



智慧生活 安全连结

SECURE CONNECTIONS
FOR A SMARTER WORLD

NXP 移动支付安全解决方案 和合作展望

罗煜华 | 2015年10月

联系方式: 13528869330



NFC移动支付快速发展



关于NFC 的近况...



- ▶ **2014年近4亿NFC手机出货总量，提供了巨大的NFC手机支付服务用户数基础**
- ▶ **2015年NFC支付服务快速发展，不可阻挡**
 - Apple Pay在美国和欧洲快速发展
 - Google 在9月10日开始推广Android Pay，NFC刷卡将是Android手机的重要功能
 - 三星推出Samsung Pay作为手机重要销售亮点和公司的长期战略服务产品
 - 中国手机厂商积极尝试移动支付“NFC Pay”，涵盖金融支付和公交支付
 - 移动运营商持续推动NFC手机移动支付服务，北上广深等多个重要城市已经可以手机NFC刷公交
 - NFC重要的便民服务：NFC公交外卡充值，读取NFC卡片信息并充值等
 - HCE银行服务推动用户使用NFC支付的习惯
- ▶ **NFC+ eSE带来手机移动安全技术的重大创新**
 - eSE是手机内唯一 一个独立的、有EAL6+安全级别的存储硬件
 - 支持FIDO，TEE等合作，为手机指纹识别加密，保障用户生物识别信息安全
 - eSE与TEE的SPI安全连接，为手机带来EAL6+的安全级别保护，保障手机用户关键数据和财产安全



PN6xT 产品介绍

NFC RF 领先的性能

带给手机厂商的价值

- ▶ 节省NFC Booster 芯片成本
- ▶ 支持手机金属后盖设计

NXP 优势

- ▶ 超强的RF信号输出
- ▶ 支持各种超小天线设计



RF

EAL6+ 安全级别

带给手机厂商的价值

- ▶ 保护手机用户信息安全和财产安全，保护手机品牌
- ▶ eSE SPI连接TEE，提供应用的安全级别

NXP 优势

- ▶ 银行芯片的最高的安全级别 (EAL6+)
- ▶ eSE SPI 连接到 TEE



Security

NFC兼容性好

带给手机厂商的价值

- ▶ 手机用户体验好，促进手机销售
- ▶ 快速过检测认证，支持移动运营，银联，公交等认证测试

NXP 优势

- ▶ 检测认证技术积累最多
- ▶ 已经在金融和公交领域进行了大量的预测试工作
- ▶ NXP在非接POS/闸机市场长期占据领先份额

Services

技术领先, 稳定成熟

带给手机厂商的价值

- ▶ 与芯片平台厂商集成稳定和高效，节约开发时间和成本
- ▶ 与Android 同步保持版本更新发布，支持Android 6.0

NXP 优势

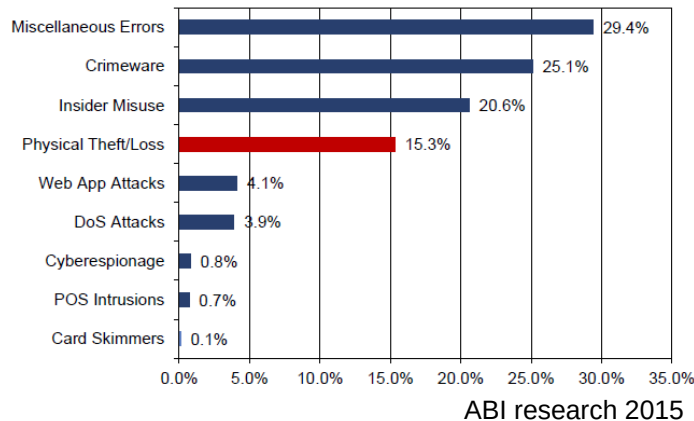
- ▶ PN6xT系列与平台厂商达成战略合作，兼容性最佳
- ▶ PN6xT系列拥有**15500个测试专利**
- ▶ 有全球的安全认证，获得Visa、Mastercard、银联等支持



安全问题是手机用户的痛点



手机安全问题日趋严重...



- ABI数据显示，恶意攻击，木马病毒，滥用权限威胁等安全问题占55.7%，严重威胁用户手机财产安全；
- 2015年7月，CNN报道95%的安卓手机可被恶意短信攻击，即使该短信未被打开；影响超过9.5亿台手机；
- 2015年6月，网络安全公司NowSecure公布某品牌手机存在被远程劫持的漏洞，影响超过6亿台手机用户
- 某著名公司APP程序被恶意盗取手机用户的银行账户和第三方支付账户信息。。。

Android phones can get infected by merely receiving a picture via **text message, according to research published Monday.**

This is likely the biggest smartphone flaw ever discovered. It affects an estimated **950 million phones worldwide** -- about 95% of the Androids in use today.

xxx Smartphone Software Security Flaw Discovered

Over **600 million** xxx mobile device users may be at risk due to a significant security threat, according to researchers at mobile security specialist NowSecure.



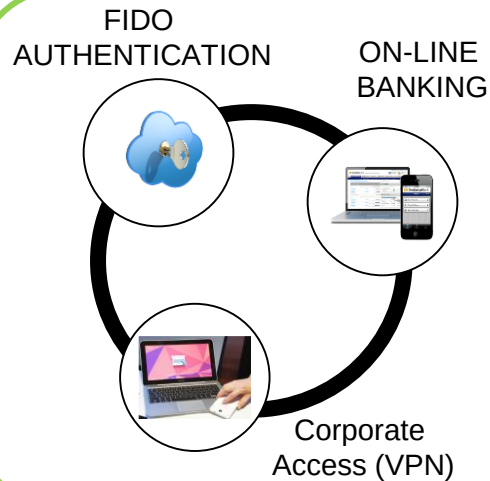
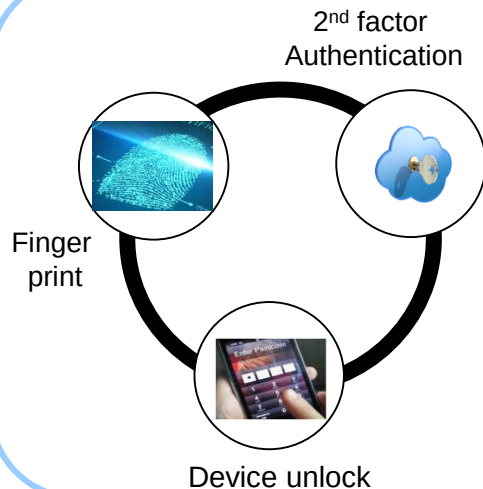
Hackers are draining bank accounts via the XXXX app (reported by CNN)

Thieves are **stealing money from people's credit cards, bank and PayPal accounts** -- by first tapping into their XXXXX mobile app.

XXXX on Wednesday acknowledged that criminals have been breaking into individual customer rewards accounts. The XXXXX app lets you pay at checkout with your phone. It can also reload XXXX gift cards by automatically drawing funds from your bank account, credit card or PayPal.



eSE为手机用户提供EAL6+级别的安全保护



手机用户的财产信息保护

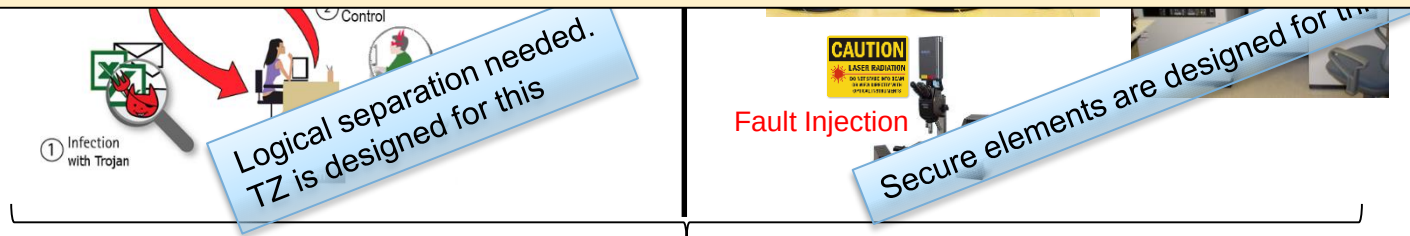
支持硬件加密和支持指纹加密

账户登录加密保护
在线服务证书保护

哪一种技术是最佳保护手机安全的技术？

TEE和eSE共同为手机提供E2E的安全保护

- ✓ TEE 保护应用运行在安全可信环境
- ✓ eSE 为用户关键财产和生物信息提供存储和加密



TEE : Remote / Online / Logical Attacks

eSE: Local / Offline / Physical Attacks

TEE提供TA安全运行的环境

- 充足的空间支持应用和服务，提供程序运行的安全环境
- 保护用户虚拟键盘输入安全
- 可以存储大量数据和进行加密

eSE是独立硬件芯片，EAL6+级别保护

- 芯片密钥管理体系基于GP国际规范，安全可控，可远程管理
- 符合银行业EMVco的安全标准，被银行业广泛接受
- 可存储关键的加密数据保障服务应用的安全
- 防物理攻击

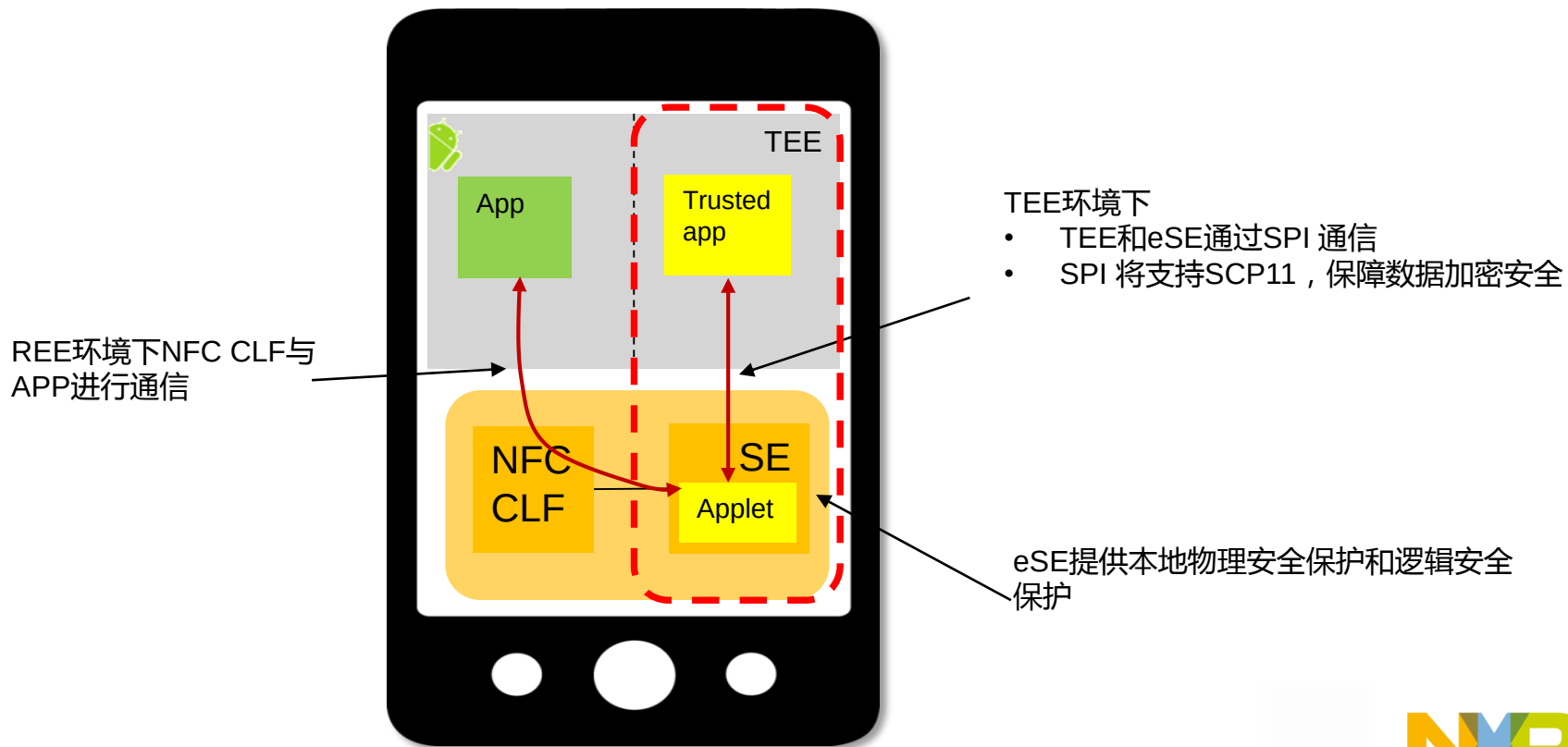
TEE and Secure Element are complementary to provide End to End security



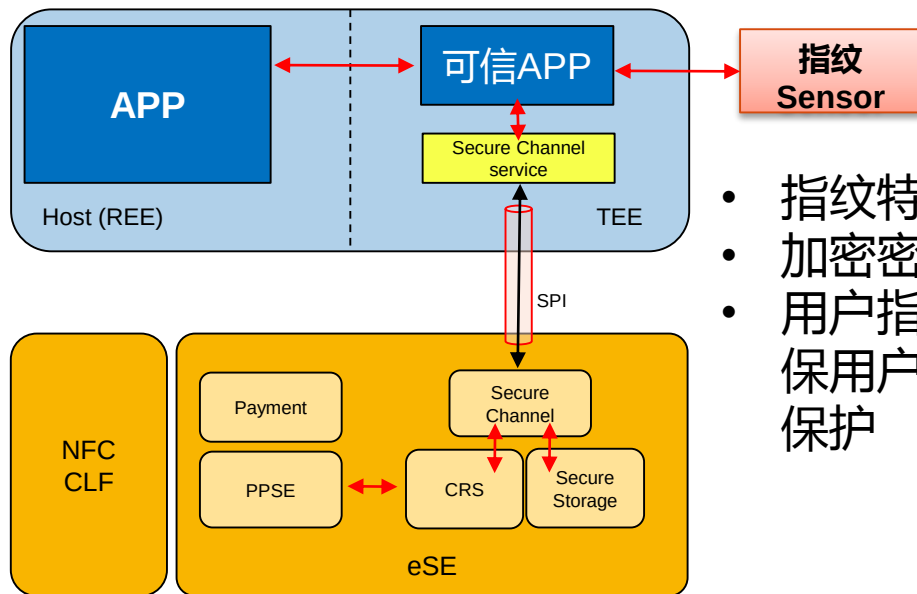
恩智浦为手机移动安全生态 提供安全的基础环境



NFC eSE+ TEE 系统结构



eSE+TEE+指纹加密保护



- 指纹特征值在TEE环境内加密存储
- 加密密钥通过SPI存储到eSE指定辅助安全域
- 用户指纹特征值由TEE和eSE共同保障安全，确保用户指纹信息在存储状态下达到EAL6+的安全保护

手机移动安全的长期演进

NXP deliverables	Payment 	Authentication 	Cloud Security  e.g. FIDO	Secure Email 
Secure Channel TEE/SE + Ext CRS applet Applet secure storage Applet FIDO, Key master extension	线上/线下支付 功能			手机平台和手机应用的高级别安全保障



Ready



Under developing



SECURE CONNECTIONS
FOR A SMARTER WORLD