

基于智能卡的分布式数据传输安全模型

于正东¹, 李艳²

(1. 中国民航机场建设集团公司东北分公司, 沈阳 110043; 2. 辽宁省交通高等专科学校, 沈阳 110122)

摘要: 针对分布式环境下的数据分发和管理问题, 以智能卡与口令作为身份认证与密钥交换的基础, 设计一个分布式数据传输安全模型。对该模型从敌手攻击角度和模型自身满足安全性角度进行安全性分析, 结果表明, 该模型不仅可以保证数据的完整性、不可否认性以及达成双方认证, 还可以在最大程度上实现机密性信息在分布式环境下的安全传输过程。

关键词: 分布式数据传输模型; 智能卡; 口令认证

Secure Model of Distributed Data Transmitting Based on Smart Card

YU Zheng-dong¹, LI Yan²

(1. Northeastern Filiale of China Aerodrome Building Group, Shenyang 110043;

2. Liaoning Province College of Communications, Shenyang 110122)

【Abstract】 To solve the problem of data distribution and management in the distributed environment, this paper proposes a secure communication model based on smart card and password authentication. The model is also analyzed from the point of view of adversary attacks and oneself security. Results show that the model not only guarantees the integrity, non-repudiation, and authentication, but also realizes the confidentiality during the data transmitting.

【Key words】 model of distributed data transmitting; smart card; password authentication

1 概述

近年来, 随着分布式网络环境下数据分发与管理应用的推广和普及^[1-2], 其对传统数据分发和管理方式产生了重大的改变, 例如以往需由人工制作与传递的数据逐渐改由计算机自动或半自动完成并经由网络进行快速的传递。这样的转变不仅加快了组织整体作业流程, 而且也大幅降低了人力成本及人为疏忽。但在这种分布式、不可信的数据分发环境中缺乏控制数据通信的权威机构, 且进行通信的各实体之间也不存在信任关系, 这就给数据的机密性、完整性和不可否认性带来了极大的安全性威胁。因此, 如何在不可信的分布式网络环境下, 实现安全的数据传输, 已成为当前最基本、最重要的安全需求之一。

本文针对分布式环境下数据分发和管理所面临的安全性问题, 提出了一个基于智能卡^[3]、口令身份认证^[4]和密钥交换协议^[5]的数据传输安全模型, 并对该模型进行了安全性分析。

2 模型设计

下面给出本文在设计该安全模型中所使用的一些符号标识。U: 用户; A: 数据服务代理; S: 数据源; ID: 用户ID; $h()$: 单向哈希函数; $Sig()$: 签名算法; $E()$: 非对称密钥加密函数; $D()$: 非对称密钥解密函数; K_{AS} : 数据源和数据服务代理的共享密钥; X_i : 随机数, $i=1\sim N, N \in \mathbb{Z}^+$; K : 数据源的私钥; T : 时戳(Timestamp); U_{pw} : 用户U的口令; $alias$: 用户别名; p, q : 素数, $n=p \times q$; R : 随机数。

本文将从用户注册、用户登录、用户验证以及数据传输过程这4个方面对安全模型进行描述。该模型的整体执行过程如图1所示。

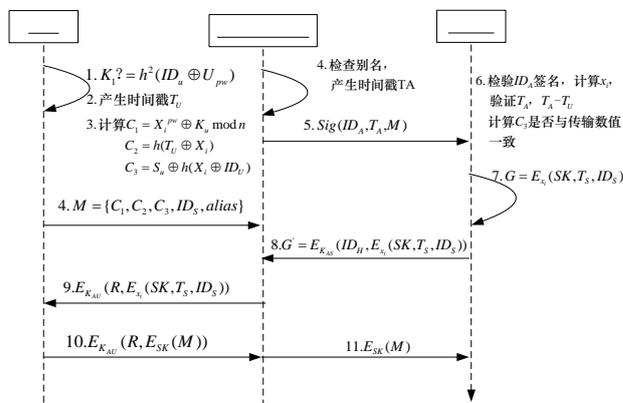


图1 数据安全传输过程

2.1 用户注册

(1) 用户通过安全信道(SSL)或 Diffie-Hellman 密钥交换向数据源注册其身份 ID 及口令, 口令可由用户自选或由数据源统一分发。

(2) n 为数据源所选取, $n=p \times q$, 其中, p, q 为大素数; n 公开且为其所有用户所掌握, p, q 只有数据源掌握。

(3) 数据源为每个用户生成别名 $alias$ 来代表用户 U 的 ID。

(4) 数据源计算如下:

$$K_u = h(ID, K) \oplus U_{pw} \tag{1}$$

$$K_1 = h^2(ID_u \oplus U_{pw}) \tag{2}$$

(5) 数据源通过安全信道(SSL)将 $K_u, alias$ 和 K_1 返回给用户

作者简介: 于正东(1959-), 男, 高级工程师, 主研方向: 网络与信息安全; 李艳, 讲师

收稿日期: 2010-02-13 **E-mail:** mhdbfgs@163.com

户, 并将 K_u 、 $alias$ 保存在系统数据库中, 而 K_u 、 $alias$ 和 K_1 则存入智能卡中, 由用户保存。

2.2 用户登录

(1) 当用户需要向系统提交数据时, 需要向系统提供身份 ID 和口令, 由智能卡验证其身份 ID 和口令是否符合 $K_1 = h^2(ID_u \oplus U_{pw})$, 如果符合, 则智能卡为其提供 K_u 、 $alias$ 。

(2) 系统计算如下:

$$C_1 = X_i^{pw} \oplus K_u \text{ mod } n \quad (3)$$

$$C_2 = h(T_u \oplus X_i) \quad (4)$$

$$C_3 = S_u \oplus h(X_i \oplus ID_u) \quad (5)$$

(3) 用户通过网络传送 M 与 ID_S (数据源 ID) 到数据服务代理:

$$M = \{C_1, C_2, C_3, ID_S, alias\} \quad (6)$$

2.3 用户验证

(1) 数据服务代理收到用户发送的数据 M , 加入其 ID_A 与时间戳 T_A 后, 即进行签名 $Sig(ID_A, T_A, M)$, 并将该签名发送给数据源。

(2) 数据源收到 $Sig(ID_A, T_A, M)$ 后, 进行下列计算:

- 1) 检查 ID_A 签名是否正确, 以确保消息的来源可靠性。
- 2) 利用别名 $alias$ 在数据库中查询用户 ID、口令和 K_U 。
- 3) 由 ID_A 、 U_{pw} 和 K_U , 并通过式(3)解出 x_i 。
- 4) 利用式(4)计算出时间戳 T_u , 以验证是否存在重放攻击。
- 5) 利用式(5)检验数据服务代理所传送的 C_3 是否与数据源计算的 C_3 一致。

2.4 数据传输过程

(1) 数据源在对用户身份验证后, 立即将共享加密函数的密钥设为 x_i 。

(2) 数据源选定双方通信密钥 SK , 并产生系统时间戳 T_S , 将 SK 和 T_S 加密:

$$G = E_{x_i}(SK, T_S, ID_S)$$

(3) 用数据源和数据服务代理所共享的密钥 K_{AS} 将 G 加密, 并传送给数据服务代理:

$$G' = E_{K_{AS}}(ID_H, E_{x_i}(SK, T_S, ID_S))$$

(4) 数据服务代理利用 K_{AS} 解密出 ID_S , 检验是否由数据源所发送, 如果是, 则产生一个随机数 R , 并将 $E_{K_{AU}}(R, E_{x_i}(SK, T_S, ID_S))$ 传送给用户。

(5) 用户解密出随机数 R , 利用 x_i 解密出 SK 、 T_S , 并验证时间戳是否在合理的时间范围内, 如果是, 则确定 SK 为通信的会话密钥。

(6) 用共享密钥将 R 加密后, 即 $E_{K_{AU}}(R, E_{SK}(M))$, 发回给数据服务代理。

(7) 数据服务代理解密出 R 后, 检查是否正确, 如果正确, 将 $E_{SK}(M)$ 转发给数据源。

(8) 用户和数据源可以用新的密钥开始通信。

3 安全性分析

为证明本文所提出的数据传输模型的安全性, 下面从敌手攻击角度和模型自身满足安全性角度进行分析。

3.1 抗敌手攻击分析

(1) 仿冒攻击

如果敌手取得合法用户身份 ID 及口令, 并利用此组认证信息进行假冒攻击, 但由于敌手未能取得存在于智能卡中的信息 K_u 值, 使其无法通过数据中心的认证。在式(1)中, 敌手如果要完成合法认证, 其必须先破解 $h(ID_u, s)$ 之值, 然而由于

单向哈希函数特性, 使其难以破解。

(2) 重放攻击

为避免敌手使用重放攻击造成机密信息泄露, 本模型采用时间戳作为防御重放攻击的机制。在式(3)、式(5)与式(6)中, 对每个阶段分别执行传递时间检查, 同时在本模型中, 时间戳也通过单向哈希函数进行保护, 从而增加了敌手的破解难度。

(3) 中间人攻击

敌手在本模型中可以使用如下方式进行攻击:

1) 对用户及数据服务代理之间信息的攻击

敌手位于用户及数据服务代理之间, 转发通信双方的认证信息, 因此, 攻击者可以接收式(5)和式(7)的信息。然而这些认证信息均已经加密, 敌手只能转发信息而无法从中获取机密信息。

2) 对数据服务代理与数据源之间信息的攻击

当敌手位于数据源及数据服务代理间时, 转发通信双方的认证信息, 敌手可以从中窃取到式(6)和式(8)。然而这些认证信息均已使用数据服务代理与数据源间所共享的密钥及用户自选密钥进行加密, 敌手无法获取有效信息。

3) 针对三方通信实体间的认证信息攻击

当敌手转发通信三方之间的认证信息, 可以从中窃取到整个机制间的认证信息。然而这些认证信息均已使用彼此间所共享的密钥及用户自选密钥进行加密, 攻击者无法从中获取信息。

(4) 口令猜测攻击

1) 在线口令攻击

针对此种攻击, 可以让数据源通过认证次数限制方式进行避免和防御。

2) 离线口令攻击

敌手利用窃听获取通信双方信息, 进而获取式(2)~式(4), 用所得到的信息进行解密, 除要破解口令外, 在其进行认证时由于未能提供数据源所产生的 K_u 值, 因此仍无法通过合法认证。

(5) 智能卡冒用攻击

如果智能卡丢失或被敌手窃取, 则获取智能卡的人必须先破解式(2)。然而因为身份 ID 和口令均已经过单向哈希函数处理, 敌手很难从中获取信息, 所以无法产生正确的认证信息 C_1 、 C_2 和 C_3 , 故无法成功假冒合法使用者。

3.2 模型自身安全性分析

(1) 匿名性

为实现用户身份的匿名性, 同时避免敌手取得用户身份信息, 并利用其身份达到各种信息窃取或身份伪造等攻击行为, 本模型在用户注册阶段, 由与数据源配发相对应的别名保护用户的真实身份, 并将用户真实的身份和用来代替用户身份的别名存储在数据源的数据库中。只有数据源与数据服务代理才能得知用户的真正身份, 在最大程度上保护用户的匿名性。

(2) 三方实体认证

用户在注册阶段, 经由安全秘密通道向数据源取得其身份 ID、口令及由数据源所提供的相关秘密认证信息 K_u 。敌手若要进行仿冒攻击来欺骗数据源, 须先获取用户身份 ID、口令外, 同时破解由数据源私钥所加密的认证信息 K_u , 其破解难度显然强于基于身份 ID 和口令的安全保护系统。本模型除可有效认证出使用者, 避免遭受攻击外, 也可使用户对数据

源身份进行认证,从而实现双向认证机制,以保证后续机密信息的安全传送。

(3)不可否认性

信息的来源可靠性也是安全通信模型不可或缺的一部分。因此,在系统中必须存在不可否认机制,在本模型中除了结合智能卡与口令机制外,也通过数字签名、密钥共享等手段达到不可否认性的要求。

(4)保密性

本模型对于整个信息传递过程均采用了公钥密码体制、单向哈希函数等手段进行安全保护,敌手如截取到传递过程中的任一信息,其所要面对的是解密的困难问题。数据服务代理是进行数据的上传和下载,因此,访问次数会较多,也容易成为敌手攻击的目标。然在信息交互过程中采用了数字签名机制与密钥共享机制,使敌手难以攻击。

4 结束语

本文针对分布式环境下的数据分发和管理所面临的安全性问题,提出了一种新的基于智能卡技术的数据传输安全模型。该模型将智能卡技术、口令认证、密钥交换技术进行有

效融合,通过安全性分析表明该模型保证了数据在传输过程中的机密性、完整性和不可否认性。

参考文献

- [1] Luo Qiong, Krishnamurthy S, Mohan C, et al. Middle-tier Database Caching for E-business[C]//Proc. of ACM SIGMOD International Conference on Management of Data. [S. l.]: ACM Press, 2002: 600-611.
- [2] 张琳娜, 王映辉. 基于节点自治的分布式数据共享模型[J]. 计算机工程, 2009, 35(3): 32-35.
- [3] Hwang M S, Kumar M. A New Remote User Authentication Scheme Using Smart Cards[J]. IEEE Trans. on Consumer Electronics, 2000, 46(1): 28-30.
- [4] Katz J, Ostrovsky R, Yung M. Efficient Password-authenticated Key Exchange Using Human-memorable Passwords[C]//Proc. of EUROCRYPT'01. [S. l.]: IEEE Press, 2001: 475-494.
- [5] Diffie W, Hellman M. New Directions in Cryptography[J]. IEEE Trans. on Information Theory, 1977, 22(6): 644-654.

编辑 顾逸斐

(上接第 150 页)

$$R_{n-2}^4 \oplus G_n = V_{n-2}, R_{n-1}^3 \oplus G_n = V_{n-1}, R_n^2 \oplus G_n = V_n$$

通过以上 3 个方程式可以看出,虽然攻击者知道了 V_{n-2} 、 V_{n-1} 、 V_n , 但仍有 R_{n-2}^4 、 R_{n-1}^3 、 R_n^2 以及 G_n 这 4 个未知数,因此,他不能推导 G_n 。

7 结束语

本文研究了低成本 RFID 系统的安全问题,提出了一个基于 PUF 的低成本 RFID 安全协议。本协议能抵抗重放攻击、跟踪攻击、物理攻击、窃听攻击等多种攻击。实验证明:协议执行时间很短,可以忽略不计,同时,标签只需要不超过 1 400 个门电路。因此,本协议有效地解决了低成本 RFID 系统的安全问题。

参考文献

- [1] Juels A, Weis S A. Authenticating Pervasive Devices with Human Protocols[J]. Advances in Cryptology, 2005, 6(3): 293-308.
- [2] Feldhofer M, Reiberger C. A Case Against Currently Used Hash

Functions in RFID Protocols[C]//Proc. of Workshop on RFID Security. Montpellier, France: [s. n.], 2006: 372-381.

- [3] Tan C C, Sheng Bo, Li Qun. Serverless Search and Authentication Protocols for RFID[EB/OL]. (2007-03-12). <http://www.cs.wm.edu/~cct/pub/percom07.pdf>.
- [4] Suh G E, Devadas D. Physical Unclonable Functions for Device Authentication and Secret Key Generation[C]//Proc. of Design Automation Conference. San Diego, California, USA: [s. n.], 2007: 9-14.
- [5] Kumar S, Guajardo J. Extended Abstract: The Butterfly PUF Protecting IP on Every FPGA[C]//Proc. of IEEE International Workshop on Host. Anaheim, CA, USA: [s. n.], 2008: 67-70.
- [6] 裴友林, 杨善林. 基于密钥矩阵的 RFID 安全协议[J]. 计算机工程, 2008, 34(19): 170-173.

编辑 顾逸斐

(上接第 152 页)

6 结束语

本文提出了用第一类分段 Lorenz 系统通过驱动-响应式同步的方法实现语音混沌保密通信的方案。在硬件实现方面,由于模拟电子电路参数的离散性和失配等问题,使得还原出语音信号的质量得不到保证,失真较大。解决这一问题的有效途径是采用数字化处理技术,对连续时间无量纲状态方程进行离散化处理,利用 5509 系列 DSP 器件实现了语音混沌保密通信系统,并给出了该系统的方案设计与硬件实现结果,理论设计与实验结果相吻合,从而证实了该方法的可行性。

参考文献

- [1] Pecora L M, Carroll T L. Synchronization in Chaotic Systems[J]. Physical Review Letters, 1990, 64(8): 821-824.
- [2] Yang Tao, Chua L O. Chaotic Digital Code-Division Multiple Access (CDMA) Communication Systems[J]. International Journal of

Bifurcation and Chaos, 1997, 7(12): 2789-2805.

- [3] Apostolos A, Syvridis D, Larger L, et al. Chaos Based Communications at High Bit Rates Using Commercial Fibre-optic Links[J]. Nature, 2005, 438(7066): 343-346.
- [4] Kamata H, Endo T, Ishida Y. Communication with Chaos via DSP Implementation[C]//Proc. of IEEE International Symposium on Circuit and System. [S. l.]: IEEE Press, 1997: 1069-1072.
- [5] Ling Cong, Wu Xiaofu. Design and Realization of an FPGA-based Generator for Chaotic Frequency Hopping Sequences[J]. IEEE Trans. on Circuits and Systems, 2001, 48(5): 521-532.
- [6] Elwakil A S, Ozoguz S, Kennedy M P. Creation of a Complex Butterfly Attractor Using a Novel Lorenz-type System[J]. IEEE Trans. on Circuits and Systems, 2002, 49(4): 527-530.

编辑 顾逸斐