浅析基于支付标记化技术的移动支付安全方案

张慧琳[1] 赵云辉[2]
(1.清华大学信息化技术中心 北京 100084;2.北京江南天安科技有限公司 北京 100085)

【摘 要】为探索迅速发展和广受关注的移动支付安全问题,分析了支付标记化技术的特点和优势,研究了 Apple Pay 的支付应用模式和关键技术,阐述了 Android 平台的 HCE 技术以及基于 Token 技术的 Android 设备移动支付安全模式,表明了基于支付标记化技术的移动支付问题的发展趋势。

【关键词】支付标记化技术;令牌;Apple Pay;HCE
【中图分类号】TN409 【文献标识码】A

Research on Mobile Payment Security Solutions Based on Payment Tokenization Technology

Zhang Hui-lin[1] Zhao Yun-hui[2]
(1. Information Technology Center, Tsinghua University Beijing 100084;
2. Beijing JN TASS Technology Co.,Ltd Beijing 100085)

【Abstract】In order to explore the rapid developing and widely discussed mobile payment security issues, analyzes the characteristics and advantages of payment tokenization technology, studies payment application mode and key technology of Apple Pay, and demonstrates the HCE (Host-based Card Emulation) technology of Android platform and the token technology applied in the mobile payment security control process on Android devices, which indicates mobile payment security solution development trend in the near future.

【Keywords】tokenization; token; apple pay; hce

1 引言

随着智能手机和移动网络的迅猛发展,移动支付进入了千万人的生活,移动支付的安全问题也随之而来。支付标记化技术(Payment Tokenization)的推出为支付业务提供了一个相对安全且便捷的解决方案,苹果公司和谷歌公司在 IOS 和 Android 平台下都进行了相应的探索和实践。本文将针对基于支付标记化技术的移动支付安全方案进行探讨。

2 支付标记化技术(Payment Tokenization)

支付标记化技术是由国际芯片卡标准化组织 EMV Co 于 2014 年正式发布的一项最新技术,原理在于通过支付标记(Token)代替银行卡号进行交易验证,从而避免卡号信息泄露带来的风险。支付标记化使用唯一数值替代传统的银行卡主账号,同时确保该值的应用被限定在特定的商户、渠道或设备上。支付标记可以运用在银行卡交易的各个环节,与现有基于银行卡号的交易一样,可以跨行使用,具有通用性。简单地说,支付标记就是银行卡卡号的别名,这个别名可以在一个开放的支付环境中使用,代理机构和银行间的网络是安全和可信的,使用时由银行信任的代理机构与银行间进行银行卡卡号和别名的交互,来完成支付操作。

长期以来,在使用贷记卡(信用卡)进行支付操作时,POS 机与银联之间所传递的交易信息主要是银行卡

卡号，所生成的标记即是手工签名。当然，近年来国内的信用卡可以设置个人密码来保障交易安全，但这仅限于在国内的交易，在网上支付时，所采用的保障主要是信用卡背面的 CVV 码。

目前针对银行卡的交易风险主要是银行卡卡号的盗取，但随着国内金融 IC 卡的推广和普及，银行卡的复制、盗刷将会大大减少，而针对移动支付的便捷性和安全性还有待于进一步的加强。由国内电信运营商主导的基于 SIM 卡的 NFC 支付方案因其复杂的应用模式及众多的参与方，至今还未得到广泛的应用，而 EMV 组织推出的标记化技术在支付的便捷性和安全性则具有一定优势。

3 苹果支付（Apple Pay）应用模式

2014 年 9 月 9 日，苹果公司在加州库比蒂诺德安萨学院的弗林特艺术中心正式发布新一代产品 iPhone 6/6 Plus，最引人注目的是苹果公司在发布会上提出了新的支付方式 Apple Pay。Apple Pay 由 NFC 近场通信技术、Touch ID 指纹识别、安全控件以及 Passbook（电子票券管理工具）组成，使用时只须手指按在 home 键的指纹识别上，手机靠近支付 POS 终端，即可完成支付。Apple Pay 目前已与美国运通、万事达以及 Visa 合作，支持包括赛百味、麦当劳等 22000 家商店进行支付。2014 年 10 月 20 日，苹果公司的“苹果支付”服务正式在美国上线，使用者需要先将设备的操作系统升级到最新的 iOS8 版本，支持该功能的手机只有 iPhone6 和 iPhone6 Plus，仅限于美国境内使用。

一直以来，苹果公司推出的产品以极致的用户体验而著称，Apple Pay 更是如此。可以说 Apple Pay 集成了苹果公司的多项尖端的产品应用技术和其对移动支付领域极其深入的理解。简单地说，Apple Pay 就是用 iPhone 代替了信用卡实体卡片，并且省去了手动签名。

深入地理解 Apple Pay，会发现实质并不像表现那样简单。想使用 Apple Pay，首先要绑定信用卡，在 iPhone 输入信用卡信息，Apple Pay 把信用卡信息发送到卡组织处验证，卡组织验证通过后，会为这张信用卡生成一个 Token，并将 Token 发送到 Apple Pay，Apple Pay 再把这个加密的 Token 发送到 iPhone。iPhone 上不直接存储信用卡信息，而是将 Token 存放在 iPhone 中的独立安全芯片中（SE 芯片），用它代替信用卡的卡号，可以理解为 Token 和信用卡的卡号等价，但即使 Token 泄漏，也无法逆向还原出信用卡信息。这个 Token 的存储和管理也不容小看，它是由苹果公司早在 2012 年推出的一个电子票证、登机牌、积分、优惠券等的管理工具 PassBook 来管理的。Token 的格式其实是一个 16 位字符串，它与传统 POS 机协议里的格式是兼容的，这意味着 Apple Pay 兼容整个传统信用卡支付网络。无论是刷信用卡，还是用 Apple Pay，在整个传统支付体系中都是透明的。在使用时，还有关键一环“Touch ID”，只有指纹认证通过的时候，iPhone 才允许利用 NFC 读取 Token 出来。

图 1 传统信用卡支付与 Apple Pay

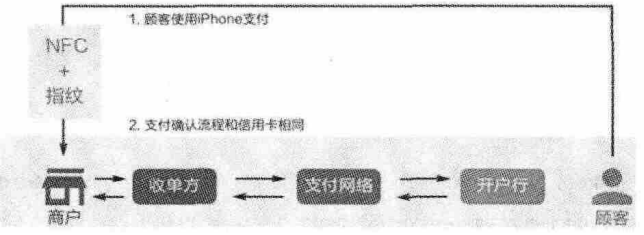

图 2 Apple Pay 支付确认流程

可以看到，Apple Pay 中有几个关键因素。NFC：全终端的方案，摆脱了电信运营商的羁绊；SE（Secure Element）：苹果公司自家芯片的硬件解决方案；Touch ID：指纹保存在 Secure Enclave 中；PassBook：之前采用蓝牙技术（iBeacon），目前配合 NFC 管理 Token；Token：标记化支付应用。

通过以上解决方案，Apple Pay 为用户带来了极致的体验，最大的特点是没有减少传统支付体系中的任何一方，但是给了这个支付行业最便捷和安全的支付体验。Apple Pay 可以看作是基于 Token 技术的典型应用，在这个新型的支付模式中有几个新的参与方使得这种模式的推广充满新的机遇。

传统的支付方式中参与方包括：顾客——刷卡方；商户——提供商品，接收刷卡方式；支付通道——POS 终端及通讯网络；收单方——一般为卡组织，如 Visa、Master 等，在国内主要是银联或第三方支付公司；发卡行——信用卡发行银行。

Apple Pay 中应用了 Token 技术，所以较上述流程又增加了两个环节：TR（Token Requestor）：Token 申请方，即 Apple Pay；TSP（Token Service Provider）：Token 服务方，在 Apple Pay 体系中，为 EMV 组织。

TSP 根据 TR 提供的用户主账号（PAN）与发卡行协商生成 Token 后，将 Token 作为 PAN 的替代值，流转在支付的各个环节，使得在支付流程中独一无二的 PAN 只在 TSP、转接方、发卡方之间传递，由于三者专线连接且彼此互信，且当 Token 被检测到风险或到期时，将再次生成新 Token 替代，从而大幅降低支付过程中 PAN 泄漏的可能性，极大地提高了 PAN 的安全性。

由此可以得出，Apple Pay 本质上还是一种联机刷卡的解决方案，没有改变传统的支付模式，虽然支付过程参与方增加，但增加的参与方仍是之前的各方，所做的改变是增加了安全保障和提升了用户体验，利益方并没有大的改变，对于使用者来说，这种改变是安全和高科技带来的便捷。

4 Android 平台的 HCE 技术与 Token 应用

谈到苹果公司的 IOS 系统，就不能不提及目前在智能手机行业占据大部分市场的 Android 平台。谷歌公司于 2011 年发布了基于 Android 平台的谷歌钱包（Google Wallet），较早地提出了基于 NFC 技术的虚拟信用卡支付的概念，但当时仅有使用 Sprint 运营商网络的三星 Nexus S 4G 手机能使用此项功能。由于 Android 平台采用了基于 SWP 协议的 NFC 模式，因此无法摆脱对电信运营商的依赖，该模式下的 NFC 移动技术在国内始终处于一种叫好不叫座的状态。在 2013 年 Google 公司发布了 Android 4.4 KitKat 版本，新增一种系统服务 HCE 技术，即基于主机的卡仿真（Host-based Card Emulation），这是一种以 App 或云端实现安全认证的 NFC 接口，可以取代基于 SWP 协议的 NFC 应用，改变了必须使用电信运营商 SIM 卡作为 SE 的模式。

HCE 架构由 NFC 主控芯片收集数据，直接经手机 CPU 传送到 App，HCE 使得 NFC 手机可以在没有硬件 SE 的情况下采用卡模拟模式进行 NFC 支付，任意 App 都可以模拟一张 SE 直接和 Reader 进行通信。HCE 架构的安全模式为 APP 内部认证或通过移动网络进行云端认证，App 内部认证的安全保障主要靠 Android 内部的安全域（SandBox），云端则是依靠公开密钥基础设施（PKI）。

在国内智能手机领域，Android 平台是首屈一指的，Token 技术是否适用 Android 平台呢？接下来我们以高安全度的 HCE 云端认证方式来探讨 Token 技术的应用。

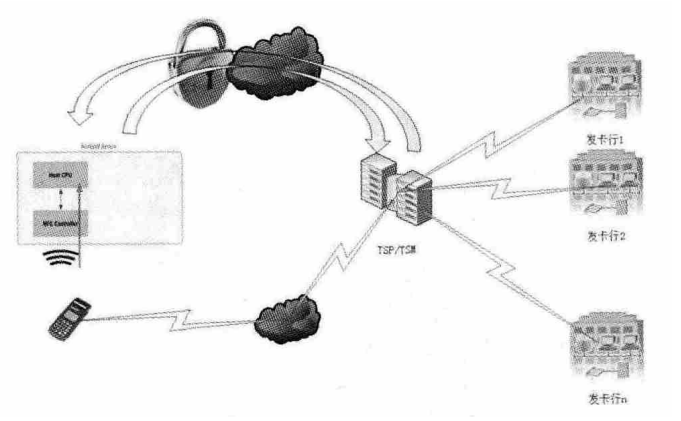

图 3 HCE 云端认证方式

HCE 模式的支付系统由手机端 App、TSP（Token Service Provider，Token 服务方）、TSM（Trusted Service Manager，可信服务管理）、发卡行、商户等几部分组成，核心是手机端 App 和 TSP、TSM 间的安全通讯。这个过程可以由非对称密钥体系来保护。非对称密钥体系可以采用国密算法 SM9，手机端和 TSP 端采用指定公钥的方式生成密钥对，其中公钥包含了三个部分：用户密码、随机数和 IMEI（International Mobile Equipment Identity，移动设备国际识别码）。

用户密码和 IMEI 不需 App 保存，IMEI 在使用时从手机内读取即可，而用户密码则是每次使用时用户主动输入，App 内保存的只有一个随机数，随机数的加入是为了防止中间人攻击。这种方式的安全性在于密钥的分散保存和用户的自主性，极大地降低了对手机安全性的要求。手机端 App 将上述三个部分经计算后的数据发送到 TSP 或 TSM，由系统根据此来计算生成对应的密钥对并用于通过程中的数据加密。

交易过程中的数据采用加密通讯，加密密钥由 TSP 端每次随机生成，使用公钥加密后传递给手机 App，由手机 App 解密后在内存中暂存。Token 由私钥加密后保存在 App 的安全域（SandBox）中，在交易过程中，手机 App 不解密，直接经由通讯加密密钥加密后传输给 TSP。TSP 使用通讯加密密钥解密后，再使用公钥解密获取 Token 原文，再将 Token 转换为用户信用卡卡号，由 TSP 通过专用网络与发卡行进行通讯，完成交易。

【下转第 14 页】

不同层次的模糊判断矩阵，根据目标层、准基层、决策层的模糊对矩阵进行判断，例如：当 C1=（1,1,1）时，C11=C12=C13=(1,1,1)。采用这种二分法或许各个层次相对应的模糊矩阵，同时把次矩阵特征化方法进行模糊。获取如下结果：准则层相对于目标层权重(wi)，物理、逻辑、安全管理数据为：0.22、0.47、0.31。随之对应用层次单排序方根法实施权重单排序，同时列出相对于的最大特征根 max。为确保判断矩阵的准确性和一致性，必须对模糊化之后的矩阵实施一致性检验，计算出一致性指标 CI、CR 数值，其中 CI=(λ_{max}—n)/(n—1)，CR=CI/RI，当 CR<0.1 的时候，判断矩阵一致性是否两否，不然实施修正。最后使用乘积法对最底层的排序权重进行计算，确保或许方案层相对于目标层的总排序权重。

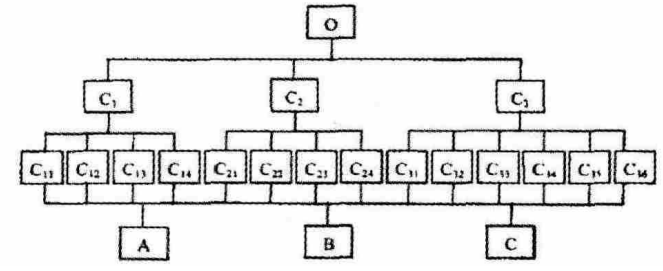

图 2 层次结构模型实例图

5 结束语

综上所述，为了能够准确地进行计算机网络安全评价，通过应用模糊层次分析法，可提高评价的客观性、准确性，进而获取最佳的评价效果，确保计算网络安全。

参考文献

[1] 代金勇.模糊层次分析法在计算机网络安全评价中的应用[J].成功(教育版),2012,(5):292.

[2] 郑刚.计算机网络安全分析研究[J].网络安全技术与应用,2014,(8):162,164.

[3] 章丽娟,王清贤.模糊层次分析法在网络安全态势评估中的应用[J].计算机仿真,2011,28(12):138-140.

[4] 李方伟,杨绍成,朱江等.基于模糊层次法的改进型网络安全态势评估方法[J].计算机应用,2014,34(9):2622-2626.

作者简介：

顾方勇(1978-)，男，汉族，河北献县人，学士，海军信息化司，工程师；主要研究方向和关注领域：信息安全。

刘福强(1976-)，男，汉族，辽宁鞍山人，硕士研究生，海军装备研究院，工程师；主要研究方向和关注领域：信息安全。

【上接第 5 页】

TSP 获取到交易成功或失败的信息后，再将此信息经由加密通讯密钥加密传送给手机端，从而完成全部交易流程。

在这个交易过程中，NFC 的安全脱离了电信运营商的 SIM 提供的 SE，APP 的安全认证由 HCE 在云端采用非对称密钥体系完成，Token 保存在 APP 中，Token 的交换过程与 Apple Pay 相同，差别在于从手机中 Token 的获取过程，Apple Pay 通过 Touch ID 来实现，而 Android 的 HCE 则由非对称密钥体系保护在云端完成，从使用的安全性来说相差不多，但从国内的金融环境和智能手机形态来说，这种方式即摆脱了电信运营商的限制，又极大的减化了安装部署的工作，提升了使用的便捷性。

5 结束语

从目前 Apple Pay 的使用情况来看，Token 化的信用卡交易确有其便利性和安全性，结合国内的情况，基于 Android 平台的 HCE 接口采用 Token 化的信用卡交易也能够在保障安全的前提下实现交易的便捷性，结合非对称国有算法以及在运算过程中增加了随机数的参与，也极大的提高了交易的安全性。可以预见不久的将来，Token 将会演化出更多的形式走进每个人的移动生活中。

参考文献

[1] 谢云，张文安.浅析 Apple Pay 对国内移动支付产业的影响[J].广东通讯技术,2014,12:2-5,37.

[2] 苏晓燕. 基于 NFC 技术的 Android 移动支付终端的设计与实现[D]. 成都：西南交通大学,2013.

[3] 李庆艳，张文安，张涛. NFC 产业分析及应用前景展望[J].电信技术,2012,05:47-49.

作者简介：

张慧琳(1983-)，女，硕士，清华大学信息化技术中心，工程师；主要研究方向和关注领域：校园卡、财务信息化。

赵云辉(1977-)，男，本科，北京江南天安科技有限公司，产品经理，高级工程师；主要研究方向和关注领域：RFID 与信息安全。