# 触摸屏是您 POS 安全性的最薄弱环节吗？

Microchip Technology Inc.
Vivek Tyagi

触摸屏显示器是每个现代支付系统和销售点（POS）终端的重要组成部分。触摸屏极大地提升了支付终端的美观度，同时提供了一种对手机、平板电脑和触摸屏笔记本电脑的用户来说都十分熟悉的现代化控制方式。尽管触摸屏拥有这些优点，但也增加了一些必须解决的安全漏洞，而银行卡盗刷者对于攻破这些漏洞意志坚决。遵循支付卡行业数据安全标准（PCI DSS）对于设计安全的硬件/软件系统至关重要，这些系统可帮助客户构建强大且受保护的支付产品，而不会牺牲易用性或优秀的工业设计。本文介绍了POS支付系统的演变、其触摸屏安全漏洞以及任何基于触摸屏的终端必须满足的PCI认证标准。

## POS 显示器中的触摸屏

几十年来，全球消费者一直在 POS 终端上使用信用卡为商品和服务付费。这些终端逐渐增加了小型低成本显示器，以帮助商户和用户更详细地了解交易状态。显示器的两侧或底部增加了按钮，与屏幕上的虚拟按钮对齐，以便用户选择商户选项，如选择卡片类型（例如，信用卡和借记卡）、选择小费金额和打印收据。用户通过机械键盘输入卡号和 PIN 码。这些描述涵盖了大部分仍在发货的 POS 终端。

支付行业的一个趋势是用更大的彩色触摸屏替换小型单色无触摸功能显示器和机械按钮。这些彩色显示器更美观，对商户和消费者都更有吸引力。有了触摸屏显示器，POS 终端供应商还能去除显示器侧面/底部的智能按钮和机械键盘。通过去除随时间推移逐渐磨损的活动部件（内部按键开关机构以及按键表面的印花），这有助于提高系统的可靠性。此外，触摸屏还有助于消除水分通过各个按键进入终端的威胁。最后，彩色触摸屏可帮助商户进行品牌推广和广告宣传，这些趋势促使现代支付终端上触摸屏的尺寸变得越来越大。

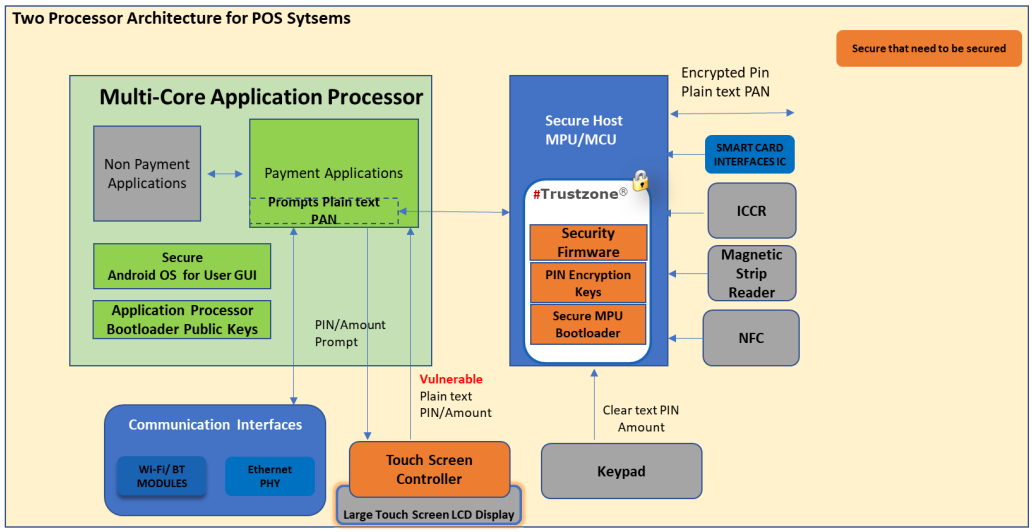

另一个涉及支付系统中采用更大尺寸触摸屏的趋势是电子现金注册机（ECR）的兴起，它们构成了 POS 终端的补充。ECR 用于传统的多通道零售环境，以及越来越受欢迎的自助结账通道。ECR 系统可帮助零售商跟踪销售、减少销售错误、跟踪库存数据，并且同时将财务交易记录到他们的系统中。在输入诸如产品类型和数量、购买购物袋和选择支付选项等详细信息时，ECR 触摸屏显示器提供了极高的灵活性。ECR 通常不是一种安全的支付设备，因此它经常与一台通过卡片、手机和智能手表处理支付的 POS 终端结合使用。

随着时间的推移，ECR 和 POS 终端开始融合，形成一套基于触摸屏的安全支付系统。触摸屏的尺寸大约在 3.5 英寸到 42 英寸之间，已经成为现代 ECR 和 POS 终端不可或缺的组成部分。用户交互、非接触式 NFC 技术的出现、手机的连接性，以及将功能整合到一个系统中，这些因素促成了固定墙壁供电的平板电脑/自助服务终端或电池供电的移动式 POS 终端的兴起，而不是单独的 ECR-POS 系统。便携式 POS 终端允许商户在商店内外任何地方收取付款。无接触支付的快速增长趋势推动了无人值守和自助式公共支付终端的兴起，这些终端广泛用于自动售货机、停车计时器、自动燃油分配器和电动汽车充电站。更大尺寸的触摸屏不仅使商户能够显示更多关于所购买商品的产品信息，而且还能通过产品促销和广告宣传帮助产生额外的收入流。

## POS 安全性和 PCI 合规性

保护主账号 PAN、信用卡凭证（号码、到期日期和 CVV）和用户 PIN 等用户数据成为设计支付系统的最高优先级。磁条（刷卡）卡交易存在固有的安全漏洞，而且随着时间的推移，当磁条磨损和暴露在磁场中时，更容易出现故障。Dip（芯片和 PIN）和 Tap（近场通信：NFC）等更安全的卡片支付方法是可用的替代方案。这些方法由二维码（纸或手

机上）和生物特征（如手指、脸或眼睛）等其他认证机制补充。然而，当触摸屏取代机械键盘时，它们的引入对 PIN 输入系统的安全性也造成一种特殊的新影响。




触摸数据/PIN 的传输容易受到通过触摸传感器覆盖层、底层甚至在触摸 IC 和安全主机 MPU 之间的通信总线探测攻击的影响。触摸控制器上的固件容易被黑客插入后门来提取卡片详细信息。触摸控制器的配置易于修改，这可能会在已经通过安全认证测试的系统上打开漏洞。

此外，户外触摸屏设计要求包括处理极端环境噪声、主动 NFC 干扰、极端发射标准、扩展温度范围、厚手套检测和极端防水（包括高导电清洁液体，否则会导致错误的触摸屏事件）的技术。未经认证的配置和软件更新漏洞也可能导致与勒索攻击相结合的拒绝服务攻击，如果终端连接到中央更新系统，则可能导致整个网络瘫痪。 比如一个带集成支付终端的电动汽车充电站网络。对于触摸屏支付系统开发者而言，这意味着额外的挑战和机会。

## PCI 合规性来挽救局面

由主要的支付卡品牌（Visa、MasterCard、American Express、Discover 和 JCB）创建的支付卡行业安全标准委员会（PCI SSC）已经开发并管理了全球知名的 PCI DSS，以保护持卡人的数据。支付品牌和收单机构有责任创建符合 PCI 标准的产品，以保护用户数据的存储、传输和处理。根据支付应用类型，PCI 合规要求可能会有所不同，这可能会推动开发者考虑硬件/软件/系统级设计等不同因素。

大多数 POS 终端供应商现在都符合 PCI 数据安全标准。PCI 安全机制力图将 PIN 与 PAN 和其他持卡人数据隔离。这确保了通过软件应用输入 PIN 时的安全性和完整性，并且要求对此类软件进行主动监控，以及使用安全密钥对用户数据进行加密。应实施访问控制以对设备用户或所有者进行身份验证。建议设置故障报警以针对篡改、黑客攻击或功能故障发出警告。

如果支付系统使用一个针对 PCI DSS 预先认证的单独支付模块，以便使用带有机械键盘的读卡器进行安全卡交易，那么触摸屏不会在通信线路上传输任何安全信息。只有当触摸屏用于输入信用卡和/或 PIN 码数据（所谓的 PoG，即 PIN on Glass）时，才需要对触摸屏进行 PCI PIN 交易安全（PTS）认证。在这种情况下，需要屏蔽触摸控制器的通信接口，或者加密触摸消息数据。加密为 POS 终端供应商提供了将触摸控制器 IC 移动到连接到触摸传感器的单层柔性印刷电路（FPC）尾板的机会，这种尾板结构简单且经济高效。这种配置允许触摸传感器供应商设计、测试并向 POS 终端供应商交付整套触摸系统，从而降低成本并简化供应链。

## 一般的 PCI 认证要求

与触摸屏显示器相关的PCI合规指南由PCI-PTS管理。PIN交易安全要求可大致总结如下：

- 系统中内置了在发生物理或软件篡改时关闭的措施
- 机密用户数据必须始终以加密方式传输，并且仅在必要时才保留
- 只有在可以验证软件完整性的情况下，才能进行软件更新或启动
- 只有经过身份验证的用户才能更新软件
- 密钥应存储在受保护的区域内，并且应创建安全机制来保护生产中的初始密钥加载
- 设备应进行自检并报告异常

为了方便遵守最新的PCI要求，可以在系统级别将以下功能构建到触摸控制器产品中：

- 每隔24小时重启计划
- 手动输入存在15分钟超时
- 采用ISO格式4的高级加密标准（AES）PIN加密
- 更严格地使用加密密钥，客户密钥层级与制造商密钥层级之间分离
- PAN加密
- TR-34远程密钥加载（RKL）协议

PCI实验室会验证触摸屏显示器，以检查它能否满足PIN交易安全标准的安全要求。此验证包括以下测试：

- 通过黑客攻击评估PIN输入安全性的漏洞
- 通过篡改访问敏感数据，并检查系统中使用的响应机制
- 验证生产中的密钥管理技术和文档。

## 快速直达重点

支付终端的设计需要了解如何实现完整的系统解决方案和稳健的安全标准。像Microchip的maXTouch®控制器产品组合这样的解决方案具有集成的模拟前端和专有固件，可为任何最终用户应用配置安全的加密通信，从而解决此类复杂的系统问题。

像 Microchip 的触摸控制器专家这样的专门支持团队可以指导客户进行系统级设计，并在软件/驱动程序集成过程、产品测试和调试中为他们提供支持。他们在应对一些世界领先的支付终端供应商和认证实验室方面拥有丰富的经验，这意味着客户可以获得他们需要的帮助，从而通过至关重要的认证过程。

*关于作者：*

*Vivek Tyagi 在半导体行业拥有 10 多年的工作经验，目前是 Microchip 人机界面部门的产品营销经理。他负责工业产品部分，包括销售点（POS）和电动汽车充电器。*

## 参考资料

https://ww1.microchip.com/downloads/aemDocuments/documents/HMID/ApplicationNotes/ApplicationNotes/DS00004863A.pdf