doi:10.3772/j.issn.1002-0470.2021.06.002

一种基于 TPM 的手机第三方安全移动支付协议①

刘永磊②[*,**] 金志刚[*] 郝 琨[**] 张伟龙[***]

([*]天津大学电气自动化与信息工程学院 天津 300072)

([**]天津城建大学计算机与信息工程学院 天津 300384)

([***]河北交通职业技术学院质量管理中心 石家庄 050035)

摘 要 为解决 in-APP 第三方支付中密钥泄漏、信息显示不全、商家 APP 缺乏预信任等问题,采用着色 Petri 网(CPN)模型对现有的订单篡改、通知假冒、订单替换、非授权查询 4 种攻击进行建模分析,并通过推导不安全状态的可达性验证 in-APP 第三方支付系统存在的安全漏洞。提出了基于可信平台模块(TPM)的新的支付协议模型,该模型利用 TPM 生成安全私钥用于改进数字签名和防止用户和商家 APP 串谋攻击等方面。安全性分析表明,相较于原协议,新的安全模型引入随机数抵御重放攻击,通过 TPM 安全芯片生成公私钥对,抵御因密钥泄漏引发的订单篡改与替换、通知假冒和非授权查询 4 种网络攻击,并通过协议中的额外安全性补偿机制解决了串谋攻击和订单信息显示不全等问题。

关键词 电子商务;移动支付;第三方;着色 Petri 网(CPN);可信计算模块(TPM)

0 引 言

随着我国国民经济的发展以及移动通信、物联网与人工智能等相关领域的发展,移动电子商务[1]发展迅猛,已成为我国经济增长和产业转型的重要力量。在移动电子商务中,整个移动交易包含了商品推送、商品浏览、下单、移动支付、收货以及交易评价等环节。其中,移动支付[2]是用户使用其移动终端对所消费的商品或服务进行账务支付的方式,现今已衍生出缴费、借贷、权属交易等多种金融业务。然而移动终端为多接口网络设备,存在多个网络出入口,如近场通信(near field communication, NFC)、Wi-Fi、4G/5G 等,以及不同于传统个人电脑机的体系结构,其安全性更为复杂[3]。相较于传统的移动支付系统,微信[4]、支付宝[5]、PayPal[6]等第三方交付系统结合各种手机应用内(in-APP)支付,如手机游戏、手机电子书、手机电子商城等,用户无需切换到其他应用或者网页浏览器通过 PIN 码、指纹、刷脸等多种认证和输入密码方式完成支付,极大地提高了用户便利性和体验,迅速占领市场。但系统涉及多个交易参与者(如 in-APP 支付),加之商家 APP 的自主开发,欠缺安全编码规范等问题导致第三方支付的安全性面临更多威胁[7]。

目前,国内外学者从移动支付系统的体系结构各层出发,对各层安全性进行分析和评价并提出了一些安全改进与防御策略。应用层安全主要针对各种手机恶意代码、Web 安全威胁对移动支付系统的危害,相关研究包括了手机恶意软件的检测,安全的编程接口,统一的安全支付软件标准,手机隐私保护、Web 服务安全等[8-10]。传输层安全主要针对移动支付协议的安全性分析和改进。其典型包括 SET 协议的建模和漏洞分析[11],SET 协议改进如预付款机制等,基于预信任与公共服务域的移动支付协议

① 国家自然科学基金(61902273)资助项目。

② 男,1983 年生,博士,副教授;研究方向:网络安全,区块链;联系人,E-mail: liuyonglei@tcu.edu.cn

(收稿日期:2020-06-14)

族[12]，基于 EMV 信用卡的手机支付协议[13]，基于 SMS 的移动支付协议[14]，基于对称密钥的中心支付网关模型的安全支付协议，基于 U2F 的移动支付双向认证协议[15]，专门针对 NFC 手机支付的安全移动支付协议[16-17]。网络层安全主要研究移动支付系统中网络通信技术的安全性，如 NFC 通信技术、无线局域网、移动通信技术安全等[18-20]。物理层安全主要针对智能手机控制的硬件安全与操作系统（Android 和 iOS）安全，以及进行数据处理与支付的云服务器安全等[21,22]。另外，从总体安全性分析角度，有学者对移动支付系统建立安全指标进行安全性评估[23]，使用层次分析法、D-S 证据理论、神经网络、粗糙集理论等。也有学者从交易者本身出发，从社会学角度考虑交易声誉、交易双方样貌与性别和交易数额，来对交易的安全风险进行评估[24]。

随着第三方 in-APP 支付的持续发展和安全研究工作的深入，已有以下成果涌现。（1）针对第三方支付服务器和电子银行之间支付协议安全性的改进，文献[25]提出一种修正的 HARQ 加密方案，利用群签名和椭圆曲线函数提高加密协议的执行效率。文献[26]利用第三方支付各参与方相互认证，并利用动态密钥和哈希运算来加强安全性抵御假冒攻击、APP 被盗、字典攻击等。（2）针对用户与第三方支付服务器之间的支付协议安全，文献[27]利用 NTRU 密钥体制，构建公钥基础设施，提高系统安全性抵御量子攻击。文献[6]针对 in-APP 第三方支付的流程分析了现有的 4 种攻击，包括订单篡改、通知假冒、订单替换和非授权查询，并进行了攻击案例研究。但该研究仅限于经验分析，并未给出攻击建模与验证，也未给出明确的改进建议和措施。（3）有学者认为第三方支付虽然方便了用户，但存在第三方依赖、系统更新困难、交易延迟等问题，因此从网络架构规划角度提出了直接连接银行和用户的移动支付通信模型[28]。亦有学者使用量子盲签名和引入可信第三方来解决第三方支付隐私性、整体安全性和系统计算复杂性高等问题。由于现今第三方支付在我国已经绝对垄断了市场，鉴于第三方支付服务器与电子银行之间，以及用户最后一步手机支付由微信和淘宝等巨头安全公司开发维护，其在安全设备、算法、通信协议等方面安全强度较高，鲜有漏洞，因此本文重点研究第三方 in-APP 支付内安全漏洞较多的前端协议如订单生成、订单协商等过程中的系统安全性。

本文通过分析 in-APP 第三方支付的体系结构和支付流程，并与传统 Web 支付进行比较，指出 in-APP 第三方支付易造成密钥泄漏、信息显示不全、商家 APP 缺乏预信任等问题。使用着色 Petri 网（color Petri net，CPN）模型进行建模分析现有的针对 in-APP 第三方支付的网络攻击，并推导不安全状态的可达性。最后，提出了基于可信平台模块（trusted platform module，TPM）的新的支付协议模型，该模型利用 TPM 生成安全私钥用于改进数字签名和防用户和商家 APP 串谋攻击等方面。安全性分析表明，新的安全模型可以抵御现有的针对 in-APP 第三方支付的网络攻击并解决了密钥泄露、订单信息显示不全等问题。

1 in-APP 第三方支付支付模型

本节主要对现有的移动支付系统，以及 in-APP 第三方支付系统进行描述和建模。并且全文的第三方支付系统讨论范围限定为微信与支付宝。

典型的移动支付系统[29-30]分为应用层、传输层、网络层和物理层（如图 1 所示）。其中应用层为交易双方提供移动支付服务的 APP 软件和 Web 服务。传输层为保障交易安全所使用的各种移动支付网络协议。网络层为交易双方提供网络接入服务如 RFID、NFC、4G、WiFi、有线网络等。物理层为用户使用的安全移动终端以及为交易双方提供存储、计算、数据分析等服务的云服务器。

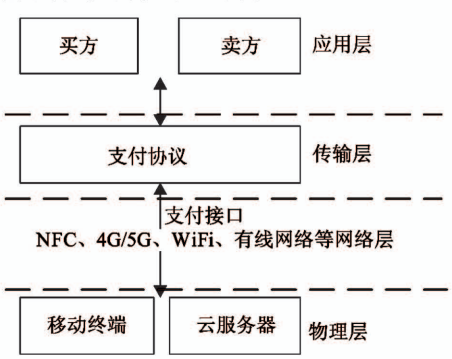

图 1 移动支付系统体系结构

传统的 Web 支付(如图 2 所示),用户直接通过浏览器访问商家服务器浏览商品和服务,订单生成后,用户直接向银行发起支付流程(往往存在支付网关提供网络接入、认证转发等功能,图中略去),获取商品。而 in-APP 第三方移动支付系统[6],相较于传统 Web 支付,如图 2 所示有以下特点。(1)用户通过安装在手机上的商家 APP 内浏览商品和服务。(2)用户在商家 APP 订购商品或服务后,商家 APP 生成订单,并发给远程的商家服务器。(3)商家服务器核实订单(订单 ID、商品数量、金额、商家 ID、支付 URL 地址等),回复给商家 APP 确认,其中微信由第三方支付服务器生成订单确认,支付宝直接由商家服务器生成。(4)商家 APP 在屏幕显示订单支付信息。(5)用户确认后进行第三方支付,如输入 PIN 码、刷脸、指纹等。(6)第三方支付服务器通过安全支付协议与银行进行买家扣款,卖家收款操作。(7)第三方支付服务器向买卖双方发送支付成功确认。(8)买家支付成功向商家获取商品或服务。(9)商家服务器向第三方支付服务器核实订单,或者查询历史订单数据。

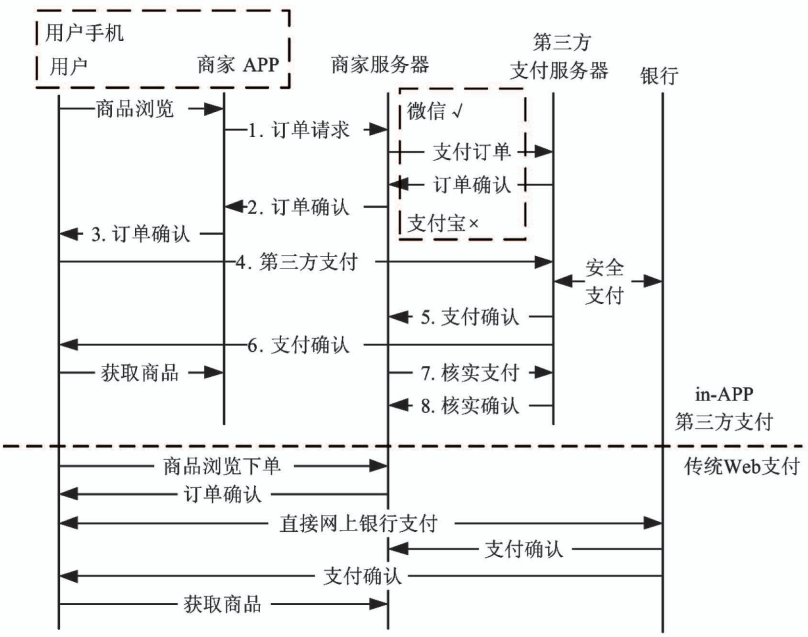

图 2　in-APP 支付流程

2　in-APP 第三方支付攻击建模

本文将使用着色 Petri 网(CPN)模型对 in-APP 第三方支付进行建模,并进行安全性分析。

2.1　攻击描述

in-APP 第三方支付系统为保证支付协议数据完整性和防篡改,使用数字签名机制,其中微信采用带密钥的密钥双方共享,支付宝使用 RSA 公私钥签名机制。相较于传统 Web 支付,由于商家 APP 就驻留在用户手机内,恶意代码和提权漏洞等极易造成攻击者较易获得手机控制权发动攻击。同时由于缺乏安全开发规范,还存在 APP 订单界面显示不全、安全算法错误配置(不验证签名)、不确认等漏洞。另外,对于第三方支付平台和银行之间的安全设备、算法、通信协议的预信任,本文不做讨论。假设攻击者已经攻破用户手机,签名密钥泄露,$M_1 \sim M_8$ 对应图 2 中的 8 个流程。

(1)订单篡改与替换攻击,攻击者通过仿冒商家 APP,或者在商家 APP 与商家服务器之间充当中间人,最终导致用户接收篡改的订单 M_3',由于订单显示不全,如未显示商家名称或订单所有者,因此用户无法识别被篡改的订单,导致资金损失。

(2)通知假冒,攻击者选择商品或者服务后,通过仿冒第三方支付服务器给商家服务器发送伪造的支付确认消息 M_5',而商家也忽视了支付核实 M_7、

M_8，导致攻击者可以不付费就享受商品或服务。

（3）非授权查询，由于密钥泄露，攻击者可以通过与第三方服务器交互 M_7 和 M_8，非法获取历史数据，经过数据分析进行打击商业对手、获取用户隐私等活动。

2.2　CPN 模型

CPN 是一种建模和验证系统的语言，用来设计、描述、模拟和验证复杂的系统。在网络通信、协议分析、资源共享、安全协议形式化验证等领域有广泛的应用[31]。本文采用 CPN 对 in-APP 第三方支付进行建模和安全性分析。限于篇幅，本文以支付宝订单替换的中间人攻击为例，说明 in-APP 第三方支付的安全性，并对模型做适当简化仅保留 $M_1 \sim M_6$，引入攻击后的 CPN 模型如图 3 所示。

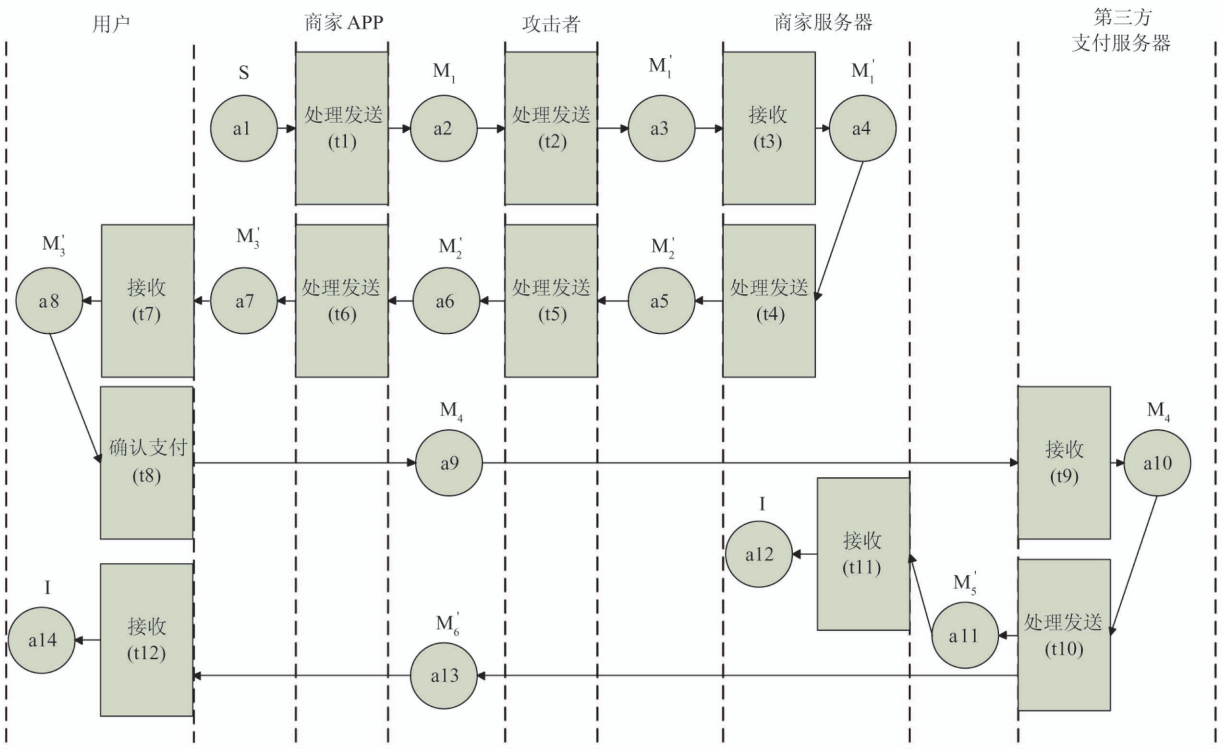

图 3　订单替换攻击模型

基于着色 Petri 网的 in-APP 第三方支付协议分析步骤如下。

（1）确定要分析的协议，并给出协议的 CPN 模型。

（2）确定 CPN 模型中攻击者可能修改的变量，并进一步找出 CPN 模型中不影响合法用户数据接收而可以被入侵者篡改的输出数据，然后给出引入攻击者的协议攻击者模型，包括初始状态、不安全状态等。

（3）根据协议攻击者模型建立状态方程，如式（1）所示。

$$M_n = M_0 + \boldsymbol{A}\sum_{i=1}^{m}\boldsymbol{\sigma}_i^t \tag{1}$$

其中，M_n 为不安全状态，M_0 为初始状态，$\boldsymbol{\sigma}_i^t$ 为变换向量表示哪个变迁发生，$\sum$ 为求和符号表示每个变迁可点火多次，$\boldsymbol{A}$ 为变换矩阵。

（4）利用矩阵分析法，结合线性代数中方程组解的判别方法判定方程有否有解向量 $\boldsymbol{\sigma}^t$。如果方程有解，表明不安全状态 M_n 可由初始状态 M_0 可达。如果可达，证明协议有安全漏洞。

在 in-APP 第三方支付协议中，定义不安全状态为 a12 和 a14，M_4 表示第三方支付流程，虽然用户支付了恶意订单，但第三方支付过程并未被攻击，因此依然用 M_4 表示。假定此时攻击者通过获得手机控制权，破解了商家 APP 用于签名的私钥，因此可以伪造订单，最终导致用户因为订单显示不全，支付了错误的恶意订单。类似地，微信安全风险更高，若破解商家服务器，第三方支付服务器的签名密钥也造

成泄漏。

$\boldsymbol{M}_0^{\mathrm{T}}=[\mathrm{S},0,0,0,0,0,0,0,0,0,0,0,0,0]$ 为 14 维行向量,表示用户浏览下单开始协议流程。

$\boldsymbol{M}_n^{\mathrm{T}}=[0,0,0,0,0,0,0,0,0,0,0,\mathrm{I},0,\mathrm{I}]$ 为 14 维行向量。表示用户支付非法的恶意订单并获得确认完成。

$\boldsymbol{\sigma}_i^t$ 为 12 维列向量。$\boldsymbol{A}(S_i,\ T_j)$ 为变换矩阵,S_i 依次为 a1 ~ a14。T_j 依次为 t1 ~ t12。$\boldsymbol{A}$ 为 14 × 12 矩阵($A_{[1][1]}$ - $A_{[14][12]}$),篇幅所限不详尽列出,如 $A_{[1][1]}=-\mathrm{S}$, $A_{[7][6]}=\mathrm{M}_3'$, $A_{[12][11]}=\mathrm{I}$, $A_{[13][12]}=-\mathrm{M}_6'$。同理可确定变换矩阵 $\boldsymbol{A}$ 的取值。

将 $\boldsymbol{M}_0^{\mathrm{T}}$、$\boldsymbol{M}_n^{\mathrm{T}}$ 和 $\boldsymbol{A}(S_i,\ T_j)$ 代入式(1),利用线性代数中方程组解的判别方法可判定 $\boldsymbol{\sigma}^t$ 有解,说明不安全状态 M_n 由初始状态 M_0 可达,因此 in-APP 第三方支付协议存在安全漏洞,据此可发动订单替换攻击。

3 基于 TPM 的 in-APP 第三方支付改进

可信计算[32]在系统中引入基于 TPM 并带有信任根的安全芯片[33],通过信任链条,将信任关系传递到整个系统中的其他组件或程序,从而形成整体的系统安全解决方案。因此,本文设计了基于 TPM 的 in-APP 第三方支付安全协议(以 M_1 ~ M_8 协议交互为例)。以图 2 中支付宝的支付流程为例,订单确认直接由商家服务器生成,由于篇幅所限,原协议细节可参阅文献[6]。

3.1 机制描述

假定所有主体(商家 APP 除外)都嵌入了 TPM 模块或移动 TPM[34]模块(用于智能手机),并生成用户(U)的公私钥对($\mathrm{PK_U}$,$\mathrm{SK_U}$),商家服务器(S)的公私钥对($\mathrm{PK_S}$,$\mathrm{SK_S}$),第三方支付服务器(T)的公私钥对($\mathrm{PK_T}$,$\mathrm{SK_T}$)。由于商家 APP(A)安装在用户智能手机内,其公私钥对($\mathrm{PK_A}$,$\mathrm{SK_A}$)由用户手机的内嵌 TPM 生成并保证各不同 APP 的公私钥对相互独立。但无法防止用户和商家 APP 串谋攻击问题,因此后续给出安全补偿机制。用户 id 协议流程为原协议[6]交互的每步均由对应的参与者对消息进行签名,接收者使用发送者的公钥验证签名,如图 4所示。

$(\mathrm{M_1})$A->S: $\mathrm{r}||\{\{\mathrm{r}\}\ \mathrm{SK_U}\}\mathrm{SK_A}$
$(\mathrm{M_2})$S->A: $\mathrm{c}||\{\mathrm{c}\}\mathrm{SK_S}$
$(\mathrm{M_3})$A->U: $\mathrm{c}||\{\{\mathrm{c}\}\ \mathrm{SK_S}\}\mathrm{SK_A}$
$(\mathrm{M_4})$U<->T: 第三方支付交互(忽略改进)
$(\mathrm{M_5})$T->S: $\mathrm{a}||\{\mathrm{a}\}\mathrm{SK_T}$
$(\mathrm{M_6})$T->U: $\mathrm{aa}||\{\mathrm{aa}\}\mathrm{SK_T}$
$(\mathrm{M_7})$S->T: $\mathrm{v}||\{\mathrm{v}\}\mathrm{SK_S}$
$(\mathrm{M_8})$T->S: $\mathrm{vc}||\{\mathrm{vc}\}\mathrm{SK_T}$
说明: $\mathrm{r=ID_U||ID_S||Goods_{info}||Price||N_1}$;
$\mathrm{c=ID_{Order}||ID_U||ID_S||Goods'_{info}||Price'||N_1||N_2}$;
$\mathrm{a=ID_U||ID_S||Pay\ time||ACK||N_3}$;
$\mathrm{aa=ID_U||ID_S||Pay\ time||ACK||N_4}$;
$\mathrm{v=ID_S||Query\ parameters||N_5}$;
$\mathrm{vc=ID_S||Pay\ query\ results||N_6}$;

图 4 第三方支付协议模型

主要改进和安全补偿机制有如下步骤。(1)增加 Nonce 保证协议的新鲜性,抵御重放攻击,同时接收方比对 Nonce 也是辅助认证手段。(2)第一步 $\mathrm{M_1}$ 用户在商家 APP 内发出的订单请求应包含用户签名。(3)协议中订单确认消息只能有商家服务器发出,第三步 $\mathrm{M_3}$ 修改为商家 APP 转发订单确认并保留 S 的签名。(4)第四步用户第三方支付,交互消息如 PIN 码、指纹、刷脸等,商用应用广泛,安全强度良好,因此本协议忽略改进。(5)由于商家 APP 驻留在用户手机内,其公私钥是由用户 TPM 生成,为防止串谋攻击,商品或者服务均应正确付费后从商家服务器上远程获取,而不能从 APP 上直接获取。(6)若需要提供数据机密性防止基于数据分析的恶意商业信息泄露和保护用户隐私,可以使用 TPM 芯片派生会话密钥用于保密数据传输。

3.2 安全性分析

本节将从新提出的安全机制是否能抵御现有 4 种攻击的角度来分析其安全性。

安全假设。TPM 和相关组件正确部署,使用的数字签名不可伪造,选取的 Hash 函数是抗碰撞的。协议 4 个参与方除商家 APP 外均身份(私钥)无法仿冒。

(1)订单篡改与替换

攻击发生在 $\mathrm{M_1}$,由于各个商家 APP 的 $\mathrm{SK_A}$ 相互独立,攻击者无法通过自己发布商家 APP 驻留用户手机后获得其他 APP 的 $\mathrm{SK_A}$,根据安全假设,未获得 $\mathrm{SK_A}$ 敌手不能伪造订单的签名,因此攻击失败。若攻击者通过提权、手机操作系统漏洞等破解

SK_A，由于 M_1 保留有用户签名，根据安全假设，未获得 SK_U 敌手依然不能伪造订单的签名，攻击失败。攻击发生在 M_2，商家服务器的 SK_S 无法仿冒，敌手无法伪造签名，攻击失败。攻击发生在 M_3，同 M_1 类似，未获得 SK_A 敌手不能伪造订单的签名，攻击失败。同理，若攻击者通过提权、手机操作系统漏洞等破解 SK_A，由于保留商家服务器签名，根据安全假设，未获得 SK_S 敌手依然不能伪造订单的签名，攻击失败。若用户与商家 APP 串谋攻击，比如修改订单支付一本电子书，商家 APP 开放两本书阅读权，因改进第(5)步，商品和服务都是商家服务器发出和获取，因此攻击失败。

(2)通知假冒

在通知假冒中，攻击发生在 M_5，第三方支付服务器的 SK_T 无法仿冒，未获得 SK_T 敌手无法伪造签名，攻击失败。

(3)非授权查询

在非授权查询中，攻击发生在 M_7 和 M_8，商家服务器的 SK_S 和第三方支付服务器的 SK_T 无法仿冒，未获得 SK_S 与 SK_T 敌手无法伪造签名，攻击失败。

(4)实用性

随着 TPM 和移动 TPM 的普及，许多笔记本厂商如联想、DELL 等相关智能移动设备出厂就已经安装有 TPM 安全芯片和相关组件，更有学者开发出基于手机 SIM 卡的 simTPM[35]，加之可信软件栈和相关应用开发接口 API 和规范的日趋完善，因此未来本方法具备良好的商用前景。

(5)其他讨论

由于 in-APP 第三方支付受限于开发标准规范难以统一、手机屏幕尺寸、用户体验等问题，订单信息显示不全是 in-APP 通病(用户浏览商品时往往有耐心阅读商品的各个属性和细节，但支付时专注力和耐心下降，希望快速核对订单并支付，继续显示订单的全部属性和细节则会导致多次翻页降低用户体验)。本文的改进第(2)和(3)步可以保证用户和商家之间的订单协商未被篡改，但订单信息显示不全问题仍然会存在，即用户只能看到确认订单的子集。如用户原订单购买的商品或服务，商家确认有 1 个属性发生变化但总价未发生变化，而该属性未在手机界面显示，用户看到总价未变而支付后续将导致买卖纠纷。将协议修改为商家不能修改订单，只能确认或者拒绝订单。可以抵御订单信息显示不全，因为在后台验证签名正确所获得的 $Goods_{info}||Price$ 等于用户先前发送的 $Goods_{info}||Price$ 即可(用户下单时已经认可 M_1)。但本质上属于单方协商，降低了交易成功率，不利于移动电子商务的合理健康发展，值得专家学者进一步探讨。

4 结 论

近年来，随着智能手机、移动通信技术、大数据、云计算和人工智能产业的迅猛发展，移动电子商务已经成为国民经济的重要支柱。第三方支付作为现在的主流支付方式，其安全性更是引来各方关注。本文针对传统的 Web 支付和现在流行的 in-APP 第三方支付从体系结构和支付流程角度进行了详细的分析。并就国内外对于移动支付系统安全性研究的现状进行了总结和综述，在此基础上，针对现有的订单篡改、通知假冒、订单替换、非授权查询 4 种 in-APP 第三方支付攻击利用 CPN 模型进行建模分析攻击的必然性和严重性。接着，本文提出了基于 TPM 的新的安全机制，给出了新的支付协议模型和改进策略。安全性分析表明新协议抵御了上述 4 种网络攻击并解决了密钥泄露等问题，最后，对订单信息显示不全问题进行了探讨。下一步将继续使用 CPN 等相关形式化工具挖掘 in-APP 第三方支付的安全漏洞并作出分析，同时进一步研究订单信息显示不全情况下如何避免交易纠纷的方法。

参考文献

[1] Tang A. A systematic literature review and analysis on mobile apps in m-commerce: implications for future research[J]. *Electronic Commerce Research and Applications*, 2019, 37: 100885

[2] Zhou T. An empirical examination of continuance intention of mobile payment services[J]. *Decision Support Systems*, 2013,54(2):1085-1091

[3] 刘永磊, 金志刚, 高天迎. 移动支付系统安全性研究综述[J]. 信息网络安全, 2017, 2:1-5

[4] 腾讯. 微信支付[EB/OL]. https://pay.weixin.qq.com:腾讯,2020

[5] 阿里巴巴. 支付宝[EB/OL]. https://www.alipay.com:阿里巴巴,2020

[6] Thiel P, Levchin M. PayPal[EB/OL]. https://www.paypal.com:PayPal: PayPal,2020

[7] Yang W B, Li J R, Zhang Y Y, et al. Security analysis of third-party in-app payment in mobile applications[J]. *Journal of Information Security and Applications*, 2019, 48: 102358

[8] 杨宏宇, 那玉琢. 一种 Android 恶意软件检测模型[J]. 西安电子科技大学学报,2019,46(6):45-51

[9] 许艳萍, 马兆丰, 王中华, 等. Android 智能终端安全综述[J]. 通信学报, 2016, 37(6):169-184

[10] Dahlberg T, Guo J, Ondrus J. A critical review of mobile payment research[J]. *Electronic Commerce Research and Applications*, 2015, 14:265-284

[11] 肖茵茵, 苏开乐, 马震远, 等. 实例化空间逻辑下的 SET 支付协议验证及改进[J]. 华中科技大学学报(自然科学版), 2013, 41(7):97-102

[12] 王红新, 杨德礼, 姜楠, 等. 一种终端认证简化的在线移动支付模式与协议[J]. 计算机研究与发展, 2013, 50(2):291-301

[13] Luo J, Yang M. EMV-compatible offline mobile payment protocol with mutual authentication[J]. *Sensors*, 2019, 19(21):4611

[14] Thammarat C, Kurutach W. A secure fair exchange for SMS-based mobile payment protocols based on symmetric encryption algorithms with formal verification[J]. *Wireless Communications and Mobile Computing*, 2018, 2018:1-21

[15] Fan K, Li H, Jiang W, et al. Secure authentication protocol for mobile payment[J]. *Tsinghua Science and Technology*, 2018, 23(5):610-620

[16] Bojjagani S, Sastry V. A secure end-to-end proximity NFC-based mobile payment protocol [J]. *Computer Standards and Interfaces*, 2019, 66: 103348

[17] Thammarat C, Kurutach W. A lightweight and secure NFC-base mobile payment protocol ensuring fair exchange based on a hybrid encryption algorithm with formal verification[J]. *International Journal of Communication Systems*, 2019, 32(12):1-21

[18] Coskun V, Ozdenizci B, Ok K. A survey on near field communication (NFC) technology[J]. *Wireless Personal Communications*, 2013, 71(3):2259-2294

[19] 冯登国, 徐静, 兰晓. 5G 移动通信网络安全研究[J]. 软件学报, 2018, 29(6):1813-1825

[20] 张玉清, 王志强, 刘奇旭, 等. 近场通信技术的安全研究进展与发展趋势[J]. 计算机学报, 2016, 39(6):1190-1207

[21] Zdziarski J. Identifying back doors, attack points, and surveillance mechanisms in iOS devices[J]. *Digital Investigation*, 2014, 11(1):3-19

[22] 卿斯汉. Android 安全研究进展[J]. 软件学报, 2016, 27(1):45-71

[23] Zhang Y J, Deng X Y, Wei D J, et al. Assessment of e-commerce security using AHP and evidential reasoning [J]. *Expert Systems with Applications*, 2012, 39(3): 3611-3623

[24] Yue D, Greory V, Eunsin J, et al. Risk assessment in e-commerce: how sellers' photos, reputation scores, and the stake of a transaction influence buyers' purchase behavior and information processing[J]. *Computers in Human Behavior*, 2018, 84:342-351

[25] 沈荃, 赵宇枫. 修正的 HARQ 加密方案第三方支付系统安全设计[J]. 科技通报, 2014, 30(8):89-91

[26] 莫淦清. 基于相互认证的第三方支付系统认证方案[J]. 控制工程, 2017, 24(3):693-697

[27] Xia Y H, Ying C, Lin G F, et al. A third-party mobile payment scheme based on NTRU against quantum attacks [J]. *IEEE Access*, 2019, 7:56070-56080

[28] Obaid M, Bayram Z, Saleh M. Instant secure mobile payment scheme [J]. *IEEE Access*, 2019, 7: 55669-55678

[29] Lim S, Kim D, Hur Y, et al. An empirical study of the impacts of perceived security and knowledge on continuous intention to use mobile fintech payment services[J]. *International Journal of Human-Computer Interaction*, 2019, 35(10):886-898

[30] Isaac J, Zeadally S. Secure mobile payment systems[J]. *IT Professional*, 2014, 16(3):36-43

[31] 刘靖, 吴海博, 王少帅, 等. 着色 Petri 网模型驱动的云测试生成方法与实现[M]. 北京邮电大学学报, 2016, 39(5):89-93

[32] 冯登国. 可信计算——理论与实践[M]. 北京:清华大学出版社, 2013:18-36

[33] Trusted Computing Group. Trusted platform module (TPM)[EB/OL]. https://trustedcomputinggroup.org/work-groups/trusted-platform-module: Trusted Computing Group, 2020

[34] Trusted Computing Group. Trusted mobility solutions [EB/OL]. https://trustedcomputinggroup.org/work-groups/mobile: Trusted Computing Group, 2020

[35] Dhiman C, Lucjan H, Sven B. simTPM: user-centric TPM for mobile devices[C]//The 28th USENIX Conference on Security Symposium, Santa Clara, USA, 2019: 533-550

A novel third-party in-APP mobile payment protocol based on trusted platform module

Liu Yonglei[*,**], Jin Zhigang[*], Hao Kun[**], Zhang Weilong[***]

([*]School of Electrical and Information Engineering, Tianjin University, Tianjin 300072)

([**]School of Computer and Information Engineering, Tianjin Chengjian University, Tianjin 300384)

([***]Quality Management Center, Hebei Jiaotong Vocational and Technical College, Shijiazhuang 050035)

Abstract

To solve the problems of key leakage, incomplete display of order information and lack of pre-trust of merchant APP in in-APP third-party payment, a new secure payment model for in-APP third-party payment is proposed. In view of the existing attacks of order tampering, notification forging, order substituting and unauthorized querying, the mobile payment protocol is analyzed by color Petri net (CPN) model, and the accessibility of the unsafe state is proved. Therefore the security vulnerabilities of in-APP third-party payment are verified. A new payment protocol model and improvement strategy based on trusted platform module (TPM) are proposed. The model uses TPM to generate the secure private key for improving digital signature and preventing colluding attack between user and merchant APP. Security analysis shows that compared with the original protocol, the new security model introduces nonce to resist replay attack, generates public and private key pairs through the TPM security chip, and prevents four kinds of network attacks of order tampering and substituting, notification forging and unauthorized querying which are brought by key leakage. The new security model also solves the problems of colluding attack and incomplete display of order information through the additional security compensation mechanism in the protocol.

Key words: e-commerce, mobile payment, third-party, color Petri net (CPN), trusted platform module (TPM)