终端主芯片入侵演示及安全探讨

北京智慧云测科技有限公司

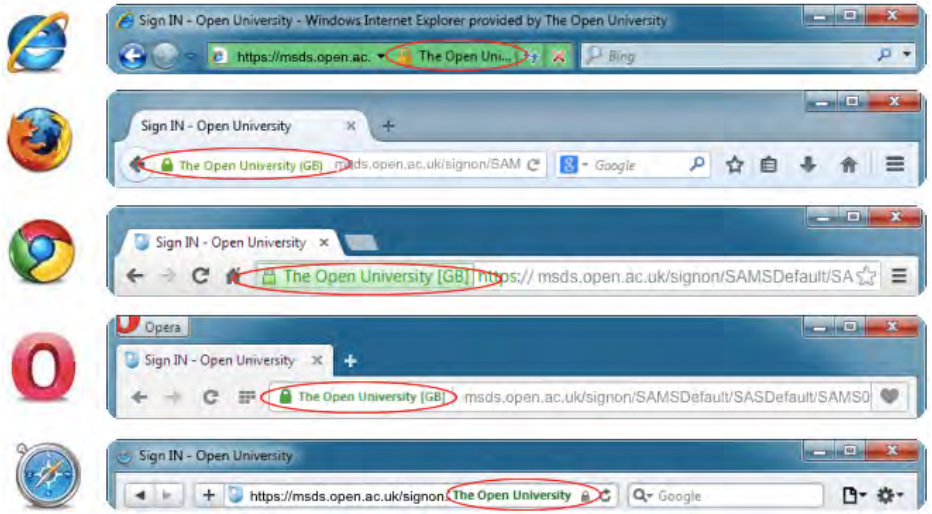
关注智慧云测官方微信，获取更多资讯！

目 录

传输安全：https

什么是 **https**？

https=http+SSL



Developer Discover Design Develop Distribute

Supporting App Transport Security

December 21, 2016

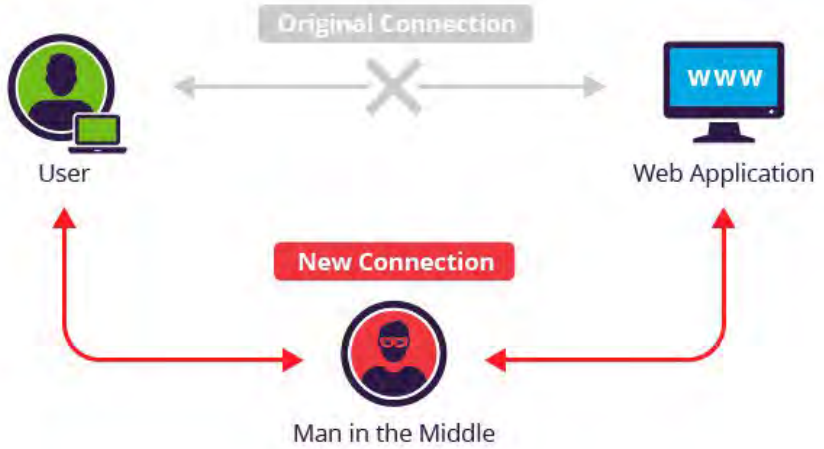
App Transport Security (ATS), introduced in iOS 9 and OS X

WWDC16

Http为什么不安全

可进行中间人攻击：

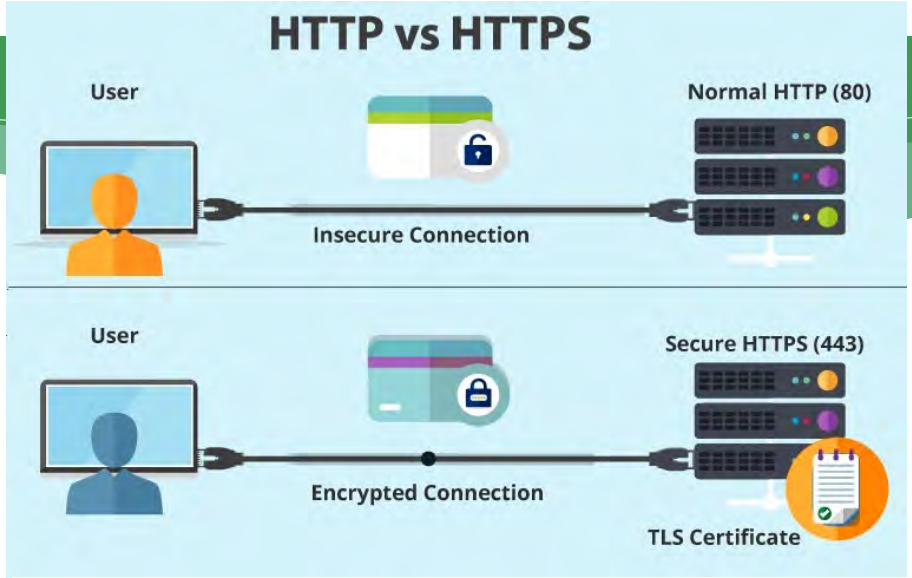
- 伪造签名证书
- 伪装成真实的服务器
- 获取会话秘钥
- 最终获取机密信息，如：支付密码



Https如何保障安全？

Http本身无任何防护机制，通过加入SSL（安全套接字层）来进行加密传输

SSL已经基本成为了互联网安全加密的事实标准。从Google、Facebook、BAT、银行、券商等机构，都在大量使用SSL技术进行加密通信。



HTTPS = HTTP + TLS/SSL

层次	风险	优势
HTTP	信息窃听 信息篡改 信息劫持	
TLS/SSL		信息加密 完整性校验 身份验证
TCP		

SSL应用在哪里？

SSL应用：

- 手机中的多种app
- 智能家居产品
- 无人机
- 摄像头
- 汽车车机，车联网
- 关键基础设施

SSL被破解的危害：

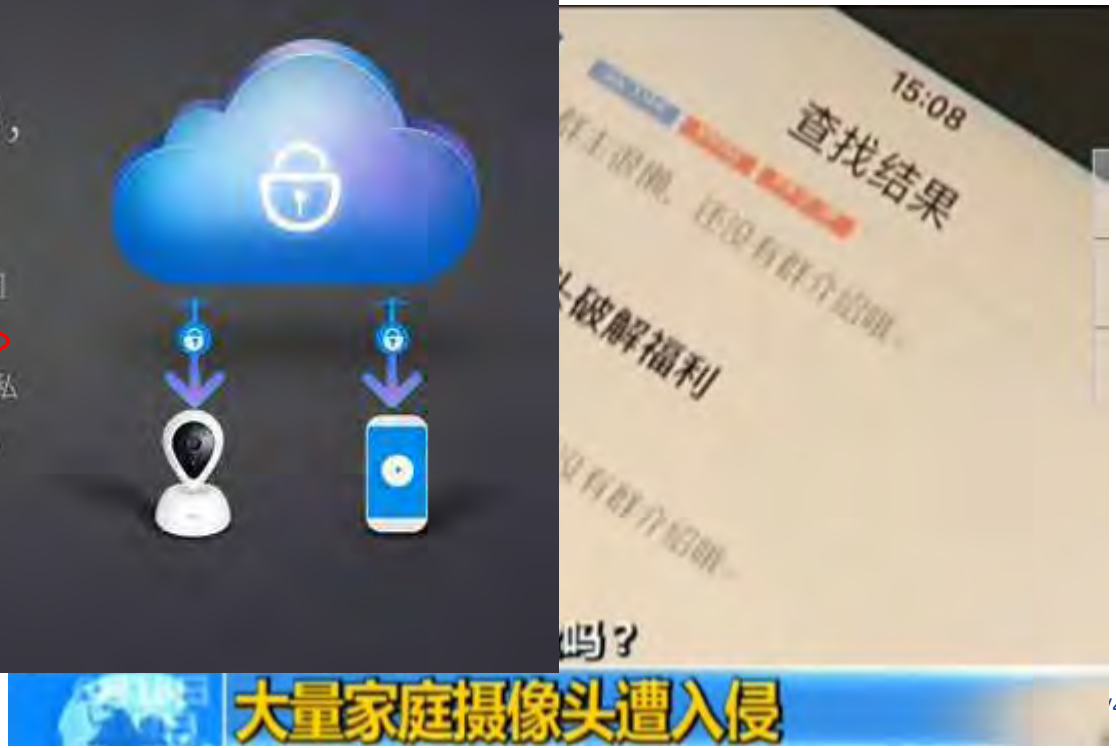
- 密码被截取
- 设备被控制，监控
- 危害人身安全
- 获取基础设施操作权限

SSL应用一：

各种app中嵌入支付宝付款

SSL应用二：

智能家居IoT 数据链接



SSL应用三：
车联网

網易汽车 网易首页 > 汽车频道 > 正文

宝马/劳斯莱斯被曝存安全漏洞 车门“形同虚设”

2015-02-02 15:42:00 来源: 人民网(北京)

分享到：

人民网2015年2月2日报道 人民网北京2月2日电（鄂智超）综合外媒消息，宝马集团旗下的宝马与劳斯莱斯等车型所搭载的ConnectedDrive数字服务系统被发现存在严重漏洞，黑客可轻易地远程打开车门，使车门“形同虚设”。

宝马通过HTTPS强化车载系统安全性

2015-02-04 来源：《中国汽车报》网 作者：

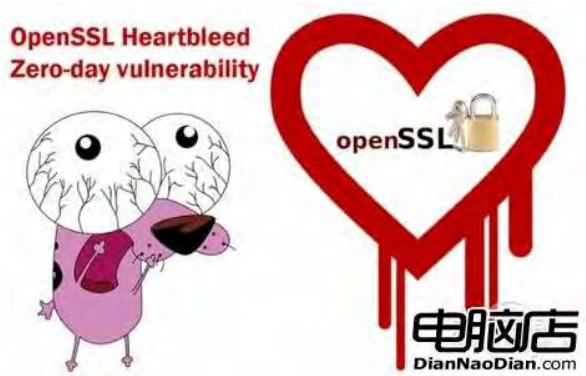
日前，关于部分宝马互联汽车存在安全脆弱性的新闻，被国内外多家媒体转载。也让这家汽车制造商不得不站出来，对这个问题做出回应。宝马方面表示，已经对安全漏洞进行修补；使用HTTPS（是以安全为目标的HTTP通道，简单讲是HTTP的安全版）协议的新配置将确保汽车互联安全。

史上SSL攻击事件

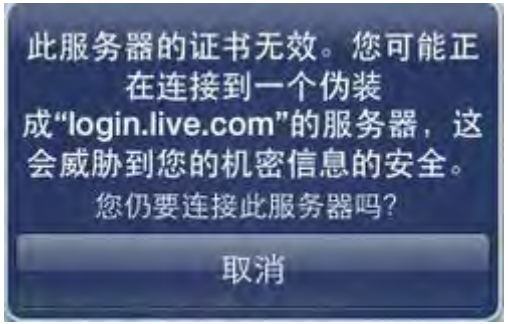
已有的针对SSL的攻击案例主要是证书伪造攻击，数据库攻击，和软件漏洞攻击。但还未见有针对硬件的攻击。

SSLv3 —— Poodle（贵宾犬）攻击

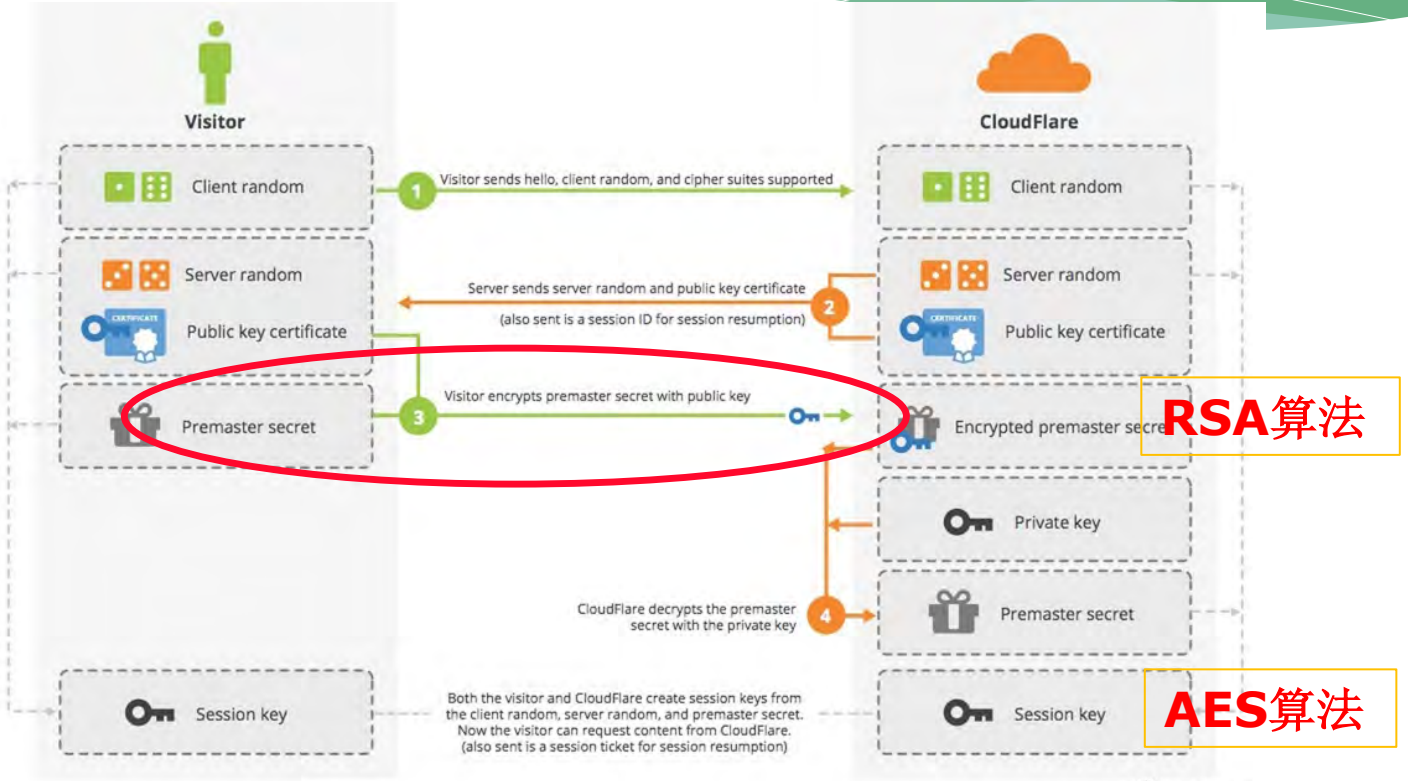
“Heartbleed”（心脏出血）漏洞攻击



SSL Strip 攻击



SSL的安全作用机制


Visitor
CloudFlare
Client random
Visitor sends hello, client random, and cipher suites supported
Client random
Server random
Public key certificate
Server sends server random and public key certificate
(also sent is a session ID for session resumption)
Server random
Public key certificate
Premaster secret
Visitor encrypts premaster secret with public key
Encrypted premaster secret
RSA算法
Private key
CloudFlare decrypts the premaster secret with the private key
Premaster secret
Session key
Both the visitor and CloudFlare create session keys from the client random, server random, and premaster secret. Now the visitor can request content from CloudFlare. (also sent is a session ticket for session resumption)
Session key
AES算法

SSL的经典算法库：RSA和AES

- SSL的RSA和AES算法库是安全业界认可的经典算法库，经过多年迭代，是非常成熟的加密算法库。
- RSA和AES具有广泛的应用，除了SSL，还有本地加密，如硬盘全盘加密，PDF加密。

目 录

芯片攻击

破解成果

我们成功地破解了在Android手机芯片上运行的OPEN SSL 的 RSA+AES算法库，并得到了全部密钥。

电磁错误注入攻击

■ 攻击对象

某型号Android手机

- 手机 AP芯片： QXXX和MXX
- 攻击算法：OPEN SSL 的 RSA 算法库

■ 攻击平台

型号：**D-Injector-EM**

■ RSA攻击原理

输入 消息 M、p、q、d

输出 签名 S

1：计算： $d_p=d(\mathrm{mod}(p-1))$，$d_q=d(\mathrm{mod}(q-1))$；

2：利用模幂算法预计算： $m_p=M^{d_p}(\mathrm{mod}p)$；

3：利用模幂算法预计算： $m_q=M^{d_q}(\mathrm{mod}q)$；

4：利用模逆算法预计算： $q_p=q^{-1}(\mathrm{mod}p)$；

5： $u=(m_p-m_q)q_p(\mathrm{mod}p)$；

6： $S=m_q+uq$；

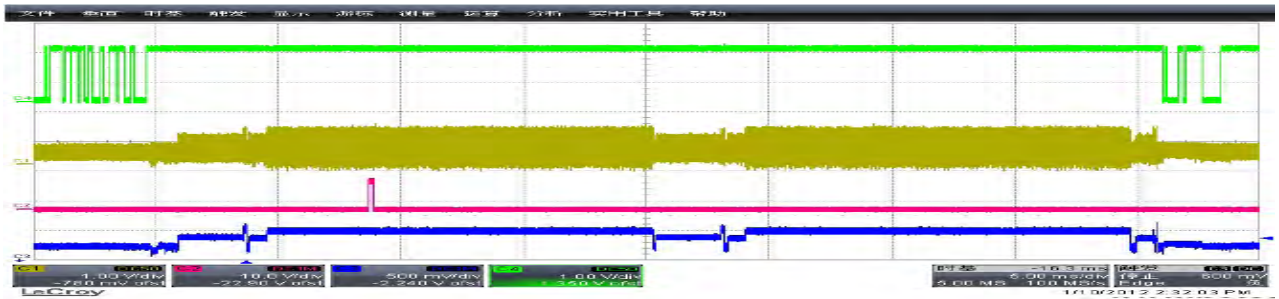
7：return S。

在 RSA 签名算法执行过程中，假设消息 M，$s=M^d \bmod N$ 为 M 的正确签名，$s'=M^d \bmod N$ 为错误的签名，d 为签名密钥。则正确和错误的签名分别为：$s=m_q+uq$ 和 $s'=m_q'+u'q$。假设在计算 m_p 或 m_q 时发生故障，首先假设 m_q 发生错误。即 $m_q \neq m_q'$，$m_p=m_p'$，因为有 $u=(m_p-m_q)q_p(\mathrm{mod}\,p)$，$q_p=q^{-1}(\mathrm{mod}\,p)$，则有 $q\times q_p(\mathrm{mod}\,p)=1$，则有如下推导：

$$s-s'\equiv(m_q+uq)-(m_q'+u'q)\equiv$$
$$(m_q-m_q')+(m_q'-m_q)\bmod p\equiv 0\bmod p$$

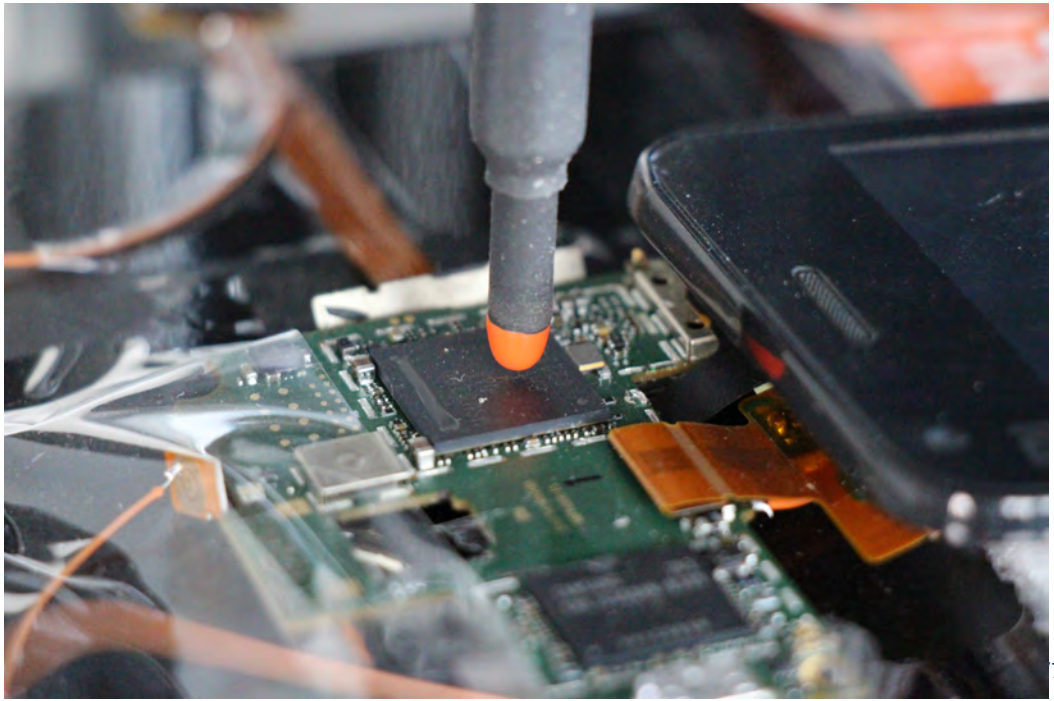
即 $s-s'=tp$，t 为整数，所以 $\gcd(s-s',N)=\gcd(tp,N)=p$。

仅需一个有效错误密文，即能恢复私钥p，q



■ 攻击步骤

- ✓在手机芯片上运行RSA算法库
- ✓暴露芯片
- ✓注入精确电磁波
- ✓进行差分运算破解
- ✓获得秘钥



■ 攻击代价

时间	• 攻击识别时间:4小时 • 攻击实施时间:即时复现
设备	• 电磁探头、电磁发生器、示波器、错误处理软件
样本	• 对样品不做任何破坏
人员知识	• 电磁攻击技术

■ 攻击结论

安全威胁较大： 无需对样品进行任何破坏

普适性强： 对FPGA芯片、IC卡芯片，智能手机主芯片等终端类产品均有效

攻击实施难度： 能量需被束缚在较小的物理空间内；电磁脉冲宽度窄且托尾小；能量需要调节适中

目 录

芯片攻击

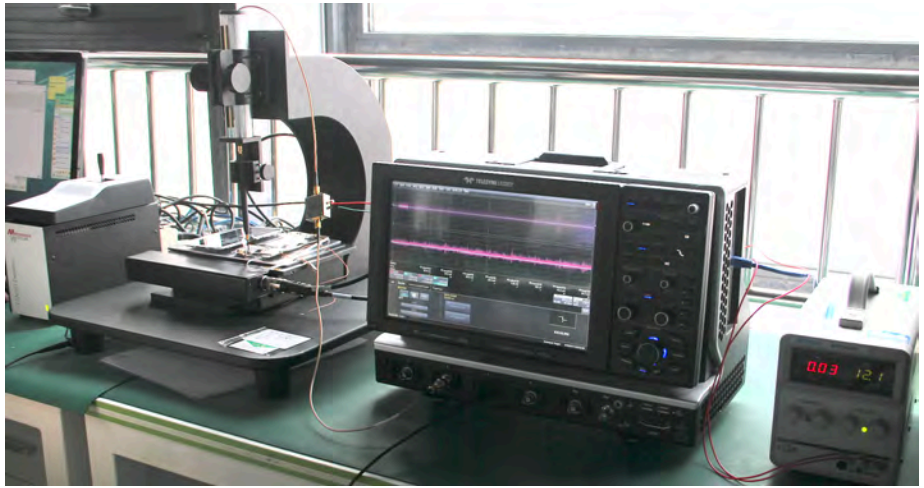
■ 攻击对象

某型号Android手机

- 手机 AP芯片： QXXX
- 攻击算法：OPEN SSL 的 AES 算法库

■ 攻击平台

D-Observer



■ 攻击代价

时间	• 4小时
曲线数	• 5000条
设备	• 电磁探头、示波器、算法分析软件
样本	• 市面上购买的手机，需要拆开外壳
人员知识	• Android APP开发、侧信道技术

■ 攻击结论

安全威胁较大： 无需对样品进行任何破坏

普适性强： 对FPGA芯片、IC卡芯片，智能手机芯片等产品均有效

攻击实施难度： 需要软件分析能力强大，攻击人员需经验丰富

AES算法的广泛应用

AES应用：

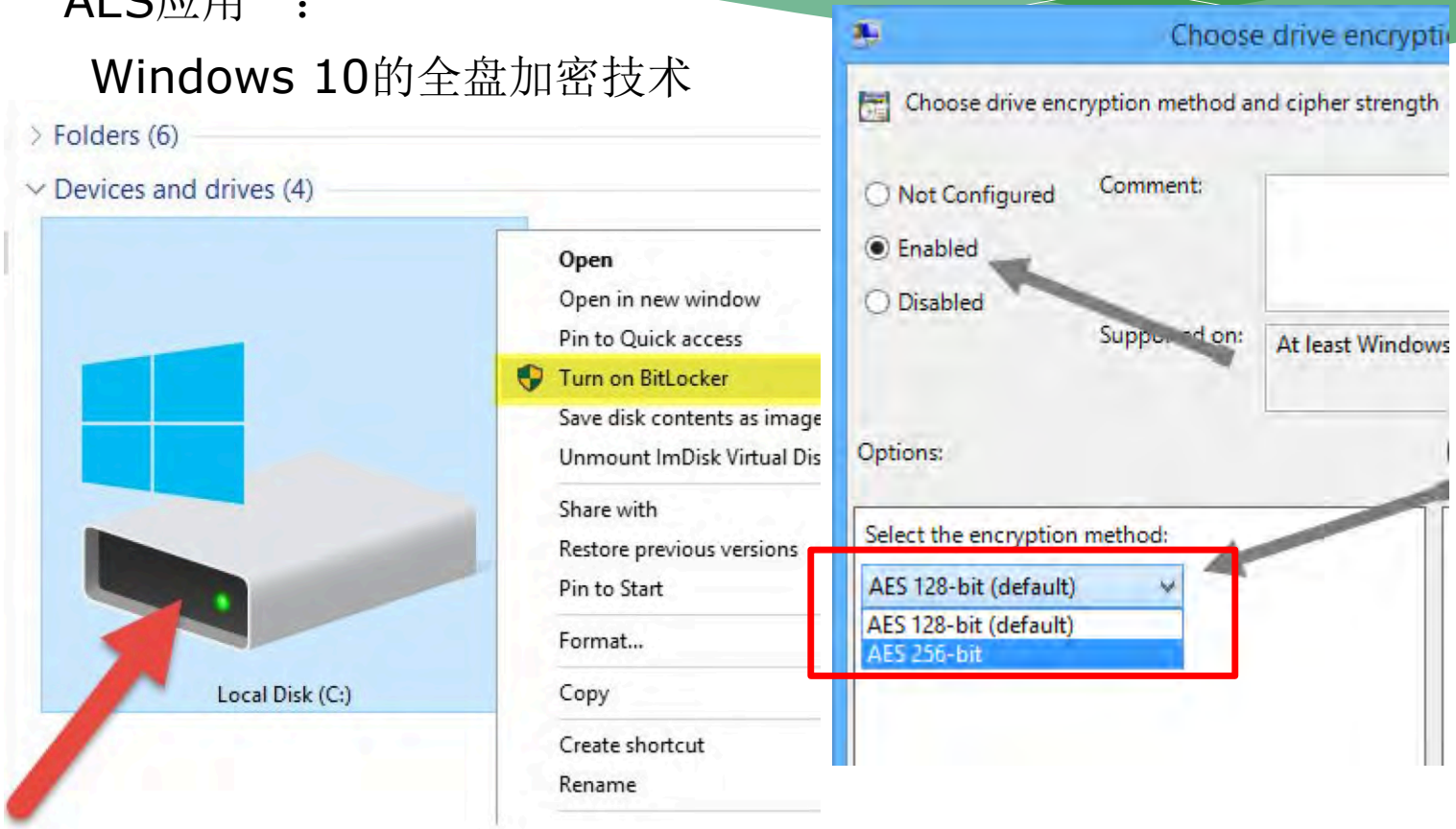
- Windows 10/Android手机全盘加密
- App本地存储内容泄露，可被篡改
- WiFi密码
- Word，pdf加密
- 加密u盘
- VPN加密
- 网络云盘加密

AES算法被破解的危害：

- 硬盘加密失效，可不输入密码直接读取加密内容
- WiFi链接的设备被监控
- 加密文档失效，内容可直接被读取
- 网络云盘内容可被他人下载

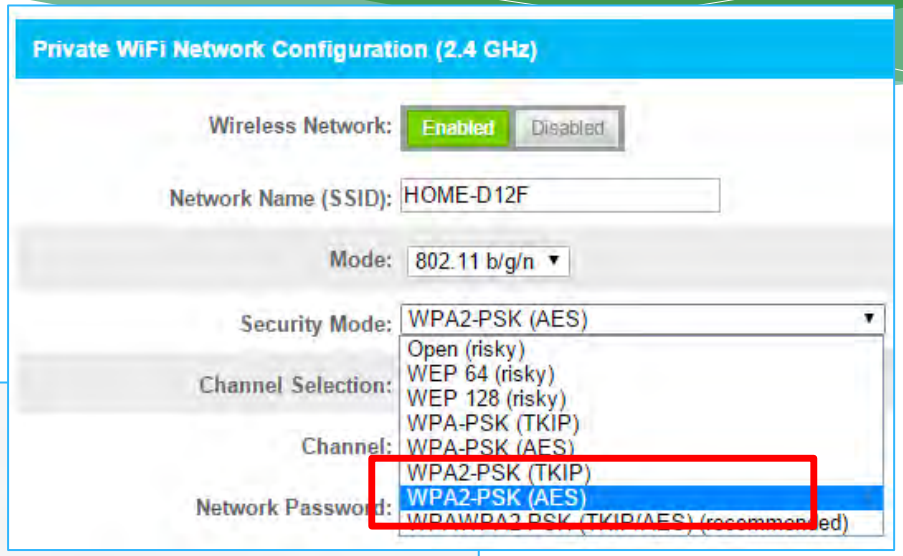
AES应用一：

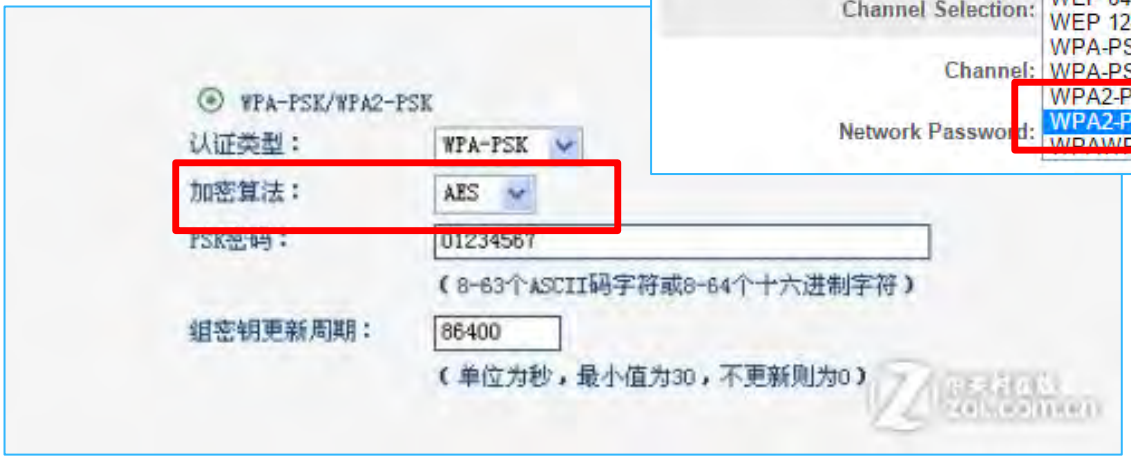
Windows 10的全盘加密技术



AES应用二：

WiFi通信密码加密方式





AES应用三：
PDF加密

选项

兼容性： Acrobat 7.0 和更高版本

加密级别： 128-bit AES

加密所有文档内容

加密除元数据外的所有文档内容（与 Acrobat 6 和更高版本兼容）

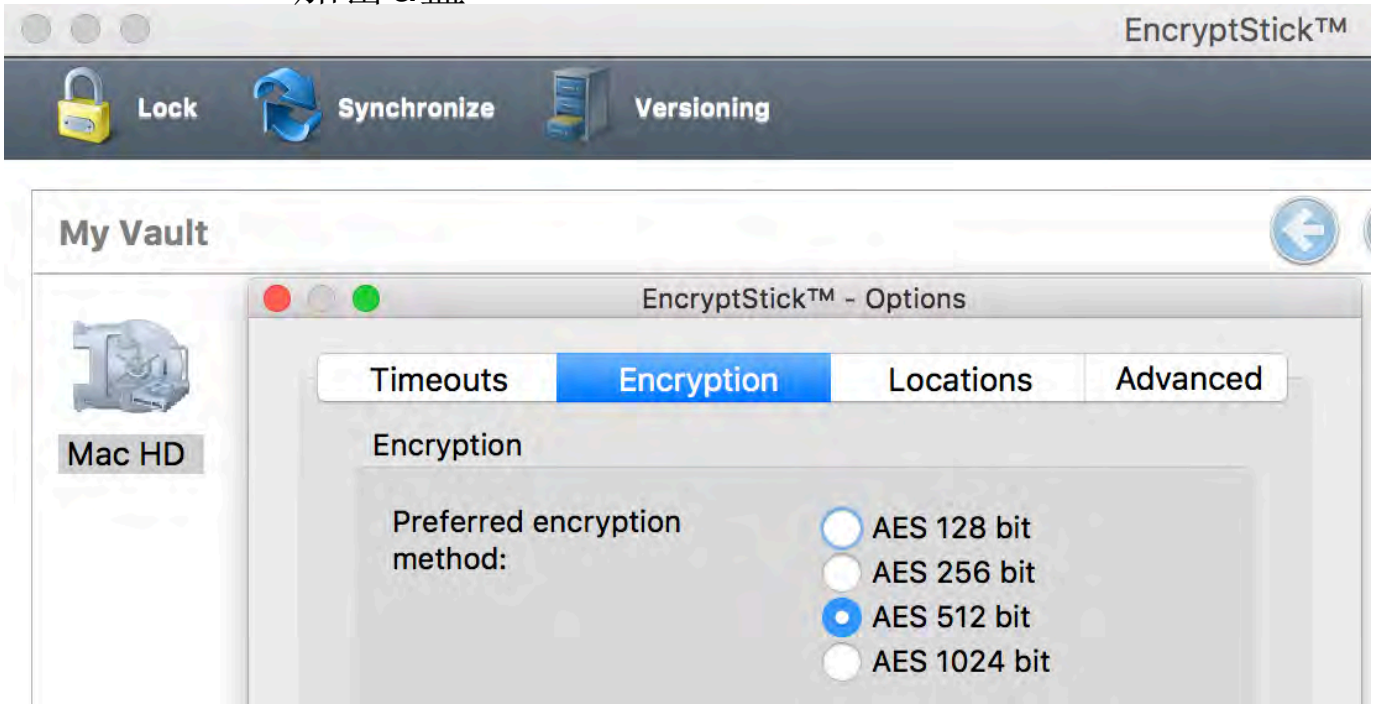
仅加密文件附件（与 Acrobat 7 和更高版本兼容）

文档所有内容均将被加密，且搜索引擎将无法访问文档的元数据。

帮助

AES应用四：

加密u盘

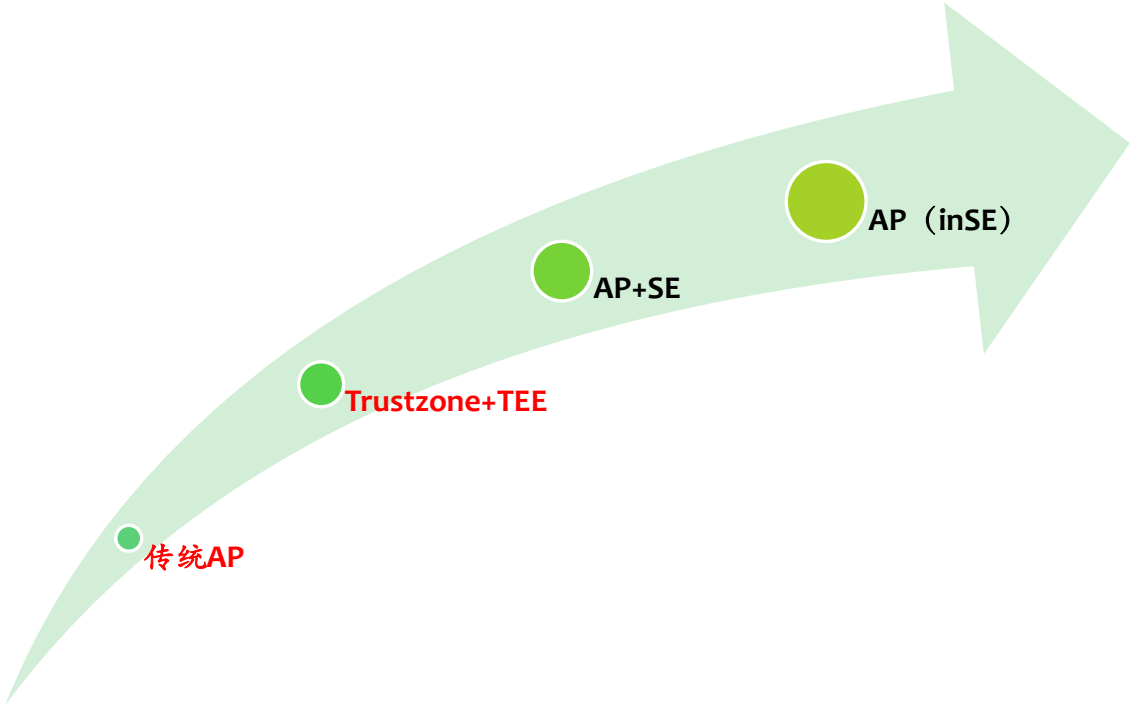

EncryptStick™
Lock
Synchronize
Versioning
My Vault
Mac HD
EncryptStick™ - Options
Timeouts
Encryption
Locations
Advanced
Encryption
Preferred encryption method:
AES 128 bit
AES 256 bit
AES 512 bit
AES 1024 bit

AES应用五： VPN服务

AES应用六： 云盘加密


大容量与你成长
会员用户可享 100GB 起超大存储空间，每天使用扩容 100MB。单个文件上传上限达 25GB 。
不限制传输速度
全国三线机房接入，CDN 智能加速，上传下载无速度限制，最大可传输 25GB 单个文件。
更安全
SSL, AES-256 bit
制可随时恢复任何
手机照片自动传
自动上传备份手机相册照片，永久珍藏回忆时刻，释放存储卡空间，更能与家人朋友轻松共享。
同步任何文件夹
任意选择本地文件夹上传，让手机、平板与您的电脑保持同步。无需手动复制，从此告别 U 盘。
多功能外链分享
支持创建外链及在线预览，可设置访问密码、验证问题、下载限制、过期时间，便于灵活分享。

■ 攻击威胁



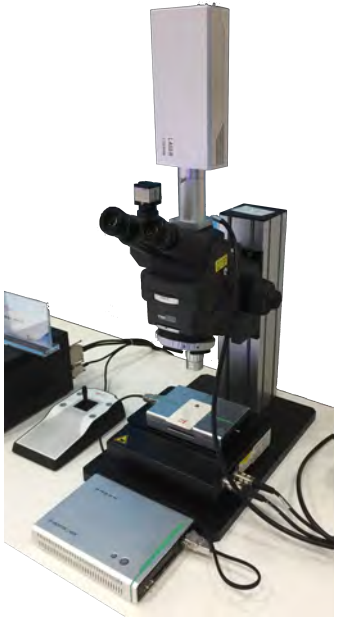
目 录

修复措施

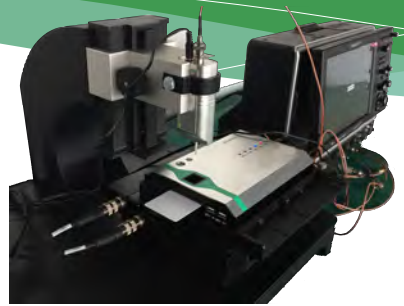
没有绝对的安全。
即使密码算法如此安全，但仍然可以被破解。

我们提供的安全咨询服务可以先于真正的黑客之前找到这些漏洞。

这是我们实验室对产业界的责任。



激光注入设备



侧信道设备

电磁注入设备

设备优势

国产优势

- 符合国家信息安全大战略
- 符合国内金融、PBOC、EMVCo、CC等标准规范
- 国内首家全系列商用安全检测工具
- 设备具完全自主知识产权

技术优势

- 团队拥有超过6年安全领域行业经验
- 多人获得人民银行科技进步特等奖
- 参与行业内多个标准编写
- 领域内发表论文10余篇；发明专利10余项

支持优势

- 国内本地化技术支持团队
- 承诺7*12小时电话技术支持
- 承诺96小时解决技术问题
- 按需定制升级设备
- 兼容国际主流检测设备

平台优势

- 合作运营模式灵活
- 平台化、操作维护简单

Secure Your Life

*谢谢！

黄天宁

联系电话：18610887190

邮箱地址： huangtn@dplslab.com

公司地址：北京市石龙经济开发区莲石湖西路98号院7号楼701室