南京大学
NANJING UNIVERSITY

物联网与安全

殷亚凤
智能软件与工程学院
苏州校区南雍楼东区225
yafeng@nju.edu.cn，https://yafengnju.github.io/

物联网与安全

- **物联网中的密码学基础**
- 物联网安全现状与特点
- 物联网安全案例
- 总结

物联网中的密码学概述

密码技术功能

- 提供机密性、完整性、真实性、不可否认性的保障
- 密码学是确保数据安全与隐私的重要工具

密码学算法

- 加解密算法：机密性
- 摘要算法：完整性
- 消息认证码：真实性
- 数字签名：不可否认性
- 随机数生成算法

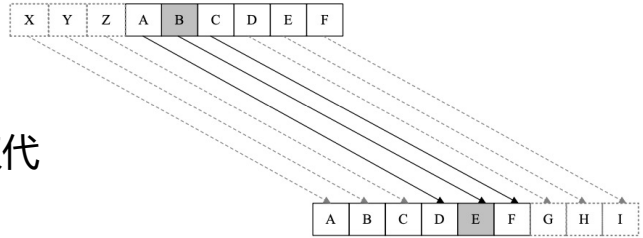
加解密算法

秦兵书《六韬》

太公曰：“主与将有阴符，凡八等：有大胜克敌之符，长一尺；破军擒将之符，长九寸；降城得邑之符，长八寸；却敌报远之符，长七寸；警众坚守之符，长六寸；请粮益兵之符，长五寸；败军亡将之符，长四寸；失利亡士之符，长三寸。诸奉使行符，稽留者，若符事泄，闻者告者皆诛之。八符者，主将秘闻，所以阴通言语，不泄中外相知之术。敌虽圣智，莫之能识。”

凯撒密码

- 相传由古罗马帝国的凯撒皇帝发明
- 做法：每个字母被往后位移 3 个字母所取代



现代密码学

- 对称加密
- 非对称加密(也称为公钥加密)

加解密算法

常见对称加密算法

DES(data encryption standard，数据加密标准)

- 将固定长度的明文通过一系列复杂的代换操作变成同样长度的密文的算法

AES(advanced encryption standard，高级加密标准)

- 基于代换操作
- 根据密钥长度不同，代换的轮数不同
- 比DES要小，速度更快

SM1、SM4 和 SM7

- SM4算法密钥长度为128位，加密采用32轮迭代完成，是我国无线局域网标准WAPI中所采用的分组密码标准
- SM1、SM7算法不公开，需要使用专用芯片

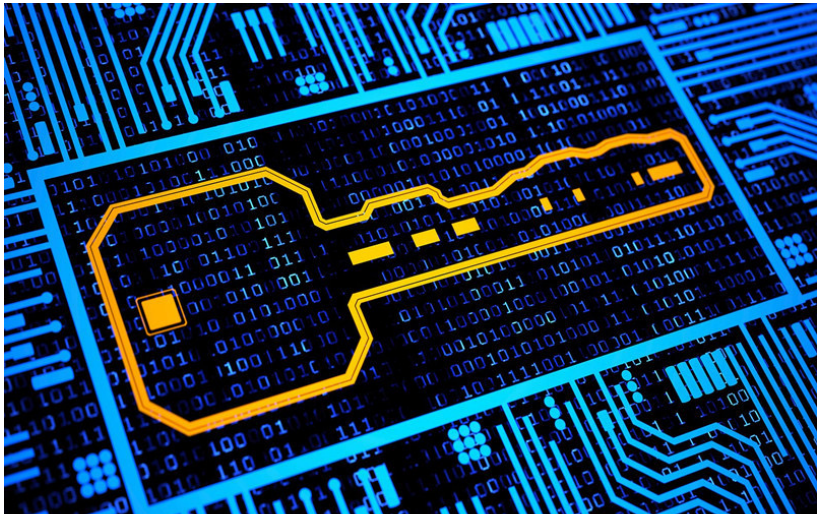
Salsa20、ChaCha20

- 流加密算法
- 对数据流加密，加密和解密双方使用相同伪随机加密数据流作为密钥，明文数据每次与密钥数据流顺次对应加密，得到密文数据流

加解密算法

工作模式(mode of operation)

简介：分组加密算法的加、解密操作单位都是块，通常较小(如DES 的块大小为8B)， 在实践中，如果加密多于一块的数据，就需要工作模式的支持



常用的工作模式

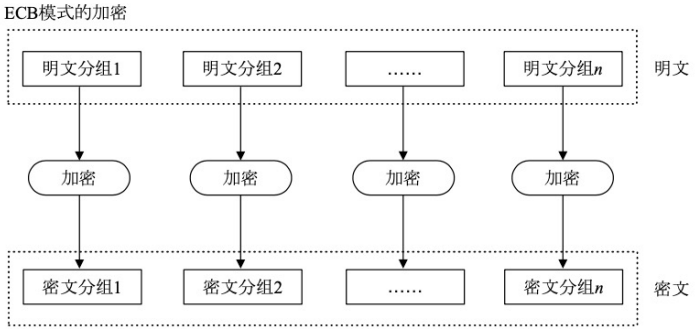
- 电子密码本模式
- 分组链接模式
- 计数器模式

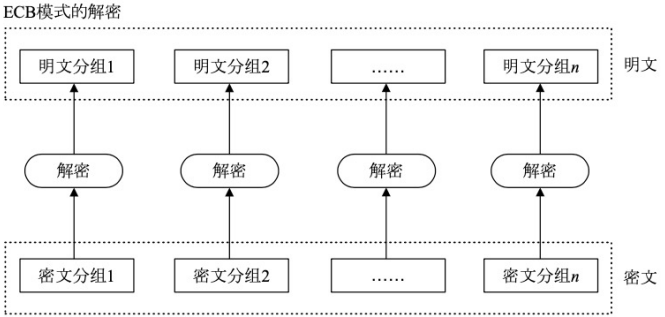
加解密算法

电子密码本(electronic codeBook，ECB)模式

加密的消息按照加密算法的块大小分为若干块，每个块独立加密

缺点：相同的明文块会被加密成相同的密文块，加密数据容易被分析，因此并不常用





加解密算法

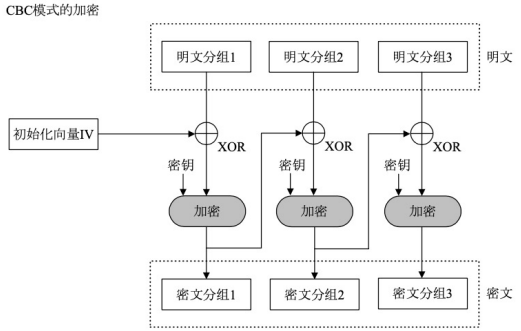
分组链接模式

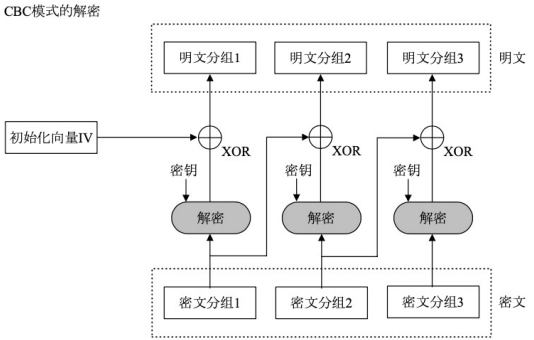
先加密的块会影响后加密的块

同样的明文块加密后，不会得到相同的结果

分类

- 密文分组链接(cipher-block chaining，CBC)模式: 除首块外的每个明文块先与前一个密文块进行异或后再进行加密，而第一个块需要与初始化向量(initialization vector，IV)异或
- 密文反馈(cipher feedBack，CFB)模式
- 输出反馈(output feedback，OFB)模式



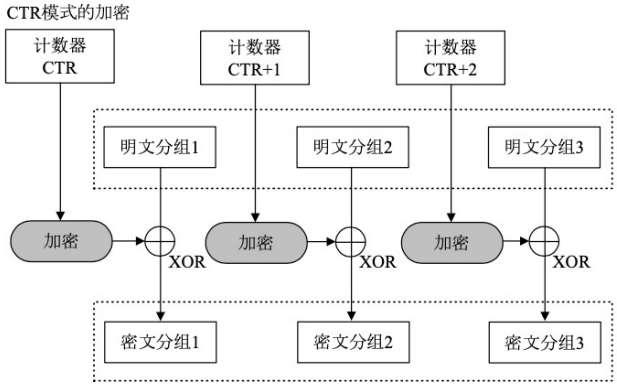


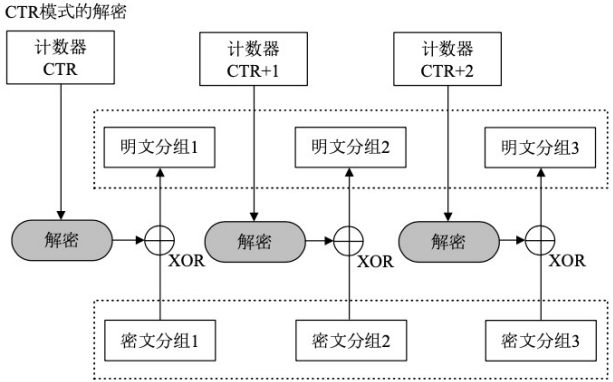
加解密算法

计数器(counter，CTR)模式

使用递增的计数器，通过对计数器的值加密产生连续的密钥流，与明文异或得到密文分组

在加密和解密的过程都可以并行处理





加解密算法

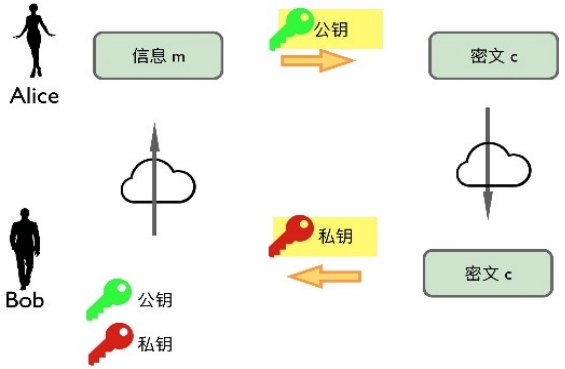
非对称加密算法(也叫公钥加密算法)

需要两个密钥

- 一个是公开密钥， 通常用作加密和验证签名；另一个是私有密钥，通常用作解密和签名

常见算法

- RSA 算法和椭圆曲线算法



RSA 算法

依赖于大整数不易分解质因数的数论难题

记 RSA 算法中，用户的公钥和私钥分别为K^+和K^- ，相应的操作为函数$K^+(\cdot)$和$K^-(\cdot)$ ，$K^+(K^-(m))=m=K^-(K^+(m))$

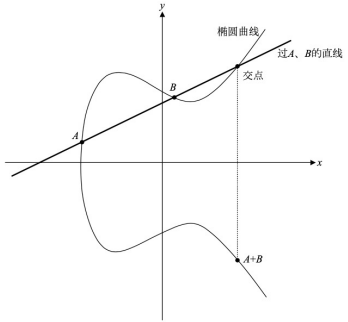
加解密算法

椭圆曲线(elliptic curve)算法

- 相比于 RSA，密钥长度较短。
- 长度为 256 位的椭圆曲线密钥，安全性与长度为 3072 位的 RSA 密钥相当。
- 可以表示(或经过变换)为下面的方程，即

$$y^2 + axy + by = cx^3 + dx^2 + ex + f$$

- 考虑一组特殊的曲线: $y^2 = x^3 + ax + b$，在曲线上定义两点 A 和 B 的加法为: 两点连线(两点重合时为切线)与椭圆曲线交点关于 x 轴的对称点。
- 取一个随机的大数k 作为私钥，计算曲线上一点 G 的 k 倍点 kG (即 k 个 G 相加)作为公钥。



椭圆曲线上的加法

摘要算法

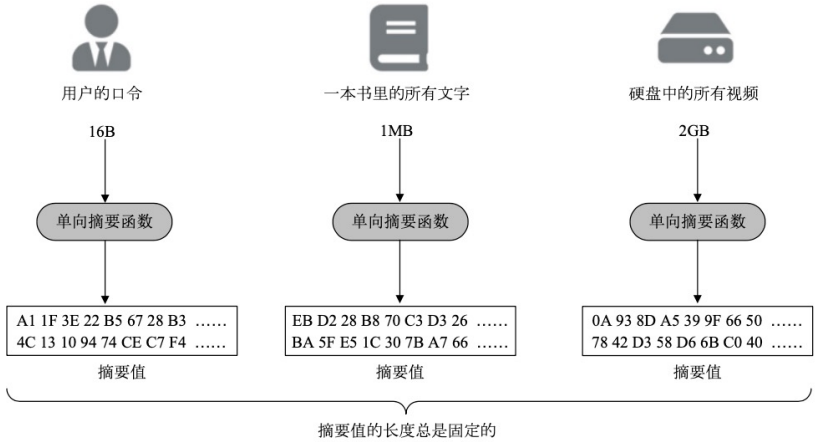
也叫散列算法或哈希算法，是一种从任意数据创建出小数据的算法

特点

- 单向的，无法从摘要中恢复出任何消息
- 根据任意长度的输入都可计算出固定长度的摘要值
- 不同的输入通常产生不同的输出，相同的输入一 定产生相同的输出
- 不同的输入产生相同输出(称为“碰撞”)的概率极低

用途

- 保护用户口令: 数据库里存储用户的口令(往往还需一些额外的数据处理)的摘要值而非原始值
- 数据校验: 验证文件的完整性
- 作为消息验证码或数字签名的一部分



摘要算法

常用的摘要算法：

MD5

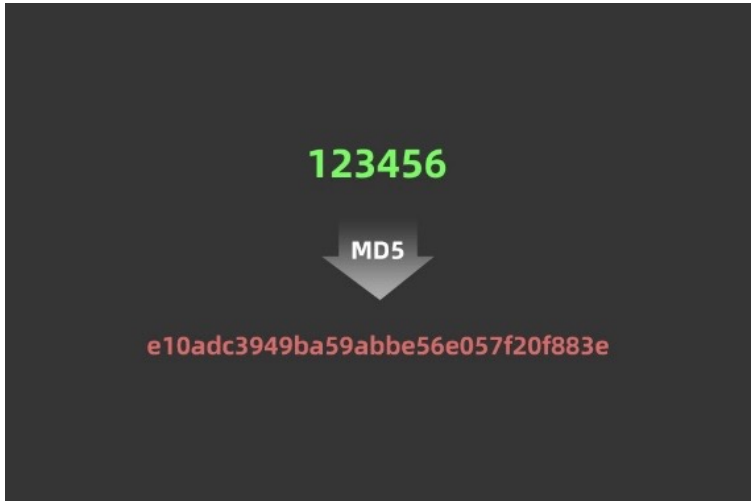
曾经非常常用，输出长度为 128 位

SHA-1/2/3

由于 MD5 存在碰撞攻击的缺陷，美国国家标准技术研究院制定了 SHA-1 算法作为 MD5 的继任者，但 SHA-1 也被发现存在安全问题。截至目前，还未出现对 SHA-2/3 系列算法的有效攻击

SM3

我国国家密码管理局 于 2010 年发布的摘要算法，目前已被收录于国际标准 ISO/IEC 10118-3:2018 中

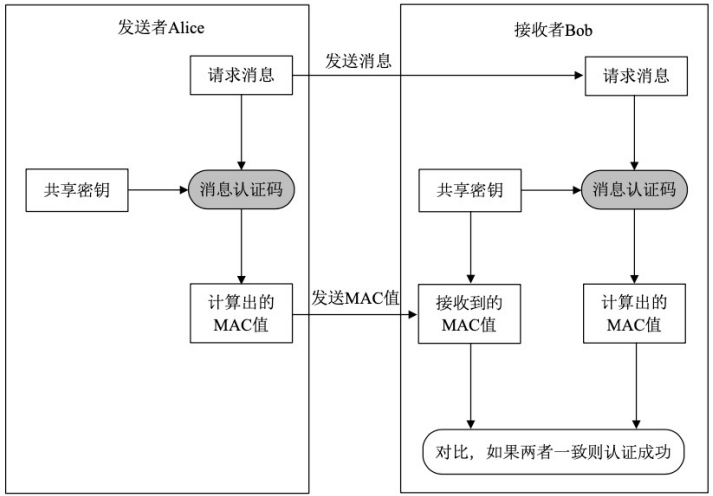


消息认证码

既确认消息完整性，又对消息进行认证的算法

常用的消息认证码算法

- 基于摘要算法的 HMAC 算法
- 基于分组密码的 CBC-MAC 算法
- 基于流密码的 MAC 算法



消息认证码的使用方法

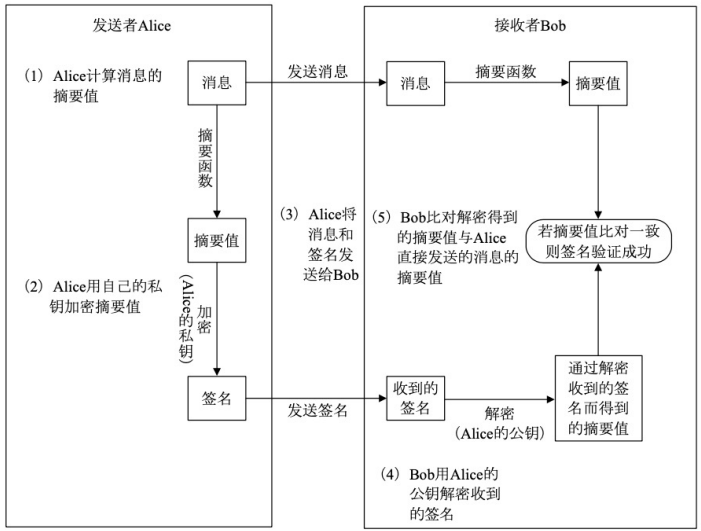
数字签名

使用非对称密钥的方法，来区分生成消息签名和验证消息签名两个行为

必须使用私钥才能签名，可以同时做到识别篡改和防止抵赖

常用的数字签名算法

- RSA 算法
- DSA 算法
- ECDSA 算法



数字签名的常用流程

随机数生成算法

分类

弱伪随机数

- 使用伪随机数生成器生成的随机数
- 只具备随机性，即满足一定的概率分布

强伪随机数

- 使用密码学伪随机数生成的随机数
- 除了具备随机性外，还具备不可预测性，即攻击者知道过去生成的伪随机数列也无法预测下一个伪随机数

真随机数

- 使用真随机数生成器生成的随机数
- 除了具备上述的随机性和不可预测性外，还具备不可重现性，即无法重复随机数的生成过程

物联网与安全

- 物联网中的密码学基础
- **物联网安全现状与特点**
- 物联网安全案例
- 总结

物联网的安全现状

对物联网的常见攻击方式

拒绝服务攻击(denial-of-service，DoS)

- 目标：让被攻击的机器或网络资源无法向目标用户提供服务
- 分布式拒绝服务(distributed denial-of-service)DDoS

物理攻击

- 目的：破坏硬件设备

隐私攻击

- 窃听和被动监测

物联网新的安全需求与挑战

身份验证和管理：安全地管理用户和设备对信息的访问权限

访问控制：人或物在通过身份验证后，有没有访问特定资源的权限

信任机制：参与通信的实体之间的信任和用户对物联网系统的信任

物联网与安全

- 物联网中的密码学基础
- 物联网安全现状与特点
- **物联网安全案例**
- 总结

低功耗蓝牙安全

低功耗蓝牙 BLE

一种低功耗、低成本的通信技术，由蓝牙技术联盟设计并制定规范，广泛应用于个人穿戴设备、智能家居和智能医疗设备中，如手环、智能手表、智能锁等

在实验室场景下，通信范围可达到 250m，同时保持 100Kb/s 的数据传输速率

参与 BLE 通信的两个设备分别叫做中心设备和外围设备

中心设备

- 请求数据的一方，功耗相对较高
- 多为个人计算机、智能 手机等拥有更多计算和内存资源的设备

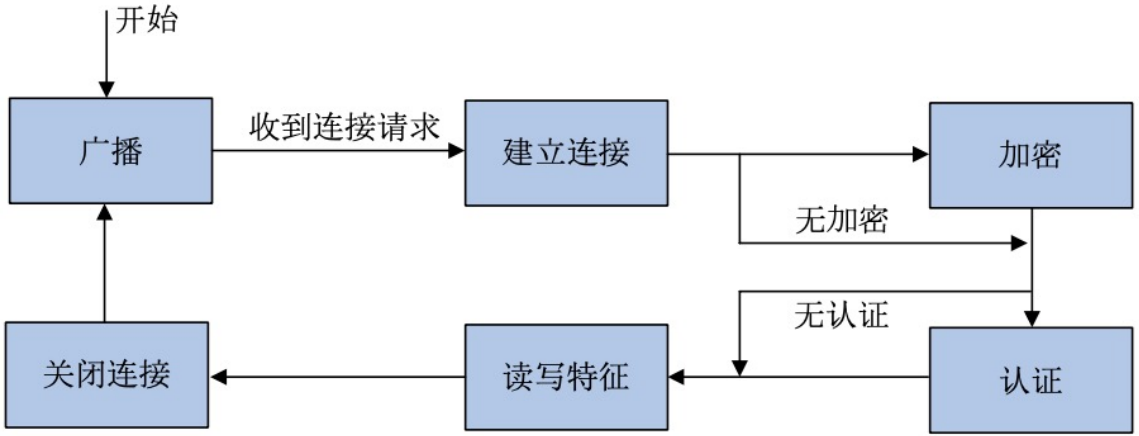
外围设备

- 提供数据和相关功能的设备，功耗通常较低
- 多为各种手环、智能手表等计算和内存资源较少的设备

低功耗蓝牙安全

中心设备与外围设备通信的主要过程

- 外围设备发送广播数据(advertising data)
- 中心设备和外围设备建立连接
- 完成要求的加密和认证过程，读写数据
- 关闭连接， 外围设备重新进入广播状态



BLE通信流程

低功耗蓝牙安全

协议层加密方法目的

- 对敏感信息进行保护，防止第三方的窃听

配对

- **定义**：加密密钥的协商生成过程。
- 一般仅发生在两个设备还未共享过加密密钥的情形
- 可以由中心设备或者外围设备的任意一方发起，交换配对参数后计算出加密密钥

根据中心和外围设备的输入输出能力协商加密密钥的方式

- Just Works
- Numeric Comparison
- Passkey Entry

低功耗蓝牙安全

具体过程

- 双方共享加密密钥后，就可以对通信连接进行加密以防止窃听
- 一方发送加密请求(LL_ENC_REQ)包
- 另一方回复 LL_ENC_RSP 包接受加密请求，或回复 LL_REJECT_IND 拒绝加密请求，中断加密流程
- 加密过程可以在任何需要的时间由任意一方发起或中断

安全挑战

- 协议层的身份欺骗
- 构造虚假的数据包来伪造自身的能力
- 中心设备长时间未收到同意加密请求的 LL_ENC_RSP 数据包，会中断加密请求
- 设备再次重新连接时，身份验证是可选的而非强制的

近场通信安全

NFC Forum 组织3 种通信模式

- 读写器模式、卡模拟模式和点对点模式

特点

- 工作距离短、通信速度快、标签或卡无须电源

应用场景

- 非接触式支付、门禁、票务等智慧城市 和家居场景，电子钥匙、个性化驾驶等智能驾驶场景，以及设备认证、固件升级等智能工业场景

NFC 标签根据物理层和数据的组织方式分为 5 类（Type1-5）

- 在我国应用最广泛的是 Type 2 和 Type 4
- Type 2 普遍用于非金融领域，典型的应用场景是一般的身份验证
- Type 4 适用于更复杂的数据交换，特别是各种支付(如公共交通、金融)和密钥交换认证等应用

近场通信安全

NFC 技术的安全性

- 针对智能卡(或标签)的攻击
- 针对银行卡的攻击：利用特殊的装置窃取信用卡和 POS 机之间的非接触式交易，提取有用信息
- 中继攻击：利用一些设备做数据的转发，将 NFC 的通信距离延长

LoRaWAN安全

LoRaWAN

由节点、网关、网络服务器和应用服务器(入网服务器)构成

协议 1.1 版中规定

- 使用对称加密算法(AES-128) 对节点和服务器发送的数据载荷
- 使用 MAC 命令进行加密和解密

激活

一个节点在加入网络时， 需要进行设置与激活来获取相应的密钥，从而能够与服务器进行通信

激活的方式

- 手动激活(activation by personalization)
- 无线配对激活(over-the-air activation)

LoRaWAN安全

手动激活

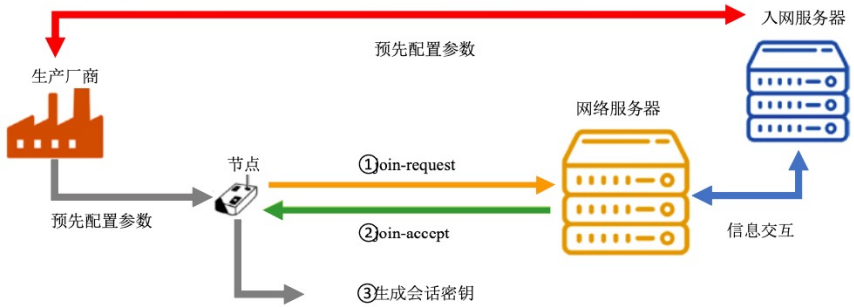
所有的密钥和相关信息通过数据线直接烧录到节点中安全的存储单元内

无线配对激活

节点通过发送加入请求（join-request）命令申请加入网络，入网服务器回复允许入网（join-accept）命令，将一些加密参数发送给节点，用于生成节点与服务器通信所需的对称密钥

对LoRaWAN的攻击

- 拥塞攻击
- 重放攻击
- 信标同步攻击
- 网络流量分析
- 中间人攻击



LoRaWAN入网流程

物联网攻击检测

蜜罐系统

一种特殊的系统，在被全面监控的情况下接入网络，本身不提供任何有用的功能，就是等待着被入侵和攻击

正常情况下，任何人或程序都不会访问蜜罐

分类

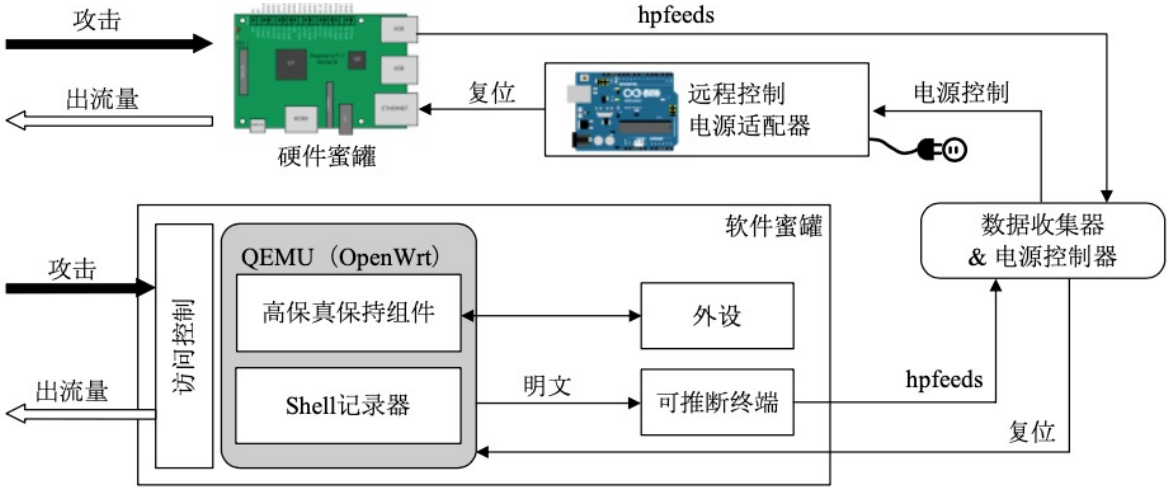
- 高交互式蜜罐(high-interaction honeypot)
- 低交互式蜜罐(low-interaction honeypot)

比较项	低交互式蜜罐	高交互式蜜罐
操作系统	不直接依赖	高度依赖
被攻击风险	低	高
维护代价	低	高
保真度	低，只能捕获已知类型攻击	高，可以捕获各种攻击

物联网攻击检测

蜜罐系统的搭建

- 传统蜜罐方案不易于直接迁移到物联网环境中
- 硬件蜜罐（单板机）：具有最高的保真度，可以直接捕获针对设备的攻击和威胁，因而是了解针对物联网设备网络攻击的最直接、最有效的工具
- 公有云蜜罐（HoneyCloud）：降低成本，提高可靠性，并且能方便地在全球部署

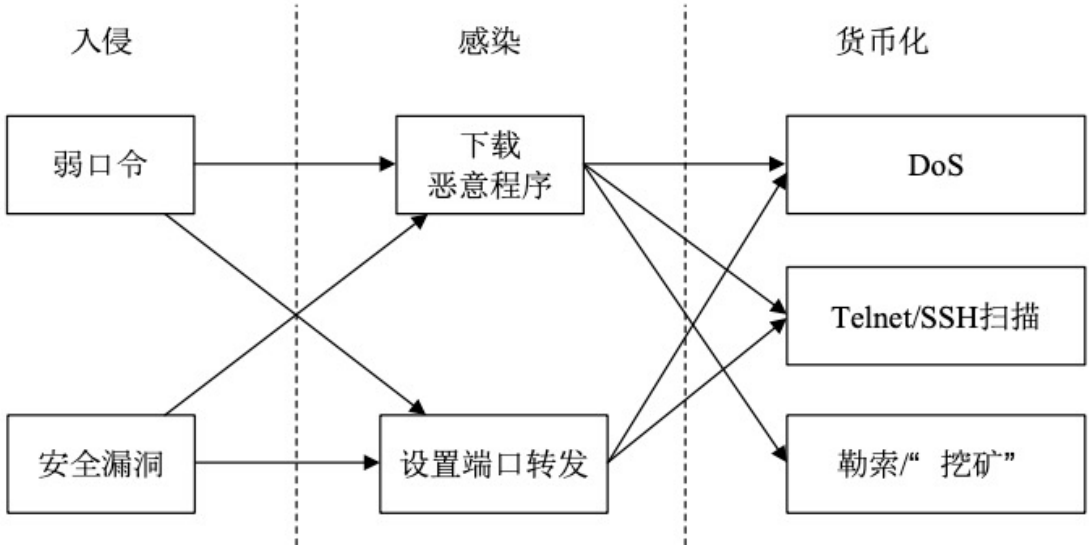


HoneyCloud系统架构

物联网攻击检测

攻击步骤

- **常规**：入侵、感染、货币化
- **无文件攻击**：在感染和货币化两个步骤的操作与常规攻击有所不同



HoneyCloud系统捕获到的攻击流程

物联网与安全

- 物联网中的密码学基础
- 物联网安全现状与特点
- 物联网安全案例
- **总结**

总结

由于设备性能有限，目前还难以在物联网设备内部署较高级的安全防护产品(如防火墙、杀毒软件及入侵检测系统等)

这给黑客以及网络黑色产业带来了可乘之机，网络攻击也逐渐从传统的信息空间向物理空间渗透， 攻击不仅仅是破坏信息系统，更有可能造成物理世界的破坏

随着网络攻击向物理世界的不断渗透，物联网安全问题将尤为突出

设备安全、系统安全及法律保障等多层次物联网安全，将是全方位构建更安全可信的物联网的关键手段

提问

Q & A

殷亚凤
智能软件与工程学院
苏州校区南雍楼东区225
yafeng@nju.edu.cn，https://yafengnju.github.io/

南京大学 NANJING UNIVERSITY