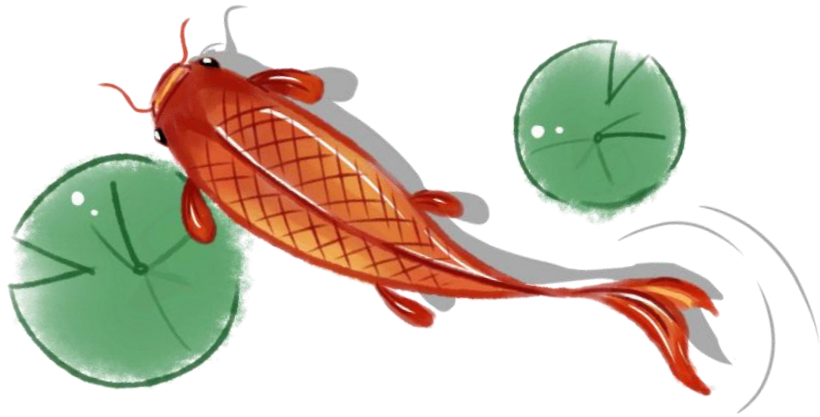
计算机网络安全技术

- 课程代号：*40240572*
- 课程对象：本科生
- 授课教师：尹　霞
- 开课单位：计算机系网络所

主要内容

- 无线网络概述
- 无线局域网安全威胁
- 无线局域网加密认证技术

无线网络概述



无线网络概述

- 计算机与移动通信技术的结合，使得移动无处不在；
  无线网络技术是实现6A梦想/移动计算/普适计算的核心技术

- 5W：
  - 何人（Whoever）
  - 何时（Whenever）
  - 何地（Wherever）
  - 与何人（Whomever）
  - 能以何形式（Whatever）通信的移动计算技术

- 6A：
  - 任何人(Anyone)
  - 任何时候(Anytime)
  - 任何地点(Anywhere)
  - 采用任何方式(Any means)
  - 与其他任何人(Any other)
  - 进行任何通信(Anything)

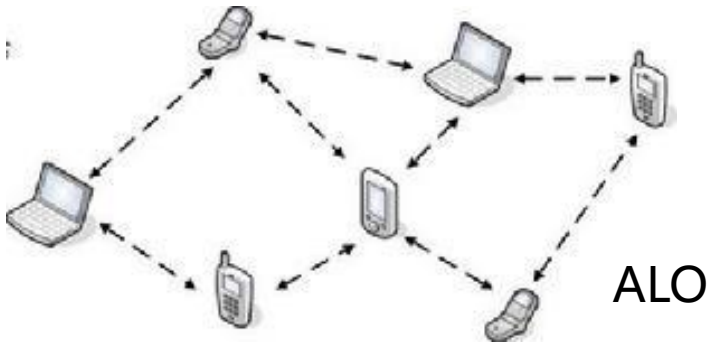
无线电通信技术发展史

- 无线电通信技术是在没有物理连接的情况下多个设备之间能够互相通信的技术

  - 1901年，意大利物理学家马可尼跨越大西洋3200公里的无线电试验 (莫尔斯码)
  - 1921年，移动无线电开始使用2MHz频段
  - 1924年，贝尔实验室发明了具备双向通话能力的无线电话系统
  - 1935年，首次采用调频技术FM，提高了传输质量
  - 1947年，AT&T第一次推出了商业性的移动电话服务，蜂窝技术经历了漫长的发展之路
    - 美国联邦通信委员会FCC限制了可用频率的数量，1976年，纽约市只有不到600名移动电话用户，申请者超过了3500人
    - TDMA->CDMA->GSM->3G->4G

无线网络的诞生

- 1968年，美国夏威夷大学设立了一项研究计划ALOHA，目的是要解决分散在各岛的多个用户通过无线电信道使用中心计算机，从而实现一点到多点的数据通信
- 1971年，世界上最早的无线电计算机通信网ALOHA建成
  - 7台计算机双向星形拓扑跨越4座夏威夷岛屿
  - ALOHA采用无线电广播技术和著名的Pure ALOHA协议
  - ALOHA net是第一个使用无线电通信来代替点到点连接线路作为通信设施的计算机系统，无线网络正式诞生
- 现代的数字无线系统性能更优，但基本思想并没有变化
  - WPAN、WLAN、WMAN、WWAN



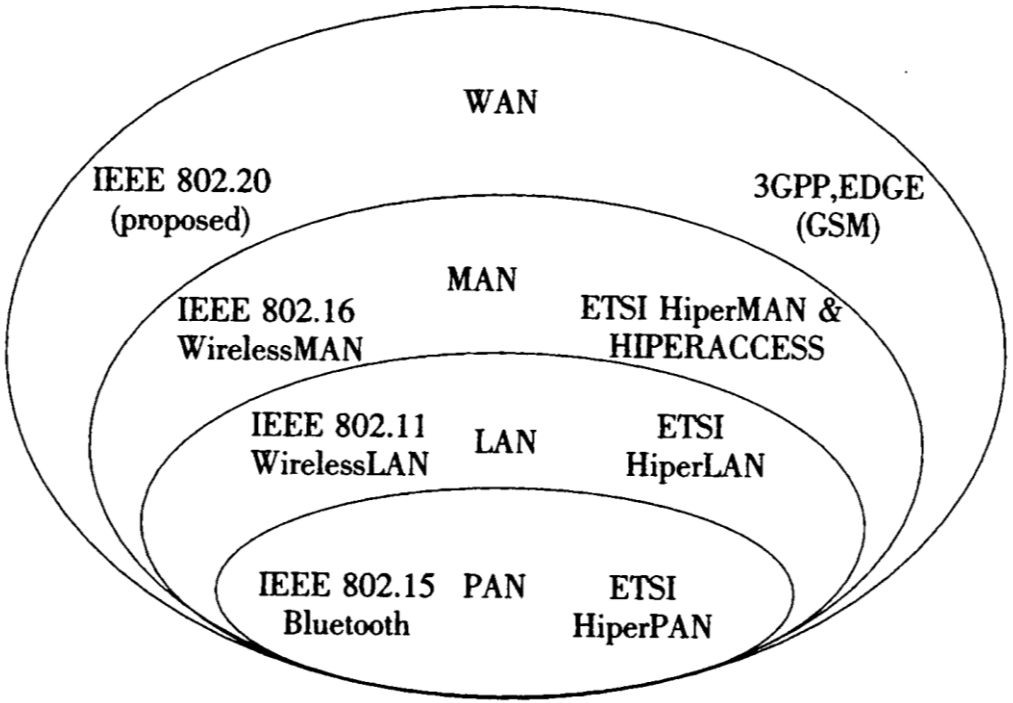
ALOHA示意图

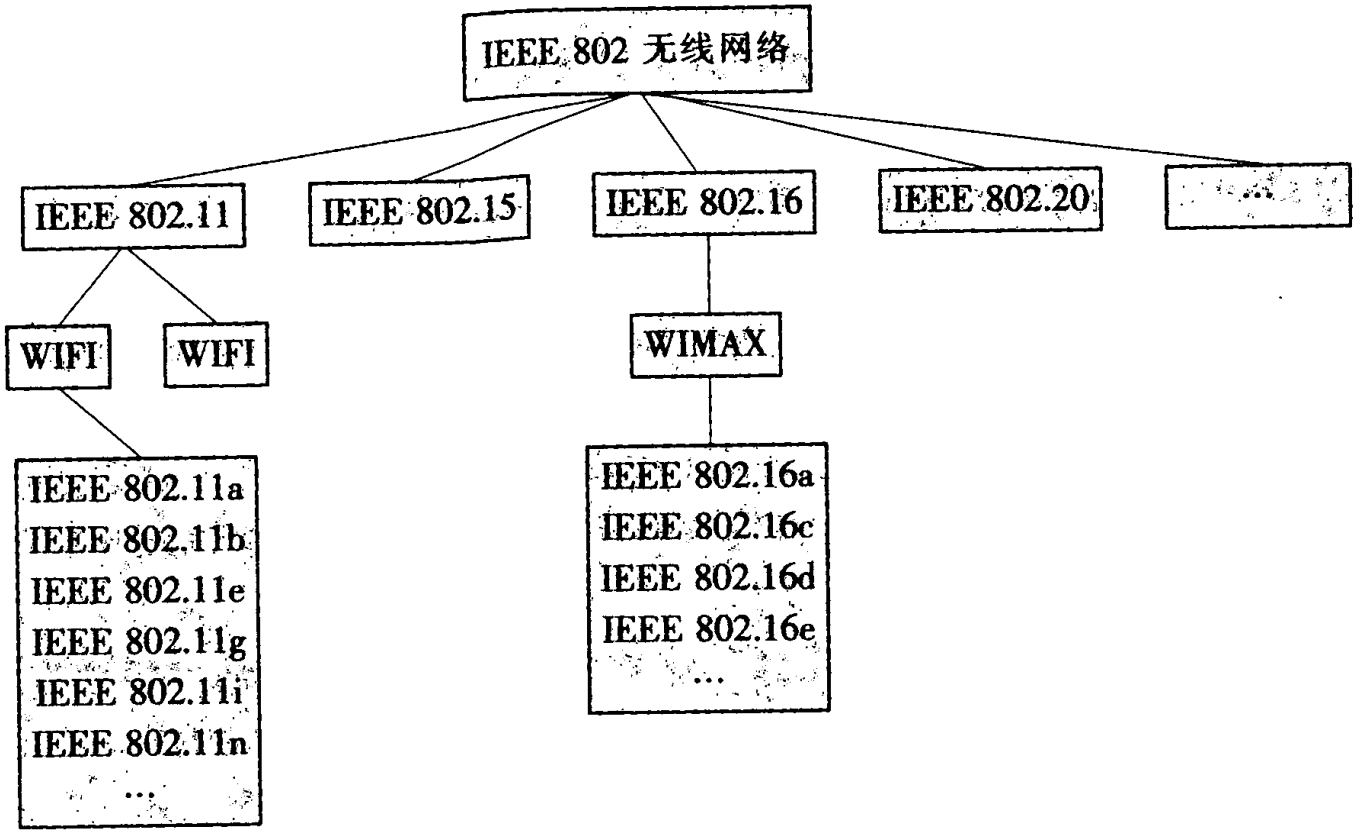
无线网络分类

	网络类型	应用范围/典型技术	传输距离
无线网络	无线个域网WPAN (Wireless Personal Area Network)	点对点短距离链接，个人办公家庭环境 IEEE 802.15x/Bluetooth/ZigBee等	10m左右
	无线局域网WLAN (Wireless Local Area Network)	点对多点无线连接，支持AP间切换 IEEE 802.11（a,b,g,i,n）等	100m
	无线城域网WMAN (Wireless Metropolitan Area Network)	点对多点无线连接，支持基站间漫游与切换 IEEE 802.16等	1-50KM
	无线广域网WWAN (Wireless Wide Area Network)	全球通讯，通信卫星 IEEE 802.20等	1-15KM

全球无线网络技术标准

- 电气与电子工程师协会IEEE制定了IEEE 802系列标准
- 欧洲电信标准化协会ETSI制定了HiperLAN标准

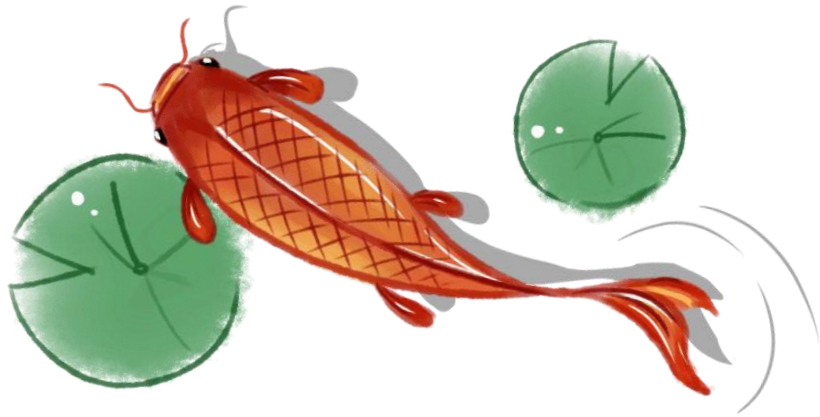




新技术层出不穷、新名词应接不暇

- 无线网络现状
  - 从移动Ad Hoc网络到无线传感器网络(WSN)、无线Mesh网络
  - 从Wi-Fi到WiMedia、WiMAX
  - 从IEEE 802.11、IEEE 802.15、IEEE 802.16到IEEE802.20
  - 从固定宽带无线接入到移动宽带无线接入
  - 从蓝牙到红外、HomeRF、ZigBee
  - 从GSM、GPRS、CDMA到3G、4G、5G……
- 从应用的角度看，无线网络还可划分出Ad hoc 网络、无线传感器网络WSN、无线Mesh网络、无线穿戴网络……这些是基于已有的无线网络技术，针对具体的应用而构建的无线网络

无线局域网安全威胁



无线局域网WLAN

- 无线局域网WLAN利用无线射频（RF）电波作为信息传输的媒介构成的局部无线网路，与有限局域网的用途十分类似，最大的不同在于传输媒介的不同，它利用无线电技术取代网线，可以和有限网络互为备份
- 与有线局域网相比，无线局域网通信范围不受环境条件的限制，用户能够更方便，灵活，快捷的访问网络资源；无线局域网已成为INTERNET宽带接入的重要手段
- 便捷的无线局域网同时带来了新的安全问题：无线电波无法向传统线缆或光纤一样采用物理隔离，无线局域网安全面临巨大挑战

WLAN的安全威胁


窃听
漫游造成的问题
通信阻断
服务区标识符的安全问题
数据的注入与篡改
隐匿无线信道
中间人攻击
客户端对客户端的攻击
客户端伪装
接入点伪装
匿名攻击

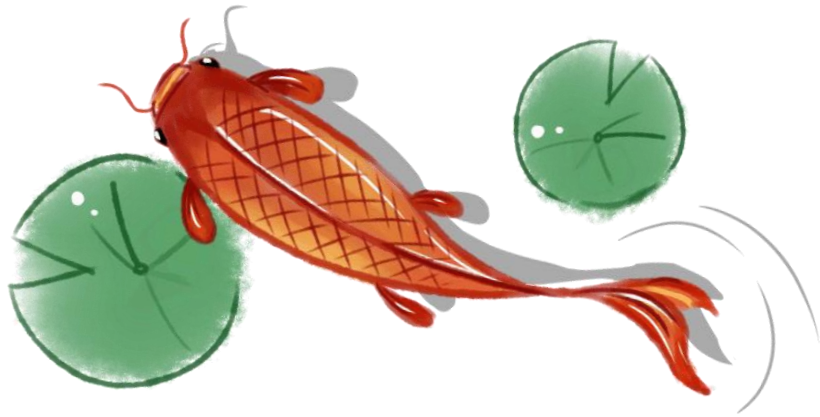
WLAN的安全威胁

- 无线窃听
  - 无线信道是一个开放性信道，任何具有适当无线设备的人均可以通过窃听无线信道而获得上述信息
  - 无线窃听可以导致信息泄露，移动用户的身份信息和位置信息的泄露可以导致移动用户被无线跟踪
- 假冒攻击
  - 攻击者截获到一个合法用户的身份信息时，就可以利用这个身份信息来假冒该合法用户的身份入网
- 信息篡改
  - 主动攻击者将窃听到的信息进行修改（如删除或替代部分或全部信息）之后再将信息传给原本的接收者

WLAN安全威胁

- 重放、重路由、错误路由、删除消息
  - 重放攻击是攻击者复制有效的消息事后重新发送或重用这些消息以访问某种资源
  - 重路由攻击是指攻击者改变消息路由以便捕获有关信息
  - 错误路由攻击能够将消息路由到错误的目的地
  - 删除消息是攻击者在消息到达目的地前将消息删除掉，使得接收者无法收到消息
- 网络泛洪
  - 入侵者发送大量伪造的或无关消息从而使得AP忙于处理这些消息而耗尽信道资源和系统资源，进而无法对合法用户提供服务

无线局域网加密认证技术



无线局域网加密认证技术

- 无加密认证 （SSID，Mac）
- 有线等效加密技术WEP
  - 多用于小型的、对安全性要求不高的场合
- WPA（Wi-Fi Protected Access）
  - TKIP （Temporal Key Integrity protocol） 临时密钥完整性协议
  - AES（Advanced Encryption Standard）高级加密标准
  - IEEE 802.1x认证协议(基于端口的访问控制协议)

无加密认证

- 无线接入点AP(Access Point)
  - AP是一个无线网络的创建者，是网络的中心节点
  - 一般家庭或办公室使用的无线路由器就一个AP
- STA站点
  - 每一个连接到无线网络中的终端都可称为一个站点

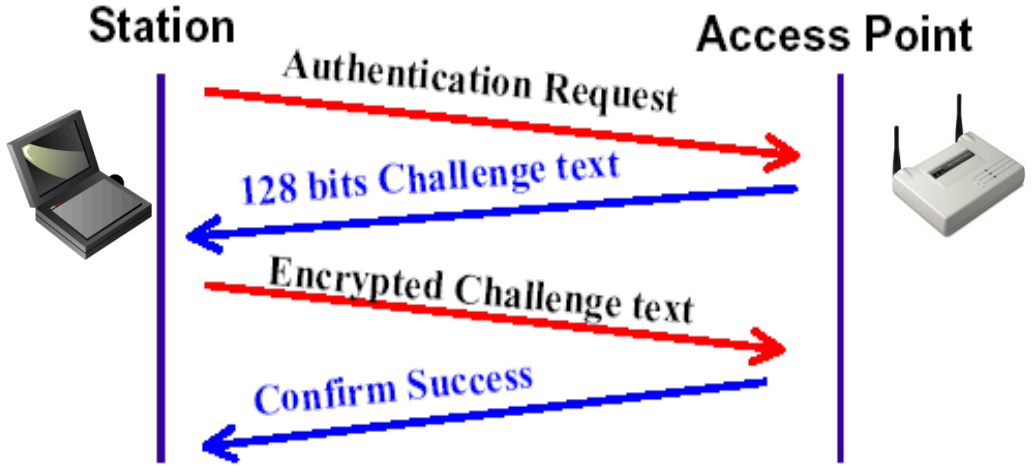
- SSID(Service Set Identifier):
  - SSID是为了便于用户识别，为每个AP配置的标志名，俗称wifi名
  - 只要使用者能够提出正确的SSID，AP就接受用户端的登入请求
  - 通常情况下，AP会向外广播其SSID
    - 可以通过Disable SSID Broadcast来提高无线网络安全性

有线等效保密协议WEP

- 有线等效保密协议WEP（Wired Equivalent Privacy）目的是为无线局域网提供与有线网络相同级别的安全保护，协议标准为IEEE 802.11b
  - 1999年成为WLAN安全标准，2003年被WPA替代，现在的WLAN产品依然广泛支持
- WEP使用对称加密算法，保证无线局域网的数据传输安全性
  - 采用RC4流加密算法
  - 提供访问控制和保护隐私的功能
- 在无线局域网中，要使用WEP协议，无线AP首先要启用WEP功能，创建密钥；然后在每个无线客户端启用WEP，并输入该密钥，这样就可以保证安全连接

WEP的安全措施

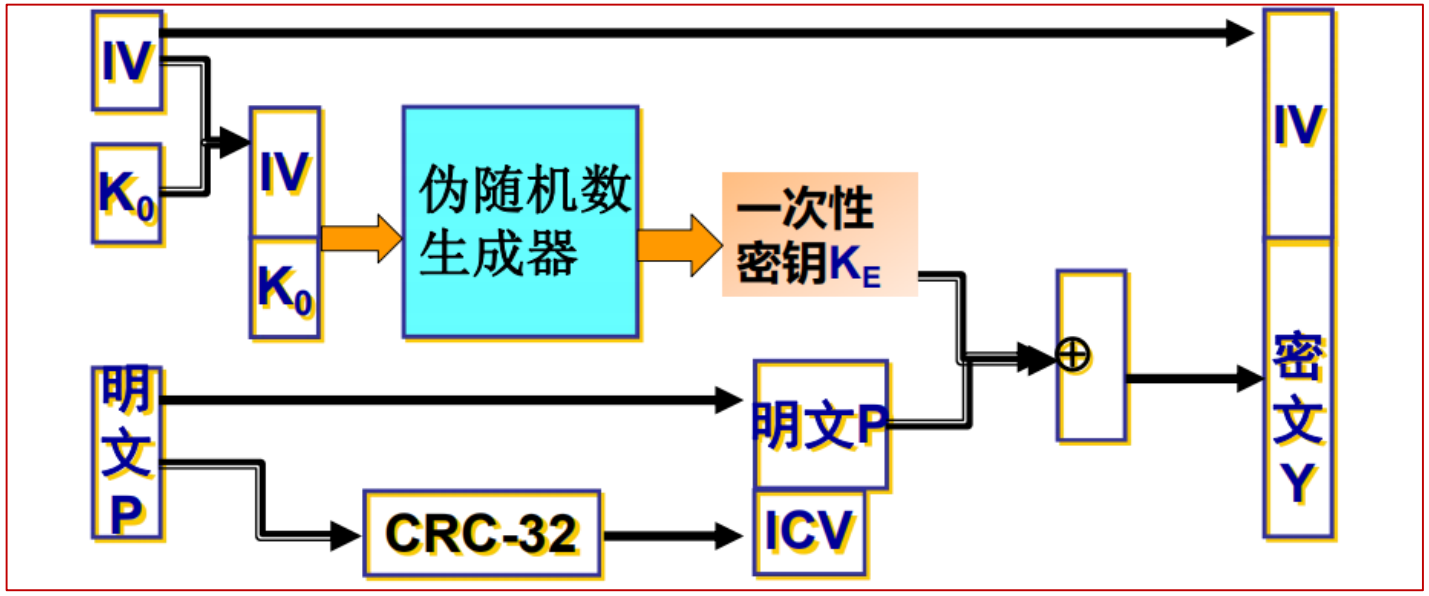
- 认证：
  - 开放系统认证
    - 默认认证方式
    - 对请求认证的任何人提供明文认证
  - 共享密钥认证



- 保密性：RC4流密码加密，密钥长度40bit/104bit
- 完整性：循环冗余校验CRC32
- 密钥管理：
  - 各个设备与接入点共享一组默认密钥，可能被泄露
  - 每个设备与其他设备建立密钥对关系，密钥人工分发困难

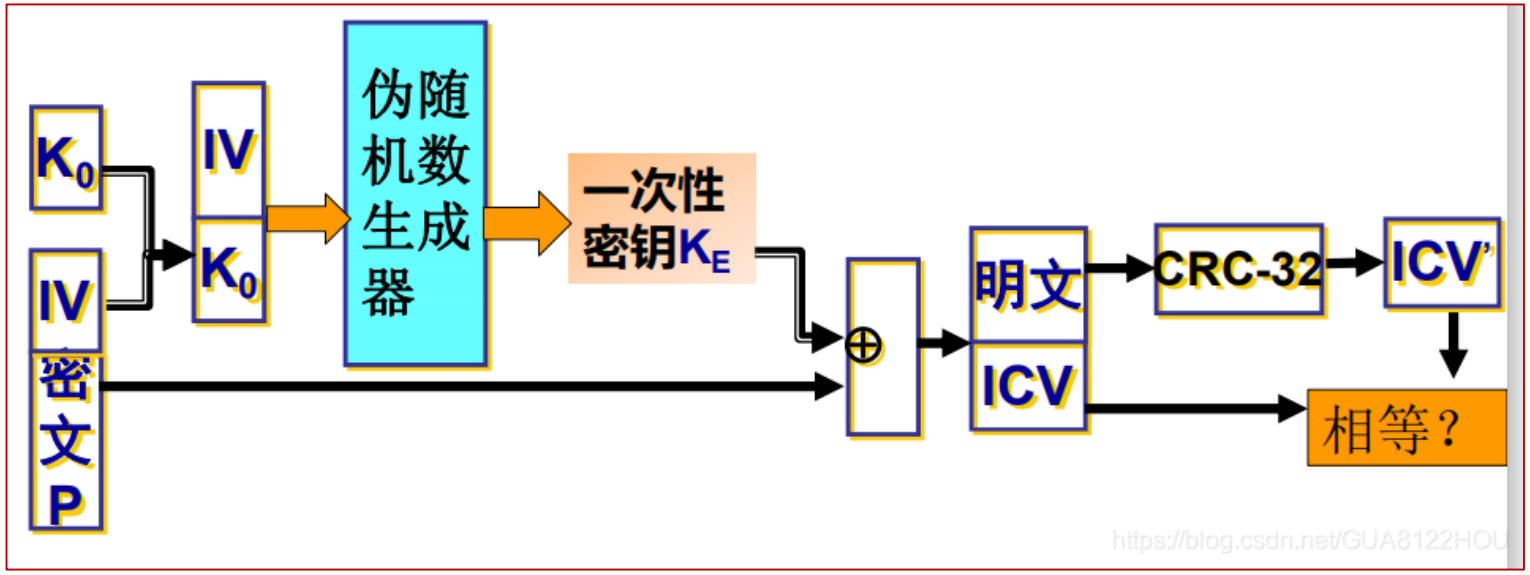
WEP 加密过程

- 计算校验和
  - 对明文P进行完整性CRC-32计算，得到校验和ICV
  - 串接明文P和校验和ICV，用于下一步加密过程的输入
- 加密
  - 将24位初始化向量IV和40位共享密钥K0连接得到64位的数据，输入到虚拟随机数产生器中，产生一次性秘钥KE
  - 将KE和上一步的计算结果进行按位异或运算，得到密文Y
- 传输
  - 将24位初始化向量IV和密文Y串联起来，在无线链路上传输



WEP 解密过程

- 计算一次性密钥KE
  - 将收到的信息中初始化向量IV和共享密钥K0串接，输入到虚拟随机数产生器中，产生一次性密钥KE
- 解密
  - 将收到信息中的密文P和一次性密钥KE进行按位异或运算，得到明文P和ICV串接信息
- 认证
  - 将计算得到的明文P进行完整性CRC-32计算，得到校验和ICV’
  - 比较ICV和ICV’，相等接收，不相等丢弃



WEP的安全性分析

- 同一个SSID中，所有STA和AP共享同一个密钥，容易泄露
- 生成RC4密码流的初始化向量IV明文发送
- 24 bits的初始化向量IV过短，容易重复
- 完整性校验算法CRC-32是非加密的线性运算，主要用于检测消息中的随机错误，不是安全的杂凑函数，无法实现消息认证
- RC4是一个序列密码加密算法，发送者用一个密钥序列和明文异或产生密文，接收者用相同的密钥序列与密文异或恢复出明文，容易被破译
- WEP协议中不含序列号，无法确定帧顺序，无法提供抵抗重放攻击

WPA1

- 因为WEP的严重安全漏洞，2002年Wi-Fi联盟制定了WPA1，这是一个过度性的中间标准，其核心就是IEEE 802.1x和TKIP
- 采用TKIP协议（Temporary Key Integrity Protocol）认证有两种模式
  - 使用802.1x协议进行认证（WPA企业版）
  - 预先共享密钥PSK(Pre-Shared Key)模式（WPA个人版）
- 保密性
  - RC4流密码加密，密钥长度128位
- 完整性
  - WPA 使用了称为 “Michael” 的更安全的消息认证码MIC
  - WPA 使用的 MIC中 包含了帧计数器，可以防范重放攻击

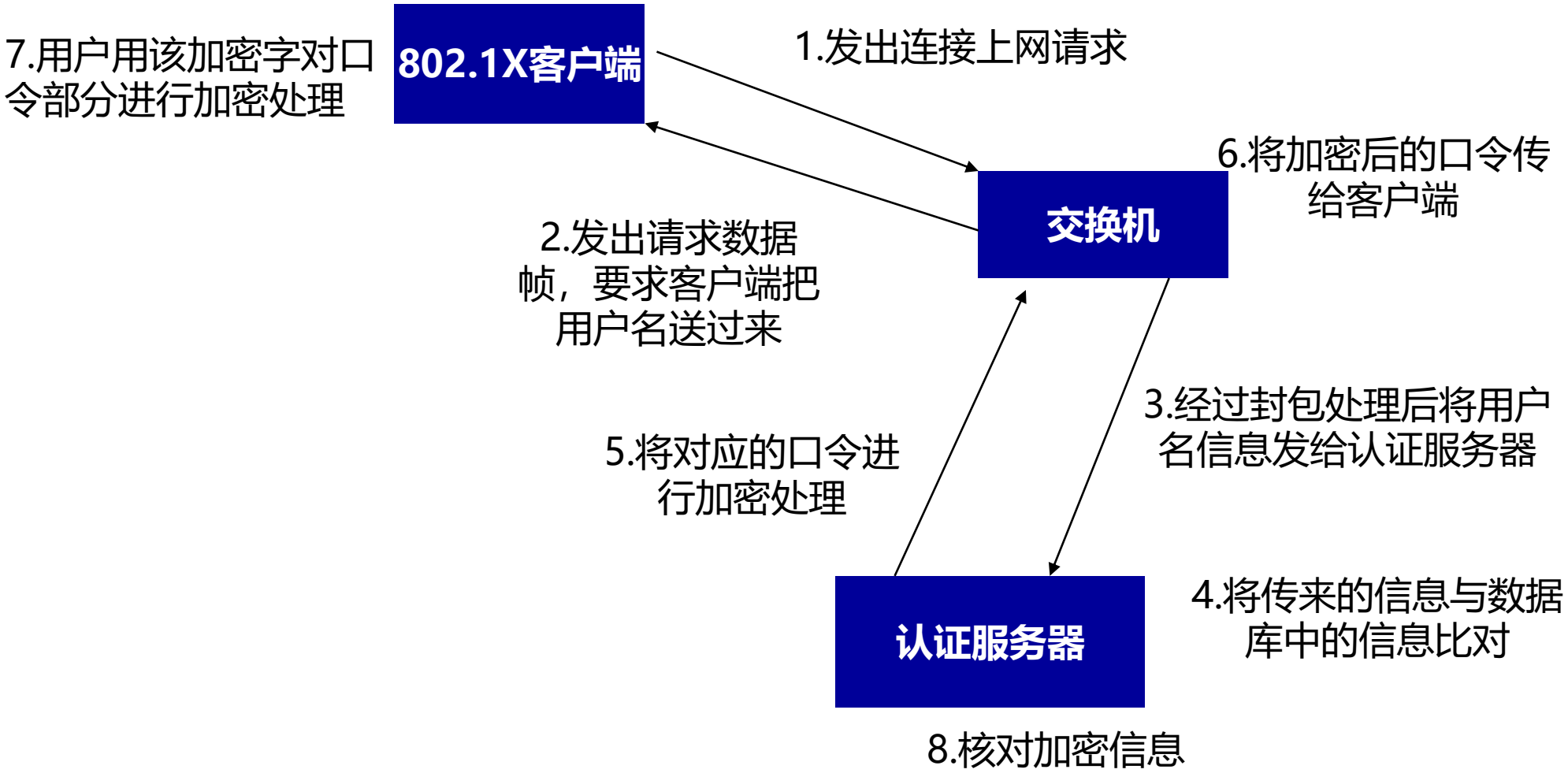
临时密钥完整性协议TKIP

- 临时密钥完整性协议TKIP（Temporal Key Integrity Protocol）是包在已有的WEP密码外围的一层“外壳”
- TKIP使用WEP同样的加密引擎和RC4算法，但是TKIP中密码使用的密钥长度是128位，解决了WEP密钥短的问题
- TKIP另一个重要特性就是动态变化每个数据包所使用的密钥；密钥通过将多种因素混合在一起生成，使它不能被轻易破译
- 利用TKIP传送的每一个数据包都具有独有的48位序列号，可以有效防范重放攻击

IEEE 802.1x

- IEEE 802.1x是针对以太网而提出的，基于端口的网络访问控制利用物理层特性对连接到无线端口的设备进行身份认证
- IEEE 802.1x基于客户/服务器模式，可以在无线终端与AP建立连接之前，对用户身份的合法性进行认证
  - 当无线终端向AP发起连接请求时，AP会要求用户输入用户名和密码，再把这个用户名和密码送到验证服务器上去做验证
  - 如果验证通过才允许用户享用网络资源，如果认证失败，则禁止该设备访问，大大提高整个网络的安全性
- IEEE802.1x需要和上层认证协议EAP（Extensible Authentication Protocol）配合来实现用户认证和密钥分发

IEEE 802.1X的认证过程



WPA2的提出

- 当IEEE完成并公布IEEE 802.11i无线局域网安全标准后，Wi-Fi联盟也随即公布了WPA第2版 -- WPA2
  - 更安全的CCMP消息认证代替了Michael算法
  - AES对称加密算法代替了RC4流密码
  - WPA2支持802.11g或以上的无线网卡

WEP-WPA1-WPA2比较

加密技术	全称	加密算法	协议
WEP	Wired Equivalent Privacy (有线对等保密)	RC4	IEEE 802.11b
WPA	Wi-Fi Protected Access (WiFi安全存取)	RC4，使用TKIP	IEEE 802.11i draft 3
WPA2	Wi-Fi Protected Access 2 (WiFi安全存取 第二版)	支持AES，使用CCMP 需要新硬件支持	IEEE 802.11i

- WPA使公共场所和学术环境安全地部署无线网络成为可能
  - WEP使用一个静态的密钥来加密所有的通信，这意味着为了更新密钥，技术人员必须亲自访问每台机器，而这在学术环境和公共场所是不可能的
  - WPA采用有效的密钥分发机制，不断转换密钥


Thanks a lot !

Activity is the only road to knowledge!

Computer Network Security @ 2022Fall