第 36 卷 第 9 期 计 算 机 工 程 2010 年 5 月
Vol.36 No.9 Computer Engineering May 2010
·安全技术· 文章编号：1000—3428(2010)09—0142—03 文献标识码：A 中图分类号：TP309.2

支持属性选择性披露的 ATN 证书描述方案

肖淑婷[1]，吴国新[1,2]，孙啸寅[1]
(1. 东南大学计算机科学与工程学院，南京 210096；2. 东南大学计算机网络与信息集成教育部重点实验室，南京 210096)

摘 要： 为了在自动信任协商(ATN)中实现属性选择性披露，借鉴内容抽取签名的思想，以 W3C 的 XML 加密和签名推荐标准为技术支撑，提出一种支持属性选择性披露的 ATN 证书描述方案，使接收方在收到经过属性加密或移除处理的证书时仍能对其完整性和数字签名进行验证。与 SDSA 方案相比，该方案具有简单、灵活、计算量小等优点。

关键词： 自动信任协商；证书描述；属性选择性披露

Credential Description Scheme for Automated Trust Negotiation Supporting Selective Attributes Disclosure

XIAO Shu-ting[1], WU Guo-xin[1,2], SUN Xiao-yin[1]
(1. School of Computer Science and Engineering, Southeast University, Nanjing 210096;
2. Key Laboratory of Computer Network and Information Integration of Ministry of Education, Southeast University, Nanjing 210096)

【Abstract】 In order to realize selective attributes disclosure in Automated Trust Negotiation(ATN), by using the thoughts of content extraction signature and W3C XML encryption and signature standards as technical basis, a credential description scheme is designed to support fine-grained property protection function, which makes the receiver be able to check the integrity and signature of the credentials after encryption or removal. Compared with Selectively Disclosing Sensitive Attributes(SDSA) scheme, the new scheme is simpler, more flexible and has less calculation.

【Key words】 Automated Trust Negotiation(ATN); credential description; selective attributes disclosure

1 概述

传统的基于身份的认证授权方式假定通信双方都已熟悉或者信任对方，在分布式、异构和动态的开放系统中，往往需要在 2 个陌生的实体间建立信任关系，这使传统的基于特定域身份标识的认证授权方法不再可行。针对此问题，研究者提出基于属性的访问控制(ABAC)。自动信任协商[1]是 ABAC 机制的一种实现，通过访问政策指导和规范属性证书在交互实体之间的交换，从而在保护敏感信息的前提下在 2 个陌生实体间建立信任关系。在自动信任协商模型中，属性证书是经颁发者用其私钥签名的对证书拥有者的一个或多个属性的描述断言，对证书的信任基于对证书颁发者的信任。

颁发者在为实体颁发属性证书时，通常将其能证实的所有或者某一类别的多个属性都封装在一个属性证书中，然后对证书进行整体签名。目前的自动信任协商(Automated Trust Negotiation, ATN)证书描述方案只支持在证书这一粒度上实行访问控制，即要么向对方显示证书中的所有内容，要么全部不显示。而在实际应用中，有时只需要将证书中的一部分属性暴露给对方，同时又要保证对方能验证这部分证书内容的完整性和签名。因此，设计一种支持属性选择性披露的证书描述方案是十分必要的。

文献[2]提出一种保护证书中敏感属性的方案 SDSA (Selectively Disclosing Sensitive Attributes)，其设计基于离散对数非对称密码体制，密钥管理简单，但需要一个同时被证书颁发者和申请者信任的管理员生成并维护系统参数，接收者在接收和解密证书前也需要获得对应的系统参数。此外，在颁发者生成证书和接收者解密敏感属性值时均需要进行大量的非对称加解密计算，拥有者在每次将证书发送给对方之前也需要进行一定量的计算，因此，SDSA 在系统实用性方面有较大的缺陷。

本文提出一个支持属性选择性披露、基于 XML 的自动信任协商证书描述方案，证书拥有者可以采用加密属性元素或从证书中将其移除的方法来保护敏感属性，并通过一种灵活设计的签名生成方法，使接收方仍然能够验证证书中对其可见的属性内容的完整性和数字签名。

2 支持属性选择性披露的ATN证书描述方案

本文的方案吸收了内容抽取签名[3]的思想，将证书中的属性元素看成子文档，利用 W3C XML 签名标准[4]中推荐的签名处理方法，加密[5]或移除证书中要保护的敏感属性，但接收方仍能验证对其“可见”的属性内容的完整性和有效性，从而在多级粒度上对证书中的敏感属性进行保护。如图 1 所示，对于一个证书，除了有保护整个证书的政策 1 外，其中包含的属性也可以单独定义披露政策，同时约定在属性披露政策不满足时对相应属性的保护方式(加密 E 或移除 R)。证书签名根据内容抽取签名思想，用 W3C 推荐的 XML 签名格式封装签名元素。由于图 1 中 3 个协商方分别只满足政策 1、政策 1&2 和政策 1&3，因此在请求同一个证书时，证书拥有者发给它们的证书包含的内容不一样(E_k(属性)表示对属性加

基金项目： 国家“863”计划基金资助项目“分布式多信任域间信任管理技术研究与开发”(2007AA01Z422)

作者简介： 肖淑婷(1986－)，女，硕士研究生，主研方向：信息安全，自动信任协商；吴国新，教授、博士生导师；孙啸寅，硕士研究生

收稿日期： 2009-11-27 **E-mail：** xstsky@163.com

密后的密文)。

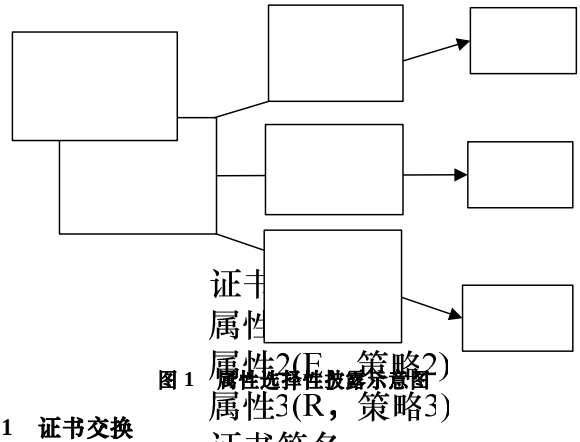

图 1　属性选择性披露示意图

2.1　证书交换

在证书交换过程中，索取证书的一方称为请求方，证书拥有者为被请求方。证书交换过程如图 2 所示，被请求方(Requestee)首先判断请求方(Requester)是否满足对应证书的整体披露政策(a)，如果不满足，拒绝此请求；若满足，则逐一检验证书中为各属性单独定义的披露政策，根据保护模式标识，对属性进行加密或移除(b)，然后将处理过的证书发送给请求方(第 4 步)。在随后的协商过程中，请求方通过发送满足特定属性披露政策的证书到被请求方(第 5 步)获得特定属性的内容。被请求方验证属性的披露政策是否满足(c)，若满足，将对应的解密密钥(加密模式)或属性元素内容(移除模式)发送给对方(第 6 步)。

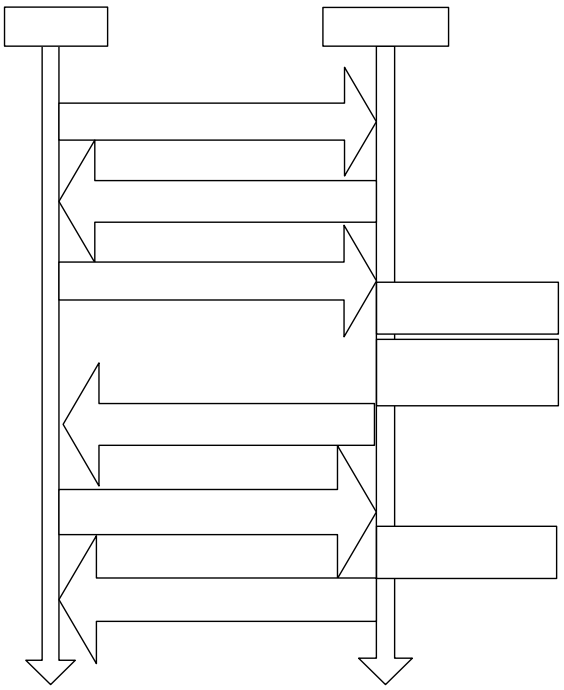

图 2　证书交换流程

在证书交换过程中，双方实体执行自动信任协商的 SA (Security Agent)要保存当前活动的协商会话的历史交互信息，包括发送到各协商方的证书中加密了哪些属性、使用的密钥和移除了哪些属性。这样，对已交换过的证书，在其后的交互过程中只需要增量地发送或接收证书内容。

2.2　证书结构

本文的证书结构中使用的符号和记法如下：属性用大写字母 A 表示，属性 A 的值用 A.value 表示；属性证书形如：Cred{A1, A2,…}，{}内为此证书包含的属性；属性 A 的元素内容的摘要和签名值分别记为 H(A)和 Sig(A)；用密钥 k 对属性 A 的元素内容对称加密后得到密文 c 用 Ek(A)表示，对 c 解密记为 Dk(c)；用“URI”表示对内容的引用。

实体在向证书颁发机构(CA)请求颁发属性证书时，需要说明哪些属性使用证书整体政策，哪些属性需要更细粒度的保护和保护模式(加密 E 或者移除 R)及相应披露政策。CA 生成一个证书要经过封装属性信息元素(CredInfo)和生成签名(Signature)2 个操作。在将属性信息封装到证书文件时，CA 对申请者指明在属性粒度上进行保护的属性元素增加保护模式(Mode)和政策(Policy)2 个属性。生成证书签名的步骤为：(1)进行规定的 XML 转换操作后，对各元素计算摘要值，生成 XML 签名标准的<Reference>元素。(2)将标准化和签名方法说明及<Reference>元素封装成<SignedInfo>元素。(3)对<SignedInfo>元素执行标准化操作，用签名私钥对其加密即可得到证书的签名。

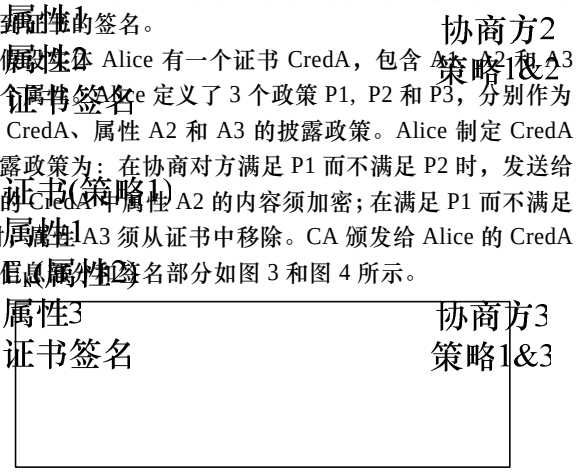

图 3　证书 CredA 属性信息部分

例如，在 Alice 有一个证书 CredA，包含 A1、A2 和 A3 共 3 个属性，Alice 定义了 3 个政策 P1, P2 和 P3，分别作为证书 CredA、属性 A2 和 A3 的披露政策。Alice 制定 CredA 的披露政策为：在协商对方满足 P1 而不满足 P2 时，发送给对方的 CredA 中属性 A2 的内容须加密；在满足 P1 而不满足 P3 时，属性 A3 须从证书中移除。CA 颁发给 Alice 的 CredA 属性信息部分签名部分如图 3 和图 4 所示。

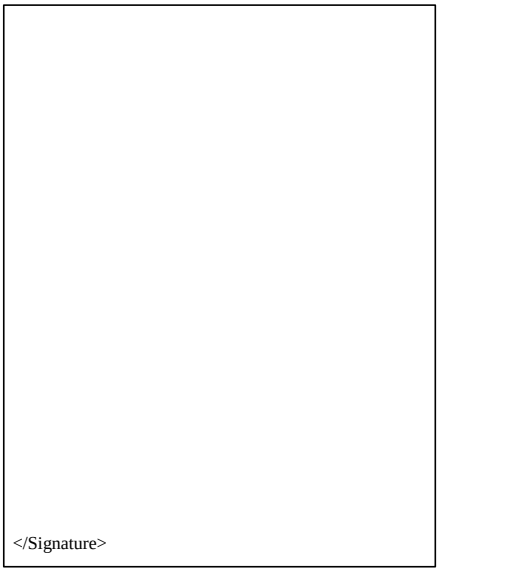

图 4　证书 CredA 签名部分

2.3　属性保护

在信任协商过程中，在对方满足证书披露政策但不满足特定属性的披露政策时，本方案使用加密和移除 2 种方法使相应的属性对对方不可见，前者适合敏感度不太高且在进一步的协商之后往往需要向对方披露的属性；后者适用于敏感度很高，需要防已知密文攻击或者该属性的拥有与否也是敏

感信息的属性。

2.3.1 加密模式

加密模式使用对称加密算法加密属性元素使其对对方不可见，其使用 W3C XML 加密标准推荐的封装方法：当实体判定从对方收到的证书不能解锁特定属性元素的披露政策时，用一个扩展自 EncryptedDataType 类型的元素(本文记为 ProtectedData)将其替换，其内容是对应属性的密文内容。它比 EncryptedData 多一个 policy 属性，类型为“xsi:anyURI”，指向此属性的披露政策，作用是引导对方进行进一步的协商，以得到此元素的明文。在随后的协商过程中，当此属性的披露政策满足时，证书拥有者将对应的解密密钥发送给对方。

SA 在启动时创建一个(属性标识，密钥)映射区来保存当前活动的协商会话中用于加密属性的密钥。当协商对方不满足属性的披露政策时，SA 随机生成一个二进制串作为此属性的加密密钥，然后将属性标识和该密钥添加到 SA 的(属性标识，密钥)映射区，属性标识的格式为“协商对方 ID#证书 ID#属性 ID”，密钥的生存期是一个协商会话。

2.3.2 移除模式

移除模式指在对方未满足特定属性的披露政策时，证书拥有者将相应属性元素从证书中移除，从而使该属性对对方不可见。移除模式有简约和标准 2 种模式：简约模式只将对应元素从证书中删除；标准模式在将对应元素从证书中删除后，还附加一个内容为空的<RemovedData>元素，该元素有 2 个属性——ID 和 Policy，值分别是原属性名和属性披露政策的 URI，以使对方感知该属性的存在，并引导对方进行进一步的协商。

3 证书签名验证

由上文介绍的签名生成过程可知，证书签名中的<SignedInfo>元素通过一组<Reference>元素封装了所有属性元素的摘要值，这样，即使证书拥有者对部分属性进行了加密和移除处理，这部分内容的摘要值仍包含在证书的签名中，而证书的整体签名是始终包含在发送给对方的证书中的，因此，接收方仍能验证证书的整体签名，但不能也不需要验证被加密或移除的这部分内容的完整性。

证书签名验证的过程如下：(1)进行引用验证。计算证书中明文属性元素的摘要值，与对应<Reference>元素中的摘要值进行比较，若相等，则完整性验证通过。(2)验证签名。用 CA 的公钥解密<SignatureValue>中的内容，检查其与<SignedInfo>元素标准化后的内容是否相同，若相同，则签名验证通过。如果上述 2 步验证均通过，则认为此证书是有效的。如果在协商后续过程中收到了证书的增量属性，计算其摘要值，与之前收到的证书中对应<Reference>元素中的摘要值进行比较以验证完整性。

4 应用实例

假设 Alice 向颁发者 CA 申请证书，CA 颁发给 Alice 的证书 CredA 由属性信息(图 3)和证书签名(图 4)两部分内容组成。Bob 希望与 Alice 建立信任关系，记 Alice 和 Bob 的安全代理分别为 SA(A)和 SA(B)。当 SA(B)向 SA(A)请求 CredA 时，SA(A)将根据已从 SA(B)处获取的信息，按照以下规则决定如何披露证书 CredA(签名元素 Signature 的内容如图 4 所示，在图 5 中用省略号代替)：

(1)若 P1 不满足，不发送 CredA 的任何内容。

(2)若 P1 和 P2 满足，P3 不满足，SA(A)将属性 A3 从证书 CredA 移除(简约模式如图 5(a)所示，标准模式如图 5(b)所示)，SA(A)将已移除 A3 的 CredA'发给 SA(B)，从而保护 A3。如果在后续的协商过程中，当 SA(A)从 SA(B)收到更多的证书，使 P3 也满足，SA(A)将属性 A3 的内容发给 SA(B)。

(3)若 P1 和 P3 满足，P2 不满足，SA(A)临时生成一个密钥，并用其对属性 A2 加密，如图 5(c)所示，将密文封装到<ProtectedData>元素，替换 CredA 中的属性 A2，得到 CredA″，SA(A)将 CredA″发给 SA(B)，这样就通过加密的方式保护了属性 A2。当 SA(A)从 SA(B)收到更多证书使得 P2 满足时，SA(A)将属性 A2 的解密密钥发给 SA(B)。

(4)若 P1 满足，P2 和 P3 都不满足，SA(A)加密属性 A2，移除属性 A3，这种情况是(2)和(3)的混合，SA(A)的处理方法可根据前面的描述类推，在此不再赘述。

(a)移除模式(简约)

(b)移除模式(标准)

(c)加密模式

图 5 满足不同政策时披露的 CredA 证书

5 结束语

本文的证书描述方案利用 W3C XML 安全标准，以一种简单、灵活的方式使证书拥有者可以在多级粒度上对证书内容进行访问控制。如果考虑证书文件大小这一因素，可以将属性分组，以属性组为保护单位。与 SDSA 相比，本文提出的方案具有简单、灵活、计算量小的优点。

参考文献

[1] Winsborough W H, Seamons K E, Jones V E. Automated Trust Negotiation[C]//Proceedings of DARPA Information Survivability Conference and Exposition. [S. l.]: IEEE Press, 2000: 88-102.

[2] 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.

[3] 龚 俭, 吴 桦, 杨 望. 计算机网络安全导论[M]. 南京: 东南大学出版社, 2007.

[4] Bartel M, Boyer J, Fox B, et al. XML Signature Syntax and Processing(2nd Edition)[EB/OL]. [2008-06-10]. http://www.w3.org/TR/2008/REC-xmldsig-core-20080610/.

[5] Imamura T, Dillaway B, Simon E. XML Encryption Syntax and Processing[EB/OL]. (2002-12-10). http://www.w3.org/TR/xmlenc-core/.

编辑 张 帆