第 33 卷 第 9 期 计 算 机 工 程 2007 年 5 月
Vol.33 No.9 Computer Engineering May 2007
·安全技术· 文章编号：1000—3428(2007)09—0182—02 文献标识码：A 中图分类号：TP393.08

银证系统中数据安全传输的综合防御措施

周克江
(湖南省第一师范学校信息技术系，长沙 410002)

摘 要：2004 年 8 月，在美国召开的国际密码学会议上，来自中国山东的王小云教授宣布成功破译了 MD5、HAVAL-128、MD4 和 RIPEMD 算法，并在任何初始值下用 2^40 次 Hash 运算给出了 SHA-0 的碰撞。这意味着目前广泛应用于电子商务、银行系统、证卷系统的安全认证算法——Hash 函数分析领域堡垒的轰然倒塌。面对严峻而残酷的现实，依赖于 Hash 算法的银证系统数据安全传输问题，也就成为人们不得不及时解决的实际问题。该文给出了一种银证系统数据安全传输的综合防御措施。

关键词：SHA-1；MD5；WAP；AES；WTLS

Integrated Security Recoery Method for Data Transmission in Stock and Bank System

ZHOU Kejiang
(Dept. of Information Technology, Hunan First Normal College, Changsha 410002)

【Abstract】On the conference of the international cryptology association which was convened at the United States in August 2004, professor Wang who comes from Shandong of Chinese declared that they had successfully broken the algorithms of MD5, HAVAL-128, MD4 and f RIPEMD, and used the two of the fortieth power Hash operates under any initial value to give the collision of the SHA-0. This means that the algorithms of security authentication extensively applied currently in the electronic commerce, bank system, and stock system tumblingly breaks down, which is the field of Hash function analysis. Confronting with the rigorous and ruthlessness reality, people have to try to resolve this problem in time,which is the Hash functions based data transmission problems of the stock and bank system. Therefore, this paper provides a comprehensive defense measure of data transmission in the stock and bank system.

【Key words】SHA-1; MD5; WAP; AES; WTLS

2004 年美国加州圣巴巴拉召开的国际密码学会议(Crypto'2004)安排了 3 场关于杂凑函数的特别报告。在国际著名密码学 Antoine Joux 给出 SHA-0 的一个碰撞之后，来自山东大学的王小云教授作了破译 MD5、HAVAL-128、 MD4 和 RIPEMD 算法的报告。她的研究成果作为密码学领域的重大发现宣告了固若金汤的世界通行密码标准 MD５的堡垒轰然倒塌。作为 MD5 算法应用的重要领域：电子商务，银行系统，证券系统等引起了一阵恐慌，因为在这样大的领域中重新更换 SHA-1 数据保密算法，谈何容易。为此，本文给出了一种银证系统数据安全传输的综合防御措施。

1 银证系统的特点

银行证券系统，一方面采用 WAP 技术实现手机上网，由移动终端、移动网络、WAP 网关服务器(WAP Getway)、网络内容供应商(ICP) 、网络服务供应商(ISP) 与 Internet 对接完成；另一方面通过卫星通信与外地营业网点联接。交易需要实时行情的昭示和实时操作。前者涉及的是公开信息，它要求数据能够迅速、准确；后者涉及的是私人信息，它不仅要求数据能够迅速、准确，还要求数据能保密、安全可靠，在传输过程中不被窃取。行情和交易数据源自银证公司内部网络，为保证内网的安全，也必须在与外部的 Internet 互联当中架构有效的防御体系。

2 数据传输安全措施

2.1 WAP 安全措施

WAP 的安全性同Internet一样也是在传输层实现的。Internet 模型将它的多数安全特性在TLS 中实现，而WAP 则在WTLS 中，WTLS 是以TLS 为基础的[1]。WTLS 可以保证手机与WAP 网关之间的通信是安全的，而WAP 网关使用HTTP 111 协议与Web 服务器通信，TLS 可确保WAP网关与Web服务器之间的通信是安全的。但WAP在会话中需将WML与WMLScript翻译成二进制代码，以适宜在低带宽的网络上传输，也使终端易于处理。WAP 网关负责这种转换，这时网关就会将WAP手机与网关间加密传输的数据进行解密,然后用其它方法再次加密，经TLS 发给Web服务器，这样就会因WAP网关能够看见所有的数据明文而可能发生数据的不安全。针对上述的情况，在 3 个方面采用安全防范措施：

(1)将 WAP 网关放置在银证公司内部,使网关与 Web 服务器间的通信在公司内部完成，防止第 3 方获得这些信息；

(2)在应用层，针对 WAP 手机处理能力较低的特点，只需对关键的信息进行加密(如股东账号、密码) ，这样做，既可以保证用户或股东的储蓄、股票资料等私人信息不会泄露，又可提高手机处理数据的速度，保证交易的快捷性；

(3)将银证券公司的内部网络与 Internet 隔离开，设计通信中间件传递二者的信息，防止内部网被非法侵入。通信中间件将 Web 服务器与内部网络分开,它根据 Web 服务器的请求负责将该请求传给内部网络的相应服务器，并将结果反馈

作者简介：周克江(1968－)，男，讲师、硕士，主研方向：网络安全，移动计算，网络计算等

收稿日期：2006-06-19 **E-mail：**kejiang_zhou@hotmail.com

给 Web 服务器。采用资金与行情分开的 3 层结构，通信中间件包括行情传输通信中间件和交易数据通信中间件。其中，交易数据通信中间件负责储户或股东认证和关键数据的解密工作。

传输层及会话层安全措施：

(1)无线网段，选用 WTLS 加密传输机制；有线网段，选用 SSL 加密传输机制，有效地保证敏感数据的传输安全。

(2)Web 服务器设置防火墙,仅开放 WWW 服务，以确保内部网络的安全。

(3)通信中间件的网关中仅开放与 Web 服务器之间的专用通信服务，确保柜台交易系统的安全。

2.2 数据加密措施

系统以Brower/Server 方式设计。用户或股民使用移动终端或个人计算机上网，通过浏览器，连接至Web服务器，即可进行储蓄或股票的查询、委托，完成交易。系统采用WML、WMLScript 和Java开发，具有高效、安全、易扩展的特点。采用多层次的设计，实现界面、通信和业务接口的分离，使交易得到最大限度的保证。其中最重要的数据莫过于用户的账户和密码，以及储蓄、交易数据，对这些数据的加密，采用基于AES算法的密钥更新方案[2]。

常用 Hash 函数的分组长度一般为 64B，而密钥更新算法的输入总长度才为一半左右，把 Hash 函数用于密钥更新根本就体现不出优势来，必然带有很大的局限性。RES(RijnDael)算法[3]的分组和密钥长度与密钥更新算法的输入长度接近，这样选择RES算法[4]作为密钥更新主算法是很合适的。RES 算法经受了 3 年多全世界密码学者的密集评估，评选过程公开，会有陷门的可能性很小。分析表明，RES算法具有良好的非线性，可抗差分和线性攻击及相关密钥等攻击[5]，安全性高，速率又快[6]。

基于AES密钥更新算法K_{IV}=rekey_AES(K,IV,TA)，定义如下：

TA 为发送地址；

CTR=IV||TA (||表示串联)；

$K_{IV}=E_K(CTR)\oplus K$ (⊕表示按位异或)

或$K_{IV}=E_{CTR}=(K)\oplus K$ (大于 16B时可分段)

其中，CTR可根据实际需要扩展为 16B，E_K(CTR)表示AES算法采用密钥K对CTR进行加密。采用TA的目的是保证“从终端 1 到终端 2”和“从终端 2 到终端 1”使用不同的密钥通信；与K异或的目的是保证更新算法的单向不可逆性。测试表明：基于AES的密钥更新算法速率是SHA方案的 3 倍，是MD5 方案的 5 倍。

采用 AES 算法作为密钥更新主算法，对 WEP 进行了改进，以较小的代价实现了一次一密，解决了 WEP 对 RC4 算法的误用问题，给出了一个安全性高、速率快、灵活性强的实用方案。该方案不失为一个极佳的过渡方案，适用于目前常用的对称密钥算法，并且可扩展。

2.3 无线网络安全措施

为了确保无线网络安全，采用分离分析技术(Split-Analysis)。分离分析技术(Split-Analysis)是一种混合式的射频安全解决方案。它解决了以服务器或者传感器为中心的解决方案所存在的问题。分离分析方案用智能的、特定制造的传感器来完成前期分析工作，用服务器来实现复杂的数据分析和异常监测工作。这种分布式智能可以提高监测的准确率、系统的可扩展性并简化系统管理。通过将分析功能分离，传感器只需进行一些不针对特定攻击或者漏洞的基本的分析工作。例如：传感器能够监测所有的上行的 WLAN 行动，并且可以从 802.11 协议、扩展认证协议(Extensible Authentication Protocol， EAP)、IP 和 UDP/TDP 协议的数据包报头提取服务集标识 SSI(Service Set Identifier)和地址等信息。传感器除了可以压缩和加密数据外还可以收集无线信道的信息，比如接收信号强度指示 RSSI(Received Signal Strength Indication)、噪声等。使用分离式的处理方式，传感器同服务器之间通信所占的带宽只有大约 1Kbps~3Kbps。因此，利用分离式处理方式回程网络可以比较容易地进行扩展，从而实现对数千个的远程传感器的 WLAN 监视和分析数据的相关操作。

通过分离分析，服务器可以集成来自数千个传感器的数据，对所有覆盖区域有重叠的任意两个传感器数据进行相关，并使用复杂的异常监测算法来识别各种安全异常和性能异常。另外，服务器还可以生成警报和进行数据统计，帮助银证部门来选择正确和及时的行动。

对于无线入侵监测系统 IDS 来说，分离分析解决方案使得 IT 人员能够通过对服务器进行简单的警报升级就可以应对快速变化的各种威胁了。传感器上的固件并不需要升级，因为它们只进行基本的分析，因此分离分析的解决方案使得管理变得非常方便，特别是对于无线 IDS 来说，分离分析提供了更多的好处。智能的瘦传感器分担了服务器的分析工作，减少了对回程带宽的消耗，提供了更好的可扩展性。多传感器相关和实时网络状态数据库可以帮助减少错误识别，增加高级报警功能，从而提高了监测的准确性。

对于有线网络安全措施，这里就不一一谈及。

3 结语

总之，根据银证系统的特点，从上述 3 个方面加强了安全防范措施，有效地保证了数据传输的安全性。以后的工作，侧重在 Internet 的安全防范措施。

参考文献

1 殷长友, 宋 震. WAP 技术应用于证券交易的一种安全措施[J]. 小型微型计算机系统, 2002, 20(8): 30-31.

2 黄玉划, 胡爱群, 宋宇波, 等. 网络安全中密钥更新算法研究与实现[J]. 计算机工程与应用, 2003, 39(35): 26-27.

3 Daemen J, Rijmen V. AES Proposal:Rijndael(V2)[Z]. 1999. Http://csrc.nist.gov/encryption/aes/rijindael/Rijndael.pdf.

4 FIPS PUB 197. Announcing the AES[Z]. 2001. Http://csrc.ncsl.nist.gov/pubications/fips/fips197/fips-197.pdf.

5 Gladman B. A Specification for Rijndael, the AES Algorithm (V33)[Z]. 2002. Http://fp.gladman.plus.com/cryptographytechnology/rijndael/ aesspec.pdf.

6 耿 嘉. 无线局域网安全系统[M]. 北京：电子工业出版社, 2004-03: 116-132.