可信计算授权协议分析与改进

池亚平[1]，李志鹏[1,2]，魏占祯[1]，方 勇[1]

（1. 北京电子科技学院 通信工程系，100070 北京，chiyp@besti.edu.cn；
2. 西安电子科技大学 通信工程学院，710071 西安）

摘 要：针对TCG授权协议OIAP和OSAP的安全缺陷、功能重叠等问题，提出了一种新的可信计算授权协议（OICAP）. 该协议通过引入Diffie_Hellman密钥交换算法产生的会话密钥保证其机密性，适用于多个实体，能够抗重放攻击，保证了通信数据的完整性和机密性. 通过对新授权协议进行BAN逻辑分析，表明该协议能够达到预期效果.

关键词：可信计算；授权协议；DH算法；重放攻击；BAN逻辑
中图分类号：TN918 **文献标志码**：A **文章编号**：0367－6234(2012)03－0119－04

Analysis and improvement of trusted computing authorization protocol

CHI Ya-ping[1], LI Zhi-peng[1,2], WEI Zhan-zhen[1], FANG Yong[1]

(1. Dept. of Communications Engineering, Beijing Electronic Science and Technology Institute, 100070 Beijing, China, chiyp@besti.edu.cn; 2. School of Communications Engineering, Xidian University, 710071 Xi'an, China)

Abstract: To overcome the problems that there are unsafe loopholes, functional duplication in TCG authorization protocols, a new trusted computing authorization protocol is proposed in the paper, in which the session key is introduced in the new protocol generated by Diffie_Hellman algorithm to guarantee its confidentiality. The new protocol can provide the function of anti-replay attack and can be applied to multiple entities. It can also guarantee the communication integrity and confidentiality of data effectively. The security properties are analyzed and verified by BAN logic in the paper.

Key words: Trusted Computing; authorization protocol; Diffie_Hellman algorithm; replay attack; BAN logic

在可信计算中，访问TPM资源（如某些函数或某个实体）需要使用授权协议来证明访问者具有合法的授权. TCG联盟在授权数据管理协议中，依靠rolling nonce机制和消息认证码HMAC机制来保证授权过程的完整性和抗重放能力.

TCG规范基于密码技术实现了多种应用安全机制，如TCG定义了5种证书、6种协议以及7种密钥，以满足多种应用场景的需求. 由于TCG在设计规范时有意回避对称密码体制，以及联盟内多个厂商解决方案之间的妥协都造成了这种复杂体系.

国内外学者对TCG规范中使用最为频繁的两个授权协议OIAP（Object Independent Authorization Protocol）和OSAP（Object Specific Authorization Protocol）进行了大量研究，对两个协议的安全性进行了分析. 文献[1]提出了一种针对OIAP的中间人攻击. 文献[2]针对弱口令和口令泄露等问题提出了增强安全性的协议改进. 文献[3－5]引入对称密码体制提升协议的机密性，并简化TCG复杂的授权协议簇. 在众多的改进协议中，存在假设不合理、会话密钥无法得到授权保证和无法抵抗中间人攻击等问题. 本文针对TCG协议规范中存在的漏洞和功能重叠、效率低的特点提出了1个改进的授权协议，该协议有效地解决了一种特定情况下的中间人攻击，采用Diffie_Hellman密钥交换算法生成会话密钥加密敏感数据，最后对其安全性进行了分析.

收稿日期：2010－08－25.
基金项目：国家自然科学基金资助项目（60951001），北京市自然科学基金资助项目（4102057），国家科技支撑计划重点资助项目（2009BAH52B06）.
作者简介：池亚平（1969—），女，副教授；
方 勇（1963—），男，教授.

1 可信计算中授权协议分析

TPM 主要提供了两种使用实体的授权协议(OIAP、OSAP). 在两种协议中,通信双方通过哈希 nonce 数据和共享秘密作为授权来抵抗可能的中间人攻击,同时这种授权方式也具有抗重放攻击的特点.

1.1 TCG 授权协议概述

OIAP 协议被设计为用来提供授权给 TPM 管理的任何实体,授权数据通常为口令的 hash 值. OIAP 协议通过会话模式创建,1 个 OIAP 一经创建可以为任意的实体提供授权,同时可以进行多个 OIAP 授权会话. 与 OSAP 协议相比,OIAP 使用 1 个会话便可以为不同的实体提供授权,更具通用性.

OSAP 协议使用共享秘密,在针对某个具体的实体运行时,安全性要高于 OIAP 协议. OSAP 协议的设计相对 OIAP 协议更具有效率,在针对某个特定的实体进行会话时,OSAP 被设计为只传送授权数据一次,其后通过临时共享秘密来提供授权. OSAP 减少了授权数据的传递次数,减低了口令等敏感数据的暴露危险,它的不足之处是不同的实体需要建立不同的会话来进行授权.

1.2 OIAP 潜在的隐患

OIAP 协议通过 rollingnonce 机制,由使用者和 TPM 轮流生成 nonce 值,来保证消息的新鲜性. 同时在数据交互过程中使用了 HMAC 值 H_{HMAC}, 用 hash 函数校验输入、输出数据的完整性,保证了消息不被篡改和替换. 在 HMAC 的输入中使用授权数据,达到认证的目的,拒绝了非法的访问者. 文献[1]提出了一种针对 OIAP 协议的重放攻击方法,使得 OIAP 暴露出了一定的缺陷. 攻击方法如图 1 所示.

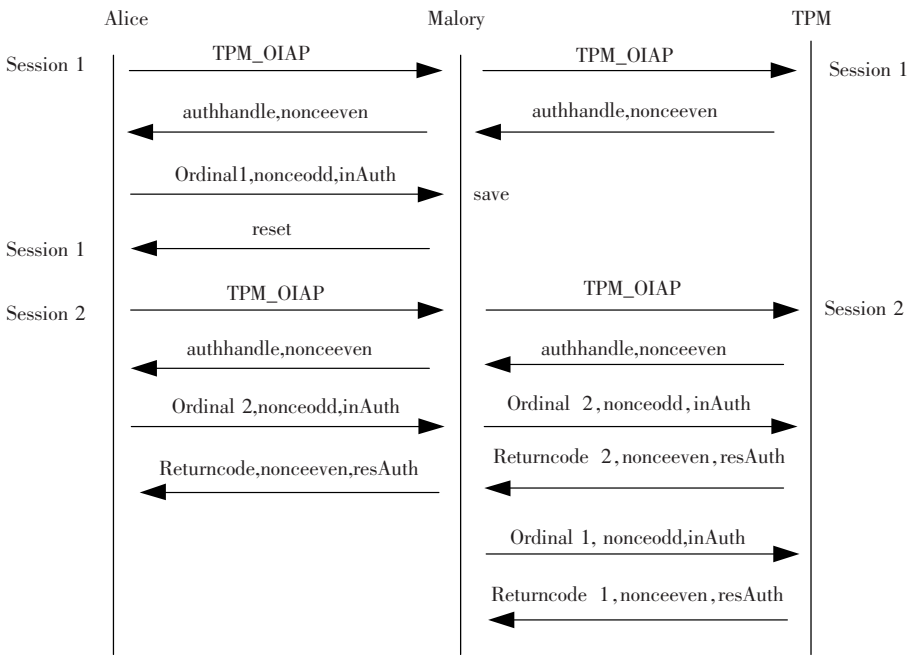

图 1 OIAP 的重放攻击

1 个恶意的中间人可以使用拦截、欺骗、转发的方法改变 Ordinal 命令的执行顺序. 如图 1 所示,中间人先拦截并保存使用者的命令,通过向使用者返回 1 个 TPM 故障重启的信号使得使用者重新开启新的会话,并执行命令. 对于新的会话,可能出现的情况有:1)原命令与原数据;2)原命令与新数据;3)新命令与新数据. 这种攻击方法对情况 1)没有什么效果,而对情况 3)则可以进行新一轮的攻击. 对于在情况 2)下潜在的攻击方式,中间人可以重放授权命令,更改了命令顺序. 如果攻击目标是度量值的更新操作,则可以用被捕获的失效值来替换新产生的值,使得可信不再可信.

1.3 TCG 协议缺陷分析

出于对效率和安全性的不同侧重,TCG 联盟设计了两种不同的授权方式. OIAP 协议更侧重于效率,但是经过分析发现,存在一种攻击方式可以利用错误会话产生的授权数据. 同时 OSAP 协议在功能上与 OIAP 协议相同,出于安全性考虑,采用临时共享秘密来减少对共享秘密的使用. 由于采用了相同的 HMAC 机制来加强私密性,导致了安全性没有得到保证,同时这种冗余的协议体系不利于 TPM 芯片高效率地工作.

2 OICAP 协议

2.1 OICAP 协议描述

为避免敏感信息的直接传输,在借鉴 TCG 标

准的基础上,本文提出了一种新的授权协议 OICAP(Object - Independent Confidential Authorization Protocol),该协议采用对称密码方法加密敏感信息且具有抗重放攻击的能力.

协议中用到的符号如下: C_{CMD} 代表使用者 C 想在可信平台 T 上执行的授权命令;R 为受保护的资源;S_r 代表 Alice 与 TPM 之间共享的秘密,通常为口令的哈希值;D 为命令中的数据;R_{RES} 为在 R 上执行 C_{CMD} 的结果; N_e 为 160 B 的随机数用来保证新鲜性;N_o 为 160 B 的随机数,同 N_e;K_h 代表密钥句柄;T_p 代表可信平台当前状态. 协议流程如图 2 所示.

1. $C \rightarrow T: C_{MD\_OICAP}, N_o, T_p, K_h, Y_a, A_i$.
2. $T \rightarrow C: T_p, N_e, T_p, Y_b, A_r$.
3. $C \rightarrow T: E_{sk}(D), N_o, R, C_{CMD}, A_i$.
4. $T \rightarrow C: R_{RES}, E_{sk}(D), N_e, A_r$.

图 2　OICAP 协议流程

图 2 的步骤 1 中 Caller 向 TPM 发送 OICAP 请求,可信平台 TPM 当前状态 T_p, 标记了 TPM 当前状态(如未知、正常或故障); Y_a 用于与 TPM 协商会话密钥. A_i 为授权数据,且

$$A_i = H_{HMAC}(S_r \| T_p \| N_o \| Y_a).$$

TPM 验证授权数据,如果使用者认为的状态符合 TPM 状态,则开启 OICAP 会话,生成

$$Y_a = g^{X_a} (\mathrm{mod}\ p),$$

保存 X_a (Diffie_Hellman 算法见文献[6]).

步骤 2 中 TPM 向 Caller 发送 authHandle, T_p, N_e, Y_b, A_r, 其中

$$A_r = H_{HMAC}(T_p \| S_r \| N_o \| N_e \| Y_b),$$

$Y_b = g^{X_b} (\mathrm{mod}\ p)$ 生成会话密钥 $K_{sk} = Y_a^{X_b} (\mathrm{mod}\ p)$ 会话共享秘密

$$K_{sr} = H_{HMAC}(S_r \| N_o \| N_e).$$

步骤 3 中 Caller 根据 N_o、N_e、S_r 生成会话共享秘密 K_{sr},计算授权数据是否有效,生成会话密钥 $K_{sk} = Y_b^{X_a} (\mathrm{mod}\ p)$,可以选择用 K_{sk} 加密输入参数,授权数据

$$A_i = H_{HMAC}(E_{sk}(D), N_o, K_{sr});$$

步骤 4 中 TPM 验证授权数据,用 K_{sk} 解密输入参数,最后执行命令,返回参数时同样使用 K_{sk} 加密返回的参数,根据 continueAuthSession 判断是否继续会话.

2.2　OICAP 协议安全性分析

OICAP 协议的安全性分析主要从以下 5 个方面.

1)认证. 认证是最重要的安全手段之一,系统中的主体进行身份识别的过程,所有其它的安全性都依赖于此. TCG 规范中授权协议采用 HMAC 机制来保证消息的认证性. 通过对口令的哈希值和其他值如 nonce 和授权句柄进行 HMAC 运算,生成消息认证码来保证消息是源自于期待的实体. OICAP 协议中采用 HMAC 机制来保证消息的认证. 与 AP 协议不同(见文献[5]),OICAP 协议采用 HMAC 机制于会话密钥的生成过程中,在防止了中间人攻击的同时无需引入可信第三方.

2)私密性. 秘密性的目的是为了保护协议消息不被泄露给未授权拥有此消息的人,即使是攻击者观测到了消息的格式,它也无法从中得到消息的内容或提炼出有用的消息. OICAP 通过可选的加密模式来保证消息的秘密性,由于采用了 DH 密钥交换算法使得加密过程具有了完美向前保密(PFS). 分享秘密的双方均会对结果施加自己的影响,密钥被丢弃后更换新的密钥,两个密钥相互之间不具有任何关系,进一步提升了保密的安全性.

3)抗重放. 通过 rollingnonce 机制在消息中添加新鲜值抵抗重放攻击.

4)完整性. 完整性的目的是保护协议消息不被非法篡改、删除和替代. OICAP 采用 HMAC 保证消息的完整性.

5)抗并行会话引起的重放攻击. OICAP 协议引入了平台状态信息 TPstate 位保证会话的真实有效性. 由于加入 TPstate 标志平台的状态,因此协议具有抗上述重放攻击的特点. 当中间人欺骗使用者,报告 TPM 当前状态为故障时,使用者标记当前 TPM 为故障. 重新建立的 TPM 会话中 TPM 状态与 TPM 方状态不一致,TPM 即撤销当前所有会话. 并将 TPM 状态位恢复为正常状态.

综上所述,OICAP 协议与 TCG 协议功能比较如表 1 所示.

表 1　安全性能对比

协议	认证	抗重放	完整性	秘密性	抗并行会话重放攻击
OIAP	✓	✓	✓	×	×
OSAP	✓	✓	✓	×	×
OICAP	✓	✓	✓	✓	✓

2.3　OICAP 协议安全性形式化分析

BAN 逻辑是一种基于信念的逻辑,是 1989 年由 Michael Burrows,Maitin Abadi 和 Reoger Neeham 提出的. BAN 逻辑的核心思想是:通过对认证协议过程的形式化分析来研究认证双方通过相互接受和发送消息,从最初各自的信任逐渐发展到协议实现的最终目标——认证双方的最终信任. BAN 逻辑中定义的基本符号和推理规则参见文献[6].

本文提出的可信授权方案 OICAP 的 BAN 逻辑分析过程如下.

1)首先建立初始条件集合.

$$T_{\mathrm{TPM}} \mid \equiv T_{\mathrm{TPM}} \overset{S_r}{\longleftrightarrow} U,$$
$$C \mid \equiv C \overset{S_r}{\longleftrightarrow} T_{\mathrm{TPM}},$$
$$T \Rightarrow X_b,$$
$$T_{\mathrm{TPM}} \mid \equiv \#(N_e),$$
$$C \mid \equiv \#(N_o),$$
$$C \Rightarrow X_a,$$

2)可信授权方案建立过程的 BAN 逻辑化.

① $C \rightarrow T_{\mathrm{TPM}}: \{C_{\mathrm{CMD\_OICAP}} \{N_o \parallel T_p \parallel Y_a\} S_r\}$;

② $T_{\mathrm{TPM}} \rightarrow C: \{\{T_p \parallel N_e \parallel Y_b\} S_r\}$;

③ $C \rightarrow T_{\mathrm{TPM}}: \{\{C_{\mathrm{CMD}} \parallel E_{sk}(D) \parallel N_o \parallel \}_{s_r}\}$;

④ $T_{\mathrm{TPM}} \rightarrow C: \{\{R \parallel R_{\mathrm{RES}} \parallel N_e\}_{s_r}\}$.

3)建立协议预期目标集合为

$$T_{\mathrm{TPM}} \mid \equiv \{C_{\mathrm{CMD}}\},$$
$$T_{\mathrm{TPM}} \mid \equiv \#(C_{\mathrm{CMD}}),$$
$$T_{\mathrm{TPM}} \mid \equiv \{D\}_{sk},$$
$$C \mid \equiv \{R \parallel R_{\mathrm{RES}}\},$$
$$C \mid \equiv \#(R \parallel R_{\mathrm{RES}}),$$
$$C \mid \equiv \{D\}_{sk}.$$

即需要证明 TPM 相信 C 发送了执行命令 C_{CMD} 的请求,且 C_{CMD} 是新鲜的,同时 C_{CMD} 的数据被会话密钥 K_{sk} 加密. 同样 C 相信 TPM 返回了命令 C_{CMD} 的执行结果及返回码,且上述信息是新鲜和用 K_{sk} 加密过的.

4)可信授权方案的 BAN 逻辑形式化证明.

(1)由可信授权方案的第 1)步知:

$$T \lhd \{C_{\mathrm{CMD\_OICAP}}, \{N_o, T_p, Y_a\} S_r\},$$

且 $C \overset{A_r}{\longleftrightarrow} T$ 由消息源规则可知,

$$\frac{T \mid \equiv C \overset{A_r}{\longleftrightarrow} T \wedge T \lhd \{C_{\mathrm{CMD\_OICAP}}, \{N_o, T_p, Y_a\}_{Sr}\}}{T \mid \equiv C \mid \sim \{N_o, T_p, Y_a\}_{Sr}},$$

即 TPM 相信 Caller 发送了消息 $\{C_{\mathrm{CMD\_OICAP}}, \{N_o, T_p, Y_a\}_{Sr}\}$ 同理

$$\frac{C \mid \equiv C \overset{A_r}{\longleftrightarrow} T \wedge C \lhd \{T_p, N_e, Y_b\}_{Sr}}{C \mid \equiv T \mid \sim \{T_p, N_e, Y_b\}_{Sr}},$$

即 Caller 相信 TPM 返回了消息 $\{T_p, N_e, Y_b\}_{Sr}$.

(2)由消息的新鲜性规则得

$$\frac{T \mid \equiv \#(N_o)}{T \mid \equiv \#(C_{\mathrm{CMD}}, \{N_o, T_p, Y_a\}_{Sr})},$$

同理可得 $C \mid \equiv \#(\{N_e, T_p, Y_b\}_{Sr})$.

(3)由临时值校验规则知

$$\frac{T \mid \equiv \#(C_{\mathrm{CMD}}, N_o, T_p, Y_a) \wedge T \mid \equiv C \mid \sim \{C_{\mathrm{CMD}}, N_o, T_p, Y_a\}}{T \mid \equiv C \mid \equiv \{C_{\mathrm{CMD}}, N_o, T_p, Y_a\}}.$$

即 TPM 相信消息 $\{C_{\mathrm{CMD}}, N_o, T_p, Y_a\}$ 被 Caller 相信.

(4)由管理权规则知

$$\frac{T \mid \equiv C \rightarrow \{C_{\mathrm{CMD}}, N_o, T_p, Y_a\} \wedge T \mid \equiv C \mid \equiv \{C_{\mathrm{CMD}}, N_o, T_p, Y_a\}}{T \mid \equiv \{C_{\mathrm{CMD}}, N_o, T_p, Y_a\}}.$$

即 TPM 相信消息 $\{C_{\mathrm{CMD}}, N_o, T_p, Y_a\}$. 同理 $C \mid \equiv \{T_p \parallel N_e \parallel Y_b\}$.

(5)由初始化条件 $T \Rightarrow X_a$ 与 $C \Rightarrow X_b$ 运用信仰规则得

$$\frac{T \mid \equiv X_b \wedge T \mid \equiv Y_a}{T \mid \equiv (X_b, Y_a)},$$

由于 $K_{sk} = Y_a{}^{X_b}$,即 $T \mid \equiv K_{sk}$,同理可以推出 $C \mid \equiv K_{sk}$. 运用信仰规则

$$\frac{T \mid \equiv (N_o, N_e, S_r)}{T \mid \equiv N_o}$$

可知 $T \mid \equiv N_o$ 同理 $T \mid \equiv N_e, T \mid \equiv S_r$,由 $K_{sr} = H_{\mathrm{HMAC}}\{N_o, N_e, S_r\}$ 可知 $T \mid \equiv s_r$.

(6)将授权数据 S_r 替换成共享秘密 K_{sr} 后,重复步骤(1) ~ (4),可以得到协议预期目标,在此不再赘述.

3 结 语

本文分析了 TCG 两个主要的授权协议,并针对 TCG 授权协议 OIAP 存在缺陷且与 OSAP 协议功能重叠,无法保证私密性等问题提出了一种新的授权协议,并对协议进行了安全性形式化分析,分析表明该协议比 TCG 原有协议具有更高的安全性.

参考文献:

[1] BRUSCHI D, CAVALLARO L. Andrea lanzi replay attack in TCG specification and solution [EB/OL]. http://citeseerx. ist. psu. edu/viewdoc/download? doi = 10. 1. 1. 98. 6254&rep = rep1&type = pdf.

[2] DIFFIE W, HELLMAN M E. Multiuser cryptographic techniques [C]//AFIPS Conference Proceedings. New York: [s. n.], 1976, 45: 109 – 112.

[3] 刘皖, 谭明, 陈兴蜀. TPM 的两个主要密码授权协议的安全性分析与改进[J]. 计算机科学, 2008, 35(3): 271 – 273.

[4] 罗芳, 徐宁, 周燕舟, 等. 可信计算中对象访问授权协议的分析与改进[J]. 计算机应用与软件, 2008, 25(12): 30 – 32.

[5] 张兴, 张晓菲, 刘毅, 等. 可信计算授权数据管理与安全协议研究[C]//全国网络与信息安全技术研讨会. 青岛: [s. n.], 2007: 252 – 257.

[6] BURROWS M, ABADI M, NEEDHAM R. A logic of authentication [J]. ACM Transactions on Computer Systems, 1990, 8(1): 18 – 36.

(**编辑** 张 宏)