2018年6月26日 星期二

BtcZen卡的安全架构说明

1. 芯片		
1.1	安全检测传感器	可检测并抵抗异常电压电流、高低频率时钟、高低温、尖峰毛刺的攻击；可检测并抵抗激光、射线、紫外线攻击； 可检测并抵抗溶解、剥离攻击
1.2	安全内核	CPU内核具备异常指令检测、指令回溯、数据安全读写、指令反复加载、寄存器状态校验等安全措施
1.3	动态存储加密	Bootloader、操作系统、应用的代码及数据、RAM均采用动态加密存储，并通过加密总线进行读写访问；
1.4	随机变频时钟	随机插入空操作，以抵御能量分析攻击； cpu及外设均采用了变频时钟，以进一步抵御能量分析攻击；
1.5	真随机数生成器	安全级别符合德国BSI AIS 31标准中的PTG.2级别，通过了美国NIST SP800.22的统计学测试
1.6	硬件实现的ECC算法	密钥对生成、大素数操作时采用了原子操作、数据完整性校验、程序执行顺序确认、掩码运算、冗余计算、开启变频时钟等手段以抵抗注入攻击、能量分析攻击等情形

2. COS （智能卡操作系统）		
2.1	应用防火墙	将不同开发者的应用隔离开来，杜绝相互的数据访问，以及代码泄露
2.2	事务机制	确保指定的一系列数据修改操作，要么全部执行，要么全部不执行，保证数据的完整性
2.3	多应用管理框架	符合国际行业标准的智能卡多应用管理机制，确保仅授权者可操作卡内应用、授权认证过程满足安全要求
2.4	ECC算法库的软件部分	配合芯片的ECC算法硬件实现，进一步检测算法的输入输出是否遭到软硬件攻击
2.5	敏感数据加密	操作系统、应用的敏感数据，例如授权密钥、计数器等，均为加密存储并具有校验码，可抵御一定程度的注入攻击、能量分析攻击等
2.6	防御型虚拟机	虚拟机并不信任卡内的应用代码和数据，执行之前会执行字节码校验、上下文检查、边界检查等安全措施

3. BtcZen （智能卡应用）		
3.1	程序执行顺序确认	执行敏感操作之前，例如签名，将通过计数器、日记，反复确认用户已输入正确的密码，以抵御注入攻击等
3.2	敏感数据加密	应用自身的敏感数据，例如计数器、日记、用户密码等，均为加密存储并具有校验码，可抵御一定程度的注入攻击、能量分析攻击等
3.3	输入输出加密	与手机app的通讯采用一次一密的动态密钥机制，防止重放攻击等、阻止窃听敏感数据
3.4	代码混淆	在不影响执行效率、不降低安全性的同时，采用多路执行、随机执行、冗余代码和数据的方式，进一步提高破解难度
3.5	自毁机制	若确认遭遇某些软硬件攻击，应用将擦除卡内敏感数据后锁死应用