以及一个本地生成的随机数 Nonce;

(3) APP 收到 $Message_D$,通过 APP.AIK 证书验证 AtorP 的平台身份并获得 AO,进而接受或拒绝 AtorP 的验证委托,并发送结果.若 APP 接受委托,协议向下执行;否则,协议终止;

(4) APP 向 AtedP 发出被验证对象 AO 的 RA 质询消息,其中包括一个第(2)步由 AtorP 生成的 Nonce;

(5) 基于"$\overset{\Delta}{\wedge}$"定义,AtedP 进行本地完整性度量 AtedP_IntegrityMeasure (AtedP.TMC, AO_i)和获取安全属性 AtedP_AcquiringSecureAttributes (AtedP.TMC, AO_i),从而 PCRs(AO)存放有多个 AO_i 的度量散列值和相应的度量顺序,此外还获得 AO 的安全属性特征值 secureAttributes,同时将此过程写入 TML;基于"$\overset{MR}{\underset{AC}{\rightleftharpoons}}$"定义,AtedP 使用平台验证身份证书 AIK 的私钥 $SK_{AtedP.AIK}$ 对 PCRs 与包含有平台标识值(如可信芯片模块标识码)的 TML 等内容进行签名,并连同 PCRs、secureAttributes、AtedP.AIK 证书和 TML 作为应答消息{Signature (PCRs|| secureAttributes||TML||Nonce, $SK_{AtedP.AIK}$), PCRs, TML, secureAttributes}通过安全信道发给 APP.

(6) APP 收到 RA 质询应答后,首先结合 Privacy CA 判定 Cert(AtedP.AIK)的有效性,并使用 AtedP 的 AIK 公钥 $PK_{AtedP.AIK}$ 对 PCRs 签名进行验证,从而判定消息的来源以及 AtedP 平台的身份,然后基于"$\overset{\nabla}{\vee}$"定义,执行平台验证操作,并基于"$\overset{\text{platformStatus}}{\underset{AR}{\rightleftharpoons}}$"定义,APP 对 AtedP 平台证明后,通过安全信道发送描述平台完整性与对象安全性状态及其签名值 Signature(platformStatus||Nonce, $SK_{APP.AIK}$),并连同 APP 公钥证书 Cert(APP.AIK)一起作为 RA 报告,返回给 AtorP 作为最终访问(或接入)请求的判定依据.

(7) AtorP 基于 APP 的 RA 报告与其他应用级安全策略进行面向应用的访问决策,并将决策结果返回 AtedP.

该协议第(6)步中的 RA 报告不使用证书机制将验证结果返回 APP,虽然证书在有效期内可多次使用,但鉴于平台软硬件的更新和基本安全策略的变化,APP 验证结果仅对激活本次协议的应用会话有效,再次应用会话需重新执行协议.

3　AP²RA 方案分析与对比

AP²RA 与已有的 RA 方案在采用机制、安全性能、抗攻击模型和系统开销等多个功能性方面进行对比,如表 1 所示,这里使用符号"√","×","+"分别表示具备、不具备、没有涉及或描述该性能.

(1) 机制对比与隐私保护:在采用的度量机制方面,由于各方案所考虑的角度不同,TCG 采用基本的基于二进制代码的完整性度量,文献[2-3]所提出的 PBRA 则基于平台属性的度量与验证,文献[4,6]分别进行软件语义与行为的度量.由于上述方案没有支持可信第 3 方的验证,他们的度量机制结合各自的报告机制会造成不同程度的平台配置及安全属性等隐私的暴露.而文中方案通过 APP 引入来实施验证过程,它仅向 AtorP 报告 AtedP 当前平台状态是否完整性保持以及是否存在安全漏洞,不暴露平台基本配置与其他信息,因此在隐私保护上文中的方案优于其他方案.

(2) 抗攻击能力分析:AP²RA 主要针对 2.1 节提出的 3 种攻击模型进行了安全协议设计.在协议中 APP 通过对验证委托请求者 AtorP 发来的 $SK_{AtorP.\,AIK}$ 签名消息,对 AtorP 进行平台身份验证.由于 AIK 是能够标识平台惟一身份的 EK 别名,通过 AIK 的私钥签名可跟踪到本次发起验证委托请求的终端平台,进而可采用相应动作以防止对 APP 发起 DoS 攻击和欺骗攻击等.在协议第(5)步,AtedP 使用平台 AIK 的私钥签名内容中存在包含平台唯一身份标识的 TML,因此即使 AtedP 拥有两台终端(一台可信终端,一台非可信终端),也无法通过传递可信平台的度量报告来欺骗 APP 通过非可信平台的验证,从而有效地阻止了共谋攻击.在协议第(4)～(5)步中实施平台证明质询-应答方式,通过 Nonce 来判定 AtedP 平台可信度量消息的新鲜性,有效地阻止了重放攻击.

(3) 引入 APP 的可行性:可信计算技术及远程证明将终端可信性扩展到网络的过程中引入可信第 3 方 Privacy CA 是解决平台身份隐私的 TCG 方案;这里引入 APP 旨在解决终端平台配置细节和安全属性特征等隐私在 RA 中的保护,同时由 APP 提供平台证明功能和服务减轻了终端平台验证远程实体的负担,简化了终端的功能实现.APP 平台验证功能可实现为一个 Web Service[8],并由不同的第 3 方提供,但在实施平台验证前,需验证双方协商认可它所提供的服务和平台隐私保护能力.

(4) 协议效率与系统开销:文中协议共有 3 次签名操作,2 次加密操作,比 TCG 的 RA 方案增加了 AtorP 与第 3 方 APP 之间的 1 轮验证委托消息交互,但 APP 的引入有效地保护了被验证平台的隐私.由于文中方案和 PBRA 中的 TC+[2]都引入可信第 3 方,所以系统开销较高.

表 1　方案的机制与性能对比

	TCG-RA[1]	PBRA[2-3]	SBRA[4]	文献[6]方案	文献[8]方案	AP²RA
可信度量与证明机制	基于二进制代码的完整性	基于平台配置推导安全属性	基于上层软件对象的语义	基于应用软件行为和完整性	基于二进制代码的完整性	基于代码完整性和安全属性
可信报告机制	基于软硬件配置的报告	基于安全属性的报告	基于软件语义检查的报告	基于应用完整性和行为报告	基于 PCR 扩展和证书的报告	平台完整性与安全状态报告
支持可信第 3 方	×	√	×	×	√	√
消息保密性	√	√	√	√	√	√
消息完整性	√	√	√	+	√	√
消息抗否认性	√	√	√	+	√	√
跟踪对 APP 攻击	+	√	+	+	+	√
抗 AtedP 共谋攻击	×	×	×	+	+	√
抗 AtedP 重放攻击	√	√	+	+	√	√
平台隐私保护	较低	一般	+	较低	一般	较高
系统开销	较低	较高	一般	一般	较高	较高

(下转第 105 页)