一种灵活实用的数字证书中敏感属性保密方案

廖俊国 凌乐真 朱 彬
(湖南科技大学计算机科学与工程学院 湘潭 411201)

摘 要 在开放式环境中,数字证书常用于身份认证和授权管理。数字证书通常包含一些敏感属性,因此,数字证书中敏感属性的保密研究受到广泛的关注。提出了一种灵活实用的数字证书中敏感属性保密方案,分析了该方案的安全性和性能。在该方案中,数字证书中不同的敏感属性分别用由同一个主密钥生成的不同子密钥进行加密,该方案具有可选择性揭露数字证书中敏感属性、密钥管理简单、时间开销少等特点。以X.509作为证书格式,实现了该数字证书中敏感属性的保密方案。

关键词 数字证书,敏感属性,保密,X.509
中图法分类号 TP309 **文献标识码** A

Flexible and Practical Scheme to Preserve Confidentiality of Sensitive Attributes in Digital Certificate

LIAO Jun-guo LING Le-zhen ZHU Bin
(School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan 411201, China)

Abstract In open environment, digital certificate is used in identity authentication and authorization management. Digital certificate often includes sensitive attributes, so the research on preserving confidentiality of sensitive attributes in digital certificate becomes concerned. This paper presented a flexible and practical scheme to preserve confidentiality of sensitive attributes in digital certificate, and analysed its security and performance. In the scheme, the different sensitive attributes in digital certificate are encrypted with different sub-keys generated from a main key. The scheme has some characteristics as follows: selectively disclosing sensitive attributes in digital certificate, simple key management, and low time cost. Based on X.509, the presented scheme was implemented.

Keywords Digital certificate, Sensitive attribute, Preserve confidentiality, X.509

1 引言

随着网络技术的发展及Internet的普及,基于网络的商务、政务及科学实验等活动逐渐成为一种主流应用模式。在开放式环境中,信任管理是常用的访问控制方法,资源访问的请求者通过提供所拥有的数字证书集合来证明是否具有对资源进行访问的权限。数字证书通常包含一些敏感属性,这些属性需要保密。因而,数字证书中敏感属性的保护成为信息安全领域研究的重点问题之一。目前,大部分已有的解决方案[1-10,12]把数字证书作为一个整体来使用,要么揭露数字证书中的所有敏感属性,要么不揭露数字证书中的任何敏感属性,不能有选择性地揭露数字证书中的部分或全部敏感属性,无法满足某些应用的安全需求,如图1所示。文献[11]提出了一种可选择性地揭露数字证书中敏感属性的保护方案。但是,该方案的时间开销较大,不能满足开放式环境下大规模应用系统的性能需求。针对上述问题,本文提出了一种简单实用而且灵活的保护数字证书中敏感属性的方案,该方案具有可选择性揭露数字证书中敏感属性、密钥管理简单和时间开销少等特点。

本文第2节提出了证书中敏感属性的保密方案;第3节和第4节分析了方案的安全性和性能;第5节基于本文提出的方案实现了一个数字证书中敏感属性保护系统,测试了该系统的性能;最后对全文进行总结。

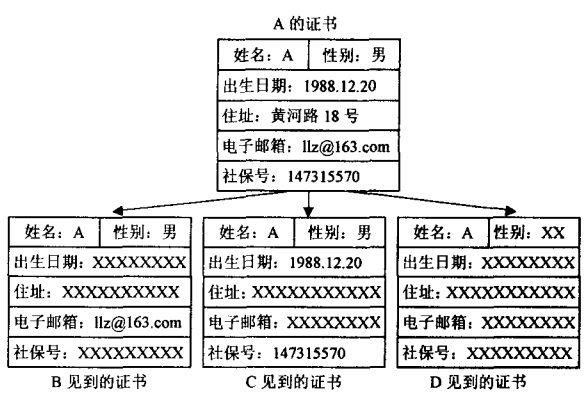

图1 可选择性地揭露证书中的敏感属性

2 证书中敏感属性的保密方案

为了便于形式化描述,用Adm和Issuer分别表示系统管理员和证书发布者;用Alice和Bob分别表示证书持有者和证书使用者;用AN和AV分别表示属性名称和属性值;用有

到稿日期:2010-01-20 返修日期:2010-03-28 本文受国家自然科学基金项目(90818004)资助。
廖俊国(1972-),男,博士,副教授,主要研究方向为信息安全研究,E-mail:liaojunguo@gmail.com。

序对$\langle AN,AV\rangle$表示属性；用$SE_K(m)$和$SD_K(m)$表示采用对称密码算法的加密函数和解密函数；用$PE_K(m)$和$PD_K(m)$表示采用公钥密码算法的加密函数和解密函数；用$H(m)$表示散列函数；用C表示证书；用(P_a,S_a)表示 *Alice* 的公私钥对，其中P_a为公钥，S_a为私钥；用"||"表示级联。

证书中敏感属性的保密方案分为三个阶段：第一阶段为准备阶段，Adm 确定并公布参数；第二阶段为证书生成阶段，Issuer 生成证书 C 并发送给 Alice；第三阶段为证书交换阶段，Alice 向 Bob 提交证书 C，并向 Bob 揭露证书 C 的部分或全部敏感属性。

2.1 准备阶段

在准备阶段，系统管理员 Adm 确定并公布以下参数：$H(m)$，$SE_K(m)$，$SD_K(m)$，$PE_K(m)$，$PD_K(m)$。一般情况下，这些参数公布后将不再发生变化，因而准备阶段的工作只需要做一次。

2.2 证书生成阶段

在证书生成阶段，证书发布者 Issuer 生成证书 C 并发送给证书持有者 Alice，主要包括以下步骤。

(1) Alice 向 Issuer 提交生成证书 C 所需要的信息。

(2) Issuer 随机生成主密钥 $MKey$。

(3) 如果证书 C 中有 n 个属性，分别记为$\langle AN_1,AV_1\rangle$，…，$\langle AN_n,AV_n\rangle$，其中有 j 个敏感属性，分别记为$\langle AN_{i_1},AV_{i_1}\rangle$，…，$\langle AN_{i_j},AV_{i_j}\rangle$。Issuer 由主密钥 MKey 计算子密钥：$H(MKey||AN_{i_1})$，…，$H(MKey||AN_{i_j})$，分别记为 K_1，…，K_j。

(4) 用 K_1，…，K_j 分别对 AV_{i_1}，…，AV_{i_j} 进行加密，即计算 $SE_{K_1}(AV_{i_1})$，…，$SE_{K_j}(AV_{i_j})$。然后生成证书 C。在证书 C 中，非敏感属性存储的是属性值的明文，即$\langle AN,AV\rangle$，敏感属性存储的是属性值的密文，即$\langle AN,E_K(AV)\rangle$。

(5) Issuer 向 Alice 发送证书 C。由于主密钥 $MKey$ 需要保密，为了防止 $MKey$ 被截取，Issuer 必须通过安全可信的信道把 $MKey$ 发送给 Alice。

2.3 证书交换阶段

在证书交换阶段，Alice 向 Bob 提交证书 C，并向 Bob 揭露证书 C 中的部分或全部敏感属性，主要包括以下步骤。

(1) Bob 向 Alice 提交公钥证书，Alice 验证公钥证书的有效性，并从公钥证书获得 Bob 的公钥 P_b。

(2) Alice 根据策略和 Bob 的权限确定证书 C 中哪些敏感属性可以向 Bob 公开，不妨假设 Alice 可以向 Bob 揭露证书 C 中的 $k(k\leqslant j)$ 个敏感属性，属性名称分别记为 AN_{l_1}，…，AN_{l_k}，对应的属性值的密文分别记为 CM_1，…，CM_k。Alice 计算子密钥 $H(MKey||AN_{l_1})$，…，$H(MKey||AN_{l_k})$，分别记为 K_1'，…，K_k'。Alice 选择一个临时对称密钥 $TKey$，并用此密钥对子密钥 K_1'，…，K_k' 进行加密，即计算 $SE_{TKey}(K_1',\cdots,K_k')$，再用 Bob 的公钥对临时对称密钥 $TKey$ 进行加密，即计算 $PE_{P_b}(TKey)$。

(3) Alice 把 $SE_{TKey}(K_1',\cdots,K_k')$，$PE_{P_b}(TKey)$，$AN_{l_1}$，…，$AN_{l_k}$ 和证书 C 发送给 Bob。

(4) Bob 用自己的私钥对 $PE_{P_b}(TKey)$ 进行解密，即计算 $PD_{S_b}(PE_{P_b}(TKey))$，获得临时对称密钥 $TKey$，然后用 TKey 对 $SE_{TKey}(K_1',\cdots,K_k')$ 进行解密，即计算 $DE_{TKey}(SE_{TKey}(K_1',\cdots,K_k'))$，获得子密钥 K_1'，…，K_k'，并用这些子密钥分别对属性 AN_{l_1}，…，AN_{l_k} 的属性值密文 CM_1，…，CM_k 进行解密，即计算 $SD_{K'_1}(CM_1)$，…，$SD_{K_k'}(CM_k)$。

3 方案的安全性分析

定义 1 在证书 C 中，Alice 可以揭露给 Bob 的敏感属性称为可揭露敏感属性；Alice 不能揭露给 Bob 的敏感属性称为非揭露敏感属性。

本文提出的证书中敏感属性保密方案的安全性包括以下三个方面：一是方案的可靠性，即 Bob 能否正确解密可揭露敏感属性；二是密钥交换的安全性，即窃听者 Jack 是否能够获取 Bob 用来解密敏感属性的密钥；三是非揭露敏感属性的安全性，即 Bob 是否能够获取非揭露敏感属性。

3.1 安全假设

本文提出的证书中敏感属性保密方案基于以下安全假设：①Bob 的私钥 S_b 和证书的主密钥 $MKey$ 是保密的；②公钥密码算法、对称密码算法和散列函数是安全的。

3.2 方案的可靠性

证书生成阶段 Issuer 由主密钥 $MKey$ 计算子密钥的公式与证书交换阶段 Alice 由主密钥 $MKey$ 计算子密钥的公式相同，他们计算的子密钥也相同。证书交换阶段的密钥交换采用公钥密码体制，Bob 能够安全地获得可揭露敏感属性的子密钥。由于证书中敏感属性的加密采用对称密码算法，因而 Bob 能够正确解密可揭露敏感属性。所以，本文提出的证书中敏感属性保密方案是可靠的。

3.3 密钥交换的安全性

证书交换阶段的密钥交换采用公钥密码体制。由安全假设可知，Bob 的私钥 S_b 是保密的，公钥密码算法是安全的，窃听者 Jack 若无法正确解密 $PE_{P_b}(TKey)$，就不可能获得临时对称密钥 $TKey$，那么就无法正确解密 $SE_{TKey}(K_1',\cdots,K_k')$，也就不可能获得子密钥 K_1'，…，K_k'。所以，密钥交换是安全的。

3.4 非揭露敏感属性的安全性

非揭露敏感属性的安全性是指：Bob 通过可揭露敏感属性的有关信息能否获得非揭露敏感属性的属性值，即 Bob 通过可揭露敏感属性的密钥计算出非揭露敏感属性的密钥是否可行。

假设任一非揭露敏感属性的属性名为 AN_t，对应的子密钥为 $K_t=H(MKey||AN_t)$。Bob 能够获得子密钥 K_1'，…，K_k'，其中，$K_1'=H(MKey||AN_{l_1})$，…，$K_k'=H(MKey||AN_{l_k})$。由安全假设可知散列函数是安全的，Bob 由子密钥 K_1'，…，K_k' 计算出主密钥 $MKey$ 是不可能的。因此，Bob 不可能根据公式 $H(MKey||AN_t)$ 计算出子密钥 K_t。由于散列函数计算结果具有随机性和不可预测性，要找到 K_t 与 K_1'，…，K_k' 之间的关系是不可能的。因此，Bob 无法由 K_1'，…，K_k' 推导出 K_t。综上所述，Bob 通过可揭露敏感属性的密钥计算出非揭露敏感属性的密钥是不可行的。

4 方案的性能分析

本文提出的证书中敏感属性保密方案的时间开销包括：在证书生成阶段，计算子密钥和加密敏感属性的时间；在证书交换阶段，加、解密临时对称密钥的时间，加、解密子密钥的时间，解密敏感属性的时间。计算子密钥采用散列函数，加、解密敏感属性和子密钥采用对称密码，加、解密临时对称密钥采用公钥密码。散列运算、对称加解密运算的时间开销比公钥

密码加解密运算的时间开销要少得多，几乎可以忽略不计。因此，本文提出的证书中敏感属性保密方案的时间开销主要是加、解密临时对称密钥的时间开销。由于临时对称密钥长度少且固定，因此加、解密临时对称密钥的时间开销较少。所以，本文提出的证书中敏感属性保密方案性能很好，实用性强。

5 方案的实现

基于本文提出的证书中敏感属性保密方案，设计并实现了一个证书中敏感属性保密系统。在该系统中，公钥密码算法采用 RSA，对称密码算法采用 DES，散列函数采用 MD5。该系统使用 Visual C++6.0 作为开发平台，系统的部分功能借助 OpenSSL 的库函数来完成，密钥交换采用 SSL 协议构建的安全信道来传送密钥。该系统的证书采用 X.509 标准，将 X.509 证书主题信息的“国家”、“省份”、“城市”、“组织机构”、“部门”、“通用名称”这 6 个属性作为用户的信息，“国家”为非敏感属性，其余 5 个属性为敏感属性，Issuer 在证书生成阶段生成的证书如图 2 所示，证书中敏感属性的属性值都是以密文的形式显示。在证书交换阶段，证书中部分或全部敏感属性可以有选择性地被揭露。当揭露证书中的“省份”和“通用名称”敏感属性时，证书的显示形式如图 3 所示；当揭露证书中的全部敏感属性时，证书的的显示形式如图 4 所示。

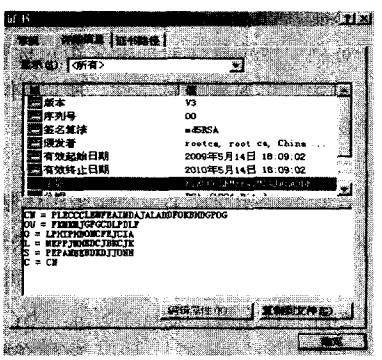

图 2 Issuer 生成的证书

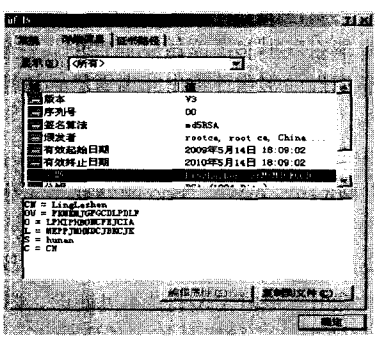

图 3 证书中部分敏感属性被揭露

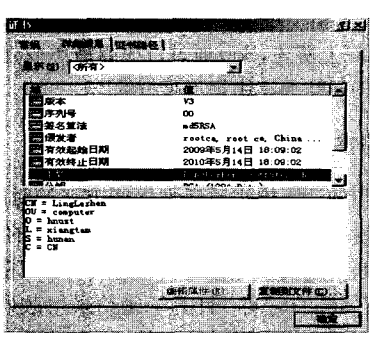

图 4 证书中全部敏感属性被揭露

配置为 2.00GHz 双核 Inter Core 2 E4400 CPU，2.00GB 内存的计算机实现本文提出的证书中敏感信息保密方案的时间开销如下：MD5 运算的时间为 0.0019 毫秒，RSA 运算的时间为 0.7203 毫秒，DES 运算的时间如表 1 所列。

表 1 DES 运算时间开销

输入长度(字节)	时间(毫秒)
8	0.0016
16	0.0016
32	0.0032
64	0.0047
128	0.0078
256	0.0188
512	0.0328
1024	0.0609
2048	0.1156
4096	0.2391

结束语 在开发式环境下，数字证书被广泛使用。由于证书中往往包含有证书持有者的敏感信息，因而如何保护证书中的敏感属性引起了大家的关注。本文提出了一种灵活实用的证书中敏感属性保密方案，该方案具有以下 3 个特点：(1) 灵活性好。可以选择性地揭露证书中的敏感属性。(2) 密钥管理简单。证书持有者只需保密一个主密钥 MKey 就能够得到多个不同的子密钥，并且子密钥与敏感属性的对应关系简单，不需要额外的信息。(3) 实用性强。从第 4 节的分析和第 5 节的实验结果可知，该方案所需的计算时间开销少。

下一步的工作是完善方案的实现，主要包括两个方面：一是使用 X.509 证书的扩展项来存储用户的属性；二是使用 SSL 协议进行密钥交换，这与本文提出的方案稍有不同，借助 OpenSSL 的库函数来编程实现密钥交换。

参 考 文 献

[1] Li Jiangtao, Li Ninghui, Winsborough W H. Automated Trust Negotiation Using Cryptographic Credentials [C]// Proceeding of the 12th conference on computer and communications security. Alexandria, Virginia, USA. ACM Press, November 2005: 46-57

[2] Yu Ting, Winslett M, Seamons K E. Supporting Structured Credentials and Sensitive Policies through Interoperable Strategies for Automated Trust Negotiation[J]. ACM Transactions on Information and System Security(TISSEC), 2003, 6(1): 1-42

[3] Li Ninghui, Du Wenliang, Boneh D. Oblivious Signature-Based Envelope [C]// Proceedings of the 22nd ACM Symposium on Principles of Distributed Computing (PODC 2003). ACM Press, July 2003: 182-189

[4] Winsborough W H, Li Ninghui. Protecting Sensitive Attributed in Automated Trust Negotiation [C]// Proceedings of the 1st ACM Workshop on Privacy in the Electronic Society. ACM Press, 2002: 41-51

[5] Holt J E, Bradshaw R W, Seamons K E, et al. Hidden Credentials [C]// Proceedings of the 2nd ACM Workshop on Privacy in the Electronic Society. Washington, DC. ACM Press, October 2003: 1-8

[6] Frikken K, Atallah M, Li Jiangtao. Hidden Access Control Policies with Hidden Credentials [C]// Proceedings of the 3rd ACM Workshop on Privacy in the Electronic Society. Washington, DC. ACM Press, October 2004: 27-28

(下转第 216 页)

非常重要。N次矩运算可全面地完成数据的各种统计分析并进而帮助我们形成对客观世界中对象性质的整体看法。

根据上面N次矩的定义，可以对N次矩运算进行定义。设对于包含空值的基于XML的概率数据库的一个实例T，n是T上的非根节点，用pS表示节点上表示概率的属性值，则T上的n的N次矩记作$\mu_{n,N}(T)$，定义如下：

$$\mu_{n,N}(T)=\{x(T)\mid(\exists y\text{是}n\text{的子女})(y(T)\downarrow\wedge x(T)=y(T))\wedge(\forall A\text{是}T\text{上除}n\text{以外的其它非根节点})(x(A)=m_{n,T,N}(y,A))\}$$

其中

$$m_{n,T,N}(y,A)=\begin{cases}\dfrac{\sum\limits_{\substack{y\in n\\ y(A)\downarrow\\ y(T)=x(T)}}(y(A))^N y(pS)}{\sum\limits_{\substack{y\in n\\ y(A)\downarrow\\ y(T)=x(T)}}y(pS)} & \text{当 } pS\text{ 不为 0 且 } A\text{ 是数值型}\\ \Omega & \text{其他}\end{cases}$$

关于N次矩运算有以下几点要说明：

(1)实际上这是一族运算，因为每给一个正整数N，就有一个运算。

(2)用N次矩运算可以定义其他一些运算，例如，标准差、失真度及突出度等。

(3)由定义可以看出，空值$*$在计算矩时不会被考虑，所以只有分布中显示给出值的部分才参与矩运算。

(4)N次矩计算对于非数值型节点在运算时会产生一种特殊的空值"Ω"。

例3　把该运算应用到例1，当使用1次矩运算后，得出的E部人数期望值为177，我方可以再通过使用标准差、失真度、突出度等参数，得出相应的结论，从而制定有针对性的作战计划。该运算同样可以用于科学研究和科学预测。

结束语　基于XML的概率数据库引入空值，使数据库对不确定信息和不完全信息的描述进行结合，可以更好地表示现实世界。该方法增加了对数据库操作的难度，虽然本文用了折中的方法解决了区间概率的运算问题，但是该方法在大多数情况下，还得具体情况具体分析，而且，该方法只适用于子节点概率值上限之和大于等于1的情况，而对小于1的情况无能为力；针对空值概率的两种解释，对于建立数学模型描述也是很不利的，需要在语义上加以解决，使其对这两种解释都适用。下一步要设计推广的代数运算，使问题可以在代数层面加以解决。

参考文献

[1] Zaniolo C. Database relations with null values [J]. Journal of Computer and System Sciences, 1984, 28(1): 142-166

[2] Klir G J, Folger T A. Fuzzy sets, uncertainty and information [M]. New Jersey: Pemtice-Hall, 1988

[3] Dey, Sarkar S. A Probabilistic Relational Model and Algebra [J]. ACM Transactions on Database Systems, 1996, 21(3): 339-369

[4] Nierman A, Jagadish H V. ProTDB: Probabilistic data in XML [C]// Proceeding of the 28th International Conference on Very Large Data Bases. Hong Kong: Morgan' Kaufmann Publishers, 2002: 646-657

[5] Hung E, Getoor L, Subrahmanian V S. PXML: a probabilistic semistructured data model and algebra[C]// Proceedings of the 19th International Conference on Data Engineering. Bangalore, India: IEEE Computer Society Press, 2003: 467-482

[6] Green T J, Tannen V. Models for incomplete and probabilistic information[J]. IEEE Date Engineering Bulletin, 2006, 29(1)

[7] 张群，王新军，吴欣. 一种扩展的基于XML的概率数据模型[J]. 山东大学学报：理学版，2007，42(9)

[8] Goldman S, Rivest R. A non-iterative maximum entropy algorithm[C]// Proceedings of the 2nd Annual Conference on Uncertainty in Artificial Intelligence (UAI'86). Elsevier Science Publishing Company, Inc., New York, NY, 1986: 133-148

[9] Dekhtyar A, Goldsmith J, Hawkes S. Semistructured probabilistic databases[C]// Proceedings of the Conference on Statistical and Scientific Database Management (SSDBM). Fairfax, VA, USA, 2001: 36-45

(上接第130页)

[7] Bradshaw R W, Holt J E, Seamons K E. Concealing Complex Policies with Hidden Credentials [C]// Proceedings of the 11th ACM Conference on Computer and Communications Security. Washington, DC. ACM Press, October 2004: 146-157

[8] Li Jiangtao, Li Ninghui. OACerts: Oblivious Attribute Certificates [C]// Proceedings of the 3rd Intenational Conference on Applied Cryptography and Network Security (ACNS 2005), Volume 3531 of Lecture Notes in Computer Science. New York, USA: Springer, 2005: 301-316

[9] Castelluccia C, Jarecki S, Tsudik G. Secret Handshakes from CA-oblivious Encryption [C]// Proceedings of the 10th International Conference on the Theory and Application of Cryptology and Information Security, Volume 3329 of Lecture Notes in Computer Science. Springer, 2004: 293-307

[10] Bertino E, Ferrrari E, Squicciarini A. Privacy-Preserving Trust Negotiation[R]. CERIAS-TR-2004-75. Center for Education and Research in Information Assurance and Security, Purdue University, 2005

[11] 廖俊国，洪帆，李俊，等. 在信任协商中保密证书的敏感属性[J]. 通信学报，2008，29(6)：20-25

[12] Ajayi O, Sinnott R, Stell A. Formalising Dynamic Trust Negotiations in Decentralised Collaborative e-Health Systems [C]// Proceedings of the 2nd International Conference on Availability, Reliability and Security. 2008: 1-8