

802.1X与WLAN安全

陈荣第

chenrd@cernet.edu.cn

清华大学信息网络工程研究中心

无线与移动网络技术研究室

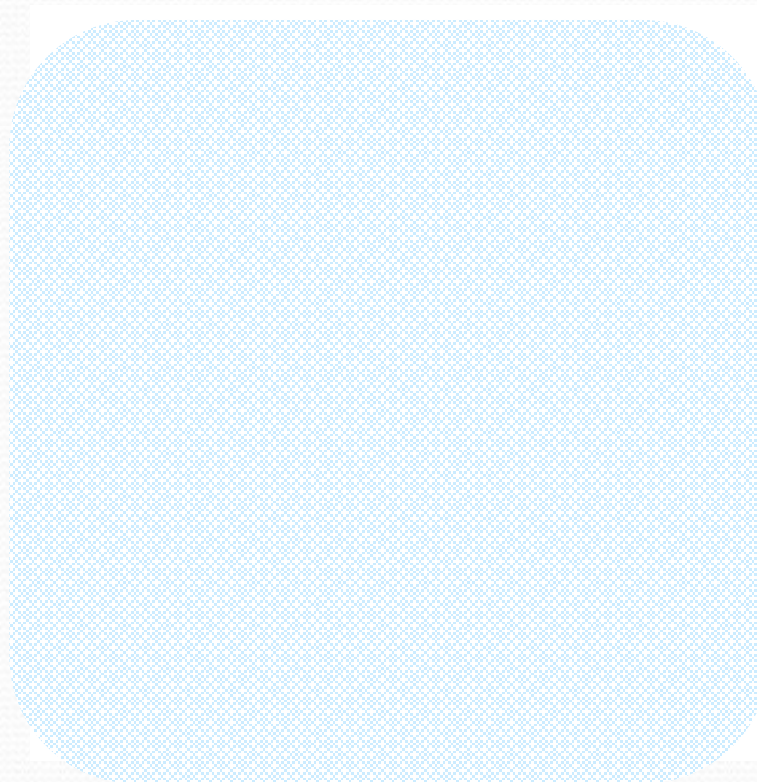
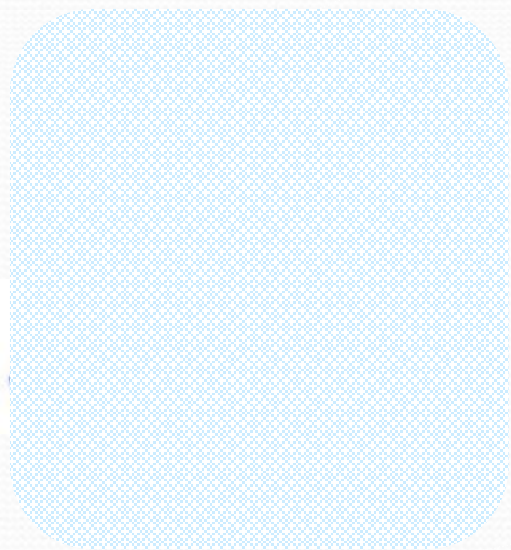
2008-01-09

Topics to Discuss

- 场景描述
- WLAN安全回顾
 - WLAN安全要素分析
 - 典型WLAN安全问题
 - WLAN安全解决方案演进
- WLAN中802.1X应用技术分析
- WLAN中802.1X应用现状
- 清华无线校园网802.1X技术实验
- 无线校园网802.1X应用思考
- 总结和讨论

场景描述

- 802.11无线局域网WLAN



WLAN安全要素分析

- 通常来讲，无线作为有线的延伸，有线网络中的安全问题在无线网络中同样存在；而由于无线网络自身的一些特性，有可能放大某些安全问题并引入新的挑战
 - 开放介质传输：射频传播特性，广播信道
 - 引入及放大安全问题：数据很容易被监听；传输易被干扰
 - 移动性：WLAN中移动性是固有现象
 - 带来新的挑战：安全解决方案需要考虑对移动性的支持
- WLAN安全考虑要点：
 - Authentication：合法用户才能访问WLAN
 - Authorization：区分不同权限
 - Protection：数据传输安全性
 - Mobility：安全方案不能以牺牲移动性为代价

系统安全问题

典型WLAN安全问题(1)

- 信息暴露：监听
- Denial of Service
- Session Hijacking
- Man-in-the-middle attack
- 流氓AP

典型WLAN安全问题(2)

- 信息暴露
 - 能监听到的信息
 - AP信息：信道、SSID、MAC地址、功率、WEP状况...
 - 数据信息：所有传播的MAC报文
 - 安全问题
 - 传输信息对攻击者“透明”

典型WLAN安全问题(3)

- 信息暴露举例：监听到的Telnet报文

The screenshot shows a network traffic capture in OmniPeek. The main window displays a list of captured packets with columns for Source, Destination, BSSID, Flags, Channel, Signal, Data Size, Relative Time, Protocol, Summary, and Expert. The traffic is identified as Telnet sessions between a telnet_client and telnet_server. A red box highlights a specific Telnet session where the client sends a password prompt and the server responds with a password.

Source	Destination	BSSID	Flags	Channel	Signal	Data Size	Relative Time	Protocol	Summary	Expert
telnet_client	telnet_server	Aruba Net:A2:56:11		6	74%	5.5 84	0.000000	TELNET	Src= 3044, Dest= 23, ..., S=4144301574, L= 0...	Wireless Client - Rogue
telnet_client	telnet_server	Aruba Net:A2:56:11	+	6	67%	5.5 84	1.928483	TELNET	Src= 3044, Dest= 23, ..., S=4144301574, L= 0...	
telnet_server	telnet_client	Aruba Net:A2:56:11		6	18%	3.0 84	2.333259	TELNET	Src= 23, Dest= 3044, ..., S= 948450564, L= 0...	Wireless AP - Rogue
telnet_client	telnet_server	Aruba Net:A2:56:11		6	68%	11.0 76	2.363149	TELNET	Src= 3044, Dest= 23, ..., S=4144301575, L= 0...	
telnet_client	telnet_server	Aruba Net:A2:56:11	+	6	74%	5.5 76	2.563894	TELNET	Src= 3044, Dest= 23, ..., S=4144301575, L= 0...	
telnet_server	telnet_client	Aruba Net:A2:56:11		6	20%	3.5 110	2.569929	TELNET	WILL/Supp - DO/Suppress Go Ahead - WILL/Suppres...	
telnet_client	telnet_server	Aruba Net:A2:56:11		6	67%	11.0 79	2.383771	TELNET	DO/Echo	
telnet_client	telnet_server	Aruba Net:A2:56:11	+	6	74%	5.5 79	2.384214	TELNET	DO/Echo	
telnet_server	telnet_client	Aruba Net:A2:56:11		6	20%	5.5 78	2.592829	TELNET	Src= 23, Dest= 3044, ..., S= 948450599, L= 0...	
telnet_client	telnet_server	Aruba Net:A2:56:11	+	6	67%	11.0 94	3.013802	TELNET	WILL/Supp Go Ahead - DO/Suppress Go Ahead - ...	
telnet_server	telnet_client	Aruba Net:A2:56:11	+	6	68%	5.5 94	3.014357	TELNET	WILL/Supp Go Ahead - DO/Suppress Go Ahead - ...	
telnet_client	telnet_server	Aruba Net:A2:56:11	+	6	20%	11.0 78	3.020349	TELNET	Src= 23, Dest= 3044, ..., S= 948450599, L= 0...	
telnet_client	telnet_server	Aruba Net:A2:56:11	+	6	68%	3.0 77	3.039629	TELNET	s	
telnet_client	telnet_server	Aruba Net:A2:56:11	+	6	68%	4.0 77	3.040070	TELNET	s	
telnet_client	telnet_server	Aruba Net:A2:56:11	+	6	77%	3.0 77	3.041011	TELNET	s	
telnet_server	telnet_client	Aruba Net:A2:56:11	+	6	21%	5.5 78	3.045093	TELNET	Src= 23, Dest= 3044, ..., S= 948450599, L= 0...	
telnet_server	telnet_client	Aruba Net:A2:56:11		6	21%	11.0 78	3.045674	TELNET	s	
telnet_client	telnet_server	Aruba Net:A2:56:11		6	70%	11.0 77	3.049584	TELNET	d	
telnet_server	telnet_client	Aruba Net:A2:56:11		6	21%	11.0 78	3.052055	TELNET	d	
telnet_server	telnet_client	Aruba Net:A2:56:11	+	6	21%	11.0 78	3.052477	TELNET	d	
telnet_server	telnet_client	Aruba Net:A2:56:11	+	6	21%	11.0 78	3.052862	TELNET	j	
telnet_client	telnet_server	Aruba Net:A2:56:11		6	77%	11.0 77	3.057122	TELNET	s	
telnet_server	telnet_client	Aruba Net:A2:56:11		6	20%	11.0 78	3.059064	TELNET	s	
telnet_server	telnet_client	Aruba Net:A2:56:11		6	20%	11.0 78	4.189910	TELNET	s	TCP Too Many Retransmission
telnet_client	telnet_server	Aruba Net:A2:56:11		6	75%	11.0 77	4.409710	TELNET	i	
telnet_server	telnet_client	Aruba Net:A2:56:11		6	20%	11.0 78	4.424117	TELNET	i	
telnet_client	telnet_server	Aruba Net:A2:56:11		6	67%	11.0 76	4.428667	TELNET	Src= 3044, Dest= 23, ..., S=4144301600, L= 0...	
telnet_client	telnet_server	Aruba Net:A2:56:11		6	71%	5.5 77	4.439597	TELNET	n	
telnet_server	telnet_client	Aruba Net:A2:56:11		6	21%	3.0 78	4.787233	TPTNPT	n	
telnet_server	telnet_client	Aruba Net:A2:56:11		6	20%	11.0 78	5.107624	TELNET	n	TCP Too Many Retransmission
telnet_client	telnet_server	Aruba Net:A2:56:11		6	68%	5.5 76	5.213803	TELNET	Src= 3044, Dest= 23, ..., S=4144301601, L= 0...	
telnet_client	telnet_server	Aruba Net:A2:56:11		6	70%	5.5 76	5.510882	TELNET	Src= 3044, Dest= 23, ..., S=4144301601, L= 0...	
telnet_client	telnet_server	Aruba Net:A2:56:11		6	75%	5.5 78	5.717007	TELNET	..	
telnet_server	telnet_client	Aruba Net:A2:56:11		6	22%	5.5 88	5.719620	TELNET	..Password:	
telnet_client	telnet_server	Aruba Net:A2:56:11		6	70%	5.5 76	6.235025	TELNET	Src= 3044, Dest= 23, ..., S=4144301603, L= 0...	TCP Slow Acknowledgement {0
telnet_client	telnet_server	Aruba Net:A2:56:11		6	67%	5.5 77	6.250117	TELNET	s	
telnet_server	telnet_client	Aruba Net:A2:56:11		6	21%	11.0 78	6.258645	TELNET	+	
telnet_client	telnet_server	Aruba Net:A2:56:11		6	68%	5.5 77	6.348350	TELNET	1	
telnet_client	telnet_server	Aruba Net:A2:56:11		6	67%	5.5 77	6.416328	TELNET	s	
telnet_server	telnet_client	Aruba Net:A2:56:11		6	20%	11.0 78	6.418291	TELNET	+	
telnet_client	telnet_server	Aruba Net:A2:56:11	+	6	71%	5.5 78	6.485550	TELNET	f1	
telnet_server	telnet_client	Aruba Net:A2:56:11		6	20%	2.0 78	6.493035	TELNET	+	
telnet_client	telnet_server	Aruba Net:A2:56:11		6	68%	5.5 77	6.548292	TELNET	+	
telnet_server	telnet_client	Aruba Net:A2:56:11		6	22%	11.0 70	6.554633	TELNET	+	
telnet_client	telnet_server	Aruba Net:A2:56:11		6	70%	8.5 76	6.705973	TELNET	Src= 3044, Dest= 23, ..., S=4144301609, L= 0...	
telnet_server	telnet_client	Aruba Net:A2:56:11		6	22%	11.0 78	6.707617	TELNET	+	
telnet_client	telnet_server	Aruba Net:A2:56:11		6	67%	5.5 76	6.907000	TELNET	Src= 3044, Dest= 23, ..., S=4144301609, L= 0...	
telnet_client	telnet_server	Aruba Net:A2:56:11		4	75%	5.5 78	6.984287	TPTNPT	..	
telnet_server	telnet_client	Aruba Net:A2:56:11		6	21%	11.0 84	7.000676	TELNET	..Owner:	
telnet_client	telnet_server	Aruba Net:A2:56:11		6	70%	5.5 76	7.107378	TELNET	Src= 3044, Dest= 23, ..., S=4144301611, L= 0...	

Packets: 50 (of 21,305) Duration: 7:00:00
无线网络连接2 Channel: 6 - 2437 M

典型WLAN安全问题(4)

- Denial of Service
 - Disable RF: 物理上干扰信道、制造噪声源
 - 利用802.11协议中的解关联帧
 - 伪造AP的MAC地址
 - 连续发送解关联帧 → 广播地址
 - 用户无法关联AP

典型WLAN安全问题(5)

- Session Hijacking
 - ARP欺骗
 - To gateway: 入侵者利用ARP Spoofing 将自己伪造为受害主机
 - To victim: 入侵者利用ARP Spoofing 将自己伪造为gateway
 - 受害主机与网络间所有通信都流经入侵者
 - 入侵者可以：修改、删除或者插入数据
- Man-in-the-middle Attack
 - 入侵者让合法客户机同入侵者AP连接：相同ESSID，更高功率
 - 入侵者接入受害网络有效AP
 - 同样，受害主机与网络间所有通信都流经入侵者
- 流氓AP
 - 如：个人将未经授权的AP插入有线网络中，从而让任何拥有笔记本电脑和无线网卡的人自由进入网络

WLAN安全解决方案演进(1)

- 第一阶段：802.11标准定义的安全性
 - SSID: Service Set Identifier ， 标识网络
 - 用于接入控制
 - WEP: static RC4 40/128 bit
 - 用于数据加密
 - MAC ACL
 - 基于用户MAC地址做过滤
- 第二阶段：
 - VLAN: 利用VLAN， 隔离WLAN流量
 - 802.1X: 接入认证
 - Dynamic 128 bit WEP: 数据加密

WLAN安全解决方案演进(2)

- 第三阶段：
 - VPN: Layer 3 安全性
 - WPA: WiFi Protected Access
 - 接入认证: 802.1X
 - 数据加密: TKIP, RC4 128bit 48 bit IV
 - 802.11i/WPA2:
 - 接入认证: 802.1X
 - 数据加密: CCMP AES 128bit 48 bit IV
 - 移动性考虑: 预认证、预鉴权
 - WAPI:
 - 接入认证: WAI
 - 数据加密: WPI
 - 移动性考虑: 预认证、预鉴权
 - IDS: Intrusion Detection System, 入侵检测系统

WLAN中802.1X应用技术分析

- 三元实体
 - 申请者（802.1X客户端）
 - Opensource: SecureW2、Open1X(XSupplicant)...
 - 商业版本1X客户端: Windows XP、Vista、Cisco、华为...
 - 校园网自行开发1X客户端: TUNet...
 - 认证者（AP/支持802.1X的交换机）
 - 目前业内厂商推出的多种无线产品已全面支持802.1X
 - Cisco、Aruba、Motorola、Nortel、Huawei.....
 - 认证服务器（Radius Server）
 - Windows server: Internet Authentication Service
 - Opensource: Freeradius、Jradius、Openradius、BSDRadius...
 - 商业产品: Radiator、Cisco Secure Access Control Server for Windows...

WLAN已具备部署
802.1X的技术能力

WLAN中802.1X应用现状

- WLAN接入认证主要采用的技术手段
 - Web Portal
 - 部署复杂度低，在大陆和台湾被普遍采用
 - 中国移动、中国网通、国内大部分高校、台湾大部分高校
 - 部署简单，用户无需加装客户端软件
 - 802.1X
 - 少数WLAN采用
 - Eduroam，欧洲、亚洲高校间漫游联盟
 - 所部署无线网络需支持802.1X，部分较老WLAN需升级
 - 部署复杂度较高：客户端需加装相应802.1X客户端
 - 管理复杂度较高：如利用EAP-TLS方式，需生成并维护大量用户证书
 - 移动性问题：用户移动时需重新完成端口认证
 - MAC Radius
 - 对WIFI手机、PDA等部分移动终端采用MAC地址认证方式
 - 安全性差

清华无线校园网802.1X技术试验(1)

- 清华无线校园网简介

- 早期

- 图书馆：2002年

- 六教：2003年

- 无线实证网(2004~2006)

- 融合多厂商无线设备

- Aruba, Nortel, Motorola, Tropos, Proxim, Huawei, Gemtec, Ruckus...

- 融合无线交换、无线Mesh多种组网技术

- 统一认证和分布式Radius

- 数据和语音同传

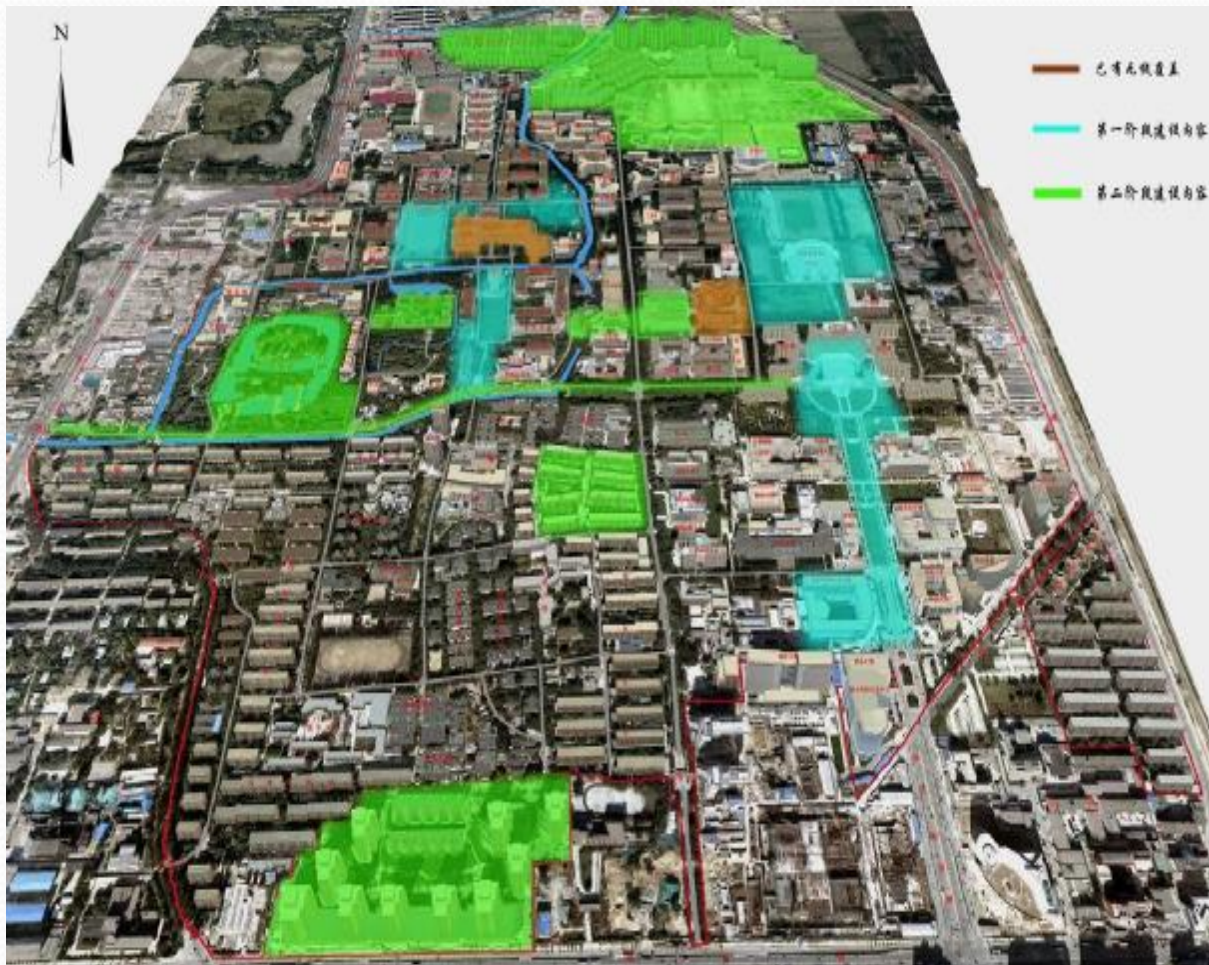
- 大规模建设(2006至今)

- 覆盖重点区域：

- 学生宿舍、教学楼

- 室内+室外

- 200+室内AP， 20+室外Mesh AP



清华无线校园网802.1X技术试验(2)

- 基于开源软件开展802.1X技术实验
 - 客户端: SecureW2, XSupplicant
 - 认证者: 多款支持802.1X的无线AP
 - Aruba、Cisco 1120、Proxim AP-4000、Motorola Hotzone ...
 - 认证服务器: Freeradius、openssl(用于生成证书)
- 支持EAP-MD5、EAP-PEAP、EAP-TLS、EAP-TTLS等多种EAP认证方式
- 完成同Eduroam互联互通的技术试验

无线校园网802.1X应用思考

- 802.1X \neq 无线校园网安全，但有助于无线校园网安全
 - 802.1X只是接入控制安全：限制非法用户使用网络资源
 - 无线链路的安全问题没有解决：需要TKIP、CCMP等加密链路 or ...
- 802.1X应用于无线校园网的阻力
 - 建设管理者
 - 设备升级的成本压力：部分设备需要升级或更换
 - 大规模用户集中式管理的复杂度
 - 证书的生成和管理
 - 使用者
 - 用户使用便利性和习惯问题：加装客户端
 - 802.1X对用户移动性的影响：如涉及三层切换，则需重新完成802.1X认证
 - 部分终端无法支持802.1X认证：如WIFI手机等

总结和讨论

- WLAN安全
 - 相比有线网络安全，放大某些安全问题并引入新的挑战
 - 无线侧安全远远不够：802.11i/WAPI等的不足
- 802.1X
 - 能否解决WLAN安全问题？
 - 关注在接入控制一侧
 - 对用户的控制会加强
 - 是否值得推广和部署？
 - 得与失
 - 如果部署替代性的安全手段，如VPN等，802.1X是否还需要？

谢谢！