浙江理工大学学报(自然科学版),第 37 卷,第 2 期,2017 年 3 月
Journal of Zhejiang Sci-Tech University (Natural Sciences)
Vol. 36, No. 2, Mar. 2017

DOI:10.3969/j.issn.1673-3851.2017.03.016

基于 AES 和 RSA 双向认证登录方案的研究

黄　静,岳梦婕
(浙江理工大学信息学院,杭州 310018)

摘　要:为了保障用户信息不被窃取同时提高系统的安全性,提出一种基于 AES 和 RSA 双向认证的安全登录方案。方案由认证和加密两部分组成,通过结合对称密钥和公开密钥技术设计了一种双向认证协议,在认证通过后再对信息进行混合加密及传输,为信息安全提供了多重保障。分析及测试结果表明该方案不仅能对信息进行加密保护,同时可以认证通信双方的身份,抵抗多种恶意攻击,与如今一些主流的登录方案相比,其在运算速度和成本方面更符合企业内部管理系统的需求。

关键词:AES 算法;RSA 算法;双向认证;混合加密
中图分类号:TP309.2　　**文献标志码**:A　　**文章编号**:1673-3851 (2017) 02-0242-04

0　引　言

如今在论坛、电子商务等网站的登录验证模块中,最为流行的登录方式是利用表单登录,用户在表单中输入用户名及密码,然后通过 HTTP 协议将信息传输到服务器端,再由服务器查询数据库来实现对客户端的认证及授权[1]。但这种方式存在很多安全漏洞,如对用户输入信息采用的编码方式较简单[2],容易被攻击者破解;由于客户端无法认证服务器,攻击者可以冒充服务器获取用户输入的信息[3]等等。很多学者对此进行了研究,郭晶等[4]鉴于 ECC 算法可以用更少的位数达到 RSA 算法所能提供的安全等级,因此提出了结合 ECC 算法的登录方案。张越等[5]发现单次 MD5 变换可被暴力破解,因此提出了对信息进行多次 MD5 加密的方案,但该方案耗时长,同时不能抵抗中间人攻击。而后肖曦等[6]介绍了基于 https 的登录方案,马永春[7]提出了基于 SAML 和签名数字信封的安全单点登录方案,https 和数字签名技术是目前登录方案中常用的技术,但其在应用的过程中会涉及到证书及公证中心[8],对企业内部管理系统来说成本过大。

针对上述问题,本文设计了一种基于 AES 和 RSA 双向认证的网站安全登录方案,拟实现服务器和客户端双向认证、加密传输且不能轻易破解、服务器与客户端之间实现“秘密”通信这三项安全需求。保护了用户的个人信息,为企业内部管理系统的登录安全作出了保障。

1　网络数据安全传输模型

在信息传输的过程中,为了保障信息的保密性和真实性,需要设计一种安全传输方案来保障信息安全,目前广泛使用的安全传输模型如图 1 所示,包括以下三方面内容:

a)发送方发送的信息需要进行相关变换。如对消息进行加密操作,攻击者即使截获到消息也不能读懂,或者将消息摘要并加密后附于原消息末尾,接收方接收到该消息后可以凭此来验证发送方的身份[9]。

b)发送方与接收方之间需要共享某些秘密信息,并且希望这些秘密信息不能被攻击者窃取到。比如当发送方用对称密钥加密信息时,发送方需要知道消息在加密时使用的密钥,才能还原出原始信息[10]。

收稿日期:2016-05-10　　网络出版日期:2017-01-03
基金项目:浙江省自然科学基金项目(1203635-D)
作者简介:黄　静(1965-),女,杭州人,教授,博士,主要从事嵌入式系统、信息安全等方面的研究。

c)要实现安全传输常常需要有可信的第三方。该第三方负责对服务器和客户端之间需要交换的秘密信息进行分配,且对攻击者完全保密。或当服务器和客户端对传输信息的真实性产生质疑时,该第三方负责对其进行仲裁[11]。

从图 1 所示的传输模型中可以看出,要实现数据的安全传输需要考虑以下四方面内容:

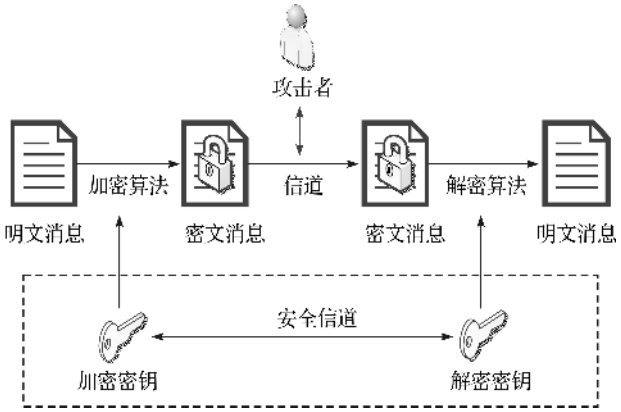

图 1　数据安全传输模型

a)设计对信息进行加密和解密的相关算法,并且要保证算法的不可攻破性。

b)生成加密和解密需要使用的密钥。

c)设计让服务器和客户端之间传递秘密信息的方法。

d)指定实现安全服务的协议,客户端和服务器利用该协议来实现数据的安全传输[12]。

2　基于 AES 和 RSA 双向认证的安全登录方案

本文设计的登录方案应用于某小型企业内部管理系统中,该管理系统采用 Java 语言编程实现,结合 Spring 框架,并运用 Hibernate 来与数据库进行交互。整个登录过程分为两步,第一步是进行服务器与客户端之间的双向认证[13],认证通过后才可进行下一步即数据的加密传输[14]。本文设计的认证协议结合了对称密钥和公开密钥技术[15],实现了一种有效的双向身份认证,具体过程如图 2 所示。

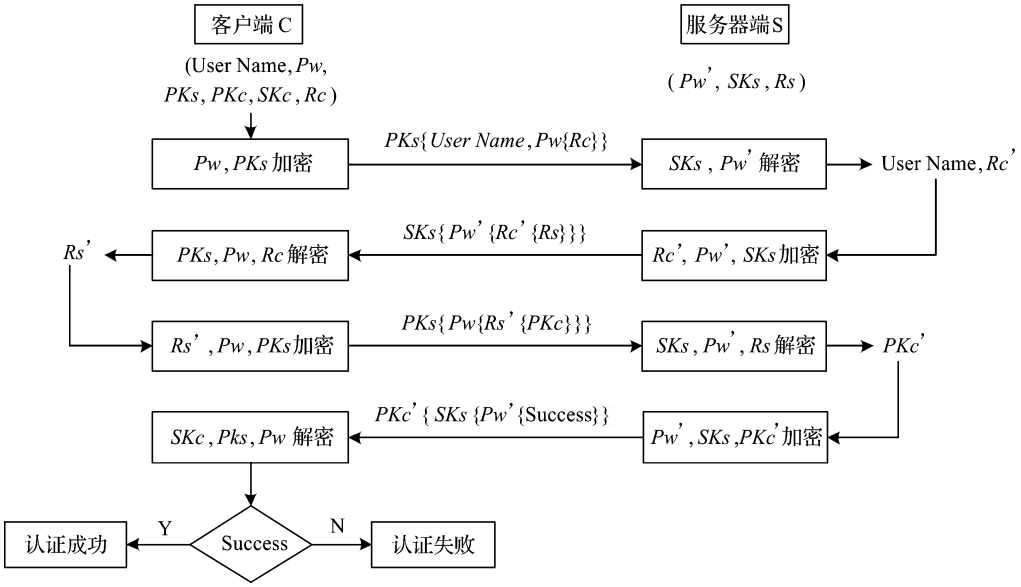

图 2　认证协议流程

服务器端(S)使用 RSA 算法生成一对公钥私钥密码对,并将公钥 PKs 发送给客户端,私钥 SKs 保存在服务器端。

a)客户端 C 随机生成一个对称密钥 Rc,首先用用户的登录密码对 Rc 进行 AES 加密得到 $Pw\{Rc\}$,再用服务器端颁发的公钥对用户名 $UserName$ 及 $Pw\{Rc\}$ 进行加密,得到 $PKs\{UserName, Pw\{Rc\}\}$ 并发送给服务器。

b)服务器接收到该密文后,首先用服务器私钥解密,得到 $UserName$ 和 $Pw\{Rc\}$,而后通过查询数据库得到 $UserName$ 对应的 Pw',用 Pw' 解密 $Pw\{Rc\}$,得到 Rc',当且仅当 Pw' 和 Pw 完全相同时,才能保证解密出的 Rc' 与客户端生成的密钥 Rc 相同。解密过程完成后,服务器端随机生成一个对称密钥 Rs,首先用 Rc' 加密得到 $Rc'\{Rs\}$,再用 Pw' 加密得到 $Pw'\{Rc'\{Rs\}\}$,最后再用服务器私钥加密得到 $SKs\{Pw'\{Rc'\{Rs\}\}\}$,并将此密文发送至客户端。

c) 客户端首先用服务器颁发的公钥 PKs 对密文进行解密，得到 $Pw'\{Rc'\{Rs\}\}$，而后用用户输入的登录密码 Pw 解密，最后再用客户端生成的对称密钥 Rc 进行解密，当且仅当 Pw' 与 Pw 及 Rc 与 Rc' 完全相同时，才能保证解密出的 Rs' 与服务器端生成的密钥 Rs 相同。此时客户端采用 RSA 算法生成一对公钥私钥密码对，私钥 SKc 保存在客户端，公钥 PKc 用解密出的 Rs' 进行加密，再用 Pw 进行加密，最后用服务器公钥 PKs 进行加密，得到 $PKs\{Pw\{Rs'\{PKc\}\}\}$ 并发送至服务器。

d) 服务器接收到该密文后首先用私钥解密，得到 $Pw\{Rs'\{PKc\}\}$，而后用 Pw'，Rs 进行 AES 解密，得到解密出的客户端公钥 PKc'。至此秘钥交换过程完成，服务器用 Pw' 加密一个成功认证的信号 $Success$，得到 $Pw'\{Success\}$，然后用服务器私钥加密，再用解密出的客户端公钥进行加密，得到 $PKc'\{SKs\{Pw'\{Success\}\}\}$，并将该密文发送至客户端。

e) 客户端接收到后依次用客户端私钥 SKc、服务器公钥 PKs 进行 RSA 解密，而后用用户输入的登录密码 Pw 进行 AES 解密，若解密出的结果为 $Success$，表示认证过程中的各项密钥完全匹配，即服务器和客户端相互认证成功，此后服务器和客户端便可以采用各自的公钥和私钥进行通信。

3 安全性分析

为了检测该方案的安全性能，本文将从以下 5 个方面进行分析和测试。

a)实现了双向认证：在用户数据传输前完成了客户端与服务器之间的相互认证，在攻击者恶意冒充客户端或者服务器时认证不予通过，后续的数据传输也随之断开，大大提高了系统的安全性。

b)采用三重混合加密：即使消息被拦截，经三重混合加密后的密文大大增加了破解的难度，有效保护了用户的个人信息，使得数据的传输更加安全。

c)抵御重放攻击：在信息传输的过程中，每次都会加入一个随机数，这样的做法保证了信息的唯一性和不可重复性，即使攻击者截获某次加密信息后也无法重用，有效地抵御了重放攻击。

d)抵御选择密文攻击：本方案中所有的签名都不是对原始消息的签名，而是对经客户端和服务器端随机数合成后的消息的签名，因此可以抵抗这种针对公开密钥体制的选择密文攻击。

e)方案耗时：查看从请求发出到收到响应的时间，结果如图 3 所示，可见该方案的运算速度快，耗时少，不会影响用户的体验。

Name Path	Method	Status Text	Type	Initiator	Size Content	Time Latency
validate... /backen...	GET	200 OK	text/html	Other	3.3 KB 3.1 KB	431 ms 429 ms

图 3 响应时间

分析与测试结果表明，本文方案对数据进行了多重加密保护，同时其双向认证的机制提高了系统的安全性，可以有效抵抗重放攻击、选择密文攻击，并且运算速度快，将其应用到某企业的内部管理系统中后，既保障了系统的安全性同时又保护了用户的个人信息。

4 结 语

本文针对目前网站登录方式上存在的口令易破解、无法抵御重放攻击等安全性问题，提出了一种结合了 RSA 和 AES 的双向认证的安全登录方案，该方案在登录过程中通过双向认证确认服务器和客户端的身份，而后将信息加密后进行传输，在某企业的内部管理系统中得到了很好的应用。测试结果表明，该方案能有效抵御重放攻击、选择密文攻击等，同时运算速度快，加密效果好，为系统的安全性提供了多重保障，具有良好的应用前景。

参考文献：

[1] 张君正. 浅谈网站用户密码泄露及对策[J]. 黑龙江科技信息，2012，31：109.

[2] CHIU R K，YU S P，LENNY KOH S C. A study on building of a common gateway for secure exchange and transmission of electronic business message [J]. Benchmarking：An International Journal，2007，14(3)：306-319.

[3] 李海华. 数据加密技术在计算机网络通信安全中的应用探析[J]. 计算机光盘软件与应用，2013，16(8)：149-151.

[4] 郭晶，陈谊. 基于 ECC 的安全登录方案设计[J]. 北京工商大学学报(自然科学版)，2006，24(3)：51-53.

[5] 张越，陈跃，刘林飞. 改进 MD5 码增强网站密码安全性[J]. 当代医学，2009(2)：10-11.

[6] 肖曦，南楠. 基于 HTTPS 的统一通信系统安全设计[J]. 物联网技术，2011(5)：67-68.

[7] 马永春. 基于 SAML 和签名数字信封的安全单点登录系统研究[D]. 衡阳：南华大学，2013：1-55.

[8] 杨莉国，欧付娜，赵静，等. 数字签名技术分析与研究[J]. 网络安全技术与应用，2011(5)：64-66.

[9] KAKKAR A，SINGH M L，BANSAL P K. Efficient key mechanisms in multi-node network for secured data transmission[J]. International Journal of Engineering

Science and Technology,2010,1(2):787-795.
[10] CHU C H, OUYANG Y C, JANG C B. Secure data transmission with cloud computing in heterogeneous wireless networks [J]. Security Communication. Networks,2012,5(12):1325-1336.
[11] 陈莹莹.浅谈身份认证技术在网络安全中的应用[J].数字技术与应用,2013(6):219.
[12] WU J, STINSON D R. Three improved algorithms for multipath key establishment in sensor networks using protocols for secure message transmission [J]. Dependable and Secure Computing, IEEE Transactions on,2011,8(6):929-937.
[13] 安雷.身份认证技术的分析与研究[J].无线互联科技,2012(7):156.
[14] 宋树军.RSA 算法在数字签名中的应用[D].东营:中国石油大学,2007:1-58.
[15] SHENGBAO W, ZHENFU C, LICHENG W. Efficient certificateless authenticated key agreement protocol from pairings[J]. Wuhan University Journal of Natural Sciences,2006,11(5):1278-1282.

Research on Mutual Authentication Login Scheme Based on AES and RSA

HUANG Jing , YUE Mengjie
(School of Information science and Technology, Zhejiang Sci-Tech University, Hangzhou 310018, China)

Abstract: In order to prevent user information from being stolen and to improve the security of the system, we present a secure mutual authentication login scheme based on AES algorithm and RSA algorithm. The scheme consists of two parts: authentication and encryption. In this scheme, we design a mutual authentication protocol by combining the symmetric key technology and the public key technology. The information will first be encrypted by hybrid encryption algorithm and then transfer to each other after the authentication is passed. This method provides multiple protection for information security. Analysis and test results show that the scheme can not only encrypt the information, but also authenticate the identity of the two parties and resist various malicious attacks. Compared with some popular login schemes, it more conforms to the needs of enterprise management system in terms of speed and cost.

Key words: AES algorithm; RSA algorithm; mutual authentication; hybrid encryption

(责任编辑:陈和榜)