第 35 卷 第 6 期 计 算 机 工 程 2009 年 3 月
Vol.35 No.6 Computer Engineering March 2009
·安全技术· 文章编号：1000—3428(2009)06—0153—03 文献标识码：A 中图分类号：TP309.2

基于时间的平台完整性证明

徐国愚，常朝稳，黄 坚，谷冬冬
(解放军信息工程大学电子技术学院，郑州 450004)

摘 要：现有的平台完整性证明协议由于使用了随机数，在实际应用中存在被动响应和欺骗问题。该文针对以上不足提出时间方案，利用 TPM 的传输会话功能，通过时间戳将完整性报告与时间绑定，实现基于时间的平台完整性证明。设备可在固定时间主动上传完整性报告，在连接中断时定时进行完整性报告，实现日志功能，杜绝欺骗问题。

关键词：可信计算；网络管理；平台完整性证明；传输会话

Platform Integrity Attestation Based on Time

XU Guo-yu, CHANG Chao-wen, HUANG Jian, GU Dong-dong
(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004)

【Abstract】 The conventional protocol of platform attestation has passivity and cheat problem in practice because of using nonce. This paper proposes platform attestation based on time, which uses transport session associating attestation with time in application layer. Equipment can upload attestation report actively on time and record log in the situation of network disconnection.

【Key words】 trusted computing; network management; platform Integrity attestation; transport session

1 概述

设备监控用于监视和管理网络中的设备。管理平台周期性地查询网络设备运行状态，如 CPU 运行负载、进程运行状态、数据吞吐量，当发现设备出现异常时，可以产生告警并采取相应的措施。但是管理平台监视的信息仅限于预先定义的信息，无法监控未知攻击等，同时信息采集模块运行于设备中，极易被破坏篡改。

可信计算组织(TCG)提出基于硬件证实远端软件状态的方法解决上述问题。通过在现有主板上绑定一个小型防篡改硬件——可信计算模块(Trusted Computing Model, TPM)，终端从平台加电开始，到运行环境的建立，再到应用程序的执行，任何实体在获得控制权前都需要经过度量(如系统配置、程序代码的完整性、进程的运行状态)，并将度量值保存在 TPM 中，防止被恶意篡改。远程验证方通过 TPM 提供的平台完整性证明机制获取终端的完整性报告，完整性报告中包含系统的度量值。将可信计算技术应用到设备监控中，管理平台可以通过定时采集设备的完整性报告，及时掌握设备的运行状况，当发现问题时产生告警并采取相应的措施。然而，TCG 规范中的平台完整性证明协议需要验证方发送随机数给终端，以保证度量值的实时性，防范重放攻击。这在设备监控应用中存在着 2 个缺点：

(1)被动响应

在现有的网络监控协议(如 SNMP)中，设备既可以响应管理平台发送的 POLL 命令返回所需信息，也可使用 PUSH 或 TRAY 命令主动将信息上传给管理平台。而平台完整性证明只能由管理平台发起，设备无法主动将完整性报告上传。

(2)欺骗

随机数的使用要求验证方和终端必须同时在线，当管理平台与设备之间的连接中断、管理平台无法对其进行监控时，设备可以运行恶意软件而不被发现。进一步，当设备遭到恶意入侵、对管理平台的完整性证明请求不响应时，管理平台将无法分清是传输中数据包丢失还是设备恶意欺骗。

该文针对以上不足，提出时间方案，实现了基于时间的平台完整性证明。

2 相关工作

基于 TCG 规范，文献[1]在 Linux 平台中设计实现了完整性测量系统，并讨论了平台完整性证明在Web 服务中的具体实施。文献[2]提出了 P2P 方式的接入证明模型。但是这些模型应用的场景都是准入控制，并不涉及第三方监控。文献[3]提出利用可信计算增强设备监控，但是并未考虑到本文所指出的问题。文献[4]与本文的时间方案采用了相同的方法，都利用了传输会话功能。该文将完整性度量与时间绑定，认为当验证方获知度量发生时间后，将有更多的信息用于决策。而本文将完整性报告与时间绑定，以解决设备监控中的被动响应和欺骗问题。

3 基于时间的完整性证明

3.1 完整性证明在设备监控中的应用及其不足

在可信计算技术中，TPM 为最核心的部件[5]。TPM 中包含一组平台配置寄存器(PCR)，用于存储平台完整性测量值。PCR 值的更新是以叠加的方式进行的：TPM 将 PCR 中的原始值与新测量值连接进行哈希运算后，将新生成的哈希值替换原始值保存在 PCR 中，这样可以完整记录终端从开机起的平台完整性变化情况。同时系统保存一个列表——度量存储日志(SML)，其中包括被测量组件的名称以及对应的哈希值。远程验证方通过 SML 和 PCR 值获得系统运行的软件状态、

基金项目：国家“863”计划基金资助项目(2007AA01Z479)
作者简介：徐国愚(1982－)，男，硕士研究生，主研方向：可信计算；常朝稳，副教授；黄 坚、谷冬冬，硕士研究生
收稿日期：2008-10-10 **E-mail：**xuguoyu@gmail.com

配置信息等。

目前平台完整性证明存在的一个难题是如何确保证明后系统的安全性。设备可以在证明之后启动恶意软件替换认证过的软件，监听进程通信，收集隐私信息，而管理平台将无从获知这一变化。在设备监控应用中，由于设备长期处于工作状态，管理平台可以通过周期性地进行完整性证明对设备实施有效监控。

完整性证明协议流程如图 1 所示。

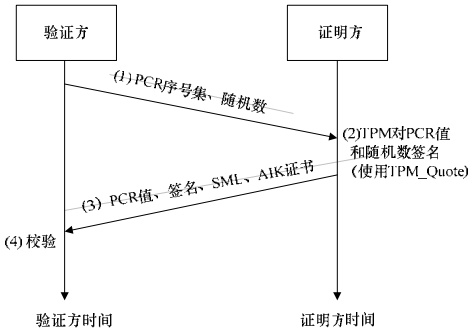

图 1　平台完整性证明协议流程

协议的具体步骤如下：

(1)验证方(管理平台)向证明方(设备)发送完整性请求，请求中包含 PCR 序号集(可包括多个 PCR 序号)及随机数。

(2)证明方调用 TPM_Quote 命令将 PCR 序号集和随机数送入 TPM 中。如图 2 所示，TPM 在内部将对应的 PCR 值和随机数绑定后，使用 TPM 的身份证明密钥(AIK)签名返回。其中，AIK 由 TPM 内部产生，经第三方认证，用于 TPM 的身份证明。

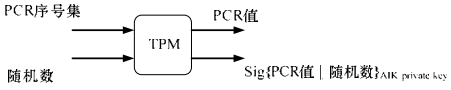

图 2　TPM_Quote 命令输入输出参数

(3)证明方将 PCR 值、签名以及 SML 作为完整性报告，连同 AIK 证书一起返回给验证方。

(4)验证方根据返回的完整性报告判断证明方是否可信。

协议使用随机数防范重放攻击，防止证明方返回事先保存的 PCR 值欺骗验证方。但如第 1 节所述，在设备监控应用中，此机制存在着被动响应和欺骗问题。

3.2　时间方案

针对上述问题，本文提出时间方案——利用 TPM 传输会话功能将 TPM_Quote 命令与时间关联，实现基于时间的平台完整性证明。在管理平台不参与的情况下，设备可以在固定时间或固定间隔自动进行完整性报告。

时间方案利用了 TPMv1.2 中新增的时间戳和传输会话功能。

(1)时间戳

在应用中，一些程序需要使用可信的时间资源，但提供可信的时间器将会大大增加 TPM 的制造成本，所以，在 TPM 中只设置了一个或多个时间戳计数器。启动一个时间戳计数器将开启一个时间会话。如图 3 所示，每个时间会话结构中包含时间戳值(TCV)、时间戳增长速率(TIR)、时间会话随机数(TSN)，其中，TCV 表示当前时间会话的时间戳；TIR 表示标准时间与时间戳的对应关系；TSN 用于标识区别不同的时间会话，在整个会话中保持不变。时间会话初始时，将 TCV 置 0，同时生成一个随机数赋予 TSN，用于标识不同的时间会话。

图 3　时间会话结构的组成

在 TPMV1.2 规范第 1 部分[5]中，介绍了一种利用可信时间服务器的方法，将时间戳值与格林威治时间相关联，生成时间证书，从而提供可信时间资源。

(2)传输会话

传输会话(transport session)用来保证 TPM 与可信程序的安全通信。对会话中的命令提供加密保护，同时提供日志功能，日志中包括所有命令的输入、输出参数以及执行时的时间戳。会话结束后，返回日志的签名。

时间方案步骤如下：

(1)将完整性报告与时间戳绑定：

1)创建一个传输会话，开启日志功能。

2)在传输会话中执行 TPM_Quote 命令，其中，随机数可以任意选取。

3)使用 AIK 作为签名密钥，执行 TPM_ReleaseTransportSigned 命令，结束传输会话，TPM 返回会话日志的签名。会话日志中包含 TPM_Quote 命令的输出参数(验证方请求的 PCR 值)、命令执行时的时间戳。

4)将会话日志、签名以及 SML 作为基于时间的完整性报告(Integrity Report Based-on Time, IRBT)保存。

(2)将 IRBT 与时间关联。IRBT 与时间戳绑定后，可以应用 TPMv1.2 规范中的方法使设备产生时间证书，通过时间戳将 IRBT 与格林威治时间相关联。也可令终端在固定时间间隔自动生成 IRBT。这不需要时间服务器的参与。但是管理平台必须事先保存终端的时间会话随机数，以防止重放攻击。

需要注意的是，当 TSN 重置时，证明方需要重新申请时间证书或通知验证方更新 TSN。由于时间会话的实现由各 TPM 制造商自行决定，在本方案中，为方便应用，假设当设备能为 TPM 提供不间断电源时，TSN 不会因为设备重启或关机而重置，至少在重启情况下 TSN 不会被重置。

3.3　重启攻击问题

时间方案存在的缺陷是易受到重启攻击：由于 PCR 为易失性存储空间，因此设备关机或重启后，PCR 值将置 0。恶意用户可以在运行非法软件或修改平台配置后，关机重启，将 PCR 值恢复到安全状态。当重启攻击发生在 2 次完整性报告之间时，管理平台将无法从 PCR 中获知这一攻击。文献[1]对重启攻击的解决方法是利用 TPM 的单调计数器。单调计数器在整个 TPM 生命中不会被清空或覆盖，只会单调增加。TPM 含有多个单调计数器，可使用 1 个单调计算器专门记录机器重启次数(简称重启数)。每次机器重启时，BIOS 执行 TPM_IncrementCounter 命令将单调计数器加 1 并将重启数存入 PCR 中，以记录系统重启，表明系统的安全有可能被破坏，远程验证方可选择放弃此次交互。但是这种方法只适用于 Web 服务等即时性应用，并不能直接应用到设备监控中，因为它只能告知设备曾经重启过，但无法获知何时重启及问题可能出现的时间。本文针对这一问题所做的改进是增加系统

重启时间的记录：BIOS 执行 TPM_GetTicks 命令获得当前时间戳，并和重启数一起写入 PCR 中，使得系统重启时间与时间戳关联。管理平台通过读取 PCR 值可获得当前设备的重启数以及重启时间。当发现设备重启时，能够获知从重启前最后一次完整性报告到重启这一时间段内可能发生过攻击。管理平台结合时间信息和其他相关信息进一步判断设备安全是否被破坏。

3.4 时间方案的具体实现

在设备中增加后台程序 PA(Platform Agent)用于实现 TCG 规范中的完整性证明，能够提供本文的时间方案。

当设备首次向管理平台注册时，管理平台保存设备的 TSN、TCV、重启数以及 AIK 证书，并将时间方案的相关策略发送给 PA。协商流程如图 4 所示。

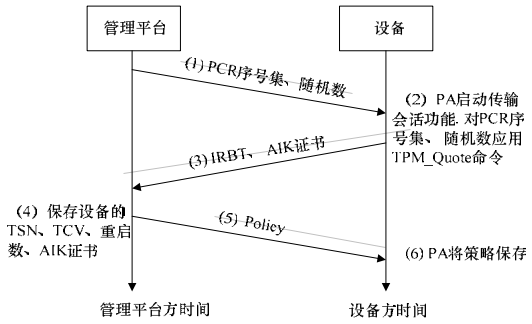

图 4 时间方案协商流程

协商的具体步骤如下：

(1)管理平台发送 PCR 序号集、随机数给 PA。

(2)PA 开启传输会话，对 PCR 序号集和随机数应用 TPM_Quote 命令，生成 IRBT。

(3)PA 将 IRBT 以及 AIK 证书返回给管理平台。

(4)管理平台检查 PA 所在设备的完整性状态，通过后，将设备的 TSN、TCV、重启数以及 AIK 证书保存。

(5)管理平台将相关策略发送给 PA。

(6)PA 将策略保存。

为解决被动响应问题，管理平台发送的策略包括上传 IRBT 的时间或时间周期。PA 根据策略可在固定时间或周期主动上传 IRBT。

针对欺骗问题，发送的策略包括管理平台采集设备完整性状态的周期时间，PA 在周期时间内未收到管理平台的完整性请求时将自动生成 IRBT，并作为日志保存，当再次接收到管理平台的完整性请求时，PA 将 IRBT 上传，此时完整性请求中包含管理平台收到设备最后一次完整性报告中的重启数 R_{save}。

由于周期性产生 IRBT 会累积大量日志，将其全部上传会产生大量通信数据，因此 PA 需要在本地进行筛选，处理流程如下：

(1)检查本地是否保存有 IRBT，若无，返回错误，结束。

(2)读单调计数器获取当前重启数 R_{cur}，与管理平台发送来的 R_{save} 比较。若 R_{cur}==R_{save}，表明无重启，将当前完整性报告返回，结束。

(3)将 R_{save} 到 R_{cur} 所有重启数对应的最后一次 IRBT 以及当前完整性报告返回，结束。

管理平台收到 PA 返回 IRBT 后的检查流程如下：

(1)若收到错误，表明 PA 被破坏或报告事件被删除，产生告警，结束。

(2)将 PA 返回当前完整性报告中的重启数 R_{cur} 与 R_{save} 比较，若 R_{cur}==R_{save}，表明未重启过，检查设备当前完整性状况，结束。

(3)记录每次重启和之前最后一次 IRBT 的时间以及当前完整性状况，并产生告警，结束。

4 性能分析

4.1 安全分析

本文提出的时间方案在底层依赖于现有 TPM 模块的安全性，本文假定 TPM 是安全的，不会被破坏。

在应用层上，时间方案利用时间服务器证明的方法，将时间戳与格林威治时间关联，会产生一定范围的误差，但由于 PCR 值的更新是累加进行的，时间误差不会对 IRBT 产生影响。另外，PA、签名、日志等并不受保护，可能会被恶意删除，但这将使管理平台发现设备的安全遭到破坏。

4.2 效率分析

产生 IRBT 时，TPM_Quote 命令和传输会话都将产生签名。但由于 TPM_Quote 命令的输入输出参数包含在会话日志中，受会话日志签名的保护，因此只需发送会话日志签名给管理平台即可。

由于 PCR 值更新的累加性，当设备在网络连接中断期间未重启时，只需要校验当前完整性报告；当设备有重启时，对于每一次重启只需要校验一次 IRBT。

5 结束语

在现有的平台完整性证明协议中，利用随机数防止重放攻击对于一个严谨的协议是必要的，但是应用于设备监控方面时，这种方法存在被动响应和欺骗问题。本文在应用层上对协议进行扩展，通过基于时间的平台完整性证明解决上述问题，能够直接应用到现在的协议中。

需要指出的是，在现有的通用 PC 上，单纯依靠平台完整性证明并不能完全解决安全问题，还需要结合访问控制、内存隔离等技术进一步加强系统的安全性。

参考文献

[1] Sailer R, Zhang Xiaolan, Jaeger T, et al. Design and Implementation of a TCG-based Integrity Measurement Architecture[C]//Proc. of the 13th Usenix Security Symposium. San Diego, USA: [s. n.], 2004.

[2] Sandhu R, Zhang Xinwen. Peer-to-Peer Access Control Architecture Using Trusted Computing Technology[C]//Proc. of the ACM Symp. on Access Control Models and Technology. [S. l.]: ACM Press, 2005.

[3] 陈 军. 可信平台模块安全性分析与应用[D]. 北京: 中国科学院研究生院, 2006-06.

[4] Sastry M R, Wiseman W M. Method for Providing Integrity Measurements with Their Respective Time Stamps: USA, 2006/0074600 A1[P]. [2008-03-12].

[5] Trusted Computing Group. TCG TPM Specification Version 1.2, Revision 103(Design Principles, Structures of the TPM, and Commands)[EB/OL]. (2007-07-09). https://www.trustedcomputinggroup.org/specs/TPM/.

编辑 张 帆