



移动互联网安全

第一章 无线网络安全基础

黄 玮

中国传媒大学



关于课程你需要了解...

中国传媒大学



课程概况

- 上课地点
 - 讲授&实验：48教 A101
 - 讲授：1-16周 周二 5-6节
 - 实验：9-16周 周二 7-8节
- 答疑地点/时间
 - A101E 周一到周五白天
 - 新浪微博 @中传黄玮 / 随时
 - 邮箱： i@huangwei.me



课程概况

- 先修课程
 - 计算机安全与维护
 - 计算机网络A
 - 密码学应用实践（推荐）
- 推荐教材
 - 无
- 硬件和软件环境
 - PC
 - Linux (Kali 2.0)
 - 具有无线数据帧收发能力的无线网卡（推荐：RT8187L芯片的网卡、TP-LINK TL-WN722N）
 - 无线AP



这是一门对实验设备要求很高的课程



中国传媒大学



在线资源

- <http://cs.cuc.edu.cn/huangwei/wiki>



关于课程的教、学方法和原则

- 教
 - 授人以渔
 - 重思路、方向讲解，轻傻瓜式重复
- 学
 - 兴趣第一
 - 尽信师，不如无师：质疑、思考、实践
 - 会用、用好互联网



课程目的

- 通过本课程的讲授和实验操作
 - 你能了解到
 - 无线网络攻防基本原理和手段
 - 物联网安全基本原理和手段
 - 智能终端攻防基本原理和手段
 - 你不能了解到
 - 如何编写恶意代码



课程体系 (1/2)

- 无线网络攻防
 - 802.11 攻防从协议到实战
- 物联网安全
 - 智能家居、智能穿戴、移动支付
- 智能终端攻防
 - 安卓为主，兼顾iOS
- 专注于信息安全分析能力培养



课程体系 (2/2)

- 加入无线网络之前
 - 嗅探、入侵（网络）、钓鱼、DoS
- 加入无线网络之后
 - 嗅探、入侵（终端）、MITM
- 使用蜂窝数据网络
 - 嗅探、MITM
- 使用移动应用
 - 嗅探、篡改、入侵（终端&云端）

不知攻，焉知防



考核方式

- 平时成绩
 - 占总评成绩的百分比为**40%**
 - 主要包括以下形式：
 - 上课考勤，作业、测验，实验上机
- 期末考试
 - 开卷
 - 占学期总成绩**60%**，着重进行能力考察



第一章 无线网络安全基础



内容提要

- 无线网络协议基础
- 无线网络设备基础
- 无线网络系统基础
- 无线网络安全的研究范围



无线网络协议基础



无线网络是什么

- Wi-Fi? WLAN? 802.11? 蓝牙? NFC?



无线网络有什么

- AP? 路由器? 热点?
- 上网卡? 电力猫? 3G? 4G?
- 手机? 平板? 笔记本? 台式机? 空调? 插座?



无线网络通信协议家谱

无线网络类别	<i>IEEE</i>	<i>ITU</i>
2G, 2.5G 最后1公里, <i>Kbps</i>		<i>GSM, CDMA, GPRS, EDGE</i>
WPAN 10米, <i>Kbps~Mbps</i>	蓝牙 (802.15.1) UWB (802.15.4a) ZigBee (802.15.4)	
WLAN 100米, 10~1000 <i>Mbps</i>	Wi-Fi (802.11)	
3G WMAN 最后1公里, 1~XX <i>Mbps</i>	WiMax (802.16e), 2007年成为3G标准	2000: WCDMA (欧洲) CDMA2000 (美国) TD-SCDMA (中国)
4G WMAN 最后1公里, 1~100 <i>Mbps</i>	WiMax (802.16m)	LTE (FDD / TDD)



802.11

- IEEE Standard for Information technology—
Telecommunications and information exchange
between systems Local and metropolitan area
networks—
Specific requirements
 - Part 11: Wireless LAN Medium Access Control (MAC) and
Physical Layer (PHY) Specifications



802.11技术架构

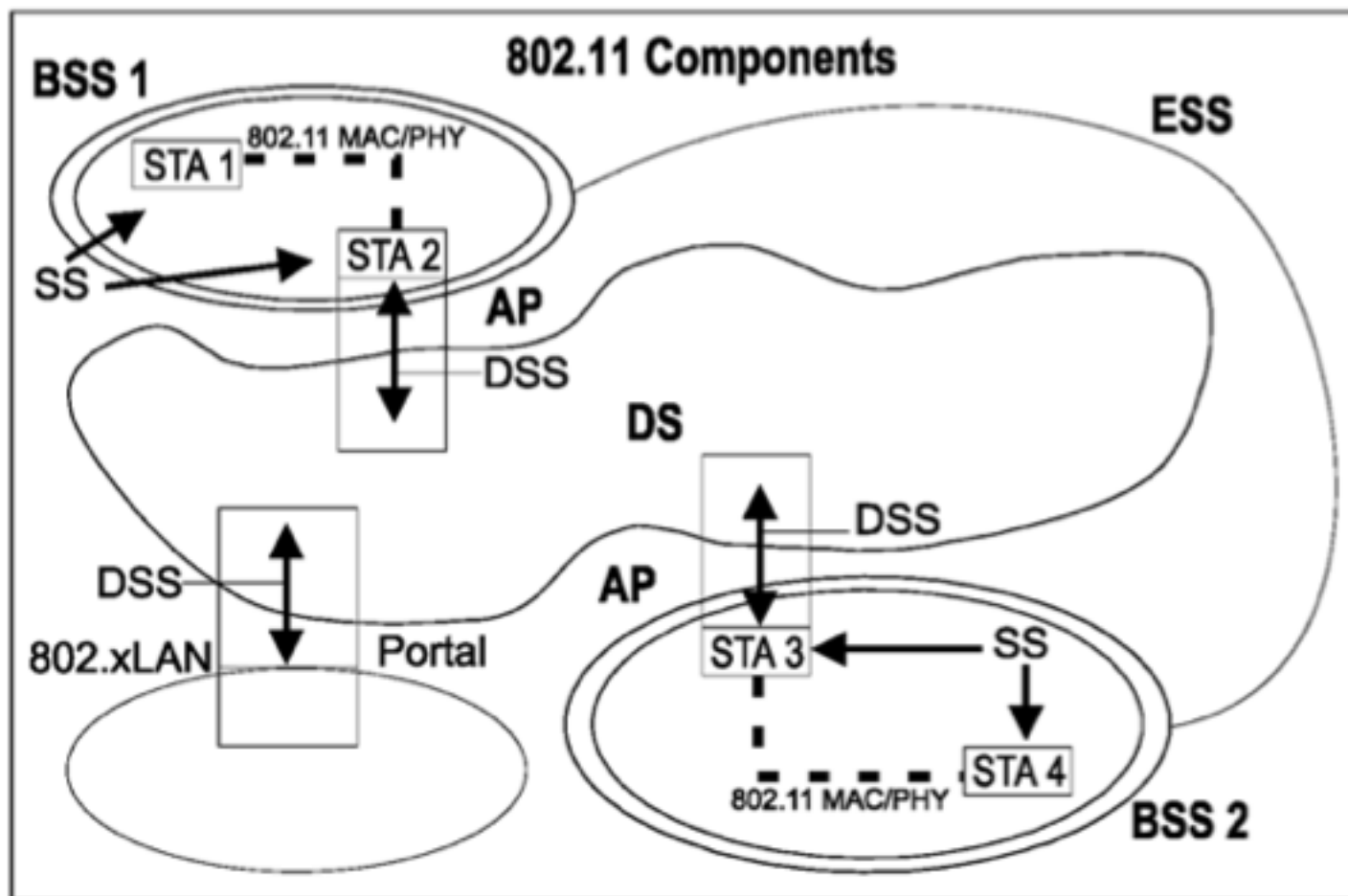


Figure 4-11—Complete IEEE 802.11 architecture



802.11技术组件

- STA
- BSS / IBSS
- SS
- ESS
- DS
- 802.x LAN
- Portal
- AP



STA

- Wireless station
 - 可寻址的设备
 - 固定地址、可移植地址、动态地址
 - 无线客户端
 - 无线路由器
 - 无线接入点



- Basic Service Set
 - STA加入的集合
 - STA之间是否可以相互可见（通信）取决于接入点设备的配置
- BSA: basic service area
 - BSS的覆盖区域



IBSS

- infrastructure BSS
 - BSS默认就是指的的基础设施BSS，IBSS特指independent BSS
 - 至少包含1个接入点
 - Portal（门户）是可选项
 - 无线服务的逻辑接入点，例如学校的无线认证页面
- independent BSS
 - Ad-hoc
 - 最少包含2个STA
 - 不支持接入分布式系统

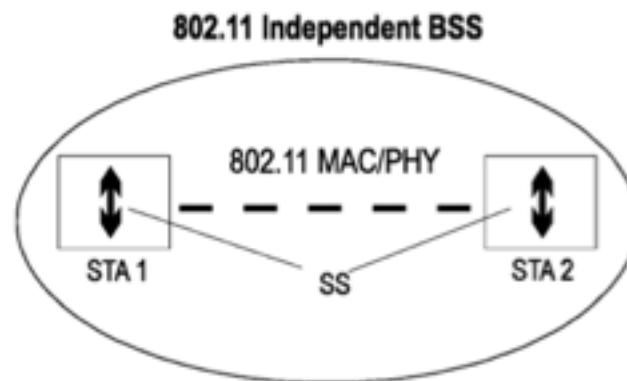


Figure 4-13—Logical architecture of an IBSS



SS

- Station Service
 - 在一个指定BSS内提供数据链路层通信服务



- extended service set
 - 物理上独立的BSS组成的一个逻辑上的独立服务集合
 - 使用相同的ESSID
 - 无线热点扩展
 - CUC、CMCC、ChinaNet ...
 - 支持漫游



DS / DSS

- Distribution System （分布式系统）
 - 增加BSS的覆盖范围（面积）
 - 又被成为WDS（Wireless DS）
- distribution system service (DSS)



802.x LAN

- 802.3
 - wired local area network
- 802.11
 - wireless local area network
 - 802.11a/b/g/n/ac
 - 802.11i



802.11

- 第一个正式版发布于1997年
- 传输速率：1-2Mbps
- 红外/无线电 (DSSS/FHS)
- CSMA/CA

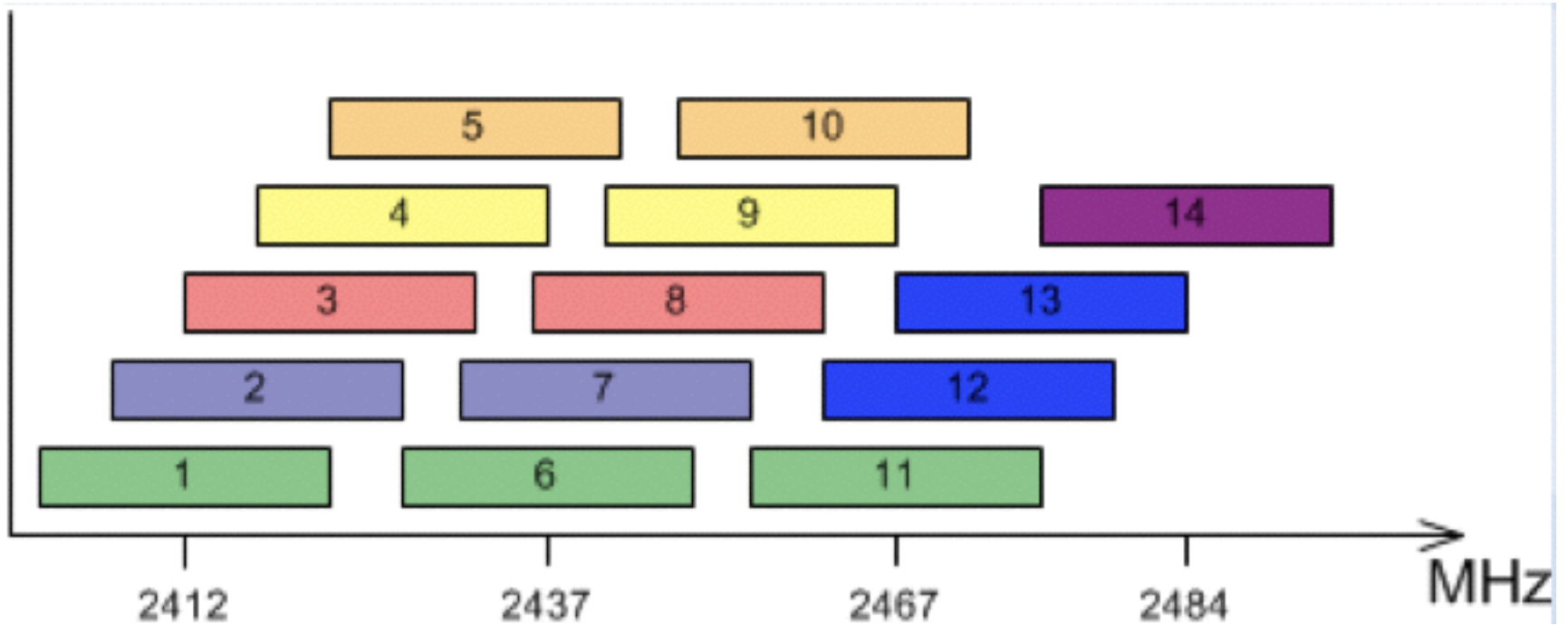


802.11b (1/2)

- 针对802.11第一版的增补修订
- CCK编码
- 新的传输速率：5.5 / 11Mbps
- 2.4GHz ISM带宽
- 14个交叠信道
- 22MHz频宽



802.11b (2/2)





802.11a

- 5GHz波段
- 超过14个非重叠信道
- OFDM
- 最大传输速率：54Mbps



802.11g

- \sim 802.11a on 2.4GHz
- 向后兼容802.11b



802.11n

- 2004年开始起草，2009年9月定稿
- 单用户MIMO
- 2.4GHz && 5GHz
- 40/80MHz频宽
- greenfield mode（绿灯区模式）



802.11ac




- 单字母名称耗尽，只得启用2个字母命名
- 第一份草案：2011年1月
- 5GHz only
- 多用户MIMO
- 多调制和编码（MCS）速率
 - 单用户传输速率最高能达到1Gbps+
- 80/160MHz频宽















身边的802.11

802.11n

Wi-Fi: 打开
关闭 Wi-Fi

✓ [Redacted]   

PHY 模式: 802.11n
BSSID: [Redacted]
频道: 11 (2.4 GHz)
安全性: WPA2 个人级
RSSI: -54
传输速率: 145
MCS 索引: 15

[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  

加入其他网络...
创建网络...
打开网络偏好设置...
打开“无线诊断”...

802.11ac

Wi-Fi: 打开
关闭 Wi-Fi

✓ [Redacted]   

PHY 模式: 802.11ac
BSSID: [Redacted]
频道: 36 (5 GHz)
安全性: WPA2 个人级
RSSI: -54
传输速率: 360

[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  

加入其他网络...
创建网络...
打开网络偏好设置...
打开“无线诊断”...



- Access Point
 - STA的一种
 - 对已关联 (associated) 的STA基于无线介质 (WM, wireless medium) 提供接入分布式服务



- BSS模式下是AP的MAC地址
- 对于IBSS来说是随机的MAC地址



ESSID (1/2)

- 一般简称为SSID，无线网络的接入唯一标识
 - 仅作为一种声明
 - 可任意声明（伪造）
- 工作站与AP关联（Associate）使用的标识
- 区分大小写、2-32字节
- 单个AP可以支持多个ESSID
 - 取决于设备与系统的支持情况
 - 常见的：客人网络



ESSID (2/2)

- 取消SSID广播
 - 客户端不能“主动发现”
 - 并不能增强无线网络安全性
 - 且听第三章分解
- 构建ESS时，所有的BSS必须使用相同的ESSID



为什么需要BSSID

- 增强识别BSS的准确性
 - 同名ESSID时，通过BSSID区分不同的BSS



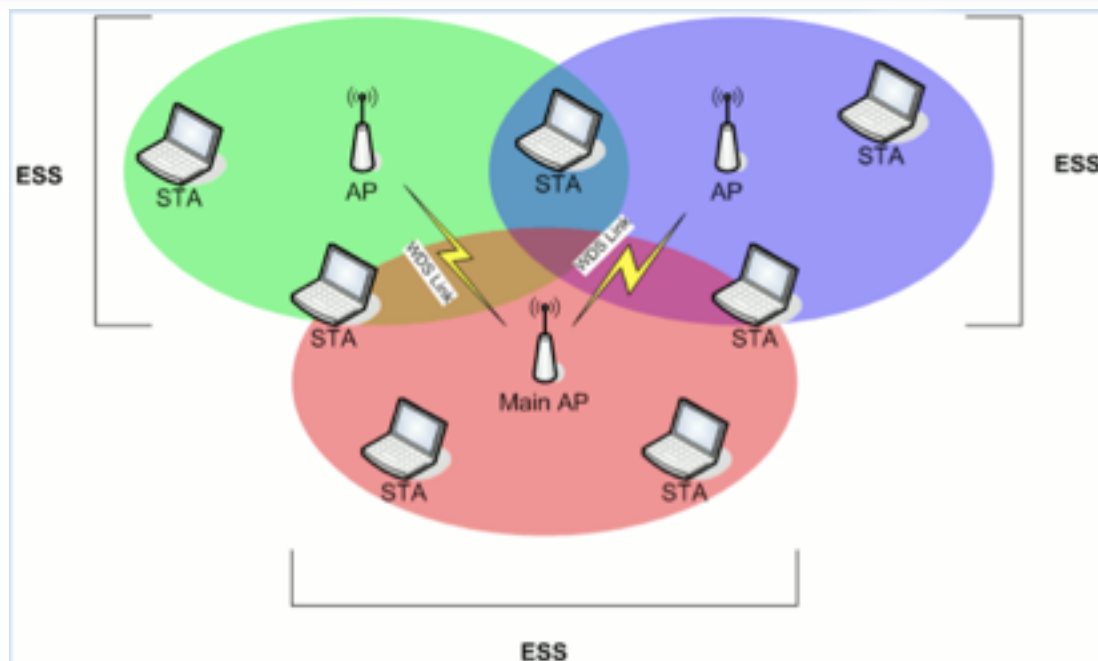
真实世界一例

KisMAC														
KisMAC 0.3.3														
#	Ch	SSID	BSSID	Enc	Type	Signal	Avg	MaxSignal	Packets	Data	Last Seen	C...		
0	11	sanx	C8:3A:29:88	WPA	managed	0	7	10	6	1.36KiB	2014-09-16 14:12:48	+C	●	
1	9	Virus	92:EE:88:70	WPA2	managed	49	49	55	46	11.32KiB	2014-09-16 14:13:22	+C	●	
2	11	MERC	C0:61:88:20	WPA	managed	0	12	15	17	4.56KiB	2014-09-16 14:13:20	+C	●	
3	11	NETO	00:0F:88:CA	NO	managed	46	39	50	95	7.33KiB	2014-09-16 14:13:23	+C	●	
4	11	www	E4:D3:88:40	WPA	managed	9	9	16	20	5.85KiB	2014-09-16 14:13:23	+C	●	
5	11	zhao	0C:72:88:50	WPA	managed	0	10	13	20	5.08KiB	2014-09-16 14:13:20	+C	●	
6	11	<hid	90:72:88:EE	WPA2	managed	47	49	83	49	10.74KiB	2014-09-16 14:13:23	+C	●	
7	11	tian	08:10:88:BC	WPA2	managed	0	6	6	1	254B	2014-09-16 14:12:31	+C	●	
8	1	TP-L	28:2C:88:8A	WPA	managed	0	4	35	64	18.20KiB	2014-09-16 14:13:21	+C	●	
9	3	<hid	8C:21:88:26	WPA	managed	41	42	60	100	21.97KiB	2014-09-16 14:13:22	+C	●	
10	4	Tend	C8:3A:29:88	WPA	managed	0	26	30	74	14.01KiB	2014-09-16 14:13:20	+C	●	
11	4	flytv	C8:3A:29:88	WPA	managed	0	9	9	1	189B	2014-09-16 14:12:31	+C	●	
12	6	360V	00:36:88:B5	WPA2	managed	0	69	72	146	38.64KiB	2014-09-16 14:13:21	+C	●	
13	6	TP-L	14:75:88:9A	WPA	managed	0	22	23	40	8.49KiB	2014-09-16 14:13:21	+C	●	
14	6	Inc	14:EE:88:F4	WPA2	managed	0	16	36	63	12.15KiB	2014-09-16 14:13:21	+C	●	
15	6	TP-L	E4:D3:88:D6	WPA	managed	0	22	30	61	15.91KiB	2014-09-16 14:13:21	+C	●	
16	6	TP-L	C0:61:88:2A	WPA	managed	0	13	18	27	7.02KiB	2014-09-16 14:13:21	+C	●	
17	6	dayu	EC:17:88:46	WPA	managed	0	6	9	6	1.90KiB	2014-09-16 14:13:18	+C	●	
18	6	xiniu	5C:63:88:F8	WPA	managed	0	9	13	17	3.87KiB	2014-09-16 14:13:18	+C	●	
19	6	<no	20:DC:88:C0	NO	managed	0	21	21	1	24B	2014-09-16 14:12:32	+C	●	
20	9	Tend	C8:3A:29:88	WPA	managed	0	7	15	23	4.38KiB	2014-09-16 14:13:20	+C	●	
21	1	TP-L	78:A1:88:F0	WPA	managed	0	24	30	43	11.12KiB	2014-09-16 14:13:22	+C	●	
22	1	<hid	D4:EE:88:80	WPA2	managed	0	36	40	56	13.25KiB	2014-09-16 14:13:22	+C	●	
23	1	jijie	9C:21:88:1C	WPA	managed	0	9	16	21	5.25KiB	2014-09-16 14:13:22	+C	●	
24	1	SAMS	EC:88:88:9A	WPA	managed	0	13	16	24	5.05KiB	2014-09-16 14:13:21	+C	●	
25	1	CMC	00:11:88:49	NO	managed	0	20	23	20	4.88KiB	2014-09-16 14:13:22	+C	●	
26	1	CMC	06:11:88:49	WPA	managed	0	18	23	17	5.13KiB	2014-09-16 14:13:21	+C	●	
27	1	<hid	D0:C7:88:86	WPA	managed	0	14	21	43	12.19KiB	2014-09-16 14:13:22	+C	●	
28	3	Feng	6C:E8:88:FC	WPA	managed	41	46	52	53	12.78KiB	2014-09-16 14:13:22	+C	●	
29	5	Tend	C8:3A:29:88	WPA	managed	10	30	41	152	28.27KiB	2014-09-16 14:13:22	+C	●	
30	9	Tend	C8:3A:29:88	WPA	managed	0	10	23	27	5.09KiB	2014-09-16 14:13:20	+C	●	
31	2	nimo	54:E6:88:22	WPA	managed	0	13	20	15	2.22KiB	2014-09-16 14:13:20	+C	●	
32	6	FAST	6C:E8:88:82	WPA	managed	0	10	18	23	5.30KiB	2014-09-16 14:13:21	+C	●	
33	5	song	CC:34:88:C6	WPA	managed	23	27	29	43	11.34KiB	2014-09-16 14:13:22	+C	●	
34	5	Louis_zhu_home	E4:D3:88:84	WPA	managed	10	0	15	17	4.65KiB	2014-09-16 14:13:22	+C	●	



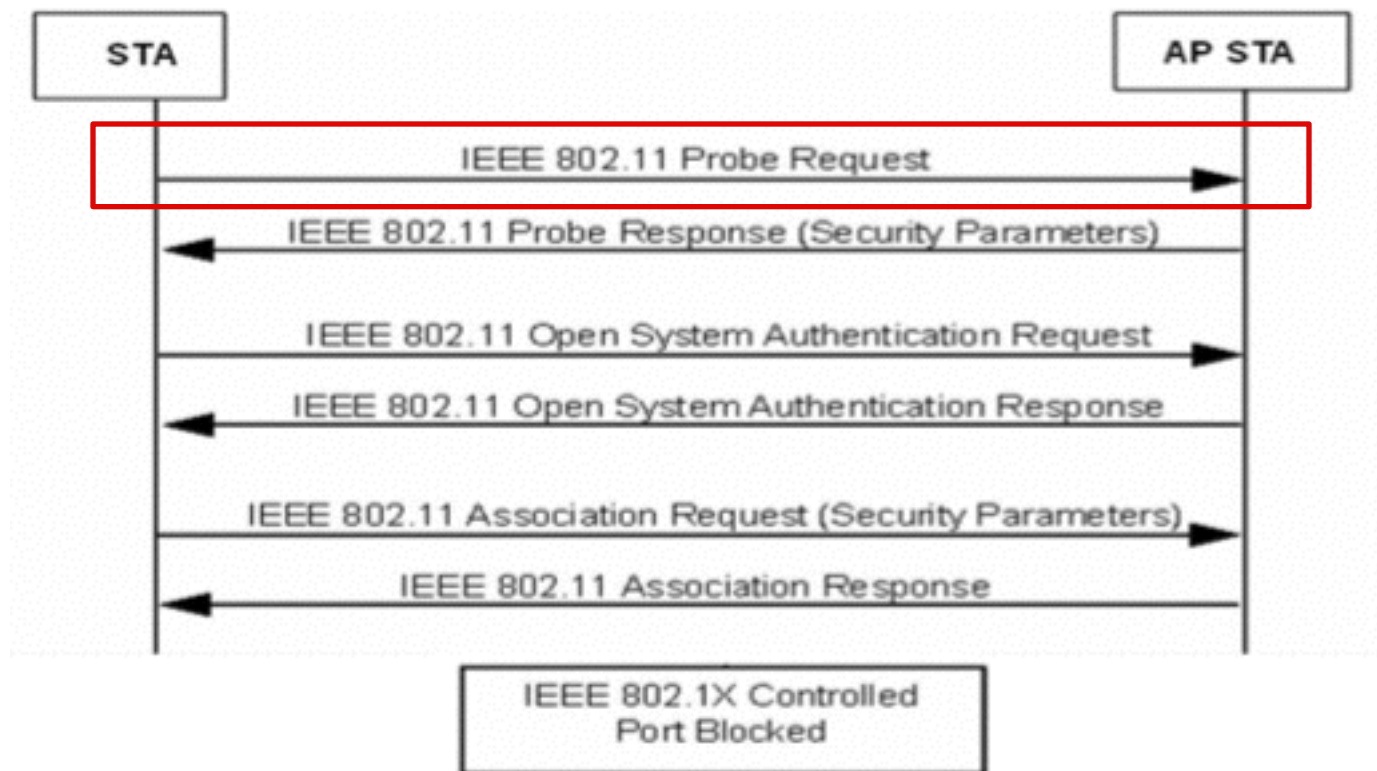
802.11工作模式

- 基础设施
 - BSS / ESS
- Ad-Hoc
 - IBSS
- 监听模式
 - 第二章讲解





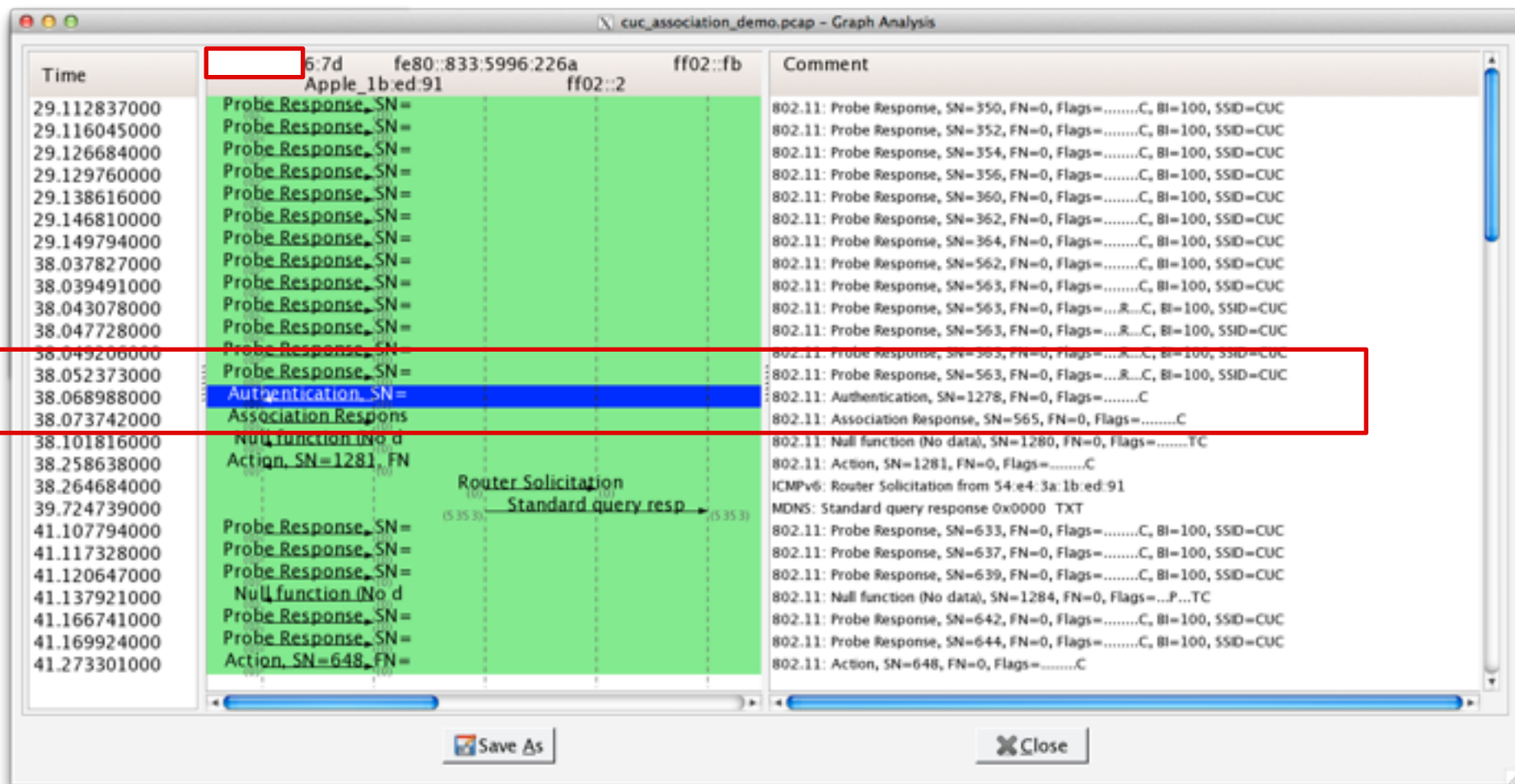
802.11 关联过程（无加密，开放认证）



可选步骤，AP如果开启了SSID广播，则STA可以通过beacon frame得到认证相关信息



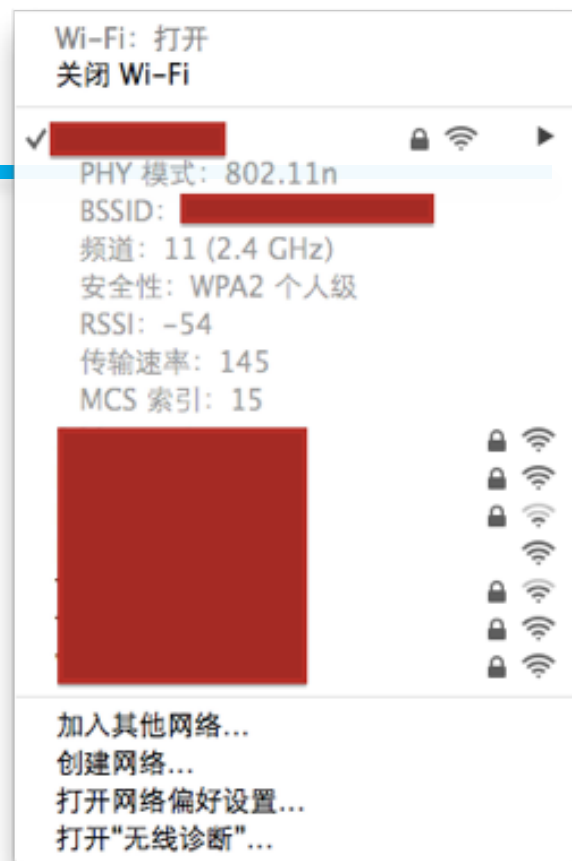
wireshark抓包实例





STA加入（关联）AP的策略

- 历史关联记录优先
- 先发现，先关联
- 信号强度高者优先
 - RSSI: received signal strength indicator
 - 接收信号的强度指示，负值
 - $RSS = 10 * \lg P$ ，P是接收到的信号功率，一般以1mW作为分母
 - dBm: 功率绝对值，0表示最强，越近0接收效果越好
 - dB: 功率相对值





无线网络设备基础



无线网络设备

- 网络基础设施
 - AP/路由器/SD卡
- 客户端
 - 网卡
 - 智能手机/平板/PC/空调





常见术语与概念

- (网卡) 芯片
- 厂商
- 驱动程序
- 信号强度
 - RSSI / dB / dBm
- ROM / Flash
- RAM / 内存
- 天线



网卡芯片选择

- Realtek 8187
- 可选配外接天线
 - 增强信号接收能力
- 查看网卡芯片的方法
 - 厂商参数表
 - *nix: lspci / dmesg / lsusb / airmon-ng
 - Windows: 设备管理器



芯片厂商

- Broadcom
 - 基于该品牌的设备商包括ASUS、Buffalo、Linksys、Netgear
- Atheros
 - 基于该品牌的设备商包括TP-Link、D-Link
- MTK / RaLink
 - 基于该品牌的设备商包括华为、中兴
- Realtek
- Marvell



Atheros (AR5XXX, AR9XXX)

- Windows平台支持良好(部分支持数据帧注入)
- Linux内核有4个主要的驱动程序提供支持
 - madwifi: 非主流内核支持, 已被ath5k替代
 - ath5k: 基于mac80211驱动, 不支持USB和802.11n
 - ath9k: 新增802.11n支持
 - AR9170usb: 支持USB接口



Broadcom (B43XX Family)

- 市场占有率高
 - 常见于笔记本内置无线网卡芯片
- mac80211驱动支持B43系列芯片
- 支持数据帧注入和监听模式
- 不支持USB和802.11n



Intel Pro Wireless and Intel Wifi Link (Centrino)

- 常见于笔记本内置无线网卡芯片
- 不适合于无线网络安全实验



Ralink (RT2X00)

- 开源支持较好
- 支持USB接口
- Linux内核的mac80211驱动支持



Antenna (天线)

- 无源器件
- 通过控制信号发射的角度，来获得信号“增益”
 - 信号的总能量由AP决定
 - 天线决定信号如何传播出去



Antenna (天线)

- 全向 (Omni)

- 水平各个方向增益相同
- 全向天线增益越大，水平方向上覆盖的范围也就越大，垂直方向上覆盖的范围越小
- 一般应用于室内环境

- 定向 (directional)

- 垂直方向和水平方向都不是360度覆盖，一般来说覆盖角度小，覆盖的范围也就越远
- 大多数情况下，使用定向天线在高空向室外热点区域覆盖，以保证可靠的信号质量



无线网络系统基础

中国传媒大学



知名的“路由器”操作系统

- OpenWRT
- DD-WRT
- tomato
- RouterOS



无线网络安全的研究范围



无线网络主要威胁与风险

- Data Interception
- DoS
- Rogue APs
- Wireless Intruders
- Misconfigured APs
- Ad Hoc and soft APs
- Evil Twin APs
- Wireless Phishing
- Endpoint Attacks
- Misbehaving Clients



Data Interception——中间人攻击

- 针对TKIP无线加密标准的完整性校验缺陷
 - AES-CCMP (WPA2 PSK)无此缺陷
- 现有大量无线设备还在使用WPA/WPA2混合模式

No Encryption

WEP Open System

WEP Shared Key

WPA-PSK

✓ WPA2-PSK

WPA-PSK/WPA2-PSK Mixed Mode

✓ auto

Force CCMP (AES)

Force TKIP

Force TKIP and CCMP (AES)



DoS——拒绝服务攻击

- 无线信号像阳光和空气一样无处不在
- 使用相近信道（工作频率）的AP之间的无意相互干扰
- 伪造数据帧强制无线客户端掉线
 - Deauth Flood
- 暴力破解口令过程对AP的CPU资源消耗



Rogue APs——非法接入点

- 非授权AP接入受保护的有线网络
 - 个人非法开启个人热点
 - Ad Hoc (Soft AP)
 - 隔离内网变为脆弱“公”网
- 部署Wireless IPS来检测组织内的非授权AP





Wireless Intruders——无线入侵

- 无线网络物理覆盖范围可以较大（50米以内）
 - 网络边界较长，需要配置的无线入侵设备较多
 - 口令破解、嗅探、DoS可以随时从任意信号覆盖的位置发起和停止



免费Wi-Fi? 公共Wi-Fi?



已覆盖 11,020,822 免费WiFi热点



延伸阅读:

免费Wi-Fi的商业模式是什么?

公共Wi-Fi的安全风险?

无线路由器被蹭网风险

局域网安全攻防异常激烈



免费Wi-Fi? 呵呵

KisMAC 0.3.3

Property	Setting
SSID	NETGEAR
BSSID	00:0F:B5:16:3B:CA
Vendor	NETGEAR Inc
First Seen	2014-09-16 14:12:31 +0000
Last Seen	2014-09-16 14:44:36 +0000
Channel	11
Main Channel	11
Supported Rates	1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36
Signal	53
MaxSignal	55
AvgSignal	49
Type	managed
Encryption	disabled
Packets	3600
Data Packets	30
Management Packets	3570
Control Packets	0
Unique IVs	0
Inj. Packets	0
Bytes	282.51KiB
Key	
ASCII Key	
LastIV	00:00:00
Latitude	
Longitude	
Elevation	No Elevation Data
Comment:	

Client	Vendor	Signal	sent Bytes	recv. Bytes	IP Address	Last Seen
00:0C:87:4E:8E:0A	NETGEAR Inc	53	275.70KiB	195B	192.168.0.1	2014-09-16 14:44:36
18:00:00:00:00:00	Dell Inc	50	6.62KiB	0B	192.168.0.4	2014-09-16 14:44:36
FF:FF:FF:FF:FF:FF	unknown	0	0B	205.40KiB	192.168.0.255	
02:00:00:00:00:00	multicast	0	0B	312B	224.0.0.22	
01:00:00:00:00:00	multicast	0	0B	656B	224.0.0.251	
02:00:00:00:00:00	multicast	0	0B	419B	224.0.0.252	
02:00:00:00:00:00	multicast	0	0B	2.10KiB	239.255.255.250	
00:00:00:00:00:00	unknown	0	0B	6.08KiB	unknown	
20:00:00:00:00:00	unknown	0	0B	1.39KiB	unknown	
9C:00:00:00:00:00	unknown	0	0B	1.39KiB	unknown	
00:00:00:00:00:00	unknown	0	0B	4.32KiB	unknown	
CC:00:00:00:00:00	unknown	0	0B	1.17KiB	unknown	
7C:00:00:00:00:00	unknown	0	0B	525B	unknown	
18:00:00:00:00:00	unknown	0	0B	1.90KiB	unknown	
A0:00:00:00:00:00	unknown	10	90B	13.53KiB	unknown	2014-09-16 14:44:36
9C:00:00:00:00:00	unknown	0	0B	525B	unknown	
64:00:00:00:00:00	unknown	0	0B	0.81KiB	unknown	
C4:00:00:00:00:00	unknown	0	0B	1.39KiB	unknown	
18:00:00:00:00:00	unknown	0	0B	300B	unknown	
60:00:00:00:00:00	unknown	0	0B	75B	unknown	
84:00:00:00:00:00	unknown	0	0B	0.81KiB	unknown	
E0:00:00:00:00:00	unknown	0	0B	150B	unknown	
64:00:00:00:00:00	unknown	0	0B	150B	unknown	
8C:00:00:00:00:00	unknown	0	0B	75B	unknown	
C4:00:00:00:00:00	unknown	0	41B	2.59KiB	unknown	2014-09-16 14:44:36
00:00:00:00:00:00	Gemtek Technolc	0	0B	75B	unknown	
00:00:00:00:00:00	Gemtek Technolc	0	0B	525B	unknown	
54:00:00:00:00:00	unknown	0	0B	150B	unknown	
88:00:00:00:00:00	unknown	0	0B	525B	unknown	
DC:00:00:00:00:00	unknown	0	0B	225B	unknown	
8C:00:00:00:00:00	unknown	0	0B	75B	unknown	
6C:00:00:00:00:00	unknown	0	0B	1.39KiB	unknown	
72:00:00:00:00:00	unknown	0	0B	225B	unknown	
8C:00:00:00:00:00	unknown	0	0B	375B	unknown	
C4:00:00:00:00:00	unknown	10	64B	0.79KiB	unknown	2014-09-16 14:44:36

Start Scan



Endpoint Attacks——攻击终端设备

- 终端设备的固件（操作系统）漏洞利用
- 终端管理软件漏洞利用
 - 路由器WEB管理系统
- 无线客户端软件漏洞利用
 - 恶意SSID
 - 格式化字符串攻击
 - XSS/CSRF



Evil Twin APs——伪造重名AP

- 更多便利工具设备和软件的出现恶化了这个问题
 - 监听无线客户端的无线网络探测请求，主动伪造热点强制客户端连入
- 802.1x认证是针对这个问题的有效解决方案



Wireless Phishing——无线钓鱼

- 使用Evil Twin AP对连入的客户端投毒，持久化控制
 - 浏览器缓存
 - DNS解析记录



唾手可得的恶意设备 (1/3)



wifi pineapple



唾手可得的恶意设备 (2/3)



USB Rubber Ducky



唾手可得的恶意设备 (3/3)



Pwn Phone



附录



参考资料

- <https://wifipineapple.com/index.php>
- [Introduction to WiFi Security and Aircrack-ng by Thomas D'Otreppe](#)
- [WikiDevi](#)
- http://www.aircrack-ng.org/doku.php?id=compatible_cards