软硬结合
物联网通信链路安全攻防实践

王科岩
青莲云联合创始人

目录

物联网设备风险无处不在

6种物联网病毒，对全球造成16亿损失

在网络安全领域，分清好人和坏人需要付出一些努力。当两者都以恶意软件的形式出现时，将它们分开几乎是不可能的。

作者：黄鼎树科技 来源：今日头条 | 2019-04-09 08:40 收藏 分享

腾讯安全团队破解亚马逊智能音箱Echo，可远程窃听并录音

澎湃新闻记者 杨鑫倢

2018-08-13 18:08 来源：澎湃新闻 字号

中国研究人员破解特斯拉自动驾驶漏洞 可能误变道驶入对向车道

2019-04-03 15:06 环球网 崔天也 7 参与

TP-LINK Wi-Fi中继器出现漏洞，可用于远程代码执行

2019-06-24 04:27 34 人阅读 0 条评论

*本文中涉及到的相关漏洞已报送厂商并得到修复，本文仅限技术研究与讨论，严禁用于非法用途，否则产生的一切后果自行承担。

HackPwn：TCL智能洗衣机破解细节分析

360安全 2015-08-25 共451821人围观，发现 15 个不明物体 资讯

智能门锁安全问题谁来管？耶鲁和盖特曼智能门锁0 day漏洞曝光！

山卡拉 漏洞 2019年5月27日发布 收藏

导语：近期，嘶吼接到胖猴实验室的爆料，市面上已发售的耶鲁（Yale）智能门锁和盖特曼（gateman）智能门锁均存在漏洞，并且这两个品牌门锁所涉及的漏洞是一样的。

目录

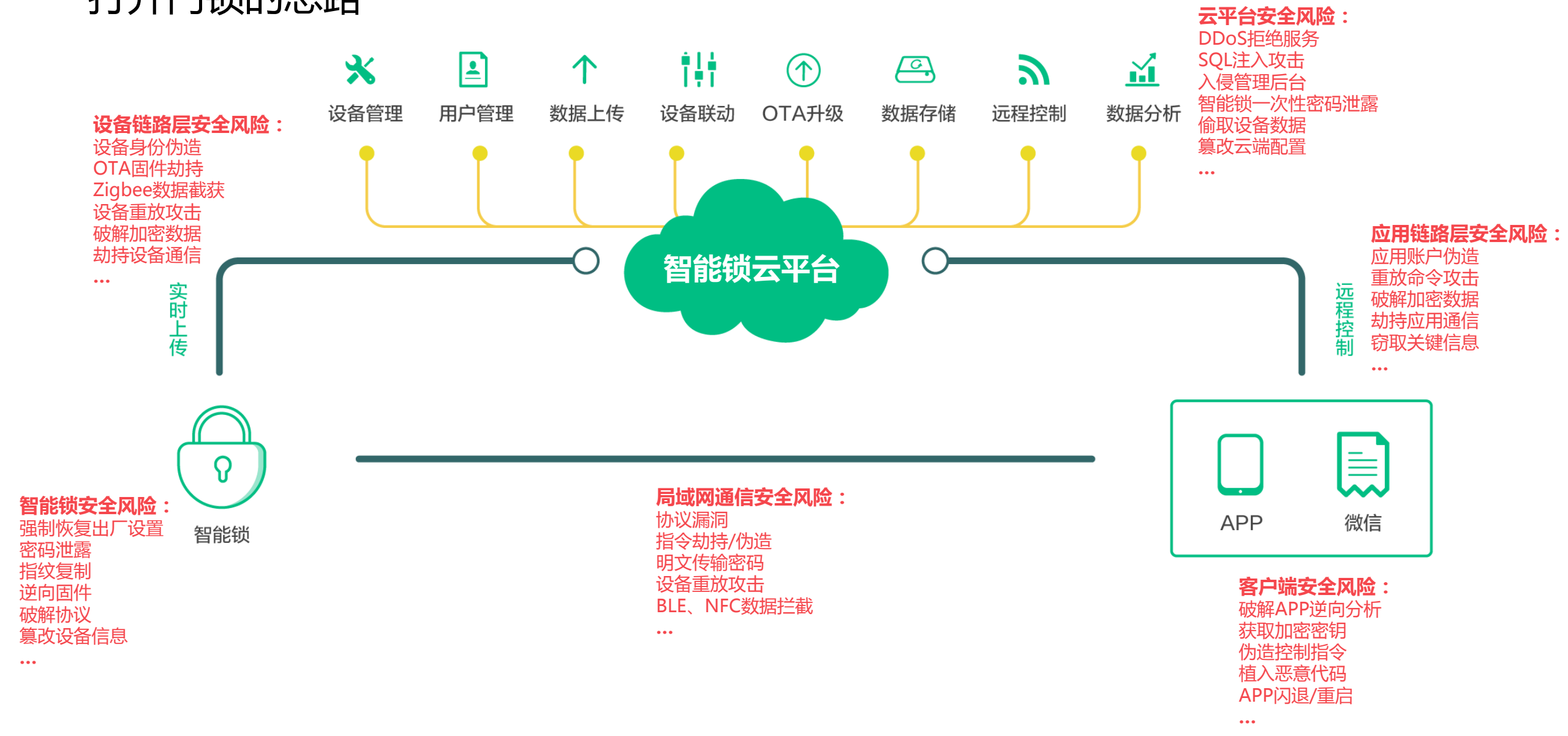
如何打开任意智能门锁？

智能门锁网络拓扑攻击面

智能硬件攻击手段

智能门锁网络拓扑攻击面

打开门锁的思路



云平台安全风险：
DDoS拒绝服务
SQL注入攻击
入侵管理后台
智能锁一次性密码泄露
偷取设备数据
篡改云端配置
…

设备链路层安全风险：
设备身份伪造
OTA固件劫持
Zigbee数据截获
设备重放攻击
破解加密数据
劫持设备通信
…

应用链路层安全风险：
应用账户伪造
重放命令攻击
破解加密数据
劫持应用通信
窃取关键信息
…

智能锁安全风险：
强制恢复出厂设置
密码泄露
指纹复制
逆向固件
破解协议
篡改设备信息
…

局域网通信安全风险：
协议漏洞
指令劫持/伪造
明文传输密码
设备重放攻击
BLE、NFC数据拦截
…

客户端安全风险：
破解APP逆向分析
获取加密密钥
伪造控制指令
植入恶意代码
APP闪退/重启
…

智能硬件攻击手段


智能设备攻击
硬件
物理篡改
物理破坏
侧信道攻击
软件定义无线电
物理接口
调试接口暴露
JTAC
串口
固件提取
串口
flash
获取用户命令行
获取管理员命令行
特权提升
重置至非安全态
移除储存介质
设备ID/序列号泄露
固件
敏感数据泄露
后门账号
硬编码密码
根密钥
加密算法
敏感信息
敏感URL
易受攻击服务
Web
SSH
TFTP
固件降级
内存
敏感数据泄露
明文用户名
明文密码
第三方凭证
加密key
应用
链路未加密
重放攻击
中间人
功能逻辑漏洞
授权设计缺陷
简易OTA
弱口令
代码
溢出漏洞

目录

如何抵御物联网设备攻击风险？

青莲云设备身份认证服务

设备认证服务安全要求

设备不可伪造

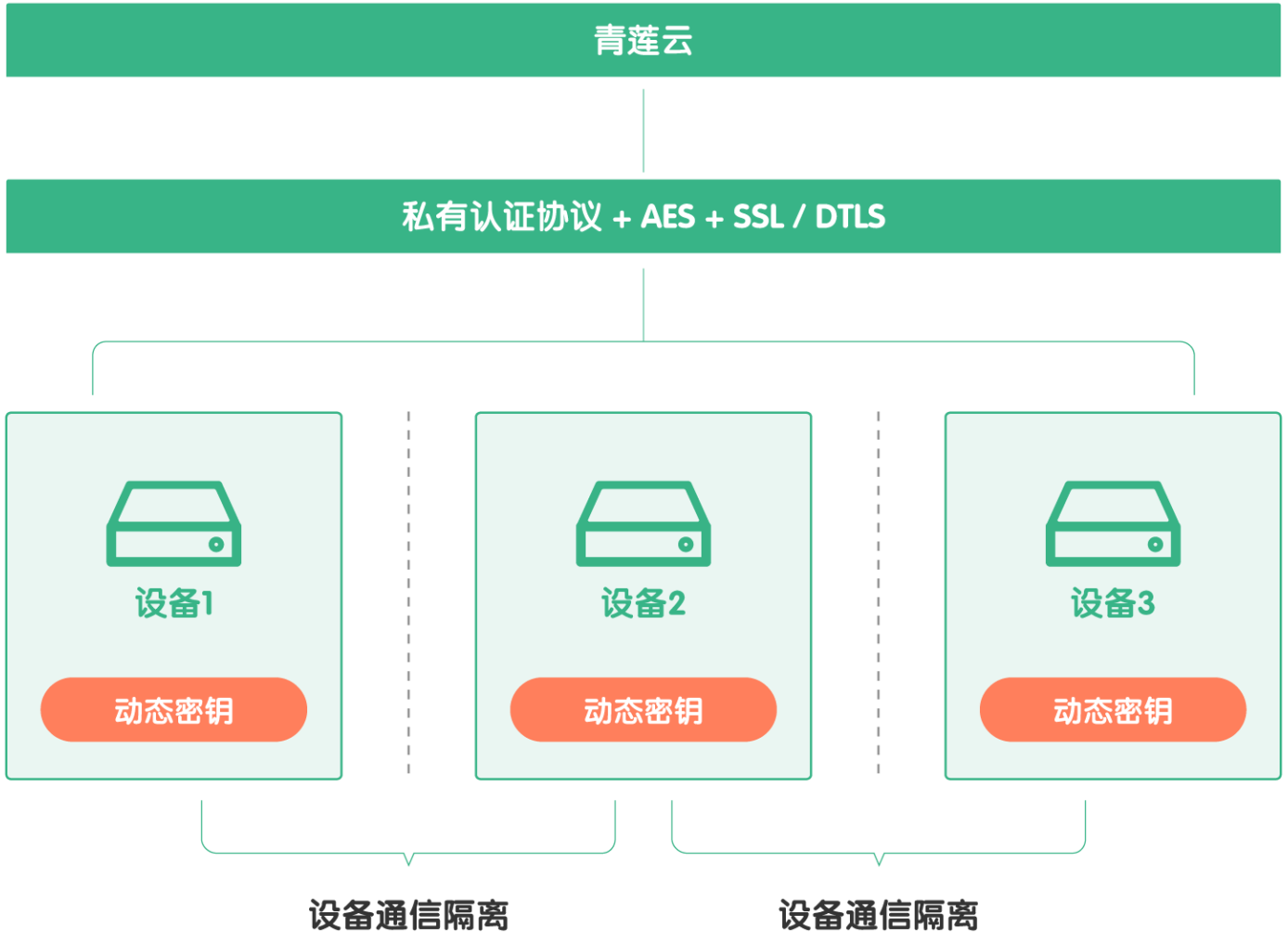
通信安全可信

链路会话唯一

水平逻辑隔离

不同设备直接的通信从逻辑上进行区分，确保会话的唯一性和安全性。

即使同一台设备上运行多个连接实例，连接通信完全没有关系，各自不会相互影响。



设备OTA服务安全要求

当软件本地更新或者远程更新时，为了保证固件不被窃取，应保证固件来源的保密性；

为了防止固件被伪造、被篡改，在所有更新安装之前检查其版本号、完整性和真实性；

为了防止黑客利用老版本固件中可能存在的漏洞，规定只能更新高版本的软件或固件，不可降级。

固件保密性

源数据强加密

固件完整性

分块传输

按块校验

固件不可伪造

固件签名

设备验签

固件不可降级

版本硬编码

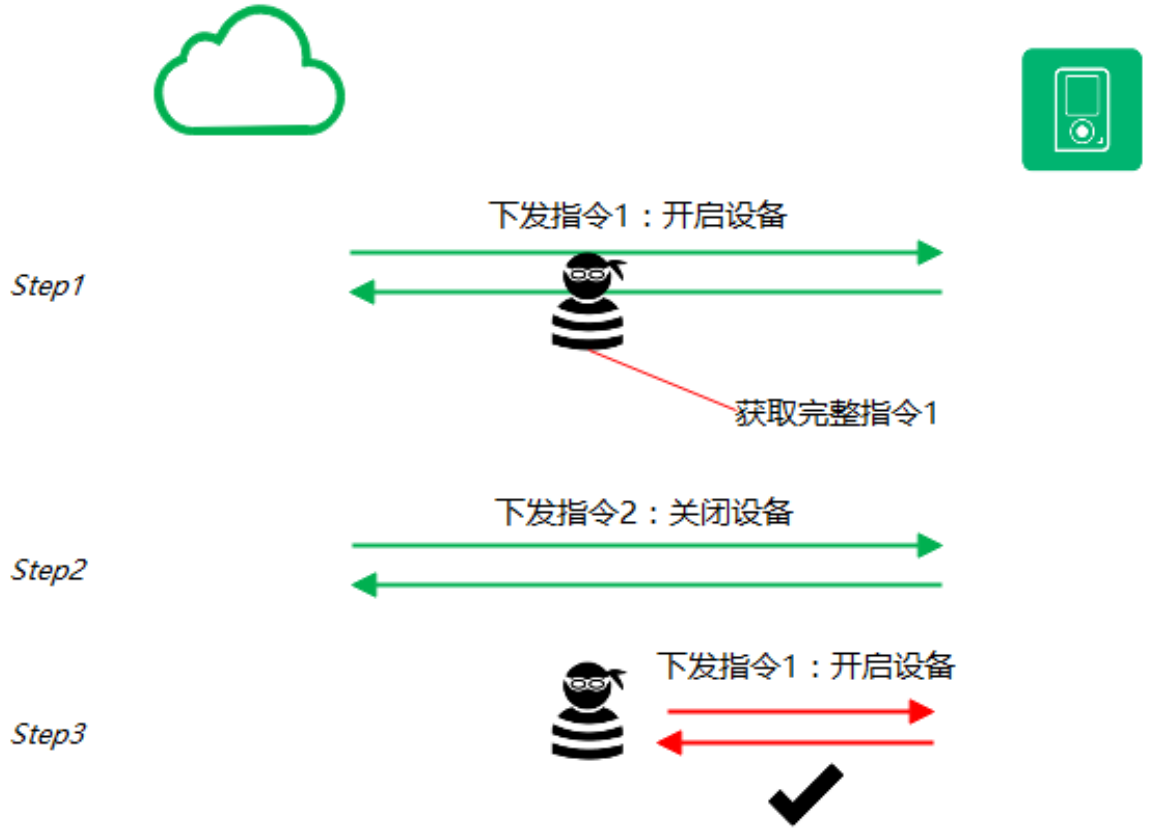
强制版本校验

青莲云防重放攻击策略

重放攻击类型

当通信数据在加密不可破解的情况下，攻击者通常会采用重放攻击的技术手段。
重放攻击主要是通过回放捕获的数据包来达到绕过认证，或者来达到非法下达指令到设备的目的。

- 直接重放
- 反向重放
- 横向重放



重放攻击防御手段

重放攻击防御手段需跟据连接的情况来确定，常用的防御技术手段有如下几种

基于时间戳

- 双方时间同步精准度要求要
- 网速要求高
- 可加时间窗口
- 时间窗口和防御效果成反比

基于序列号

- 严格有序
- 不适用于 如CoAP协议中NO-CON的通信格式

提问-回答

- 提前发送一个提问因子
- 一般发送方是数据请求发送方
- 不适用于下行主动推送命令的场景

绑定随机数

- 每次数据对应的随机数唯一
- 需要记录下来所有的随机数

ARMV8-M安全微处理器架构

ARM平台安全架构模型

基于ARMV8-M指令集的芯片

品牌	型号	内核	时钟	内存	Flash
Microchip	SAM L11	M23	32MHz	16K	64K
新唐科技	M2351	M23	64MHz	96K	512K
意法半导体	STM32L5	M33	48MHz	256K	512K
NXP	LPC5500	M33	100MHz	320k	640K
	i.MX RT600	M33	300MHz	4.5M	
兆易创新	GD32E230	M23	72MHz		
Nordic	nRF9160(NB/LTE)	M33	64MHz	256K	1M
RealTek	……				

微处理器安全技术演进

传统MCU

- Flash 锁
- UID/UCID
- 只执行存储器
- 篡改检测
- 故障注入攻击保护

物联网时代MCU

- 可信根服务
- 硬件级别隔离技术，如TrustZone
- 安全启动
- 安全存储
- 安全调试
- 安全生命周期管理
- PUF
- 硬件加解密引擎
- 物理攻击保护策略

功能应用

- 敏感数据防读取、拷贝
- 内存/flash数据防篡改
- 密钥管理
- 加解密逻辑不可见
- 固件可信
- 禁止调试
- 防侧信道攻击

方案对比

青莲云嵌入式软件解决方案提供足够强度的安全等级保障，
结合硬件本地安全特性，使整个物联网方案安全等级更进一步。

功能\方案	软件方案	软硬件结合方案
强身份认证	√	√
动态秘钥协商	√	√
全链路加密	√	√
防重放攻击	√	√
防中间人攻击	√	√
安全OTA升级	√	√
热补丁升级	√	√
实时/离线消息推送	√	√
私有保密协议	√	√
安全存储	O	√
内存隔离	O	√
硬件加解密引擎	O	√
真随机数发生器	O	√

目录

物联网安全方案产品化

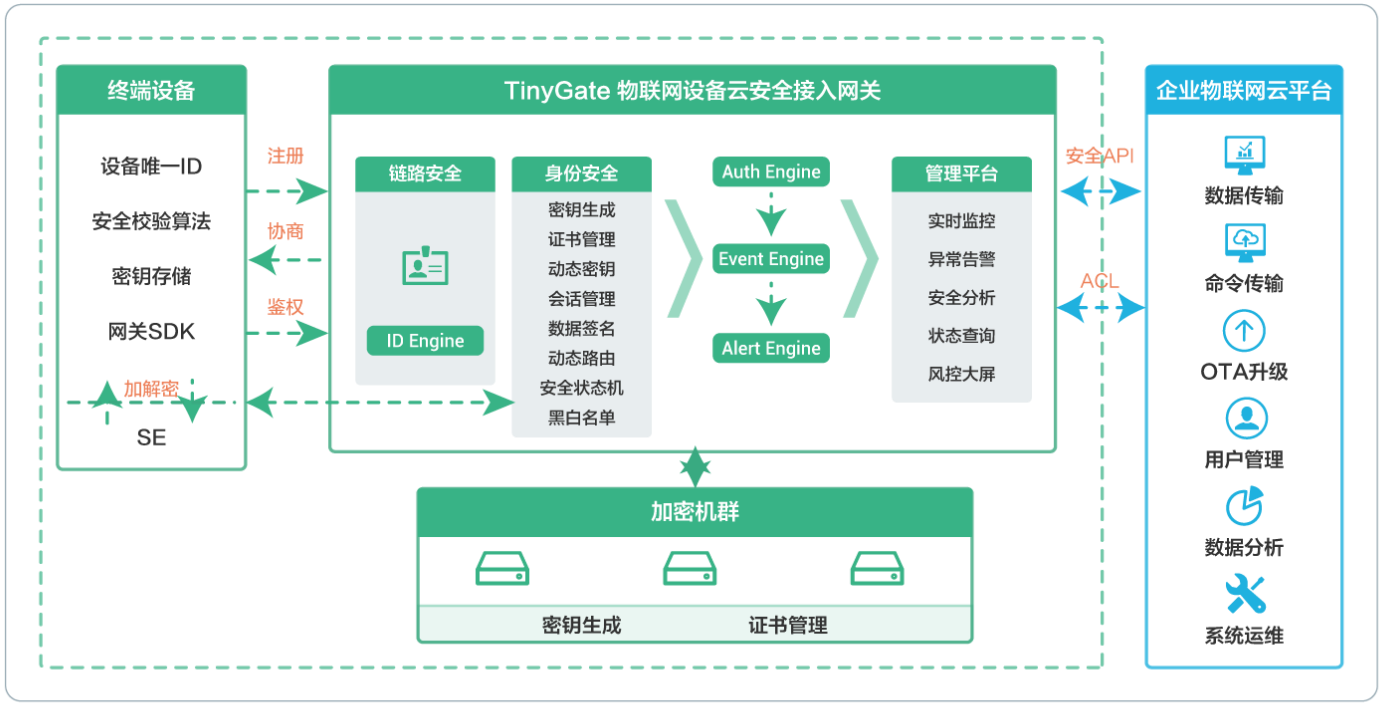
TinyGate物联网云安全接入网关

TinyGate私有化部署方案

TinyGate面向下游全品类通信模组支持

安全连接即服务

青莲云物联网云安全网关（TinyGate）提供出色智能的设备安全入网能力，覆盖设备授权、身份鉴权、密钥管理、加密传输、会话管理、数据签名等多种功能，保护物联网设备及数据免受重放攻击、伪造攻击、数据篡改、会话劫持等网络攻击，并通过安全API和RPC系统调用与企业后端业务平台无缝集成，保障整个通信链路的安全和数据完整性。此系统可以根据企业项目需求灵活调整安全防护等级，可满足多种垂直应用于业务场景的定制化需求。



技术优势

强身份鉴权
- 双向可信验证
- 动态安全协商因子
- 三重验证逻辑

传输安全
- QingLink私有协议
- AES加密
- TLS/SSL加密
- 数据包签名

会话安全
- 一机一密
- 一连一密
- 动态密钥
- 有效期管理

管理安全
- 安全状态监控
- 安全数据分析
- 设备行为分析
- 异常实时告警

TinyGate私有化部署方案

业务层

企业物联网云平台

ACL策略

内网API

安全层

- 安全加密
- 动态密钥
- 安全会话
- 数据签名
- 安全OTA
- 身份识别
- 黑白名单
- 异常分析
- 安全配置
- 安全告警
- 日志分析
- 风控大屏

TinyGate 物联网云安全接入网关

阿里云 | Amazon AWS | Microsoft Azure | 企业自有IDC

设备层

智能家电 | 机器人 | 家庭网关 | 机顶盒 | 摄像头 | 光猫

TinyGate面向下游全品类通信模组支持

NO.	网络类型	芯片品牌	型号	操作系统	配网协议	模组品牌
1	WiFi	乐鑫	ESP8266EX	NONOS	Smartconfig/AirKiss	安信可
2			ESP8266EX	NONOS		蜂汇
3		德州仪器	CC3200	FreeRTOS	Smartconfig/AirKiss	TI
4		庆科	EMW3165	MICO	EasyLink/AirKiss	庆科
5			EMW3031			
6			EMW1062			
7			EMW3080B			
8		高通	QCA4004	ThreadX	Smartlink/AirKiss	江波龙
9		联盛德微电子	W500	FreeRTOS	Oneshot/AirKiss	联盛德微电子
10		汉枫	LPB120	CONTIKI	Smartlink/AirKiss	汉枫
11			LPB125	CONTIKI	Smartlink/AirKiss	
12			LPB200U	Mbed	Smartlink/AirKiss	
13		REALTEK	8711AM	FreeRTOS	Qjoine/AirKiss	利尔达
14		锐迪科	RDA5981	Mbed	Smartconfig/AirKiss	博实结
15		全志	XR871	FreeRTOS	Smartconfig/AirKiss	全志
16	有线	英特尔	X86	Linux		英特尔
17			X64			
18		三星	ARMA9	Linux		三星
19		博通	ARMA8	Raspbian		树莓派
20		瑞萨	RenesasS7	ThreadX		瑞萨
21	GSM / GPRS	移远	M26	Nucleus		移远
22		移柯	L206			移柯
23	NB-IOT	华为	BC95			移远
24		华为	LSD4NBN-LB05000001			利尔达
25	NB-IOT GSM/GRRS	高通	ME3612			中兴物联
26		高通	SIM7000C			芯讯通
27	WIFI /GPRS /LTE	ARM/MTK/高通 ……		Android		
28	SE	华大电子	CIU98320B			
29		万协通	WI32U320			
30		宏思电子	HSC08K1			

目录

青莲云公司基本介绍

基本信息

物联网安全产品全链路业务线

青莲云公司基本介绍

- 青莲云是**业界领先的物联网安全解决方案提供商**，成立于**2016**年，专注于物联网安全研究/攻防对抗、云计算及大数据分析
- 公司总部位于**北京中关村**，在**深圳**设有华南区办事处，在**广州**设有全资子公司
- 成立以来获国内顶级投资机构千万级投资，也是**ARM**中国加速器第一期重点企业
- 核心技术团队来自**奇虎360**，具有**10**年以上企业级安全产品和物联网云平台研发及服务经验
- 围绕物联网业务安全，打造**3**大核心业务板块：**物联网安全产品，物联网安全云平台和物联网安全咨询服务**
- 服务过**200**家以上国内外企业客户，包括**中国电信、美的、TCL、万和电气、中软集团、融创集团、拓邦股份**等
- 联合中国信息通信研究院发布国内首份**《2017中国智能硬件安全白皮书》**
- 拥有工信部颁发的**“智能硬件（IoT）开放平台一致性可信认证”**资质证书
- 荣获中国家用电器协会颁发的**《AWE2017艾普兰奖》**
- 作为美的集团安全合作伙伴之一，受邀参与编写**《美的集团智能家电信息安全标准》**
- 入选IDC年度行业报告**《IDC创新者：中国物联网安全，2017》**
- 荣获中国物联网产业应用联盟：**《2017中国最有影响力物联网安全企业奖》**
- 入选安全牛：**中国网络安全《最具发展潜力初创企业20强》**
- 入选《互联网周刊》&eNet研究院：**《2018物联网企业100强榜单》**

物联网安全产品全链路业务线

业务方向：物联网安全（业务安全）

产品理念：围绕安全开发生命周期（SDL）提供全链路安全产品和服务

物联网云平台	物联网安全接入网关	物联网设备安全管理	物联网安全态势感知	物联网安全咨询服务
• 全品类通信模组支持 • 实时消息 • 安全OTA • 私有化部署 • ……	• 三重身份验证 • 动态设备密钥 • 一机一密 • 通信隔离 • ……	• 安全基线检测 • 流量分析 • 异常行为分析 • 实时告警 • ……	• 日志采集 • 自定义规则 • 人机行为识别 • 可视化展示 • ……	• 物联网安全培训 • 客户端漏洞扫描 • 设备渗透测试 • 系统安全加固 • ……
解决痛点	解决痛点	解决痛点	解决痛点	解决痛点
安全研发和架构设计	链路安全和身份管理	行为监控和基线管理	数据采集和威胁分析	安全体系和安全测试

安全培训+安全测试（体检）

使用产品和服务（治病）

青莲云公司基本介绍

THANKS

2019北京网络安全大会

2019 BEIJING CYBER SECURITY CONFERENCE