网络攻防协议课程报告

对网络攻防协议课程中无线局域网安全协议的学习总结和进一步探究

姓名　廖汉钦

学号　2018091620024

课程名称　网络攻防协议

指导老师　罗绪成

专业　软件工程互联网安全方向

2020 年 12 月 25 日

摘要

无线局域网技术从 20 几年前出现起，已经经历了一段成熟的发展历程。本文从无线局域网简介开始，介绍最开始的局域网协议 WEP。由于 WEP 本身算法的巨大致命缺陷，更安全、更健壮的 WPA 出现了。由于其优秀的性能，WPA 被使用至今，但依然存在对其实施攻击的方式。所以最后出现了 WPA2，它是 WPA 的升级版本，安全性更强。

第一节 无线局域网简介

WLAN 是 Wireless Local Area Network 的简称，指应用无线通信技术将计算机设备互联起来，构成可以互相通信和实现资源共享的网络体系。无线局域网本质的特点是不再使用通信电缆将计算机与网络连接起来，而是通过无线的方式连接，从而使网络的构建和终端的移动更加灵活。

1.1 无线局域网的组件

（1）STA：Station，具有无线网卡的客户端设备。

（2）AP：Access Point，无线接入点。

（3）DS：Distributed System，用于连接一系列基本服务集和局域网，从而创建一个扩展服务集的系统。

1.2 WLAN 的基本工作原理：

（1）AP 周期性的发送 Beacon 帧，宣布其存在。

（2）STA 发送 Probe Request 帧主动探测某个 AP。

（3）STA 发送认证请求，AP 回复认证请求。

（4）如果认证通过，STA 发送关联请求，AP 回复关联响应，实现 STA 和 AP 的关联。

（5）STA 和 AP 之间传输数据帧.

1.3 802.11 控制帧

控制对通信媒体的访问，负责域的清空、信道的取得以及载波监听的维护，并于收到数据时予以应答，借此促进工作站间数据传输的可靠性。

1.4 802.11 数据帧

携带上层协议数据并传输数据。

1.5 802.11 管理帧

管理无线网络（如节点的加入和退出等）。

1.6 常用管理帧

Beacon 帧：AP 发送它来宣布其存在，STA 接收它来感知 AP 的存在。(Beacon 就是某个无线网络的心跳帧)

Probe Request 帧：STA 发送它来搜索周围的无线网络。

Probe Response 帧：AP 收到 Probe Request 帧后，会发送它进行响应。

Association Request 帧：当 STA 想要关联某个 AP 时，会发送它，进行关联请求。

Association Response 帧：AP 收到 STA 的 Association Request 帧后，会回复它来通知关联请求的处理结果。

Authentication 帧：主要用于身份认证。

1.7 WLAN 安全

WEP，即有线等效保密，达到有线网络相同的安全性（其实并不安全）。对 WEP 的破解是基于其加密体制的缺陷，通过收集足够的数据包，使用分析密算法还原出密码。

WPA/WPA2/WPA3，依次具有更强的安全性。其中 WPA 目前没有加密体制的缺陷可被利用，破解 WPA 密码使用的是常规的字典攻击法。

第二节 WEP（有线等效保密）

2.1 加密流程

（1）利用 24 比特的初始矢量 IV 和 WEP Key 作为 RC4 算法的输入，输出密钥流，IV 随数据帧以**明文方式**发送。

（2）把要加密的数据为 CRC-32 算法的输入，输出 ICV，将其追加到明文后面。

（3）将 ICV 和密钥流做异或运算，得到密文。

2.2 WEP 通过以上的操作试图达到以下的目的

（1）采用流密钥加密算法保证通信的安全性，以对抗窃听。

（2）采用 CRC32 算法作为完整性检验，以对抗对数据的篡改。

2.3 RC4 流密钥生成算法致命缺陷

WEP 帧中数据负载的第一个字节是逻辑链路控制的 802.2 头信息，这个头信息对于每个 WEP 帧都是相同的，攻击者很容易猜测，利用猜的第一个明文字节和 WEP 帧数据负载密文就可以通过异或运算得到 RC4 生成的密钥流中的第一字节。

此外，种子密钥中的 24 比特初始矢量是以明文形式传送的，攻击者可以将其截获，存到初始矢量 IV。

S.Fluhrer，I.Martin 和 A.Shamir 证明：利用已知的初始矢量 IV 和第一个字节密钥流输出，并结合 RC4 密钥方案的特点，攻击者通过计算就可以确定 WEP 密钥。

2.4 CRC-32 完整性校验算法缺陷

攻击者可以篡改密文内容，并且 CRC-32 并不提供加密，只负责检查原文是否完整。

2.5 WEP 的安全弱点

802.2 头信息和简单的 RC4 流密码算法导致攻击者在有客户端并有大量有

效通信时，可以分析出 WEP Key。

IV 重复使用导致在攻击者在有客户端、少量通信或者没有通讯时，可以使用 arp 重放的方法获得大量有效数据。

此外，在同时获得 IV 和 WEP Key 的情况下，攻击者可以肆无忌惮地窃听任意 AP 和 STA 间的通讯。

无身份验证机制，使用线性函数 CRC32 进行完整性校验。无身份验证机制，导致攻击者能和 AP 建立伪链接。进而获得 XOR 文件。使用线性函数 CRC32 进行完整性校验，导致攻击者能用 XOR 文件伪造一个 ARP 包。然后依靠这个包去捕获大量有效数据。

第三节 WPA

WPA 全名为 Wi-Fi Protected Access，有 WPA 和 WPA2 两个标准，是一种保护无线网络（Wi-Fi）安全的协议。

WPA
=802.1x + EAP + TKIP + MIC 或者
=Pre-shared Key + TKIP + MIC

802.11i(WPA2)
=802.1x + EAP + AES + CCMP 或者
=Pre-shared Key + AES + CCMP

这里 802.1x + EAP，Pre-shared Key 是身份校验算法（WEP 没有设置有身份验证机制）

TKIP 和 AES 是数据传输加密算法（类似于 WEP 加密的 RC4 算法）

MIC 和 CCMP 是数据完整性编码校验算法（类似于 WEP 中 CRC32 算法）

802.1x + EAP 和 Pre-shared Key 是认证方式，前者为工业级，后者为家庭级。

3.1 密钥管理

WPA 和 WEP 不同，WEP 所有的 STA 采用相同的密钥进行数据加密，安全性较差。但 WPA 采用的是 RSNA，即不同 STA 和 AP 之间采用不同的密钥进行加密，但依然保留用于管理和控制网络通信的统一密钥。

上述中每个 STA 不同的密钥称为临时密钥（PTK），每个 STA 相同的密钥称为组密钥（GTK）。

3.2 四次握手

WPA 和 WPA2 均使用 802.11i 中定义的四次握手，STA 和 AP 通过四次握手相互验证和协商成对的 PTK。PTK 通过成对主密钥（PMK）、AP 随机数 ANonce、STA 随机数 SNonce 和双方 MAC 地址等计算生成，其中 PMK 由登录密码等双方均已知的信息计算生成。而后续正常数据加密所使用的临时密钥（TK）即派生自 PTK。

（1）AP 广播 SSID，并将随机生成的随机数 ANonce 发送给 STA

（2）STA 生成随机数 SNonce，利用 PMK（由网络的 SSID 和设置的密码

Password 生成)、APMAC 地址、STAMAC 地址、ANonce 和 SNonce 生成 PTK，随之利用 Hash 函数（WPA 为 MD5，WPA2 为 SHA_1）以 PTK 的前 16 个字节和第一次握手包的数据生成消息完整性校验码（MIC)。将 SNonce 和 MIC 发送给 AP。

PMK 生成算法：PMK=pdkdf2_SHA1(passphrase，SSID，SSID length，4096)

PTK 生成算法： PTK=SHA1_PRF(PMK， Len(PMK)， "Pairwise key expansion"， MIN(AA， SA) ||Max(AA， SA) || Min(ANonce， SNonce) || Max(ANonce，SNonce))

MIC 生成算法：MIC = HMAC(PTK[0:16]，802.1x data)
(HMAC=MD5 if WPA else SHA1)

（3）AP 收到 SNonce 和 STA 的 MIC。 AP 采用和（2）相同的方法生成相同的 PTK，使用和（2）一样的方法以及第二次握手包的数据生成 AP 的 MIC，并验证 STA 的 MIC。若验证成功，则和验证了 STA 的真实性：两者的 PTK 相同，中途也没有受到中间人篡改。随后将 ANonce、加了密的组密钥 GTK 和 AP 的 MIC 发送给 STA。

（4）STA 收到 GTK，并验证 AP 的 MIC。一旦验证成功，则证明 AP 拥有和 STA 一样的 PTK，从而验证了 AP 拥有正确的 PMK，继而验证了 AP 的真实性。此时，STA 安装 PTK 和 GTK，发送 ACK 确认，同时也计算新的 MIC 发送给 AP。

（5）AP 收到 ACK 和新的 MIC 后，验证这个新的 MIC。此时，AP 安装 PTK 和 GTK。握手完成。

3.3 四次握手的关键点

（1) 如果双方的 Nonce 在中途被修改了，会导致 STA 和 AP 计算出来的 PTK 不一致，从而在验证 MIC 时失败，对应的消息被丢弃。所以虽然攻击者能够修改 Nonce，但是握手过程不会成功。

（2）第三个包中也包含了 AP 的 ANonce。STA 必须验证这与第一个包中的 ANonce 是否相同，而第三个包中的 ANonce 是通过 MIC 保护的。所以如果第三个包通过了 MIC 验证，则证明 ANonce 没被篡改，进而如果 ANonce 和第一个包中的 ANonce 相同，则证明该 ANonce 是正确的。

3.4 字典攻击

由四次握手的整个过程可知，AP 或者 STA 每次验证 MIC 时，都是使用 SSID、Password、AP_MAC、STA_MAC、ANonce、SNonce 这六个元素计算出 MIC，并将其与对方发送过来的 MIC 相比较。而上述七个元素除了 Password 不是公开的，其余全是第三者可以轻易获取的元素（通过抓包并且分析），那么如果我们能够一个一个猜测 Password，利用以上元素以及四次握手时的 MIC 验证算法，就能够猜测出正确的 Password，从而破解整个网络。这并不是利用 WPA 的加密算法缺陷（即使它也没有），而是一种常规的字典攻击模式。

3.5 WPA 安全性

（1）Per-Packet Key 加密机制、动态 key 管理机制使得使用类似于 WEP 中

分析子密码攻击的方案，在 WPA 中将变得异常困难，和不可实现。

（2）身份验证机制使得 AP 和 STA 之间可以互相验证真实性，杜绝了伪连。

（3）虽然 TKIP 使用的是和 WEP 一样的加密算法 RC4，但是 TKIP 中使用 Per-Packet Key 加密机制配合 RC4，这样弥补了 RC4 加密算法的不足，抵抗基于 RC4 漏洞的攻击。而 WPA2 中的 AES 比 TKIP 有更高的安全性，对他的破解难度就更高了。

（4）使用非线性的 MIC 信息编码完整性算法，取代线性的 CRC-32。增加了攻击者伪造合法数据的难度。

所以综上，**类似于 WEP 中的无客户端破解密码的做法在 WPA 中是不存在的。**

3.6 KRACK 攻击

欧洲鲁汶大学的博士后安全研究员 Mathy Vanhoef 在 2017 年 10 月 15 日披露一个 WPA2 的高危漏洞。漏洞允许在 Wi-Fi 范围内的攻击者监听计算机和接入点之间的 Wi-Fi 流量。该漏洞影响协议本身，且对 WPA 和 WPA2 均有效。利用该漏洞进行的攻击称为 KRACK 攻击。

KRACK 攻击利用了协议中的重传机制：若 AP 无法正确接收到确认，将引发数据重传。若攻击者让 AP 无法收到来自 STA 的确认报文，AP 将重传四次握手中的第 3 个报文，客户端每次接收到第 3 个报文时都会重装相同的会话密钥。攻击者可利用此次握手过程，暴力增量式发送第 3 个报文，从而强制重置数据保密协议使用的增量传输数据包数（nonce）和接收重放计数器，导致密钥重用。攻击者可以通过这种方法重放、解密和/或伪造数据包。

第四节 WPA2

WPA2（WPA 的升级）采用 AES 算法的 CTR 模式(取代了 TKIP)和 CCMP 算法(取代了 MIC)。WPA2 和 WPA 的整体运行流程相同，只是相关算法不同而已，WPA2 依旧有重要的四次握手流程。

第五节 无线局域网攻防

5.1 DeAuth 攻击

伪装成目标 AP 已关联的设备，向 AP 发送 Deauthentication 解除认证帧，造成设备掉线，从而达到拒绝服务的目的。

该攻击不仅可以强制STA连接到一个假冒的AP上，也可抓取四次握手的帧。

5.2 AuthDos 攻击

随机生成大量 mac 地址，伪装设备向 AP 发送大量 Authenticattion 请求帧，使请求数量超出 AP 承载能力，从而造成拒绝服务攻击，使正常用户无法连接 AP。

5.3 Asso 攻击

针对空密码或已破解密码的 WLAN，伪造大量设备关联请求，淹没 AP 的关

联表，使正常用户无法与 AP 建立关联。

5.4 RF jamming 攻击

对无线信号进行干扰，用噪声信号淹没射频信号导致系统失效。 这种干扰会影响到一片区域内指定频带范围的信号。

总结

该课程总结报告从局域网通信的原理入手，步步分析 WEP/WAP/WAP2 执行过程（四次握手，身份认证流程）以及安全性现状，阐述 WEP 的致命安全性缺点以及 WAP/WAP2 相比较于 WEP 的安全性优势，介绍了大量 WAP/WAP2 面临的非算法缺陷性的攻击威胁，从而建立起一个相对完整的无线局域网协议体系。

无线局域网通信从诞生之初到现在已经过去了 20 余年，WEP 从最开始的安全到 03 年的不安全才过了短短几年，随后 WAP 便出现，并凭借其强大的安全性一直被使用到了现在。但是我们并不知道在未来的那个时候 WAP 甚至 WAP2 会变得不安全，我们不知道 WAP/WAP2 体系有着那些未被发现的漏洞，甚至我们不知道未来是否有足够强大的技术能够破解 WAP/WAP2……所以，对现有的网络协议的安全性研究以及对新协议的探索就显得相当重要。