

固网支付中密钥分发问题的一种解决方案

邓国旭, 王志谦

(北京邮电大学 信息网络中心, 北京 100876)

摘要:固网支付是中国电信与中国银联合作推出的一项固网短消息增值业务,需要较高的安全级别。为了在兼容现行固网支付安全方案并扩充业务的同时提高系统的安全强度,实现动态密钥分发以达到一次一密,并满足业务对效率的需求,从密钥分发的角度探讨了实现目标的方法。它分析了固网支付业务系统结构和安全需求,以及固网支付中现行的密钥分发机制,针对现行机制可能存在的问题并综合各种密钥分发机制提出一种适用于多内容提供商的新方案。

关键词:固网;电子支付;密钥;加密

中图分类号:TP309.7

文献标识码:A

文章编号:1673-629X(2009)07-0180-04

A Solution to Key Distribution on E-Payment Based on PSTN

DENG Guo-xu, WANG Zhi-qian

(Network Information Center, Beijing University of Posts & Telecommunications, Beijing 100876, China)

Abstract:To ensure security of e-payment on PSTN network and achieve a balance between security and efficiency, the structure of the e-payment system was analyzed in this paper and the security demand of the system was explained at the same time. Besides, the current key distribution mechanism in e-payment service network was described in detail. Finally, according to the irregularity of the current mechanism entity and different kinds of key distribution mechanism, a new scheme to secure e-payment on PSTN was presented.

Key words:PSTN; e-payment; cipher; encryption

1 研究背景

近年来,随着科技发展和人们生活习惯的改变,人们希望安坐家中就能轻松进行网上购物,线下刷卡支付,甚至足不出户就能轻松缴纳水、电、煤气等生活费用。在 market 需求的驱动下,电子商务不断深入百姓生活,电子支付事业得到了快速发展,随着互联网支付、移动支付等电子支付手段出现,固定网络上实现支付业务也提上日程。2006年4月,中国电信与银联全面展开战略合作,宣布正式启动固定电话支付业务,并计划2008年在中国电信南方21省全部开通。同时,中国网通也开始了其发展固网支付的进程。

在电子支付过程中,用户不可避免地需要输入帐号、密码等敏感信息,此类信息的安全传输不仅关系着交易的顺利进行,更重要的是,此类信息一旦被窃取还会危及用户的财产安全,电子支付系统一般采用对敏

感信息加密的方式来保障信息的机密性。

现阶段交易一般采用对称加密算法对敏感信息进行加解密,而银行系统以及支付系统主要采用对称加密中的DES/3DES加密算法。密钥是加解密过程中最重要的因素,如何安全分发使用密钥是加密系统最关键的问题。而在固网尤其是固网支付中,虽然运营商以及相关机构提出了一些密钥分发方式,但鉴于成本较高以及一些其他因素,很多系统仍然采用固定密钥方式,这种方式存在着极大的安全隐患,因此,为固网支付系统中设计一种安全可靠的动态密钥分发机制迫在眉睫。

文中首先分析固网支付系统结构和现存的密钥分发方式,然后针对系统需求并借鉴国外的成功经验,提出一套新分发机制。

2 固网支付中密钥分发

2.1 固网支付系统结构

固网支付系统平台基于中国电信固网短消息系统和相关金融机构的金融支付系统,为用户提供电子支付服务。它主要由三部分组成:支付终端,固网短消息系统和支付网关,支付网关接入银行等内容提供商。

收稿日期:2008-09-25;修回日期:2008-12-16

基金项目:信息产业部2005年度电子信息产业发展基金项目(信部运[2005]635号)

作者简介:邓国旭(1985-),女,硕士研究生,研究方向为计算机网络、电信网;王志谦,高级工程师,硕士,研究方向为计算机网络、计算机软件。

系统结构图如图1所示。

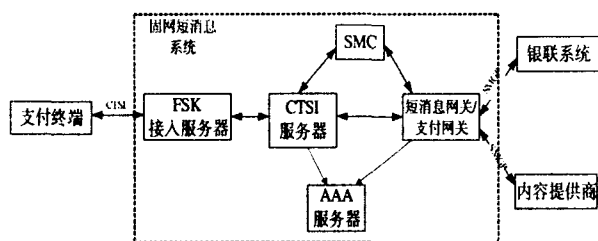


图1 固网支付系统结构

支付终端位于用户侧,可以完成电话、短信和支付功能,内置加密模块,完成支付终端的加解密,但处理能力较低。固网短消息系统位于运营商内,作为支付业务的数据流承载网络,完成数据传输和协议转换功能。支付网关又称支付应用服务器,它控制支付终端完成支付操作,并与内容提供商进行信息交换。内容提供商为用户提供各种服务,包括缴费和电子商务业务^[1]。敏感信息主要在支付终端与内容提供商之间传输,而支付终端与支付网关之间以及支付网关与内容提供商之间传输的交易信息也应得到相应保护。

与因特网支付和移动支付相比,固网支付拥有天然的安全性,但固网有限的带宽以及支付终端通过运营商支付平台与内容提供商相连又限制了系统的工作效率。同时,支付终端较低的处理能力和有限的存储空间也成为系统高效安全运行的瓶颈。

2.2 目前的密钥分发机制

固网支付系统通过每次交易前对用户身份认证鉴权验证用户的合法性。在交易过程中,涉及到用户的敏感数据一般采用硬件加密模块和对称加密方式,一次一密,实现端到端的加密传输。

上海新加 ePOS 支付业务是目前规模较大较正式的固网支付业务,它将固网短消息系统与付费通业务结合,提供一套有价值的增值服务业务,使普通用户在家就可以缴纳水、电、煤气等费用^[2]。系统结构图如图2所示。

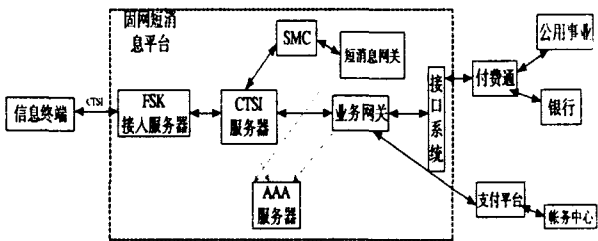


图2 新加 ePOS 支付业务系统结构图

为保证敏感信息安全,这套系统采用两套密钥体制:接口系统和支付终端之间采用基于 PSAM 卡的硬件加密机制^[3],接口系统和付费通之间采用基于直联 POS 的加密机制。

接口系统的硬加密机和付费通中保存主密钥,付费通通过发卡机使用主密钥并以支付终端的唯一性数据(PSAM 卡序列号,电话号码等)作为输入,采用某种密码算法推导出子密钥并将该子密钥导入 PSAM 卡中分发给用户,密钥推导过程不可逆。需传送敏感信息时,使用同样的推导过程生成临时工作密钥,只是推导时使用的是 PSAM 卡上的子密钥,而输入数据是由接口系统发送的分散因子(随机数)。最后用此临时工作密钥对敏感信息加密并上传。此临时工作密钥生命周期很短,在每次交易启动时派生,结束时销毁,每次参与加密的临时工作密钥互不相同。

接口系统与付费通使用密钥下载,初始化时,付费通将主密钥和付费通的密钥加密密钥导入接口系统的硬加密机,接口系统每次签到后从付费通获得用密钥加密密钥加密后的密码加密密钥并存储到硬加密机,然后采用密码加密密钥对信息加密。

2.3 可能存在的问题

新加 ePOS 支付系统采用金融系统的 PSAM 机制分发密钥,避免密钥在网络中传输,一次一密,极大增强了系统安全性。但此种方式所需的 PSAM 卡以及相关设备成本过高,以至这种方式很少在其他系统中使用,不利于这种方式推广。此外,用户的帐号密码等敏感信息在接口系统进行加解密转换,对接口系统透明,从银行和用户的角度讲不合乎安全要求。另外,系统中最重要的主密钥不仅存储在付费通管理人员所持有的 IC 卡中,还存在于付费通以及接口系统的硬件加密机中,成为系统的安全隐患。

更为重要的是,新加 ePOS 支付系统仅支持付费通一家内容提供商,而发展固网支付必然需要接入更多的内容提供商,虽然 PSAM 卡支持多应用,但现阶段仍主要由银行系统采用。如何实现用户终端和多内容提供商之间信息安全,需要一套新机制。

3 一种新方案

3.1 整体方案分析

虽然新加 ePOS 支付系统所采用的密钥分发方式不能提供支付终端与多内容提供商之间的端到端安全,但它所采用的 PSAM 安全方式能够提供支付终端与固网支付平台之间的信息安全。这也意味着,如果再有一套机制保障信息在固网支付平台与内容提供商之间的安全,这样就可以实现信息在支付终端与内容提供商之间的链路安全。

但在固网支付系统中,保护信息在支付终端与内容提供商之间的链路安全固然重要,而对于一些安全级别较高的信息而言,确保信息在终端与内容提供商

之间端到端安全更是重中之重。对于银行等安全需求级别非常高的业务而言,他们拥有自己的安全方案,运营商只需向他们提供相应的接口即可,而对于其余大量内容提供商,他们对安全有一定要求却不一定拥有成熟的安全机制,这也需要为之提供一套恰当可靠的安全方案。

综上所述,若能够在支付终端与固网支付平台,固网支付平台与内容提供商以及支付终端与内容提供商之间分别实现动态密钥分发,就可以实现支付终端与内容提供商之间信息的链路安全与端到端安全。

另外,金融系统对密钥设计有以下要求:密钥管理自动化,即在密钥管理过程中,不能存在人工管理过程;密钥在加密设备以外不能以明文形式出现;密钥必须从整个密钥空间随机选取;密钥加密密钥必须与数据加密密钥分离;生命周期长的密钥必须尽量少使用^[4]。固网支付系统作为金融类服务的提供者,也应满足这些要求。

3.2 关键技术

3.2.1 支付终端与固网支付平台之间

支付终端处理能力较低,内嵌对称加密算法 DES, 3DES 以及非对称加密算法 RSA 等加密算法,但它使用 RSA 算法加解密时速度较慢,效率较低,终端与支付平台之间信息传输较频繁。同时,终端通过固定网络直接连接到支付平台,而且支付平台连接大量支付终端,虽然它们之间采用对称加密,但若支付平台与每个终端之间都共享一对密钥却是不现实的,它不仅需要占用大量存储空间,还会影响工作效率。

为了避免在固网支付平台与每个支付终端之间共享一对密钥,可以参照 SSL 协议与 PSAM 机制设计一套密钥分发机制^[5]。支付网关产生一个主密钥,利用此主密钥针对终端的唯一性数据用某种密码算法分散得到子密钥,并将子密钥固定在终端中。在终端与支付平台之间建立会话后协商密钥生成机制:支付网关向终端下发随机数,两端分别用子密钥对随机数分散生成临时工作密钥,再用此临时工作密钥对信息加解密传输。

这种方式用软件方法实现 PSAM 机制,不仅避免了密钥在网络上的传输,也避免了使用 PSAM 卡等硬件设备,降低成本^[6]。虽然在支付平台与终端之间多了一次随机数传输过程,但它实现了一次一密。

3.2.2 固网支付平台与内容提供商之间

相比对称加密算法,非对称加密算法更容易达到更高的安全强度。只是它对计算处理能力要求较高,使得它在智能卡设备中使用不多,也较少用于数据加解密,主要用于密钥分发。对于固网支付平台与内容

提供商而言,他们不同于支付终端,处理能力较高,而且内容提供商在接入固网支付平台时需接受鉴权,方便实现可靠的公钥传输,因此可以在支付平台与内容提供商之间使用非对称加密算法进行密钥分发。即由固网支付平台和内容提供商中一端生成一对公私钥,并将公钥告知对方。当需传输敏感信息时,由持有公钥的一方随机生成交易密钥,用对方公钥加密传输给对方,对方私钥解密获得交易密钥,以此达到密钥分发的目的。

另外,若内容提供商与支付平台之间安全强度需求更高,可由内容提供商与支付平台分别生成一对公私钥然后共享对方公钥,当需传输敏感信息时先用对方公钥对信息加密,再用自身私钥对相应部分加密传输给对方,对方先用传输方公钥解密,确定信息未被篡改后再用自身私钥解密,由此达到机密性和完整性验证。

3.2.3 支付终端与内容提供商之间

支付终端与内容提供商通过固网支付平台相连,由支付平台转发他们之间的信息,为了系统效率,应尽量减少他们之间的交互,他们之间的密钥信息还应对支付平台保密。另外,终端与内容提供商的数量并不确定,而且他们之间的交互也比较随机,因此 SSL, PSAM 等方式并不适合它们之间的密钥分发,而必须思考另外的方式。

支付终端与内容提供商之间的情形有点类似于国外广泛使用的手机移动支付,手机通过无线网络连入商户,手机处理能力较低,不宜采用 RSA 等非对称加密算法。移动支付主要采用 KSL 协议来进行密钥协商,KSL 协议分为商户注册协议和支付协议:在商户注册协议阶段,手机客户在商户处注册并与商户共享一个主密钥 X;在支付协议阶段,交易发生同时生成一个交易密钥 Yi(Yi 由客户在银行注册时产生的主密钥 Y 生成),客户与商户之间的交易信息将由交易密钥 Xi 加密,而客户与支付网关之间的信息则由 Yi 加密。交易密钥通过对对应主密钥进行一个 HASH 和循环移位算法实现^[7,8]。对主密钥的每一次移位产生一个新值,对这个值的 HASH 处理将得到一个相差很大的结果。因此,可以考虑在内容提供商与支付终端之间共享一对主密钥,然后采用同样的方式来生成交易密钥。而主密钥生成次数极少,可采用非对称加密算法分发。即由内容提供商生成公钥并将公钥下发给支付终端,终端随机产生传输密钥加密上传给内容提供商。假设两端共享的传输密钥为 Ktr,每次交易时再对其执行如下处理:

$$K_{tmp} = h(1 - \text{bit-shift-of} - K_{tr}) \quad (1)$$

$$K_{tr} = \text{HASH}(K_{tmp}) \quad (2)$$

即先对传输密钥移 1bit 得到一个临时密钥 K_{tmp} , 再对此临时密钥运行单向 HASH 算法得到的 K_{tr} 作为交易密钥, 一次一密, 又因为单向 HASH 算法不可逆, 即使某个密钥被破解也不影响下一次交易安全。

3.3 新方案

结合系统中各方处理能力和系统需求, 将上述方案改进融合, 工作流程如图 3 所示。

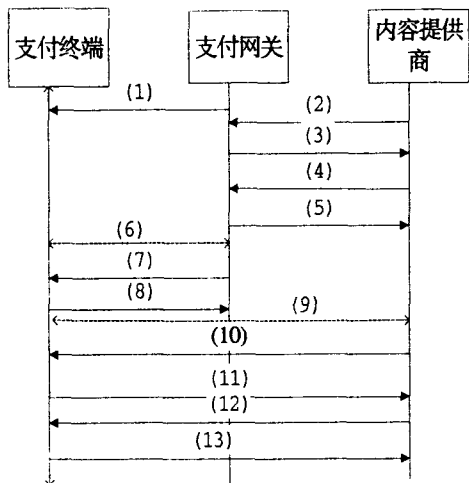


图 3 工作流程图

图中(1)~(13)说明如下:

(1)支付网关生成根密钥 $root_key$ 和一对 RSA 公私钥 K_{pri_iis} , K_{pub_iis} , 并用根密钥 $root_key$ 对信息终端标识分散得到终端子密钥 $child_key$, 固化在支付终端中。

(2)每次内容提供商登录到固网支付平台后, 检查是否有支付网关公钥, 若没有则向支付网关请求公钥。

(3)支付网关将公钥 K_{pub_iis} 传输给内容提供商。

(4)每天固定时刻内容提供商生成交易密钥 K_{tr} , 用支付网关公钥对交易密钥加密, 将加密后的密钥发送给支付网关, 进行密钥更新。

(5)支付网关用私钥 K_{pub_iis} 解密获得 K_{tr} , 并发送 ACK, 密钥更新完成, 支付网关与内容提供商之间的信息即用此密钥 K_{tr} 加解密。

(6)每次交易, 支付终端摘机, 支付网关提供内容提供商列表, 支付终端选择内容提供商。

(7)支付网关生成随机数, 将随机数下发给信息终端。

(8)支付终端获得随机数并用终端子密钥 $child_key$ 对随机数分散获得工作密钥 $work_key$, 支付终端与支付网关之间消息即用此工作密钥加解密^[9]。

(9)内容提供商下发菜单, 支付终端选择菜单, 由

内容提供商判断此项业务是否需加密。若需加密则检查内容提供商中是否有对应支付终端的主密钥 $master_key$, 若存在则执行步骤。

(10)若内容提供商中没有该支付终端的 $master_key$, 则将自身公钥 K_{pub_cp} 下发给信息终端。

(11)支付终端生成主密钥 $master_key$, 保存并用内容提供商公钥 K_{pub_cp} 加密上传, 内容提供商保存 $master_key$ 。

(12)内容提供商将移位序列号 N 下发给支付终端。

(13)支付终端 ACK。内容提供商和信息终端将对 $master_key$ 右移 N 位然后执行 HASH 生成交易密钥。支付终端与内容提供商之间的敏感信息即用此交易密钥加解密。

4 结束语

上述新方案在支付终端, 固网支付平台和内容提供商任意两方之间提供了动态密钥分发机制, 在支付终端与内容提供商之间提供了全方位的安全保护, 可用于多内容提供商业务。该方案在所有链路上均为一次一密, 安全强度高于现行方式, 为扩展固网支付系统应用提供了便利。在确定系统所采用的密钥分发方式后, 下一步将研究如何扩展支付系统中使用的 CTSS, SMGP 协议使它们适应高强度的安全需求。

另外, 还应注意到, 美国国家标准技术研究所选定安全强度更高的 AES 加密算法替代 DES/3DES 加密算法, 而椭圆曲线加密算法 ECC 在安全强度和加密效率上都优于 RSA 公钥加密算法。面对终端处理能力的瓶颈, AES 加密算法和 ECC 加密算法相比 DES 和 RSA 更加合适固网电子商务系统。从密钥分发角度提高系统安全性时, 将来的工作应致力于在兼容已有系统的同时探求应用安全性更高的加密方式。

参考文献:

- [1] 曹嘉骏, 王 彬, 蒋 力. 固网支付产品实现的技术特点和应用前景分析[C]//上海市通信学会第十一届学术年会. [出版地不详]:[出版者不详], 2005.
- [2] 上海电信技术研究所. 新家加 ePOS 支付业务技术方案 v1.2 接口技术规范[S]. 上海:[出版者不详], 2004.
- [3] 中国金融 IC 卡试点工程实施小组. 中国金融 PSAM 卡应用规范[S]. [出版地不详]:[出版者不详], 1999.
- [4] 毛小青, 刘运城. 银行卡安全问题的研究[J]. 华南金融电脑, 2006(7):60-64.
- [5] Rescorla E. SSL and TLS, Designing and building secure systems[M]. [s.l.]:Addison Wesley, 2002.

(下转第 190 页)

较大或者离开成员数 $L = 0$ 时,采用星形密钥图有较好的性能,有较小的更新开销。通过图 3 和图 4 可以得出相似的结论,就是当成员离开数 $L < N/4$ 或加入成员数 $J < N/2$ 时,密钥树比星形密钥图有好的性能,更新代价较低;其他的情况,星形密钥图有较好的性能,有低的更新代价。

4 结束语

文中分析树形结构的密钥图和星形结构的密钥图独立更新方式带来的更新代价,重点仿真星形和树形结构批量更新的性能,从而得出一个大致结论:当成员离开数 $L < N/4$ 或加入成员数 $J < N/2$ 时,采用树形结构有较好的性能,而采用星形结构有较好的更新性能。该结论对实际的应用有一定指导意义,从而降低更新密钥的代价,提高密钥服务器的性能。

参考文献:

- [1] Chung Kei Wong, Gouda M, Lam S S. Secure group communications using key graphs[C]//Proceedings of the ACM SIGCOMM '98 conference on Applications, technologies, architectures, and protocols for computer communication. NY, USA: ACM, 1998:68-79.
 - [2] 许 勇,陈 恺.安全多播中基于成员行为的 LKH 方法[J].软件学报,2005,16(4):601-608.
 - [3] 蔡延荣,王清贤,李梅林,等.安全多播密钥更新研究[J].计算机技术与自动化,2003,22(3):110-112.
 - [4] David A, Grew M, Sherman T. Key Establishment in Large Dynamic Groups Using One - Way Function Trees[M]//IEEE Transactions on Software Engineering. NJ, USA: [s. n.], 2003:444-458.
 - [5] Naor D, Naor M, Lotspiech J. Revocation and Tracing Schemes for Stateless Receivers[C]//Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology. London, UK: Springer - Verlag, 2001:41-62.
 - [6] Setia S, Zhu S, Jajodia S. A Scalable and Reliable Key Distribution Protocol for Multicast Group Rekeying[R]. Virginia, US: Department of Information and Software Engineering, George Mason University, 2002:1-14.
 - [7] 李彦希,赵 耀,林 闯,等.基于单向函数树的高效分布式组密钥管理方案[J].清华大学学报:自然科学版,2005,45(10):1417-1420.
 - [8] 杨焱林.基于 LKH 混合树的多播密钥更新方案[J].现代电子技术,2004,27:31-32.
 - [9] Heydari M H, Morales L, Sudborough I H. Efficient Algorithms for Batch Re - keying Operations in Secure Multicast [C]//Proceedings of the 39th Hawaii International Conference on System Sciences. [s. l.]:[s. n.], 2006.
 - [10] 屈 劲,葛建华,蒋 铭.安全多播密钥批更新算法研究[J].电子学报,2003,31(7):1047-1048.
 - [11] 赵 欣,吴敏强,陈道蓄,等.一个自适应的安全组通信密钥更新算法[J].电子学报,2003,31(5):656-658.
-
- (上接第 183 页)
- [6] 李 玮,侯整风. SSL 协议安全缺陷分析[J]. 计算机技术与发展,2006,16(12):224-226.
 - [7] Dandash O, WU Xiaoping, Le Phu Dung. Wireless Internet Payment System Using Smart Cards[C]//Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'05). Nevada: IEEE Computer Society, 2005.
 - [8] WU Xiaoping, Dandash O, Le Phu Dung. The Design and Implementation of a Smart phone Payment System based on Limited - used Key generation scheme[C]//Proceedings of the Third International Conference on Information Technology: New Generations (ITNG'06). [s. l.]:IEEE Computer Society, 2006.
 - [9] 邢书宝,李 刚,薛惠锋.一次一密加密系统设计与实现[J].计算机技术与发展,2007,17(3):150-152.
-
- (上接第 186 页)
- #### 参考文献:
- [1] 盛津芳,王 斌,陈松乔.方面化构件模型及其组装方法[J].计算机工程,2006,32(5):39-40.
 - [2] Hilsdale E, Hugunin J. Advice weaving in aspect[C]//Proc. of the 3rd International Conference on Aspect - Oriented Software Development (AOSD 2004). Lancaster, UK: ACM Press, 2004:26-35.
 - [3] 陈 成,李 行.基于 AOP 的 MDA 模型转换[J].计算机技术与发展,2008,18(7):87-90.
 - [4] 古全友,王恩波,胥昌胜. AOP 技术在 J2EE 系统构建中的应用[J].计算机技术与发展,2006,16(4):150-152.
 - [5] 钱竹青,邹正武. Eclipse AspectJ——利用 Eclipse 和 AspectJ 进行面向方面程序设计[M]. 北京:清华大学出版社, 2006.
 - [6] Nicholas L. Using AspectJ Enhancing Design Patterns[EB/OL]. 2005. <http://www-128.ibm.com/developerworks/>.
 - [7] 王 斌,周 亮,谭云桥,等.基于类修改和反射的动态方面编织模型[J].计算机工程与应用,2008,44(7):82-85.
 - [8] SUN. Introduction to JAAS Authorization[EB/OL]. 2002-11. <http://java.sun.com/j2se/1.4.2/docs/guide/>.