第 35 卷 第 3 期 计 算 机 工 程 2009 年 2 月
Vol.35 No.3 Computer Engineering February 2009
·博士论文· 文章编号：1000—3428(2009)03—0021—02 文献标识码：A 中图分类号：TP309

身份证实证书在可信计算中的应用

周雁舟，刘文清，朱智强
(解放军信息工程大学电子技术学院研究所，郑州 450004)

摘 要：证书体系在可信计算中具有基础支撑作用，它参与完成了信任传递的整个过程。该文研究身份证实证书(AIK)的内容、产生和其他证书的关系，分析其在远端主机证明的作用和过程。用可信计算技术和 AIK 证书加强安全套接层(SSL)协议的方法和步骤解决 SSL 协议中无法验证服务器程序真实性的问题。

关键词：可信计算；身份证实证书；远端证明；安全套接层协议

Application of Attestation Identity Credential in Trusted Computing

ZHOU Yan-zhou, LIU Wen-qing, ZHU Zhi-qiang
(Research Institute, School of Electronics Technology, PLA Information Engineering University, Zhengzhou 450004)

【Abstract】One of the Trusted Computing Group(TCG) infrastructure is credential system, which participates in trusted chain of transmission process. Attestation identity credential's type, the full definition and the relationship to other credential are discussed. Its application on remote attestation is studied. Based on the study, the way to improve the security of Secure Socket Layer(SSL) protocol using trusted computing and AIK credential is put forward for solving the application's attestation on SSL server.

【Key words】trusted computing; attestation identity credential; remote attestation; Secure Socket Layer(SSL) protocol

1 概述

可信计算组织(Trusted Computing Group, TCG)通过系统安全芯片可信平台模块(Trusted Platform Module, TPM)建立信任的源头，然后通过硬件、固件、操作系统和应用程序，按照系统启动过程的前后控制关系建立信任链的方法确保计算平台和程序的可信赖性。而如果想充分利用可信平台的安全特性，需要数字证书参与，它是信任传递的基础[1-2]。

TCG 设计的核心是 TPM 结合使用证书完成实体证明的过程。TCG 的规范中有 5 种证书：签署证书(endorsement or EK credential)，一致性证书(conformance credential)，平台证书(platform credential)，确认证书(validation credential)和身份证实证书(attestation identity or AIK credential)。每种类型的证书均有不同的内容、签署者和应用场合，这 5 种证书构成了可信计算的证书体系，为信任的建立提供基础支撑平台[3]。

AIK 证书从使用的角度而言能够代表 EK 证书，它由隐私 CA(PCA)产生，用来证明 TPM 拥有一个 AIK 证书，并且该 AIK 证书绑定一个有效 EK 证书和一个有效的平台证书，所以，AIK 证书在可信计算中的使用极为关键和广泛。本文对 AIK 证书的内容、产生和应用等问题进行深入的研究和分析，在研究如何使用该证书进行远端主机认证的基础上完善了 SSL 协议，解决了 SSL 协议无法认证服务器真实性的缺陷。

2 AIK 证书

2.1 可信计算证书体系

TPM 出厂时都有一个签署密钥对(EK)，其中，私钥只有 TPM 知道，签署证书由可信实体进行签署，它将签署密钥对的公钥与 TPM 进行绑定。TCG 中每个 TPM 的实例都有一个签署证书。TCG 认为尽管 EK 的公钥是公开的，但由于它唯一地标识了一个 TPM，因此也是一个具有隐私性质的证书，一般情况下不对外发布。一致性证书用来表明 TPM 及其平台符合相应的规范，由权威机构签署产生。平台证书由平台的生产者、销售厂商或者可信第三方颁发。它标识了平台生产者并描述了平台的特性。平台证书也被认为具有隐私性质，因为它和特定的平台相关联。确认证书证明了可测量组件、硬件和软件的参考测量值，表明该组件处于正确的工作状态，以防止后门。

AIK 的作用是证明一个实体的真实性，且它的执行操作是正确的。这种证明的原理是使用一个仅属于该实体的私钥进行签名，并且使验证方相信其相应的公钥属于 AIK 的拥有者。它的证明过程是首先生成一个新的密钥对，并对它的身份进行绑定，绑定的内容包括：相应公钥，实体的名称，将来用于认证这个身份的 CA 的公钥，该私钥对这些内容的签名。TPM 属主将其发给 CA，CA 对其进行检查。这种操作的目的是对 AIK 私钥签署的平台配置寄存器(PCR)值进行认证和鉴别，表明 TPM 拥有一个 AIK，并且该 AIK 绑定了有效的签署证书、平台证书和一致性证书。因此，AIK 证书中有对 EK 证书、平台证书和一致性证书内容的引用。由此可见在实际使用中，AIK 证书是使用最广泛的证书。

2.2 AIK 证书产生

因为 AIK 是 EK 的一个引用，而 EK 代表了一个 TPM，所以 AIK 证书的产生过程必须获得 TPM 属主的认证，在获得证书的过程中受到 TPM 的保护，并且它只能由发出 AIK 证书请求的 TPM 获得。基于以上原则，AIK 证书的生成包括 2 个过程：

基金项目：国家“863”计划基金资助项目(2006AA01Z433)；上海市科研基金资助项目(20057120126)
作者简介：周雁舟(1971－)，男，副研究员、博士研究生，主研方向：操作系统安全可信计算；刘文清、朱智强，教授、博士
收稿日期：2008-06-30 **E-mail：**zyanzhou@163.com

(1)AIK 密钥对的产生。1)验证输入参数的合理性，包括密钥长度，算法的兼容性和其他参数的合理性；2)验证用户身份的合法性；3)设置输出参数的版本；4)设置 PCR 相应的摘要值；5)使用 TPM 产生公私钥对；6)确保认证信息正确存入输出参数；7)将产生的公私钥对组合存入输出参数中；8)使用存储根密钥加密私钥部分；9)创建输出结构体，将输出的内容存入该结构中；10)使用私钥对该结构体摘要签名。

(2)AIK 证书的产生。当生成公私钥对后，CA 需要签署该公钥证书证明这个新的身份，但为了防止签署一个假冒的公私钥对，CA 使用一个随机生成的对称密钥来加密证书，然后用申请该证书的 TPM 的签署密钥的公钥加密该随机数，其产生过程如下：1)验证用户身份的合法性；2)验证输入参数的合理性；3)计算 AIK 公钥的摘要值，并与输入参数中的相应值进行比较，确定输入值的真实性；4)使用签署密钥的私钥解密对称密钥；5)赋值相应的输出参数，返回。

3 AIK 证书的应用

3.1 AIK 证书在远端证明中的应用

AIK 证书可用于远端主机证明，远端证明的目的是证明远端主机的硬件和软件的可信性，不过证明的结果却是由发起方决定是否信任远端主机的组件。

根据 TCG 的标准，可信计算提供了信任度量、信任报告和可信存储。可信度量包括了对平台特性的度量，这些度量包括度量的 hash 值，被存储在 TPM 芯片里的 PCRs 中。PCR 度量值包括：系统启动时装入的 hash 值，操作系统内核的 hash 值或运行程序的 hash 值。PCR 的值通过棘齿的方式保证了一系列的值可以装入一个 PRC 寄存器，同时通过这种方式阻止了数据的回滚以得到前一个阶段的 hash 值。可信报告则是主机通过表明可信度量和证明它们的真实性来完成的，TPM 通过返回由 AIK 私钥签名的 PCR 值进行可信度量的报告。可信计算用可信度量的值和 AIK 私钥的签名表明主机有一个特定的配置。所有远端主机需要通过 AIK 的公钥进行认证，并且通过比较 PCR 和它的可信配置值判断主机的配置是否正确。可信存储保护加密密钥和数据。

远端证明包含 2 个主要步骤：(1)信任的度量。指主机的配置以一种特定顺序被测量。(2)可信报告。被验证主机的测量值使用 AIK 进行数字签名，其他主机验证该测量值，并和可信集进行比较，验证它的真实性[4]。

根据远端证明的原则和步骤，它的验证协议如下：(1)假设每个主机都有 TPM 芯片可以产生 PCR 值，进行数字签名和验证；(2)有一个每个主机都能够信任的 CA；(3)每个主机都有可信 PCR 值，被称为可信集(TrustSet)。

使用主机 *A* 与主机 *B* 的双向认证过程如下：

(1)*A* 产生 PCR 值，并且用 *A* 的 AIK 的私钥进行签名，即 $(Sig(PCR_A, AIK_A), PCR_A)$。

(2)*A* 将 PCR 和签名值以及 AIK 证书发送给 *B*，即 $A \rightarrow B$：$(Sig(PCR_A, AIK_A), AIK_A), PCR_A, AIK_A)$。

(3)*B*验证 *A*的AIK证书的有效性，如果证书有效，*B*使用TPM验证签名的真实性，即 $Ver(Sig(PCR_A, AIK_A), AIK_A) = \text{true}$。

(4) *B* 检查它的信任集，如果 $PCR_A \in TrustSetB$，表明主机 *A* 可信。主机 *B* 调用它的 TPM 产生它的配置值，并用它的 AIK 私钥签名，即 $(Sig(PCR_B, AIK_B), PCR_B)$。

(5)*B* 将 PCR 和签名值以及 AIK 证书发送给 *A*，即 $B \rightarrow A$：$(Sig(PCR_B, AIK_B), AIK_B), PCR_B, AIK_B)$。

(6)*A*验证*B*的AIK证书的有效性，如果证书有效，*A*用TPM验证签名的真实性，即 $Ver(Sig(PCR_B, AIK_B), AIK_B) = \text{true}$。

(7)*A* 检查的它的信任集，如果 $PCR_B \in TrustSetA$，则双方主机信任彼此的组件。

3.2 AIK 证书在 SSL 协议中的应用

AIK 证书除了单独使用外，还可以加入到一些现有的认证或密钥交换的协议中使用，对原来的协议进行安全增强。

SSL 协议是在 Internet 基础上的一种保证私密性的安全协议。SSL 协议提供 3 种基本安全属性：(1)连接是保密的，使用对称加密算法用于加密传输数据；(2)对方的身份能够使用非对称密码进行认证；(3)连接是可靠的，消息传输中使用消息认证码(MAC)进行消息完整性检查，并使用哈希函数用于消息认证码计算。这些安全属性能使客户/服务器应用之间的通信不被攻击者窃听和篡改，并且能对服务器进行认证，还可选择对客户进行认证[5]。但 SSL 协议也有一个尚未解决的问题，即数据到达服务器之后会被如何处理，如何保证服务器确实提供真实的服务。因为即使服务器端提供了身份证明，客户端也无法确认服务器程序的真实性。文献[6-7]认为，通过应用 AIK 证书提供远端主机证明的功能来解决这个问题。这种方法的出发点是：用户认证加平台认证，它也可以融用户认证、平台认证和平台报告于一体，甚至可以影响会话密钥的产生，但它们的方法对 SSL 协议的修改较大。根据对 SSL 协议修改最小的设计原则，本文提出如下解决方法。

SSL 协议包括 2 个子协议：SSL 记录协议和 SSL 握手协议。本文针对 SSL 握手协议使用 AIK 证书来加强 SSL 协议。由于 SSL 握手协议中对客户端的认证是可选的，因此在设计时使用单向认证的方式，不考虑对客户端的认证和客户端主机应用程序的正确性证明。

修改后的协议如图 1 所示。

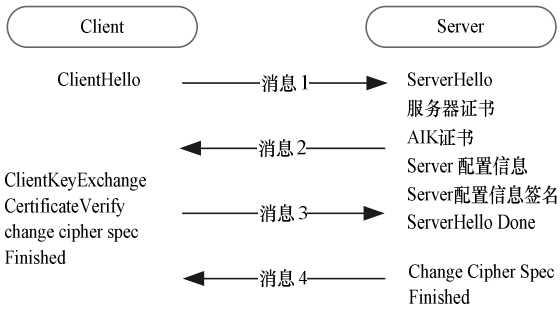

图 1 修改后的 SSL 握手协议

协议具体描述如下：

消息 1：客户端发送 Client Hello 消息，包括客户端所支持的加密算法列表及推荐的加密参数，其中有一条是密钥生成参数。

消息 2：服务器以 6 条消息进行响应，首先服务器发送从客户端的加密算法列表中选出的加密算法的 Server Hello 消息。接下来，服务器发送用户证书(Certificate)消息，将证书发送给客户端，然后发送 AIK 证书、Server 端的程序配置信息以及对该信息的 AIK 私钥签名信息，最后，服务器发送一个 ServerHello Done 消息结束当前的握手。

消息 3：客户端首先验证服务器端用户证书的有效性，如果是有效的，再验证 AIK 证书的有效性，如果是有效的，则使用 TPM 验证配置信息的真实性。如果是真实的，验证该

(下转第 70 页)