一种针对 TPM 的抗重放攻击方案

周雅洁,陈 萍,张晶伟,关焕梅
ZHOU Ya-jie,CHEN Ping,ZHANG Jing-wei,GUAN Huan-mei

武汉大学 计算中心,武汉 430072
Computer Center,Wuhan University,Wuhan 430072,China
E-mail:yjzhou@whu.edu.cn

ZHOU Ya-jie,CHEN Ping,ZHANG Jing-wei,et al.Solution of anti-replay attack in TPM.Computer Engineering and Applications,2007,43(22):120-121.

Abstract: The Trusted Platform Module (TPM) is the core of the the trusted computing technology.The trusted computing platforms need to be verified trustful by functionality of identity,measurement,protected storage of the TPM.However,the people take more care of the realization and exploitation of the TPM than the security of the TPM itself and this hampers the application of the TPM in the security technology.We prove that the object-independent authorization protocol is exposed to replay attack and propose a countermeasure to avoid this attack.

Key words: Trusted Platform Module(TPM);object-independent authorization protocol;replay attack

摘 要:可信平台模块(Trusted Platform Module,TPM)是可信计算技术的核心。可信计算平台需要 TPM 的可信测量能力、可信存储能力和可信报告能力,向用户证实平台是可信的。然而当前人们主要关心 TPM 的实现以及其上的应用开发,却很少讨论 TPM 本身的安全性。这样一方面很难使人们相信 TPM 本身是安全的,另一方面也不能很好的将 TPM 应用到安全领域中。对用户和 TPM 交互时所遵循的重要协议——对象无关授权协议 OIAP 进行分析,证明了该协议会受到重放攻击并提出了相应的解决方案。

关键词:可信平台模块;对象无关授权协议;重放攻击
文章编号:1002-8331(2007)22-0120-02 **文献标识码**:A **中图分类号**:TP393.08

由于硬件体系结构和操作系统内在的脆弱性,导致目前的通用计算平台存在诸多安全问题。近年来,随着可信计算组织(Trusted Computing Group,TCG)影响的不断扩大,其提倡的从终端平台结构上解决安全问题的可信计算思想及相关技术也越来越受到学术界和产业界的重视,已成为当前研究信息安全问题新的热点和方向。

根据 TCG 可信(trust)的定义,可信计算平台(Trusted computing Platform,TP)是一种总是能够以一定的方式按照预定的目的行为的平台。TP 应该能够抵抗窜改攻击、证实平台代码和数据的完整性和真实性、安全的执行代码、保护敏感数据的机密性。

可信平台模块(Trusted Platform Module,TPM)是可信计算技术的核心,该模块被嵌入到平台上,提供密码支持和有保护的存储功能,为各种可信机制和安全功能提供硬件保障。

本文对用户和 TPM 交互时所遵循的重要协议——对象无关授权协议(Object-Independent Authorization Protocol,OIAP)进行分析,证明协议执行期间确实会受到重放攻击,并提出了相应的解决方案。

1 可信计算平台

首先,介绍一下本文将要用到的一些符号:

(1)$X.Y$:表示主体 X 和主体 Y 连接;

(2)$A\rightarrow B:M$:表示主体 A 向主体 B 发送消息 M;

(3)S_i:表示第 i 次授权会话;

(4)A',A'',…:表示与伪随机数 A 由同一个伪随机数发生器生成,与 A 有相同特征的伪随机数。

可信计算平台(TP)是通过在现有平台基础之上增补硬件构件来保护软件系统的计算平台,其中硬件构件由 CRTM(可度量的核心信任源)和 TPM(可信平台模块)组成,CRTM 和 TPM 是主板上唯一的可信组件。

可信计算平台至少要提供以下 3 个特征:

(1)证实能力:能够证明信息是真实的能力。

(2)完整性测量:可信的测量描述平台配置的度量值。

(3)保护功能:以可信的方式执行计算和安全的存储数据。

计算平台通过执行 CRTM 代码开始。该代码对所有的硬件和软件组件(包括代码和数据)进行完整性检测。检测得到的测量值存储在由 TPM 提供的受保护存储区中。

基金项目:国家自然科学基金(the National Natural Science Foundation of China under Grant No.60373087,No.60473023,No.90104005)。
作者简介:周雅洁(1977-),女,讲师,博士,主要研究方向:信息安全;陈萍(1973-),女,讲师,博士,主要研究方向:多媒体通信;张晶伟(1975-),女,工程师,主要研究方向:计算机应用;关焕梅(1972-),女,讲师,博士,主要研究方向:信息安全。

2　TPM 授权协议 OIAP

TPM 共有两个主要协议供请求者(希望在 TPM 上执行命令或使用某个资源的任何主体)向 TPM 发送授权数据知识:即对象无关授权协议(OIAP)和特定对象授权协议(OSAP)。OIAP 向任意实体提供多个授权会话;OSAP 向单个实体提供一个授权会话。本文将重点讨论 OIAP 协议。

根据 TPM 规范,首先对 OIAP 协议进行标记:其中 U 表示请求者,R 表示受保护资源,T 表示 TPM,A_R 是 U 和 T 之间共享的秘密。另外:

(1)GC 是 U 想要在 R 上执行的授权命令,也就是说,GC 的使用是要授权的,该授权由授权协议来完成;

(2)Rc 是成功返回代码;

(3)Re 是无效授权代码;

(4)D 是与 GC 相关的数据(可能为空);

(5)RES 是在 R 上执行 GC 的结果(可能为空);

(6)Ne 是一个 160 位的用于提供新鲜性保证的随机数;

(7)No 是一个 160 位的同 Ne 有相同特征的奇随机数;

(8)$Auth=\{GC.S_1.Ne.No\}$是输入参数授权消息认证码。

则 OIAP 协议的运行步骤如下:

(1)U 通过向 T 发送命令 CMD_OIAP 请求建立授权会话;

(2)T 向 U 发送建立授权会话所必须的消息 S_1 和 Ne;

(3)如果以上步骤成功,U 将向 T 发送包含了 A_R 的命令 GC,用于执行;

(4)T 对消息的完整性和消息发送主体的真实性进行认证,如果认证通过,则 T 执行 GC 并向 U 返回执行结果。否则,T 将中断与 U 的会话。

图 1 描述了以上过程,其中 $resAuth=\{Rx,GC,S_1,N'e,No\}$(输出参数授权消息认证码),$Rx$ 是 Rc(正确时)或 Re(错误时)。

1. $U\rightarrow T$:CMD_OIAP
2. $T\rightarrow U$:S_1,Ne
3. $U\rightarrow T$:$GC.R.D.S_1.Ne.Ne.H(A_R,Auth)$

　如果 $H(A_R,Auth)$被认证通过,则 T 在 R 上执行 GC

4a. $T\rightarrow U$: $Rc.GC.RES.N'e.No.H(A_R,resAuth)$

else

4b. $T\rightarrow U$:$Re.GC.RES.N'e.No.H(A_R,resAuth)$

图 1　OIAP 协议描述

3　对 OIAP 的重放攻击

下面将阐述攻击 OIAP 的主要策略。TCG 规范中指出,在 OIAP 协议中,由 TPM_OIAP 命令建立的授权会话一直处于打开状态,除非 TPM 明确地选择关闭会话或在授权会话过程中收到了错误的消息(例如,带有错误参数的消息或是无效的 HMAC)。因此,攻击者可以按如下方法进行直接重放攻击。

在用户和 TPM 已经交换了协议中的头两条消息(图 1 中的 1、2 步)之后,攻击者拦截并存储由用户生成的下一条消息(图 1 中的第 3 步),以便将该消息插入到协议的其他回合。与此同时,攻击者向用户发送一条貌似合法的错误消息以欺骗用户(例如,貌似图 1 中步骤 4a 的消息,但有几位错误,给人造成是网络错误的错觉)。常规情况下,用户程序在遇到错误的情况下会选择关闭会话,但对于 TPM 来说,此会话还是打开的,利用这个打开的会话和截获的消息,入侵者可以进行重放攻击。为了方便阐述,用 $X*$ 表示冒充实体 X 的攻击者,将攻击分成 3 个阶段:拦截消息的消息存储阶段、观察合法用户特性的消息再发阶段和重放攻击阶段,具体步骤见图 2–图 4。

Message storing phase

1a. $U\rightarrow T*$:CMD OIAP

1b. $U*\rightarrow T$:CMD OIAP

2a. $T\rightarrow U*$:$S_1.Ne$

2b. $T*\rightarrow U$:$S_1.Ne$

3a. $U\rightarrow T*$:$GC.R.D.S_1.Ne.No.H(AR,Auth)$

3b. $T*\rightarrow U$:reset

图 2　OIAP 消息存储阶段

Message re-sending phase

4a. $U\rightarrow T*$:CMD OIAP

4b. $U*\rightarrow T$:CMD OIAP

5a. $T\rightarrow U*$:$S_2.N0e$

5b. $T*\rightarrow U$:$S_2.N0e$

6a. $U\rightarrow T*$:$GC.R.D_0.S_2.N0e.N0o.H(A_R,Auth)$

6b. $U*\rightarrow T$:$GC.R.D_0.S_2.N0e.N0o.H(A_R,Auth)$

7a. $T\rightarrow U*$:$R_c.GC.RES_0.N00e.N0o.H(A_R,resAuth)$

7b. $T*\rightarrow U$:$R_c.GC.RES_0.N00e.N0o.H(A_R,resAuth)$

图 3　OIAP 消息再发阶段

Replay attack phase

8a. $U*\rightarrow T$:$GC.R.D.S_1.Ne.No.H(A_R,Auth)$

8b. $T\rightarrow U*$:$R_c.GC.RES.N0e.No.H(A_R,resAuth)$

图 4　OIAP 重放攻击阶段

4　解决方案

针对以上攻击可采用如下对策:在每一条授权消息中引入一个新的“组件”,这样一个“组件”代表用户对授权会话状态的认识,其值由用户依据下列规则计算得到:

(1)第 i 位为 0,如果第 i 次授权会话处于“打开”或“不可知”状态(“打开”或“失败”以外的状态)。

(2)第 i 位为 1,如果第 i 次授权会话处于“失败”状态,也就是说,用户收到一个 reset 或是错误的应答(如图 2 中步骤 3b)。

通过这样一个“组件”,TPM 可以掌握用户端的会话状态,当 TPM 发现对于同一个会话,自己的状态与用户的状态不一致时(例如,用户的 S_1 是失败状态,而 TPM 的 S_1 是不可知状态)将关闭相应的会话。这样,可避免上述重放攻击。

5　结论

本文着重对可信平台模块 TPM 中的 OIAP 协议进行讨论,证明协议在执行过程中的确会遭受重放攻击,并且提出了相应的解决方案,即在 TPM 和用户之间共享会话状态。下一步的主要工作是对该解决方案进行进一步的扩展跟完善,以便该方法可以解决协议可能遭受的 MiTM 攻击(中间人攻击)。

(收稿日期:2007 年 3 月)

参考文献:

[1] Trusted platform module main specification,Part 1:design principles,Part 2:TPM structures,Part 3:TPM commands[EB/OL].[2003-10].http://www.trustedcomputinggroup.org.

[2] Balacheff B,Chen L,Pearson S,et al.Trusted Computing Platforms,TCP:a technology in context[M].[S.l.]:Prentice Hall PTR,2003.

[3] Arbaugh W A,Farber D J,Smith J M.A secure and reliable bootstrap architecture[C]//Proceedings of the 1997 IEEE Symposium on Security and Privacy,SP'97,IEEE Computer Society,1997:65-71.

[4] 卿斯汉.安全协议[M].北京:清华大学出版社,2005.