

文章编号:1001-9081(2005)12-2731-03

用隐藏证书实现访问策略

洪帆, 刘磊

(华中科技大学 计算机科学与技术学院, 湖北 武汉 430074)

(hbjmll@sina.com)

摘要:为解决在信任管理系统中使用隐藏证书的效率问题,借助于策略表达式和结束前缀,给出了一种使用隐藏证书有效实现复杂访问策略的方案,通过构造策略表达式并对其化简减少了加密和解密的次数,通过“结束前缀”方便了信息的还原。实例显示该方案具有较好的可行性和效率。

关键词:隐藏证书; 访问策略; 信任协商

中图分类号: TP309.2 **文献标识码:**A

Implementing access policies with hidden credentials

HONG Fan, LIU Lei

(Institute of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan Hubei 430074, China)

Abstract: To solve the efficiency problem of using hidden credentials in trustmanagement system, a scheme using hidden credentials to efficiently implement complex polices with "polices expression" and "final prefix" was presented. The encryption and decipherment times were reduced by constructing and simplifying policy expression, the information restore was guaranteed by using "final prefix". Example shows that the scheme is feasible and efficiency.

Key words: hidden credentials; access policies; trust negotiation

0 引言

证书是由认证中心(CA)颁发的用来证明个体身份或属性的证件。在信任管理系统中,证书用来实现信任协商。资源的请求者根据资源的访问策略向资源的拥有者提供自己的证书从而获得相应的资源,因此证书本身是作为公开信息发布。然而实际情况是证书和资源的访问策略中都可能含有敏感信息,这就要求证书和策略非公开化。秘密握手^[1]、OSBE^[2]以及隐藏证书^[3]都是为了保护证书而提出的。其中OSBE无法对访问策略实施保护,秘密握手要求所有证书来自于同一个CA,只有隐藏证书能够灵活地实现对证书和访问策略的保护。

采用隐藏证书,发送方根据保护策略来加密信息,接收方必须使用保护策略要求的证书才能还原信息。文献[3]中给出了用隐藏证书实现访问策略的方法,但是存在两点不足:1)涉及多个证书的复杂保护策略中可能存在冗余,直接根据它来加密信息效率很低;2)如果信息由若干证书多重加密,由于接收方不知道策略形式,它无法有效地判断自己是否满足策略。

本文针对以上两点不足对文献[3]中的方法加以改进,提出了一个用隐藏证书实现访问策略的具体方案,该方案能够提高根据策略加密信息的效率,同时确保信息还原过程的顺利进行。

1 隐藏证书介绍

1.1 隐藏证书

隐藏证书可以实现对敏感的请求、资源、证书以及策略的保护。借鉴基于身份的加密方案(IBE)^[4],认证中心用系统私钥对主体的<名字,属性>签名,生成属性证书并颁发给主

体,证书作为主体的私钥由主体秘密持有,不对外公开,而<名字,属性>就是其对应的公钥。发送方根据消息的访问策略来加密敏感消息,接收方则使用自己拥有的证书来解密,当且仅当接收方满足策略的时候才能还原被保护信息。有如下定义:

P_x : 敏感信息x的访问策略(其中x可以是请求、资源或者证书)。

C_{pi} : 策略“要求有证书 C_i ”。

C_{pi}^* : 策略 C_{pi} 本身是需要保密的,当且仅当接收方拥有证书 C_i ,他才能知道策略 C_{pi} 。

简单访问策略:如果策略 P 只涉及单个证书,即 $P = C_{pi}$,称 P 为简单访问策略。

$Hes(R, P)$: 根据简单访问策略 P 来加密信息 R 。

$Hds(M, G_C)$: 使用证书集合 G_C 来解密密文 M 。

加密函数 Hes 和解密函数 Hds 是用来实现简单访问策略的。对于 $M = Hes(R, P), P = C_{pi}$, 解密者需要用自己持有的证书集合 G_C 中每一个证书去尝试对 M 进行解密,如果 $C_i \in G_C$, 则有 $Hds(M, G_C) = R$, 否则 $Hds(M, G_C) = null$, null 表示解密结果无实际意义。这里 Hes 和 Hds 的具体实现参见 IBE 方案^[4,5]。

本文用隐藏证书来实现信任协商过程(用户 A 请求访问用户 B 的一份文件 M)。

(1) A 向 B 发送请求 $Ta = Hes(request, Prequest)$;

(2) B 的证书集合为 C_B , 如果 B 满足 $Prequest$, 就能还原 $request = Hds(Ta, C_B)$;

(3) B 向 A 发送资源 $Tb = (M, P_M)$;

(4) A 的证书集合为 C_A , 如果 A 能够满足 P_M , 就能还原 $M = Hds(Tb, C_A)$ 。

隐藏证书在信任协商中实现了以下功能:

收稿日期:2005-06-23

作者简介:洪帆(1942-),女,湖北武汉人,教授,博士生导师,主要研究方向:安全模型、密码技术; 刘磊(1979-),男,湖北荆门人,硕士研究生,主要研究方向:分布式访问控制。

1) 实现对证书的隐藏。证书由主体秘密持有,当且仅当信息的接收方拥有满足策略的证书时才能够恢复信息,所以接收方不需要向信息的持有者出示自己的证书。换句话说,发送方的策略被满足的同时,他不可能得到任何关于接收方证书或者其解密能力的信息。

2) 实现对策略的隐藏。资源的访问策略不需要公开,接受方必须通过枚举证书的方式来解密,只有当它满足这个策略时才能够知道策略是什么。

3) 实现对资源的隐藏。在实现证书隐藏和策略隐藏的同时,我们实现了对请求和资源的加密传送,无需额外的密钥,因为我们是以证书本身作为密钥的。

1.2 复杂访问策略

加密函数 HE_s 要求参数 P 是只涉及单个证书的简单策略,而实际应用中的策略往往是涉及多个证书的,这些证书甚至是由不同的认证中心颁发的,称之为复杂策略。举例来说,“年满 25 岁且学历本科以上才能获得面试资格”,这个策略就涉及到“年满 25 岁”和“学历本科以上”两个属性,它们分别由两个不同的证书证实。用隐藏证书实现复杂的访问策略时,函数 HE_s 就不够用了,必须对其进行扩展,下面介绍了一个用隐藏证书实现复杂访问策略的具体方案。

2 用隐藏证书实现复杂访问策略的方案

2.1 构造策略表达式并化简

复杂策略其实就是若干简单策略的一个逻辑组合,因此可以使用逻辑表达式来表示复杂策略。引入 and 和 or 运算符,对于任意两个策略 X 和 Y ,用 $(X \text{ and } Y)$ 表示“同时满足 X 和 Y ”,用 $(X \text{ or } Y)$ 表示“至少满足 X 和 Y 中的一个”。这样就可以把复杂策略用由 and,or,简单策略(形如 C_{pi})以及括号组成的逻辑表达式来表示,称之为策略表达式。

策略表达式的形式可能会过于复杂,为了提高效率,减少冗余,有必要对其进行化简,化简方法为:

(1) 通过逻辑运算的各种性质(包括交换率、结合率、分配率、等幂率、吸收率等)将策略表达式写成与之等价的析取范式;

(2) 根据等幂率和吸收率化简析取范式,得到策略表达式的最终形式。

2.2 根据策略表达式加密信息

构造好策略表达式以后,发送方就可以根据策略表达式来对信息进行加密,我们定义加密函数 HE :

- (1) 如果 P 是一个简单策略,那么 $HE(R, P) = HE_s(R, P)$;
- (2) $HE(R, P_1 \text{ and } P_2) = HE(HE(R, P_1), P_2)$;
- (3) $HE(R, P_1 \text{ or } P_2) = (HE(R, P_1), HE(R, P_2))$ 。

在(2)中, $HE(R, P_1)$ 是中间结果,在还原的时候需要接收方对解密得到的中间结果继续解密,但是接收方得到中间结果后根本无法判断他是拿到了中间结果还是自己不能满足策略。我们采用“结束前缀”来解决这个问题,由发送方给中间结果和最终结果加上不同的前缀,接受方就可以通过前缀来判断是否中间结果。“结束前缀”的具体实现方法是为原始资源 R 加上前缀“end”,为中间结果加上前缀“mid”,函数 HE 定义中(1)就变成:

(1) 如果 P 是一个简单策略,那么 $HE(R, P) = \text{mid;}HE_s(R, P)$;

注意到,对于 $HE(R, P_1 \text{ and } P_2)$,我们可以有 $HE(HE(R, P_1), P_2)$ 和 $HE(HE(R, P_2), P_1)$ 两种等价的处理方式,应该把形式相对简单的部分放在外层,这样不仅可以减少对策略

形式的暴露,而且可以提高加密效率。

2.3 使用证书还原信息

借助于“结束前缀”,接收方根据密文 M 的形式逐层解密,解密函数 HD 定义如下:

$$HD(M, C_G) =$$

$$\begin{cases} \bigcup_{i=1}^N HD(M_i, C_G) & M = (M_1, M_2, \dots, M_n) \\ HD(HDs(M - "mid:", C_G), C_G) & M \text{ 带有前缀"mid:"} \\ M - "end:" & M \text{ 带有前缀"end:"} \\ \text{null} & M \text{ 无前缀} \end{cases}$$

其中 C_G 是接收方的证书集合, \cup_+ 运算规则为: $R \cup_+ \text{null} = R, R \cup_+ R = R, \text{null} \cup_+ \text{null} = \text{null}$, 这里 R 是跟在前缀 R 后的内容。如果 $HD(M, C_G) = R$, 则 R 就是被策略保护的敏感消息,如果 $HD(M, C_G) = \text{null}$,则表示接收者不能满足访问策略从而无法得到 R 。需要说明的是,如果解密过程中出现形如 $R_1 \cup_+ R_2$ 的运算,其中 R_1 和 R_2 是不同的两份跟在“end;”后的信息,这就意味着密文 M 有误,接收方应该丢弃 M 或者重新请求。

3 应用实例

用户 B 的证书集合为 $C_B = \{C_1, C_2, C_3, C_4, C_5\}$, 用户 A 的证书集合为 $C_A = \{C_6, C_7, C_8, C_9, C_{10}\}$, 用户 B 拥有资源 RS , 用户 A 的请求 RQ 表示需要访问资源 RS , 存在以下访问策略:

$$P_{RQ} = C_{p1} \text{ and } (C_{p0} \text{ or } C_{p3})$$

$$P_{RS} = C_{p6} \text{ or } (C_{p8} \text{ and } C_{p11})$$

$$P_{cl} = (C_{p8} \text{ or } C_{p10}) \text{ and } C_{p7}$$

(1) A 直接根据策略 P_{RQ} 向 B 发送请求:

$$M_{RQ} = HE((HE(\text{end}; RQ, C_{p0}), HE(\text{end}; RQ, C_{p3})), C_{p1})$$

(2) B 收到 M_{RQ} 以后,发现 M_{RQ} 的形式如下:

$$\text{mid;}M_1$$

于是依次用 C_B 中的证书去尝试解密 M_1 ,由于 $C_1 \in C_B$,因此用 C_1 解密得到:

$$(\text{mid;}M_2, \text{mid;}M_3)$$

由于 $C_0 \notin C_B$, B 无法解密 M_2 这个分支, B 就可以肯定自己不满足该分支的策略,又因为 $C_3 \in C_B$, B 可以用 C_3 对 M_3 解密得到:

$$\text{end;}RQ$$

这样 B 就还原出了 RQ , 知道 A 要请求访问资源 RS 。

(3) B 构造 RS 的访问策略表达式,首先必须满足 P_{RS} ,但仅此是不够的。如果 A 能够正确得到 RS , 它就可以断定 B 满足它的策略 P_{RQ} , 也就是说 B 肯定拥有证书 C_1 以及 (C_0, C_3) 中的一个。而 B 的证书 C_1 是受策略 P_{cl} 保护的,因此保护 RS 的策略表达式应该是 P_{cl} and P_{RS} , 即:

$$(C_{p6} \text{ or } (C_{p8} \text{ and } C_{p11})) \text{ and } ((C_{p8} \text{ or } C_{p10}) \text{ and } C_{p7})$$

写成范式的形式为:

$$(C_{p6} \text{ and } C_{p7} \text{ and } C_{p8}) \text{ or } (C_{p6} \text{ and } C_{p7} \text{ and } C_{p10}) \text{ or } (C_{p7} \text{ and } C_{p8} \text{ and } C_{p11})$$

化简得:

$$((C_{p8} \text{ and } C_{p11}) \text{ or } ((C_{p8} \text{ or } C_{p10}) \text{ and } C_{p6})) \text{ and } C_{p7}$$

B 就构造如下密文返回给 A :

$$M_{res} = HE((HE(HE(\text{end}; RS, C_{p8}), C_{p11}), HE((HE(\text{end}; RS, C_{p8}), C_{p10}), C_{p6})), C_{p7})$$

(4) A 收到密文:

$$M_{res} = \text{mid;}M_4$$

用 C_{p7} 解密 M_4 得到:

(mid: M_5 , mid: M_6)

由于 $C_{11} \notin C_A$, A 无法解密 M_5 , 而 $C_6 \in C_A$, 于是可以由 M_6 得到:

(mid: M_7 , mid: M_8)

由于 $C_8, C_{10} \in C_A$, B 通过解密 M_7 和 M_8 都可以得到:

end: RS

至此, A 成功的得到了资源 RS 。

隐藏证书方案的性能取决于对简单策略加密和解密函数的调用次数。考虑第 3 部分 RS 的访问策略 P_{cl} 和 P_{rs} , 原形式为 $(C_{p6} \text{ or } (C_{p8} \text{ and } C_{p11})) \text{ and } ((C_{p8} \text{ or } C_{p10}) \text{ and } C_{p7})$, 加密需要 9 次运算, 最坏情况下解密需要 9 次枚举, 而化简之后形式为 $((C_{p8} \text{ and } C_{p11}) \text{ or } ((C_{p8} \text{ or } C_{p10}) \text{ and } C_{p6})) \text{ and } C_{p7}$, 加密只需要 6 次运算, 最坏情况下解密只需要 6 次枚举。如果我们允许加密时重用中间结果, 原形式加密需要 6 次运算, 化简后加密只需要 5 次运算。由此可见, 我们的方案通过化简减少了策略中的冗余, 提高了系统效率。

如果策略无须隐藏, 可以把策略连同密文一起发送, 提高解密效率。同时, 还可以考虑把敏感资源用对称密钥加密, 而用隐藏证书根据策略来保护对称密钥, 间接地实现了对敏感

(上接第 2730 页)

(3) 设计和完善组播密钥的代价评价体系。以移动 Ad Hoc 网络的动态拓扑、时变链路、节点能量的有效性出发, 设计出一套较全面合理的代价评价体系。

(4) 将组播密钥管理对分簇的需求与现有的分簇策略^[22]进行联合优化, 使网络安全与拓扑控制机制有机结合, 以得到高效、安全的移动 Ad Hoc 网络分层体系结构。

5 结语

由于移动 Ad Hoc 网络的特殊性, 组播密钥管理策略正逐步成为该领域的研究热点。本文较全面地综述了现有的组播密钥管理策略, 对不同的策略进行了分类, 分析了各自的特点, 并给出了组播密钥管理的若干研究方向。

参考文献:

- [1] RAMANATHAN R, REDI J. A Brief Overview of Ad Hoc Networks: Challenges and Directions [J]. IEEE Communication Magazine, 2002, 23 (5): 48–53.
- [2] 叶阿勇, 许力. 移动 Ad Hoc 网络安全策略研究[J]. 微计算机应用, 2004, 25(4): 385–390.
- [3] ZHOU L, HAAS ZJ. Securing Ad Hoc Networks[J]. IEEE Networks, 1999, 13(6).
- [4] HARNEY H, MUCKENHIRN C. Group key management protocol (GKMP) specification. RFC2093[S]. 1997.
- [5] HARNEY H, MUCKENHIRN C. Group key management protocol (GKMP) architecture. RFC2094[S]. 1997.
- [6] WALLNER D, HARDER E, AGEE R. Key management for multi-cast: Issues and architectures. RFC 2627[S]. 1999.
- [7] WALDVOGEL M, GARONNI G, SUN D, et al. The VersaKey framework: Versatile group key management[J]. IEEE Journal on Selected Areas in Communications (Special Issue on Middleware), 1999, 17(9): 1614–1631.
- [8] BALENSON D, MCGREW D, SHERMAN A. Key management for large dynamic groups: One-Way function trees and amortized initialization[Z]. IETF Internet Draft (work in progress), 2000.
- [9] CANETTI R, CARAY J, ITKIS G, et al. Multicast security: A taxonomy and some efficient constructions[A]. Proceedings of the INFOCOM99[C]. New York, 1999. 708–716.
- [10] SHAMIR A. How to share a secret [M]. Communications of the ACM, 1979.
- [11] LUO H, LU S. Ubiquitous and Robust Authentication Service for Ad Hoc Wireless Network[R]. Technical Report 200030, UCLA Computer Science Department, 2000.
- [12] KONG U, ZERFOS P, et al. Providing Robust and Ubiquitous Security Support for Mobile Ad Hoc Networks[A]. IEEE 9th International Conference on Network Protocols (ICNP'01)[C]. 2001.
- [13] LUO H, ZERFOS P, KONG J, et al. Self-securing Ad Hoc Wireless Networks[A]. Seventh IEEE Symposium on Computers and Communications (ISCC'02)[C]. 2002.
- [14] SETINER M, TAUDIK G, WAIDNET M. Cliques: A new approach to group key agreement[R]. Technical Report, RZ 2984, IBM Research, 1997.
- [15] DIFFIE W, HELLMAN ME. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, IT-22(6): 644–654.
- [16] RODEH O, BIRMAN K, DOLEV D. Optimized group rekey for group communication systems[R]. Technical Report, Hebrew University, 1999.
- [17] LEE PPC, LUI JCS, YAU DKY. Distributed collaborative key agreement protocols for dynamic peer groups[A]. Proceedings of the ICNP[C]. 2002. 53–62.
- [18] KIM Y, PERRIG A, TSUDIK G. Simple and fault-tolerant key agreement for dynamic collaborative groups[A]. Proceedings of the 7th ACM Conference on Computer and Communications Security [C]. 2000. 235–244.
- [19] BANERJEE S, BHATTACHARJEE B. Scalable secure group communication over IP multicast[J]. JSAC Special Issue on Network Support for Group Communication, 2002, 20(8): 156–163.
- [20] 陆军, 丁雪梅. Ad-hoc 网络动态密钥管理[J]. 信息技术, 2004, 28 (7): 76–78.
- [21] MITTRA S. Iolus: A framework for scalable secure multicasting [J]. New York: ACM Press, ACM SIGCOMM Computer Communication Review, 1997, 27(4): 277–288.
- [22] 许力, 张继东, 郑宝玉, 等. 移动自组网能量保护策略研究进展 [J]. 通信学报, 2004, 25(9): 93–103.

资源的保护。

参考文献:

- [1] BALFANZ D, DURFEE G, SHANKAR N, et al. Secret Handshakes from Pairing-Based Key Agreements[A]. Proceedings of the 2003 IEEE Symposium on Security and Privacy[C]. Oakland CA, 2003. 80–196.
- [2] LI NH, DU WL, BONEH D. Oblivious Signature - Based Envelope [A]. Proceedings of the 22nd ACM Symposium on Principles of Distributed Computing[C]. Boston Massachusetts: ACM Press, 2003. 182–189.
- [3] HOLT J, BRADSHAW R, SEAMONS K, et al. Hidden Credentials [A]. 2nd ACM Workshop on Privacy in the Electronic Society[C]. Washington DC: ACM Press, 2003. 1–8.
- [4] BONEH D, FRANKLIN M. Identity-Based Encryption from the Weil Pairing, extended abstract[A]. Proceedings of Crypto 2001, volume 2139 of Lecture Notes in Computer Science[C]. Springer-Verlag, 2001. 213–229.
- [5] BENALOH J, LEICHTER J. Generalized Secret Sharing and Monotone Functions[A]. Advances in Cryptology-CRYPTO'88, volume 403 of Lecture Notes in Computer Science[C]. Springer, 1990. 27–35.