doi:10.3772/j.issn.1002-0470.2022.09.005

一种基于非对称加密的自动信任协商模型①

田夏利② 熊 莹

(武汉华夏理工学院信息工程学院 武汉 430223)

摘 要 自动信任协商(ATN)是通过交换数字证书和访问控制策略在陌生人之间建立信任关系的一种重要手段。在协商过程中,可能存在协商模式过于复杂而无法完成协商、用户证书里的敏感信息泄露、因加密算法安全强度不足而遭受攻击等问题。针对这些不足,本文提出了一种基于非对称加密的自动信任协商模型,该模型采用灵活的证书格式、分步骤的证书交换等手段来满足访问控制策略的要求,采用非对称加密技术对传输消息进行加密,防止信息泄漏。

关键词 自动信任协商(ATN);数字证书;非对称加密;信息泄露;协商模型

0 引 言

访问控制策略在信息安全、网络安全等方面,扮演着重要角色,保护资源不被非授权访问。相比传统的访问控制策略,自动信任协商(automatic trust negotiation, ATN)[1-3]提供了一种全新的访问模式。用户只要拥有合法的数字证书或数字凭证[4-5],借用自动信任协商的模式,即可实现陌生人对不同访问控制策略[6-8]安全系统的访问。

相比传统的基于身份的访问控制方案,自动信任协商存在至少3个方面的优点:首先,陌生人之间的信任关系,是建立在协商双方的信息(或证书,或凭证,或断言,或license等)上,且信息的交互并不是一次性全部披露,而是按照最小化原则,有数字证书生成数字凭证按需提供;其次,协商双方均可自行定义访问控制策略,用以控制他人访问敏感区域资源;协商方法中,均不用涉及可信赖的第三方。

尽管如此,自动信息协商在实际应用中仍存在不足。由于数字证书可能包含敏感信息,不加限制地披露会泄露有价值的信息或危及个人隐私。然而,为了防止信息泄漏,协商协议的设计[9-11]往往会非常复杂,请求者很难获得访问权限,甚至难以完成协商过程。此外,如果加密算法的安全强度较低,则在公共信道上传输的消息容易受到攻击。

为了解决这一问题,本文提出了一种基于非对称加密算法自动信任模型,该模型提供读取特定属性的函数值,使用灵活的数字凭据格式来生成资格证书,可有效避免释放全部内容给协商另一方。同时,该模型采用非对称加密解密算法[12-13]传输消息,可大幅降低非安全通道带来的安全隐患。此外,该模型还提供了一个高效的协商协议,可以检查用户是否是证书的持有者。该协商协议仅需一轮的消息交换,有效地提高了谈判效率。

1 基于非对称加密算法的自动信任协商模型

1.1 基本定义

作为一种访问控制机制,ATN提供了规范数字交换的固定格式凭据和访问控制策略[14-15]。本文提出的基于非对称加密算法的自动信任协商模型中,相关概念定义如下。

① 湖北省科技厅科学技术研究与开发资金(CXYH2019000962)资助项目。

② 男,1973年生,硕士,副教授;研究方向:计算机网络,网络安全,计算机通信;联系人,E-mail:27797814@qq.com。

(收稿日期:2022-02-18)

(1) Cred:凭证集。Cred = $\{c_1, c_2, \cdots, c_n\}$, c_i ($1 \leqslant i \leqslant n$) 是某一数字凭证。在本文的自动信任协商模型中,数字凭证是一种临时证书,其内容来自用户的身份证书。

(2) Policy:访问控制策略集。Policy = $\{p_1, p_2, \cdots, p_n\}$, p_i($1 \leqslant i \leqslant n$) 是一个元策略。在本文的自动信任协商模型中,元策略为受保护资源的加密密钥,其解密密钥为相应的数字凭证。

(3)P:纯文本空间。尚未加密的资源或发送的消息均属于纯文本空间范畴。如果数字凭证满足访问控制策略的要求,则被加密的资源可还原为明文。

(4)C:密文空间。如果明文被加密,则变成密文。在本模型中,凡是被加密后的信息,都属于密文空间,包括加密后的资源等。

在自动信任协商中,协商策略决定了协商双方如何进行协商,而协商协议则决定着协商双方的具体步骤,指出了协商是否继续进行还是已然结束。

定义 1 协商策略 协商策略规定协商双方如何释放访问控制策略与数字凭证。在本文提出的基于非对称加密算法的自动信任协商模型中,如果数字凭证解密为相应的明文,则表示该数字凭证已披露。访问控制策略用于加密被保护的资源,鉴于任一资源访问者都可以获取到资源的访问控制策略,因此,访问控制策略中不应该包含敏感信息。同时,访问控制策略的暴露,应该是按需进行和循序渐进的。如果资源密文被解密了,则资源为已暴露。

定义 2 协商协议 协商协议指定在协商过程中协商双方会采取的行动,即协商的过程。在本文提出的基于非对称加密算法的自动信任协商模型中,协商过程包括如下步骤:(1)协商双方相互身份认证;(2)交换身份 ID;(3)发送访问请求;(4)获取加密的资源。

1.2 算法与函数

本文的自动信任协商模型,配备了一些算法或函数,用以完成信任协商的基本操作,相关算法或函数描述如下。

(1)CA _ Build( ):创建 CA 中心,为数字证书或数字凭证的持有者发布公钥。产生公钥私钥对的方法很多,通常,使用 K_{sec} 作为证书的私钥,依次产生相应的公钥。公钥的生成过程为:1)随机选择一个素数 p;2)做乘积即可,公钥 $K_{pub} = p \cdot K_{sec}$。这样,公钥 K_{pub} 对外发布,私钥 K_{sec} 用于签发数字证书或数字凭证[16-18]。

(2)Cred _ Issue ($holder$, $recipient$, $attribute$):生成数字凭证。其中,holder 是数字证书持有者;recipient 是数字凭证的接收者;attribute 是当前数字凭证的属性,该属性来自于用户的数字证书,可以使用函数 Get _ Attribute( ) 获取相应的属性。

(3)Encrypt (k, msg):使用密钥 k 对消息 msg 进行加密。Encrypt( ) 是非对称加密函数,使用密钥 k_{en} 加密后的密文,可以使用解密函数和密钥 k_{de} 进行解密,加密密钥与解密密钥满足 $k_{en} = k_{de}^{-1}$。

(4)Decrypt (k, msg):使用密钥对消息 msg 进行解密。当加密密钥与解密密钥满足 $k_{en} = k_{de}^{-1}$ 时,msg = Decrypt (k_{de}, Encrypt (k_{en}, msg))。加密密钥与解密密钥,对应为公钥和私钥。

(5)Get _ Attribute ($cert$, $attribute\_item$):根据属性项 attribute _ item 从数字证书 cert 中获取相应的属性值,比如 Tom 的证书 $cert_{Tom}$ 中,其年龄为 20 岁,则 Get _ Attribute ($cert_{Tom}$, age) =20。

(6)CR = Msg_E (R, P):使用策略 P 对资源 R 进行加密,加密后的资源可对外披露。对方只有拥有满足条件的数字凭证,借用解密函数方可查看资源信息 R。如果 $P = p_1 \wedge p_2$,则 CR = $Msg_E(R, P)$ = $Msg_E(Msg_E(R, p_1), p_2)$。如果 $P = p_1 \vee p_2$,则 CR = Msg_E (R, P) = {CR = Msg_E (R, p_1), CR = Msg_E (R, p_2)}。

(7)R = Msg_D(CR, $cred$):使用数字凭证 cred 对加密后的资源密文 CR 进行解密,解密成功后,即可获得原始资源信息 R。

1.3 灵活的数字凭证

本文提出了一种灵活的数字凭证,以满足不同的应用需求。该数字凭证格式如下:

($Credential\ holder$): ($Credential\ recipient$): ($attribute$): ($life\ time$)

数字凭证由函数 Cred _ Issue( ) 生成,其中,Credential holder 是数字凭证的持有者;Credential recipient 是数字凭证的接受者;attribute 是该数字凭证主

要存储的信息,从数字证书 cert 中获取;life time 是数字凭证的生命有效期。值得说明的是,数字凭证一般只用于信任协商过程的使用,其生命周期很短,从几分钟到几天不等,如果没有特别说明,数字凭证的默认周期为 24 h。Credential holder 与 Credential recipient 互为信任协商的双方。

例如,数字凭证(Tom):(Mary):(*product manager*):(May-04-2021, May-05-2021),其含义是:Tom 发送给 Mary 的数字凭证,承载的信息是,Tom 是一名产品经理,凭证的有效期是从 2021 年 5 月 4 日至 2021 年 5 月 5 日。

1.4　协商协议与协商过程

在本文提出的基于非对称加密算法的自动信任协商模型中,协商协议包括 3 个阶段(整个过程如图 1 所示)。

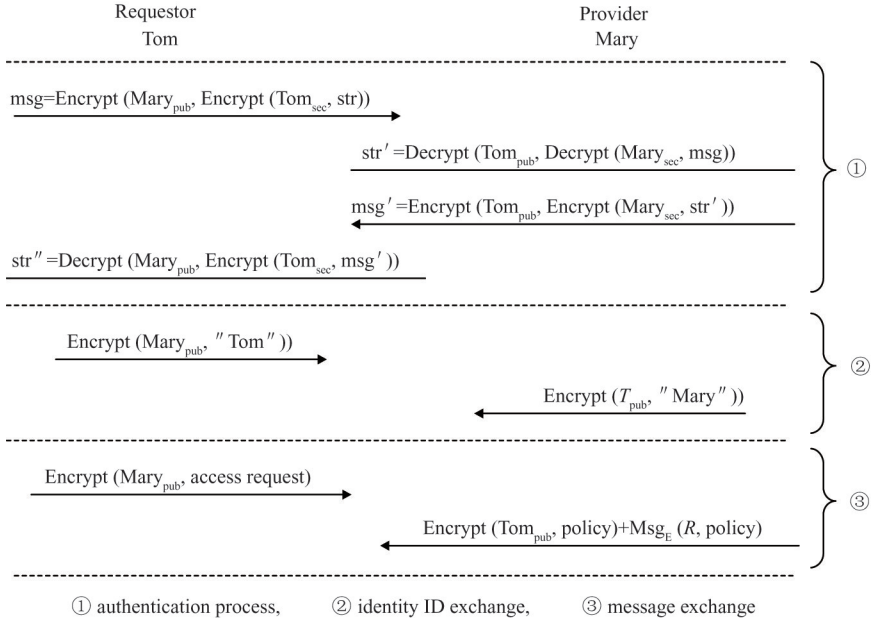

图 1　信任协商过程示意图

阶段 1:协商双方进行身份认证,认证过程如图 2所示,身份认证的过程是验证 p_0、p_1 与 p_2 是否相同的过程。假若 A、B 为协商双方,A 与 B 的认证过程,其形式化描述如下:

p_1 = Decrypt (A_{pub}, Decrypt (B_{sec}, c_1)) = Decrypt (A_{pub}, Decrypt (B_{sec}, Encrypt (B_{pub}, Encrypt (A_{sec}, p_0)))) = Decrypt(A_{pub}, Encrypt(A_{sec}, p_0)) = p_0

p_2 = Decrypt (B_{pub}, Decrypt (A_{sec}, c_4)) = Decrypt (B_{pub}, Decrypt (A_{sec}, Encrypt (A_{pub}, Encrypt (B_{sec}, p_1)))) = Decrypt(B_{pub}, Encrypt(B_{sec}, p_1)) = p_1

阶段 2:协商双方交换身份 ID,用以生成数字凭证,确保交互信息不发送给无关联的第三方。即使数字凭证被攻击者截取了,攻击者也很难获取数字凭证里的内容;若超过生命周期,数字凭证自动失效。

阶段 3:资源访问者与资源拥有者交换访问请求与加密后的资源密文。

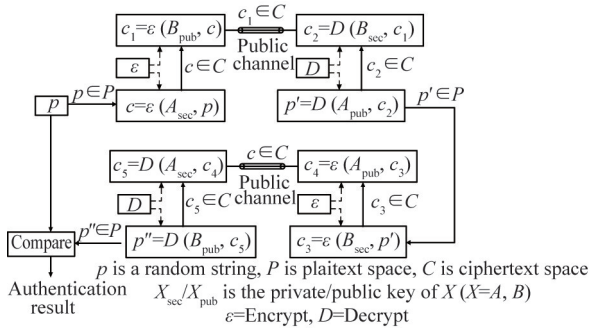

图 2　协商协议中的双边身份认证

2　基于非对称加密算法自动信任协商的应用实例

2.1　应用场景描述

某企业可向在校大学生提供助学贷款服务。在

校大学生的成绩为优良(即学生的主修课程每门课的分数均超过 80 分),即可向该企业申请。假设 Tom 为一名优秀的在校大学生,他的主修课程分数均在 80 分以上,他想申请该助学贷款。LILY 为该企业的产品经理,负责在校大学生的助学贷款业务,为优秀学生提供助学服务。

2.2 策略描述与数字凭证

基于上述场景描述,该助学贷款服务的访问控制策略可描述为

Policy $= p_1 \wedge p_2$, $p_1 = \{c_1 : x.\ role = college\ student\}$, $p_2 = \{c_2 : x.\ estimation = excellent\}$,其中,$x$ 为一变量,表示在校大学生。

Tom 为一名在校大学生,他拥有学校颁发的证书(学生证),而且,他的各门功课都非常优秀,每门主修课程的分数都在 85 分以上,超过了 80 分。在获取该企业的助学金贷款服务策略后,Tom 基于自己的学生证证书,生成了相应的数字凭证:

c_1 = (Tom):(LILY):(*collegestudent*):(March-01-2021, March-02- 2021);

c_2 = (Tom):(LILY):(*excellent*):(March-01-2021, March-02-2021)。

2.3 协商过程描述

在该应用示例中,整个协商过程如图 3 所示,具体的交互内容如下。

(1)申请人 Tom 和服务提供方 LILY 同时使用函数 CA _ Build 生成私钥 Tom_{sec} 和 $LILY_{sec}$,以及发布公钥 Tom_{pub} 和 $LILY_{pub}$。

(2)Tom 随机选择一个字符串 str,先后使用自己的私钥和 LILY 的公钥进行加密,并将加密后的密文 str 发送给 LILY。LILY 先后使用自己的私钥和 Tom 的公钥对密文 msg 进行解密,得到字符串 str',然后 LILY 先后使用自己的私钥和 Tom 的公钥对字符串 str' 进行加密,得到密文 msg',并将其反馈给 Tom。Tom 先使用自己的私钥和 LILY 的公钥对密文 msg' 进行解密,得到字符串 str''。如果 str = = str'',则双方身份认证成功,进入下一环节。否则,信任协商结束,需重新发起。

(3)Tom 使用 LILY 的公钥对自己的身份 ID 进行加密,发送给 LILY。

(4)LILY 解密 Tom 的身份 ID 后,使用 Tom 的公钥加密自己的身份 ID,发送给 Tom。

(5)Tom 使用 LILY 的公钥加密访问请求,发送给 LILY。

(6)LILY 解密 Tom 的访问请求后,使用 Tom 的公钥加密访问控制策略 Policy,并使用 Policy 对资源 *R* 进行加密,将两条密文一起发送给 Tom。后面,Tom 使用自己的私钥,先解密出访问控制策略 Policy,再使用数字凭证获取 Policy 的内容,进而解密出资源 *R* 的具体内容。

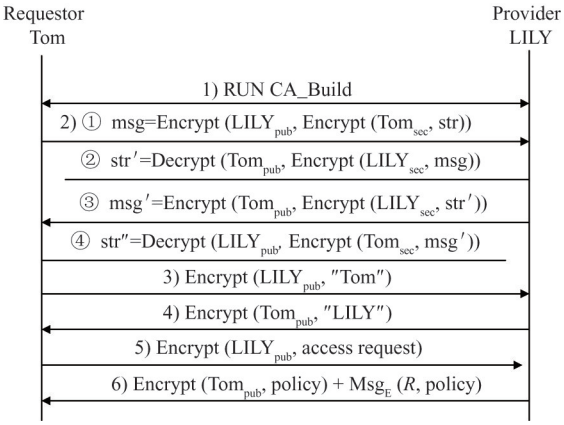

图 3 应用示例中的信任协商过程示意图

3 结 论

本文提出了一种基于非对称加密的自动信任协商模型,在该模型中,非对称加密算法是灵活的,任意选择一种算法(比如 RSA 算法等)即可产生一种协商模式。在模型中,数字凭证格式灵活,可满足各类协商模式的需求,具有很好的可复制、可推广功效。同时,在该模型中,身份认证过程具有高强度、防截取、防篡改等作用,可推广到其他模型中使用。今后将主要从两个方面开展工作。一方面,对当前的自动信任协商模型进行进一步的优化与完善,选择一定的场景或项目进行试点或应用落地;另一方面,沿着当前思路,开发更多高效的自动信任协商模型,研发相关的功能与性能指标对自动信任协商模型进行考评,通过指标的优化来达到优化信任协商模型的目的。

参考文献

[1] 王静宇,魏立香. 基于属性敏感度度量的 ATN 模型[J]. 内蒙古科技大学学报,2018,37(3):270-277

[2] 王静宇,魏立香. 云环境下一种基于资源分离的 ATN 模型[J]. 计算机应用研究,2017,34(11):3437-3440,3445

[3] 朱朝阳,丁箐,叶勇,等. 复杂云环境下基于推荐的信任协商框架设计[J]. 计算机应用与软件,2017,34(6):1-6,61

[4] 潘以桢. 基于数字水印的银行防伪凭证管理系统[J]. 金融电子化,2018,11(11):84-86

[5] 郝胜亮. 数字债权确权凭证在供应链金融中的应用[J]. 冶金财会,2020,39(8):19-23

[6] 潘瑞杰,王高才,黄珩逸. 基于属性访问控制策略管理方法[J]. 计算机工程与设计,2022,43(3):601-607

[7] 刘晶,朱炳旭,梁佳杭,等. 基于主侧链合作的区块链访问控制策略[J]. 计算机工程,2022,48(3):10-16,22

[8] 刘敖迪,杜学绘,王娜,等. 基于访问控制日志的访问控制策略生成方法[J]. 电子与信息学报,2022,44(1):324-331

[9] YANG M, ZHANG S B,ZHAO Y,et al. Dynamic negotiation of user behaviour via blockchain technology in federated system[J]. *International Journal of Computational Science and Engineering*, 2020,22(1):74-83

[10] CHAKRAVARTULA R R N,LAKSHMI V N. Trust negotiation among IoT-based objects in critical healthcare environment[J]. *International Journal of Recent Technology and Engineering* (*IJRTE*), 2020, 8(5):2756-2760

[11] KOLAR M,FERNANDEZ-GAGO C,LOPEZ J. A model specification for the design of trust negotiations[J]. *Computers and Security*, 2019,84:288-300

[12] 孙士锋. 抗密钥泄漏/篡改攻击的非对称加密算法研究[D]. 上海:上海交通大学计算机系, 2019

[13] SEPAHI R,STEINFELD R,PIEPRZYK J. Lattice-based completely non-malleable public-key encryption in the standard model[J]. *Designs, Codes and Cryptography*, 2014,71(2): 293-313

[14] 鲜开军,丁新虎,朱城超,等. 基于遗传算法的神经网络等价模型构建[J]. 高技术通讯,2021,31(11):1136-1144

[15] ADEL A A. Lightweight digital certificate management and efficacious symmetric cryptographic mechanism over industrial Internet of things[J]. *Sensors*, 2021,21(8):2810-2810

[16] 徐鹏鹏,方振宇. 基于解释结构模型的建设领域数字证书与电子签章推广制约因素研究[J]. 项目管理技术,2021,19(4):83-88

[17] DUNKELMAN O,KELLER N,SHAMIR A. A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3G telephony[J]. *Journal of Cryptology*, 2014(27):824-849

[18] 卢新元,陈华军,许超,等. 基于授权机制的抗扫描旁路攻击方法研究[J]. 高技术通讯,2020,30(9):875-883

An automatic trust negotiation model based on asymmetric encryption

TIAN Xiali, XIONG Ying

(School of Information Engineering, Wuhan Huaxia University of Technology, Wuhan 430223)

Abstract

Automatic trust negotiation is an important means of establishing trust relationships between strangers through the exchange of digital certificates and access control policies. In the negotiation process, there may be some problems, such as too complicated negotiation mode to complete the negotiation, disclosure of sensitive information in the user certificate, and attack due to insufficient security strength of encryption algorithm. In view of these deficiencies, this paper proposes an automatic trust negotiation model based on asymmetric encryption. The model adopts flexible certificate format, step-by-step certificate exchange and other means to meet the requirements of access control policy, and adopts asymmetric encryption technology to encrypt transmitted messages to prevent information leakage.

Key Words: automatic trust negotiation (ATN), digital credential, asymmetric encryption, information disclosure, negotiation model