基于无线网络 WEP 密钥的安全分析

西华师范大学教育科学与技术学院　董　屹　西华师范大学计算机学院　李　佳　焦方源

[摘　要] 针对现有无线网络中使用的 WEP 加密方案的安全问题，本文详细的分析了 WEP 加密方案的缺陷和漏洞以及出现的原因。最终给出了当前无线网络中比较安全的加密策略。

[关键词] WEP 密钥　CRC-32　初始向量

一、引言

WLAN 技术出现之后，“安全”就始终成为其发展的焦点。其中大多数无线网络中采用 WEP 密钥加密的方式来运作。但就目前而言，在无线网络中针对 WEP 的攻击与破解层出不穷，其中绝大多数攻击都是对 WEP 密钥进行破解，盗用 WEP 密钥。最终窃取合法用户的信息和数据，并影响整个无线网络的安全。针对这一问题，本文对 WEP 密钥缺陷进行了探讨，最终提出了安全策略组的理念来保障无线网络的安全。

二、无线网络中的 WEP 密钥

相对于有线网络来说，通过无线网络发送和接收数据更容易被窃听。在 IEEE802.11 标准中采用了 WEP(Wired Equivalent Privacy:有线对等保密)协议来设置专门的安全机制，WEP 是建立在 RC4 流密码机制上的协议，并使用 CRC-32 算法进行数据检验和校正从而确保数据在无线网络中的传输完整性。RC4 流密码机制其目的在于对无线环境中的数据进行加密。从而达到数据在传递过程中不被窃听和破解。它采用对称加密机理，即数据的加密和解密采用相同的密钥和加密算法。WEP 使用加密密钥(也称为 WEP 密钥)。启用加密后，两个 802.11 设备要进行通信，必须具有相同的加密[1]密钥。

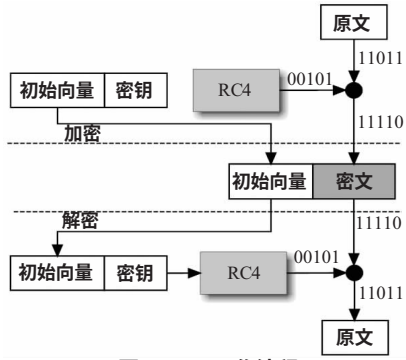

图 1　WEP 工作流程

(一)加密过程

WEP 支持 64 位和 128 位加密，对于 64 位加密，加密密钥为 10 个十六进制字符或 5 个 ASCII 字符；对于 128 位加密，加密密钥为 26 个十六进制字符或 13 个 ASCII 字符。依赖通信双方共享的密钥来保护所传的加密数据帧。其数据的加密过程如下：

1.计算校验和(Check Summing)。

(1)对输入数据进行 CRC-32 完整性校验和计算。

(2)把输入数据和计算得到的校验和组合起来得到新的加密数据，也称之为明文，明文作为下一步加密过程的输入数据。

2.加密:在这个过程中，将第一步得到的数据明文采用 RC4 算法加密。对明文的加密有两层含义：明文数据的加密，保护未经认证的数据。

(1)将 24 位的初始化向量和 40 位的密钥连接并进行校验和计算，最终得到 64 位的数据。

(2)将 64 位的数据输入到基于 RC4 流密码算法的虚拟随机数产生器中，它对初始化向量和密钥的校验以及加密计算。

(3)经过校验和计算的明文与虚拟随机数产生器的输出密钥流进行按位异或运算得到加密后的信息，即密文。

3.传输:将初始向量和密文串接起来，得到要传输的加密数据帧，在无线网络上传输。

(二)解密过程

1.恢复初始明文。重新产生密钥流，将其与接收到的密文信息进行异或运算，以恢复初始明文信息。

2.检验校验和。接收方依照恢复的明文信息来检验校验和，并将恢复的明文信息进行分离，重新计算校验和，并检查它是否与接收到的校验和相匹配。这样即确保只有正确校验和的数据帧才会被接收方接受。并获取无线网络中的数据。

三、WEP 缺陷

WEP 密钥缺陷主要源于三个方面：

1. WEP 帧的数据负载

由于 WEP 加密算法实际上是利用 RC4 流密码算法作为伪随机数产生器，并由初始向量和 WEP 密钥组合而生成 WEP 密钥流，再将该密钥流与 WEP 帧的数据负载进行异或运算来实现加密运算 (图 1)。RC4 流密码算法是将输入密钥进行某种置换和组合运算来生成 WEP 密钥流。由于 WEP 帧的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 帧的数据都是相同的，攻击者很容易猜测，利用猜的第一个明文字节和 WEP 帧的数据负载密文即可通过异或运算得到伪随机数发生器生成的密钥流中的第一个字节。

2. CRC-32 算法在 WEP 中的缺陷

在 802.11b 协议中是允许初始向量被重复多次使用，这就构成了恶意攻击者充分利用 CRC-32 算法在 WEP 中的缺陷进行数据窃听和攻击。

于 WEP 而言，CRC-32 算法的作用在于对数据进行完整性校验。但是 CRC-32 其校验和并不是 WEP 中的加密函数，它只是负责检查原文是否完整。也就是说在整个过程中，恶意的攻击者可以截获 CRC-32 数据明文。并可重构自己的加密数据并结合初始向量一起发给接受者。

3.在 WEP 过程中，无身份验证机制。恶意攻击者通过简单的手段就可以实现与无线局网客户端的伪链接。既可获取相应的异或文件，并通过 CRC-32 进行完整性校验。从而攻击者能用异或文件伪造 ARP 包。然后依靠这个包去捕获无线局网中的大量有效数据。

四、基于 WEP 密钥缺陷引发的攻击

目前针对 WEP 密钥缺陷引发的攻击，引发出的攻击可大致分为两类：

1.被动无线网络窃听，破解 WEP 密码

这种攻击模式的主要特征在于，在无线网络中进行大量的数据窃听，收集到足够多的有效数据帧，并利用这些信息对 WEP 密码进行还原。从这个数据帧里攻击者可以提取初始向量值和密文。对应明文的第一个字节是逻辑链路控制的 802.2 头信息。通过这一个字节的明文和密文，攻击者做异或运算就能得到一个字节的 WEP 密钥流，由于 RC4 流密码产生算法只是把原来的密码打乱次序，攻击者获得的这一字节的密码仅是初始向量和密码的一部分。但由于 RC4 的打乱，攻击者并不知道这一个字节具体的位置和排列次序。但当攻击者收集到足够多的初始向量值和密码之后，就可以进行统计分析运算。利用上面的密码碎片重新排序，最终利用得到密码碎片正确的顺序排列，从而分析出 WEP 的密码。

2.ARP 请求攻击模式

ARP 请求攻击模式：攻击者抓取合法无线局网客户端的数据请求包。如果截获到合法客户端发给无线访问接入点的 ARP 请求包，攻击者便会向无线访问接入点重发 ARP 包。由于 802.11b 允许初始向量值重复使用，所以无线访问接入点接到这样的 ARP 请求后就会自动回复到攻击者的客户端。这样攻击者就能搜集到更多的初始向量值。当捕捉到足够多的初始向量值就可以进行被动无线网络窃听并进行 WEP 密码破解。但当攻击者没办法获取 ARP 请求时，其通常采用的模式即使用 ARP 数据包欺骗，让合法的客户端和无线访问接入点断线，然后在其重新连接的过程中截获 ARP 请求包，从而完成 WEP 密码破解。

五、对应决策

目前针对 WEP 密钥的破解技术和相应工具已经相当成熟。通过互联网搜索引擎可以找到大量的相关信息，使得任意一个用户都可能成为恶意攻击者，并对使用 WEP 密钥的无线网络造成威胁。

基金项目 本文受西华师范大学科研启动基金项目(07B012)资助。

作者简介 董屹，男，硕士，主要研究方向为计算机网络技术与应用。李佳，女，硕士，主要研究方向为互联网络理论及技术。

为此越来越多的用户开始转向于使用 WPA 加密方案,但是由于其完整的 WPA 实现比较复杂,操作过程较为困难(微软针对这些设置过程还专门开设了一门认证课程),一般用户不容易掌握。对于企业和政府来说,很多设备和客户端并不支持 WPA,最重要的是 TKIP(暂时密钥集成协议)加密并不能满足一些更高要求的加密需求,还需要更高的加密方式,所以 WPA 的使用出现了较多的问题。同时公认为较为安全的 WPA 加密方案的破解技术也已经出现,仅因为目前计算机运算速度等多方面原因使得破解 WPA 加密需花费大量的时间。但我们可以预见的是:在不久之后 WPA 加密方案也会如 WEP 加密一样脆弱。

当今比较成熟的无线网络安全方案通常不仅仅局限于一种安全策略的方案。这是源于其单一策略的功能局限性。在本文中我们提出了安全策略组(图 2)的概念。根据这些策略自身的特点构建出一个安全的无线环境。

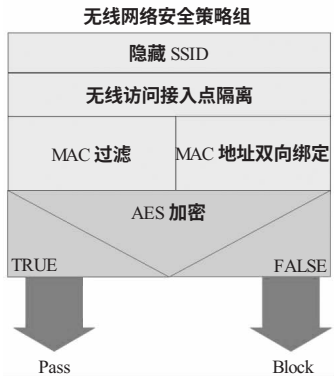

图 2 无线网络安全策略组

1.隐藏 SSID 策略

SSID,即 Service Set Identifier 的简称,让无线客户端对不同无线网络的识别,客户端只有收到这个参数或者手动设定与无线访问接入点相同的 SSID 才能连接到无线网络。SSID 策略可以保障在当前网络中的无线信道中的数据不被窃听,从而保障了对应的无线网络密码安全。这一策略为无线网络策略组的第一步,仅当通过这一策略之后,才能进入到无线访问接入点隔离阶段。

2.无线访问接入点隔离策略

无线访问接入点隔离策略类似于有线网络的 VLAN,即将所有的无线客户端设备完全隔离,使其只能访问无线访问接入点连接的固定网络。不同的 VLAN 之间不能直接通信,从而降低了无线接入点被恶意攻击者攻击的机率。当无线用户接入点进入到访问接入点隔离策略阶段时,根据各自接入交换机将会被自动划分到相应的 VLAN 上。划分完毕之后,策略组就自动对各个接入点进行第三步策略判断。

3.MAC 地址策略

在这一策略中包含两个详细的规则:(1)MAC 地址过滤,这种方式就是通过对无线访问接入点的设定,将指定的无线网卡的物理 MAC 地址输入到无线访问接入点中。而访问接入点对收到的每个数据包都会做出判断,只有符合设定标准的才能被转发,否则将会被丢弃。这样就从很大的程度上保障了非当前的无线网络中注册的计算机不能登陆网络。(2)MAC 地址双向绑定策略,MAC 地址双向绑定的方法多用于企业内部针对 ARP 欺骗病毒进行防御,不过对于伪造 MAC 地址非法入侵无线网络来说同样奏效。其从根本上防御无线网络中的 ARP 请求攻击。在这一策略过程中,仅当接入点设备满足如上两个详细规则后,才能进行最终的无线通信,并在通信的过程中使用策略 4 的加密策略。

4.AES 加密策略

AES 加密策略是整个策略组中最重要的策略,虽然上面的四种策略能从一定策略上保障整个网络的安全。但是为了更为有效的确保网络安全,则 AES 加密策略是整个策略组的核心部分。

AES 加密作为一种全新加密标准,其加密算法采用对称块加密技术,提供比 WEP 中 RC4 算法更高的加密性能,是密码学中的高级加密标准(Advanced Encryption Standard,AES),又称 Rijndael 加密法。尽管人们对 AES 还有不同的看法,但总体来说,AES 作为新一代的数据加密标准汇聚了强安全性、高性能、高效率、易用和灵活等优点。这个标准已经替代了原先的 DES,被多方分析且广为全世界所使用。经过五年的甄选流程,高级加密标准由美国国家标准与技术研究院(NIST)于 2001 年 11 月 26 日发布于 FIPS PUB 197,并在 2002 年 5 月 26 日成为有效的标准。2006 年,高级加密标准已然成为对称密钥加密中最流行的算法之一。仅当通过安全策略组时,接入点才能正常的进行网络信息通信。

总结

由上面四种安全策略构建的无线网络策略组,其中分别从 VLAN、MAC 两个方面来降低无线接入点被恶意攻击的风险。隐藏 SSID 策略则降低了接入点信息被窃听的风险。其安全系数已经完全能够抵御大多数无线网络攻击,并保证其正常工作以及无线接入点的各个用户的数据安全。

参考文献

[1] Break WEP Faster with Statistical Analysis Rafik Chaabouni, June 2006.

[2] Scott R.Fluhrer, Itsik Mantin, Adi Shamir,"Weaknesses in the Key Scheduling Algorithm of RC4". Selected Areas in Cryptography 2001: pp1- 24.

[3] Nikita Borisov, Ian Goldberg,David Wagner,"Intercepting mobile communications: the insecurity of 802.11." MOBICOM 2001, pp180 - 189.

[4] Wei Baodian,Liu Dong SU ,Wang Xinmei. The Principle,implementation and Cryptanalysis of AES Algorithm Rijndael [J].Communications Technology 2002(12).

[5] Joan Daemen, Steve Borg and Vincent Rijmen, "The Design of Rijndael: AES - The Advanced Encryption Standard." Springer- Verlag, 2002. ISBN 3- 540- 42580- 2.

[6] Nancy Cam- Winget, Russell Housley, David Wagner, Jesse Walker: Security flaws in 802.11 data link protocols. Communications of the ACM 46(5): 35- 39 (2003).

(上接第 372 页)

例:A: How do you find John's thesis?

B: Oh, it was a good typewriter that he used.

从表面上看,A.B 两句在意思上并没有多大联系,B 的回答违反了关系准则,产生了特殊的会话含义,即 John 的论文写得不好。由此看来,在英语幽默对话中,答话者往往有意或无意地违反合作准则,使会话产生特殊的会话含义,从而给问话者制造一些理解上的障碍。因此答话者必须有敏锐的观察力,根据特定的语境和共有的知识,在联想和推断之后,领悟答话者的弦外之音,从而理解其幽默所在;否则,就可能引出可笑的误解。

(4)礼貌原则与幽默

礼貌原则的提出是对合作原则的一种补救,它部分地说明了为什么人们有时会蔑视合作原则。Leech 的礼貌原则包括:策略准则、宽容准则、赞扬准则、谦虚准则、赞同准则、同情准则。简而言之,所谓的礼貌原则即"使自身受惠最小,使他人受惠最大;使自身受损最大,使他人受损最小。"(何兆熊 1999:222)

例:

Mother: I sent my little boy for two pounds of plums a pound and you sent me a pound a half.

Grocer: my sales are all right, madam, have you weighed your little boy?

杂货商通过简接的口吻指出,李子少了肯定是小孩偷吃了。杂货商既解释了李子少了的原因,又保全了妇女的面子。

3.结语

英语幽默,以其简练的语言形式,恰到好处的各种修辞,反映了现实生活中的各种乐趣和智慧,成为人们日常生活中不可缺少的一部分。同时,英语幽默从多个视角反映了英语语言的特征和规律。因此,要想真正理解和欣赏幽默,必须具备较强的语言和语用推理能力。正是基于这一点,本文试从会话含义、礼貌原则、言语行为理论和合作原则对幽默进行了语用分析,旨在分析幽默的会话含义,从而提高我们对幽默的理解能力。

参考文献

[1] Leech, G., 1983, Principles of Pragmatics [M]. London: Longman

[2] 何自然.语言学概论[M].长沙:湖南教育出版社,1988

[3] 吕光旦.英语幽默的语用学分析[J].外国语(1),1998

[4] 陈春华.会话幽默的语用分析[J].解放军外国语学院学报,1999(1)

[5] 戴琴.合作原则的违反在幽默艺术中的作用[J].湖南科技学院学报,2008

[6] 肖青云.幽默的会话含义分析[J].惠州学院学报(社会科学版),2004

[7] 王文婷.英语中幽默语的话语分析[J].消费导刊·教育时空,2009