如何在一分钟内
干掉 WiFi WPA

作者：

Toshihiro Ohigashi，广岛大学

Masakatu Morii，神户大学

编译：邹铮

审校：挨踢李@IT 专家网

1 导言

WPA（无线网络保护 Wi-Fi Protected Access）/TKIP（临时密钥完整性协议 Temporal Key Integrity Protocol）是专为保护无线局域网络通信机密性和完整性的安全协议。WPA 的出现旨在弥补 WEP（有线对等加密协议）存在的缺陷，WEP 一直是用于很多无线 LAN 产品的安全保护协议。WPA 主要使用两种形式的密钥，包括 64 位信息完整性检查（MIC）密钥和 128 位加密密钥。前者主要用于检查伪造/虚假信息，而后者主要用于加密和解密数据包。这些密钥都是从共有的主密钥（master key）中生成的。

很多安全研究人员一直都在潜心研究 WPA 的安全性，Moskowitz 就发现了 WPA 中抵御字典攻击的弱点，不过他可以通过绕开这个弱点来从任意长度的字符组中生成主密钥。多数其他分析师都对 WPA 的组件进行了分析，而这些对于 WPA 都不能构成威胁。在 2008 年的时候，Beck 和 Tews 对那些支持 IEEE802.11e QoS 功能的 WPA 部署发动了实质性的攻击，他们的攻击（被称为 Beck-Tews 攻击）可以从加密的小数据包中（如 APR 数据包和 DNS 数据包）中修复 MIC 密钥和纯文本，并且使用修复的 MIC 密钥对其加密数据包进行伪造。这种攻击的执行时间大约是 12 到 15 分钟。由于 Beck-Tews 攻击是一种基于应答式攻击的方法，攻击目标必须支持 IEEE802.11e QoS 功能。因此，他们的成果也是有限的。

在本文中，我们将提出一种针对任何 WPA 部署的根本性的攻击。首先，为了突破攻击目标无线 LAN 产品的限制，我们采用 Beck-Tews 攻击用于中间人攻击（MITM）。配合中间人攻击的 Beck-Tews 攻击并不需要目标能够支持 IEEE802.11e QoS 功能，这意味着我们的攻击可以攻击任何类型的 WPA 部署。另外，我们将探讨如何对无线局域网络实施有效的 MITM 攻击。在 MITM 攻击中，用户的通信被攻击者拦截，直到攻击结束才会解除拦截状态，这意味着当攻击时间比较长时用户可能检查到我们的攻击。因此，第三个，我们提供了几种缩短攻击执行时间的方法，正如标题所说，我们最终可以实现一分钟内干掉 WPA。

2 无线网络保护 WPA

在 WPA 中，主密钥是在访问接入点和客户端间共享的，主密钥会生成两种类型的密码，64 位的 MIC 密钥 K_和 128 位的密钥 K。64 位的 MIC 是从一个 MIC 密钥和数据中生成的，该密钥主要用于检测伪造/虚假信息，加密密钥用于加密解密数据包。

2.1 发送器的过程

发送者通过使用 Micheal 来计算（来自 MIC 密钥和 MSDU 的）MIC，该 MIC 被添加到 MSDU，如下所示：

MSDUjjmicheal(K_;MSDU); (1)

其中 micheal(K_;MSDU)是 64 位 MIC，而 jj 是连接，附有 MIC 的 MSDU 被分割到 MAC Protocol Date Units （MPDUs）中，通过使用 CRC32 从每个 MPDU 中计算出一个 32 位的校验和，并添加到 MPDU，如下所示：

MPDUjjCRC32(MPDU); (2)

其中 CRC32(MPDU)是 32 位的校验和（checksum），对每个附有校验和的 MPDU 执行 WPA 的加密。数据包密钥 PK 是从 48 位的 IV 中生成的，这是通过使用 WPA hash（）的专门 hash 功能 key K 和 MAC 地址。每个 MPDU 的 IV 都是不同的，当新的 IV 生成时 IV 的值都会增加。

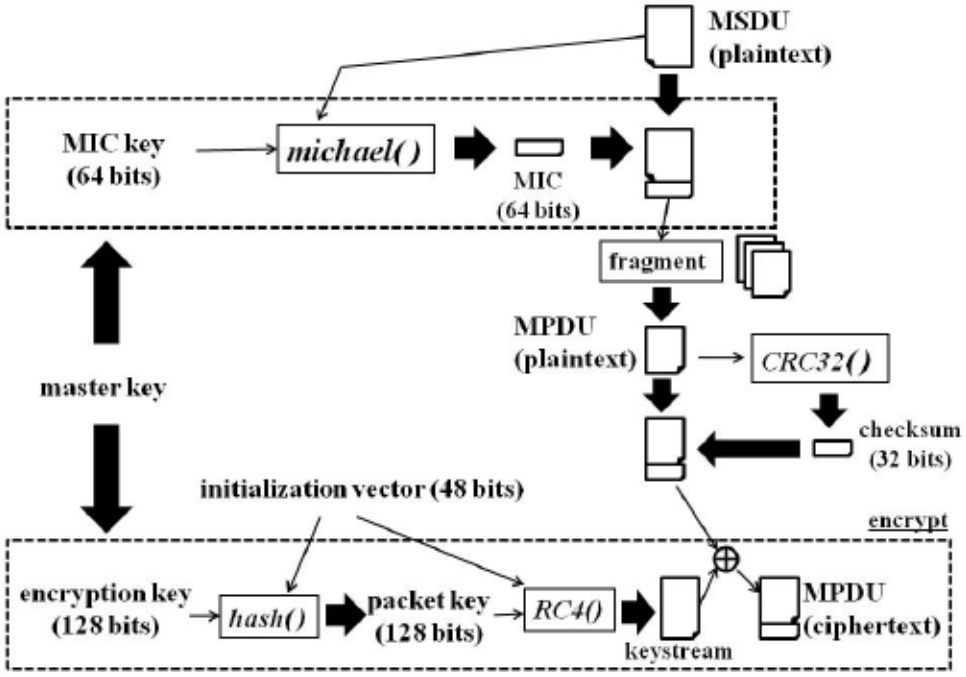

Fig. 1. Processes of sender on WPA

图 1.WPA 中发送器的过程

在 WPA 中，IV 也被称为 TKIP 序列计数器（TSC）。WPA 使用了流密码 RC4 来作为加密算法，RC4 从数据包密钥和 IV 中生成一组伪随机序列（成为密钥流）Z = (Z1;Z2; : : : ;ZL)，其中 Zi 是字节变量，而 L 是纯文本的长度。密钥流是使用纯文本 P = (P1; P2; : : : ; PL)进行 XOR 运算过的以获取密码文本 C = (C1;C2; : : : ;CL)，如下所示：

Ci = Pi _ Zi (i = 1; 2; : : : ;L); (3)

其中 Ci 和 Pi 是字节变量，那么对 WPA 的加密可以写为：

C = (MPDUjjCRC32(MPDU)) _ RC4(PK; IV): (4)

加密的 MPDU 和 IV 将被发送给发送器。

2.2 接收器的过程

接收器接受加密的 MPDU 和 IV，IV 将与 TSC 计数器（与最常接收的加密 MPDU 对应的 IV 的值）进行比较。如果接收器 IV 小于或者等于 TSC 计数器，接收到的加密 MPDU 将被丢弃。在 WPA 的解密过程中，接收器会从接收的 IV 和数据包密钥 PK 中生成密钥流ˆ Z。

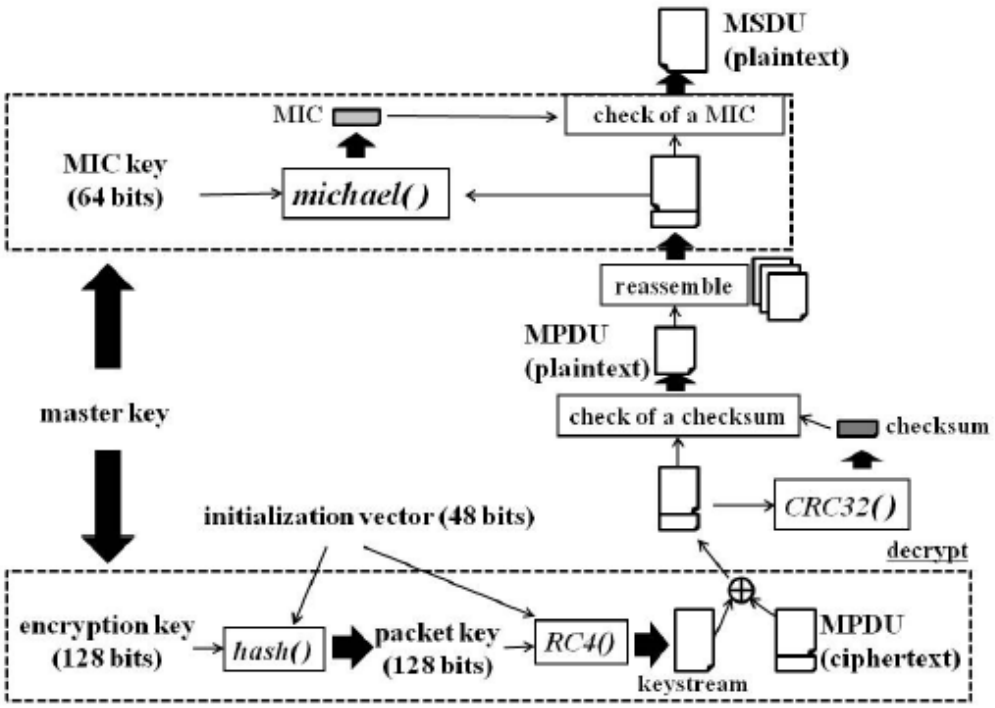

Fig. 2. Processes of receiver on WPA

密钥流ˆ Z 是与发送器 Z 相同的，通过使用ˆ Z = Z 来获取纯文本，如下所示：

Pi = Pi _ Zi _ Zi = Ci _ Zi (i = 1; 2; : : : ;L):

然后，WPA 的解密写法如下：

(MPDUjjCRC32(MPDU)) = C _ RC4(PK; IV):

接收器从接收的 MPDU 中计算出校验和，然后校验和将与接收的校验和进行比较。如果这些校验和不相同，接收的 MPDU 将会被弃用。请注意，接收器并不能够向发送器发送关于校验和错误的信息。

当所有的 MPDU 被获取后，这些将被重新集合到 MSDU 中。接收器从接收的 MSDU 和 MIC 密钥中使用 Micheal 来计算 MIC，然后这个 MIC 与接收的 MIC 进行比较。如果这些 MIC 不相同，所有接收的与 MSDU 相对应的 MPDU 都会被禁用，并且接收器向发送器发送

MIC 的错误信息（MIC 失败报告）。在 WPA 中，如果一分钟内发送给发送器两次以上的 MIC 报错信息的话，MIC 密钥将会被改变。当 MSDU 被接受后，TSC 计算器将会更新到与所有 MPDU 相对应的 IV 的最大值。

3 Beck-Tews 攻击

Beck-Tews 这种攻击方法利用了对 WEP 的 chopchop 攻击对 WPA 进行攻击，这种攻击从加密的小数据包中恢复 MIC 密钥和纯文本，并且伪造其数据包。

3.1 对 WEP 的 Chopchop 攻击

对 WEP 的 chopchop 攻击的目的在于从特定的密码文本中获取纯文本的信息，请注意这种攻击不能获取 WEP 的加密密钥。

WEP 与 WPA 主要有以下不同：

1. IV 的值没有进行检查

2.没有添加 MIC 的过程

3. 发送器向接收器发送关于校验和的错误信息

从之前接受的加密数据包中生成的虚假加密数据包并不会被禁用，因为 IV 的值没有进行检查。对信息的整体性检查只能由校验和来执行，而如果校验和不正确的话，接收器就会向发送器发送校验和的错误信息。

Chopchop 攻击集中在 CRC32 的属性上，P 是附有校验和的 MPDU，而 R 成为 P 的最不重要的字数（LSB），也就是说 R 是校验和的 LSB。另外，P0 是消减 1 字节的 P，即满足 P0jjR = P。P0 极有可能有不正确的校验和。

在 CRC32 中，我们可以修改 P0 的校验和，通过使用 f（R）对 P0 进行 XOR 处理将 P0 的校验和修改为正确，其中 f（）是 1 对 1 的字节排列。如果使用 f（R）对 P0 的校验和进行 XOR，修改的校验和就是错误的，其中 R_是除 R（正确的）字节变量。这意味着正确的 R 可以通过检查已修改的 P0 的校验和的错误信息，从 R 的 256 个候选值中判断出来。假设攻击者想要知道 R，那么攻击者就会为每个 R 的候选值制造修改的 P0，并且将其发送给访问端点或者客户端。如果被猜测的 R 是正确的，那么修改的 P0 校验和的错误信息就不会被发送给攻击者。在最多猜测 256 次（平均 128 次）后，攻击者猜测出 R 的正确值。上述的操作也可以在加密数据包中进行，因为 XOR 操作对纯文本的修改很容易在流加密的加密中执行。

当 chopchop 攻击执行时，攻击者可以从密码文本获取 P 的 LSB，也就是 R。然后，

我们同样可以获取 C0，也就是消减一个字节的 C，并且有正确的校验和。当攻击者为 C0 执行 chopchop 攻击时，将会从较低的 P 获取第二个字节。与刚才有些类似的是，可以通过执行 x 次 chopchop 攻击来获取低价位 x 字节的 P。另外，攻击者可以获取与获取的 P 信息的密码流字节。

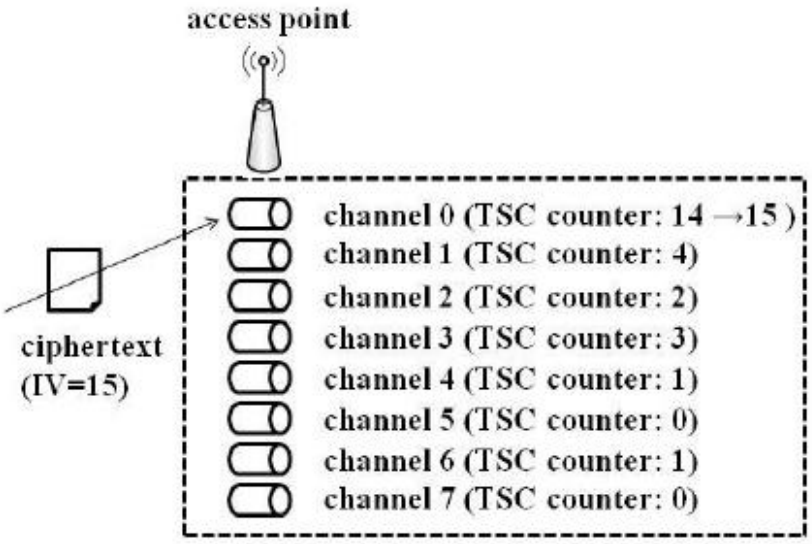

Fig. 3. A WPA implementation that supports IEEE802.11e QoS features

3.2 对 WPA 的 chopchop 攻击

在 WPA 中，从之前接受的加密数据包中生成的虚假加密数据包会被禁用，因为 IV 的值进行了检查。Beck 和 Tews 已经证明了 chopchop 攻击可以在那些支持 IEEE802.11e QoS 功能的 WPA 部署中执行，IEEE802.11e QoS 功能允许每种不同的数据流有 8 个不同的渠道，每种渠道有各自的 TSC 计数器。

假设攻击者获取了渠道 0 并且 IV=15 的加密数据包，那么攻击者不能在渠道 0 执行 chopchop 攻击，因为渠道 0 的 TSC 计数器已经被更新到 15.但是，如果该渠道的 TSC 计数器小于 15，攻击者就可以在其他渠道执行 chopchop 攻击。当 MIC 的错误信息被发送时，所有 MPDU 的校验和都是正确的，因此，对 WPA 的 chopchop 攻击检查了猜测 R 的正确性（通过使用 MIC 错误信息）。

然而，执行这种攻击是很困难的，因为 MPDU 的数量很庞大，于是，Beck 和 Tews 集中在小数据包上（例如 ARP 数据包和 DNS 数据包）。这些数据包不会导致破裂，而 MPDU 是数据包头/数据、MIC 以及校验和的结合。当攻击者执行 chopchop 攻击 x 次后，攻击的执行时间至少是 x-1 分钟，因为如果在一分钟内向发送器发送两次以上 MIC 错误信息的话，

MIC 密钥就会更改。我们把这个事件成为 MIC 错误等待时间。

3.3 攻击情况和执行时间

我们描述一下 Beck-Tews 攻击，Beck-Tews 攻击的目的不仅仅是获取纯文本，而且还要恢复 MIC 密钥并且伪造其数据包。Beck 和 Tews 集中在 ARP 请求/响应来作为攻击目标，他们讨论的攻击方式是，假设 ARP 数据包的字节是固定的或者已知的值，除了源和目的 IP 地址的最后字节。也就是说，ARP 数据包的未知字节数量为 2.我们在本文中将采用相同的假设。首先 Beck-Tews 攻击从加密 ARP 数据包恢复了一个纯文本。纯文本的未知字节数量为 14 字节，也就是包括 ARP 数据包的 2 字节，MIC 的 8 字节以及校验和的 4 字节。

攻击者通过执行 12 次 chopchop 攻击来恢复 MIC 以及校验和，这个过程要求至少 11 分钟的 MIC 错误等待时间。ARP 数据包的未知字节可以在没有 chopchop 攻击的情况下被恢复，而 ARP 数据包的未知字节的候选字节数量是 216，攻击者可以为该 ARP 数据包制造 216 个候选字节。对于 ARP 数据包的每个候选字节，校验和都是使用 MIC 进行计算的。攻击者讲计算出来的校验和与从 chopchop 攻击中恢复的校验和进行比较。如果这些校验和不是相同的，ARP 数据包的候选字节就会移除。通过这个过程，最终 ARP 数据包的候选字节缩减为 1，这样就能从加密 ARP 数据包中恢复所有的纯文本信息。另外，与纯文本想对应的密码流也会被修复。

其次，Beck-Tews 攻击能够伪造加密 ARP 数据包。要伪造数据包，攻击者需要获取 MIX 密钥。由于 Micheal 是一个可逆函数，MIC 密钥可以很容易从 ARP 数据包以及 MIC 中恢复。攻击者制造一个虚假的 ARP 数据包，并使用恢复的 MIC 密钥以及伪造 ARP 数据包来计算 MIC。然后，可以从伪造 ARP 数据包以及 MIC 中计算出校验和。最后，攻击者可以使用 Beck-Tews 攻击恢复的密钥流来制造伪造的加密 ARP 数据包。Beck-Tews 攻击的执行时间为 12-15 分钟，Beck-Tews 攻击的大部分执行时间都是 MIC 错误等待时间。Beck 和 Tews 也实现了在获取 MIC 密钥的情况下进行攻击，然后 MIC 可以使用 MIC 密钥从 ARP 数据包中计算出来。

攻击者只需要执行 4 次 chopchop 攻击就可以恢复校验和，这个过程至少需要 3 分钟的 MIC 错误等待时间。攻击者制造 ARP 的 216 个候选字节，并且可以使用每个候选中的 MIC 密钥来计算 MIC。对于 ARP 数据包的每个候选，校验和都可以使用 MIC 被计算出来。攻击者讲计算出来的校验和与从 chopchop 攻击中恢复的校验和进行比较。与不需要 MIC 密钥的 Beck-Tews 攻击方式类似，纯文本的所有信息都可以从加密 ARP 数据包中恢复，并能制造加密的伪造 ARP 数据包。该攻击的执行时间大约需要 4 分钟。

4 我们的攻击

Beck-Tews 攻击不能够攻击那些不支持 IEEE802.11e QoS 功能的 WPA 部署，现在我们将探讨的是如何对所有类型的 WPA 部署进行实质性的信息伪造攻击。首先，我们将采用 Beck- Tews 攻击来进行中间人攻击以实现攻击任何类型 WPA 部署的目的，然后，我们将研究如何缩短攻击执行时间的方法。

4.1 中间人攻击

在 WPA 上执行 chopchop 攻击的条件是，获取 IV 比使用的 TSC 计数器大的加密数据包。而满足这个条件的环境就是 IEEE802.11e QoS 功能，但是这样就减少了攻击目标的范围。因此，我们采用基于中间人攻击的方法来解决这个问题。在中间人攻击中，攻击者将拦截访问点或者客户端的加密数据包。另外，攻击者会伪造加密数据包，并将其发送给接收器，也就是客户端/访问接入点。该攻击可以获取 IV 比（在截获的数据包还没有到达接收器前使用的）TSC 计数器要大的加密数据包。因此，chopchop 攻击可以通过中间人攻击来执行。

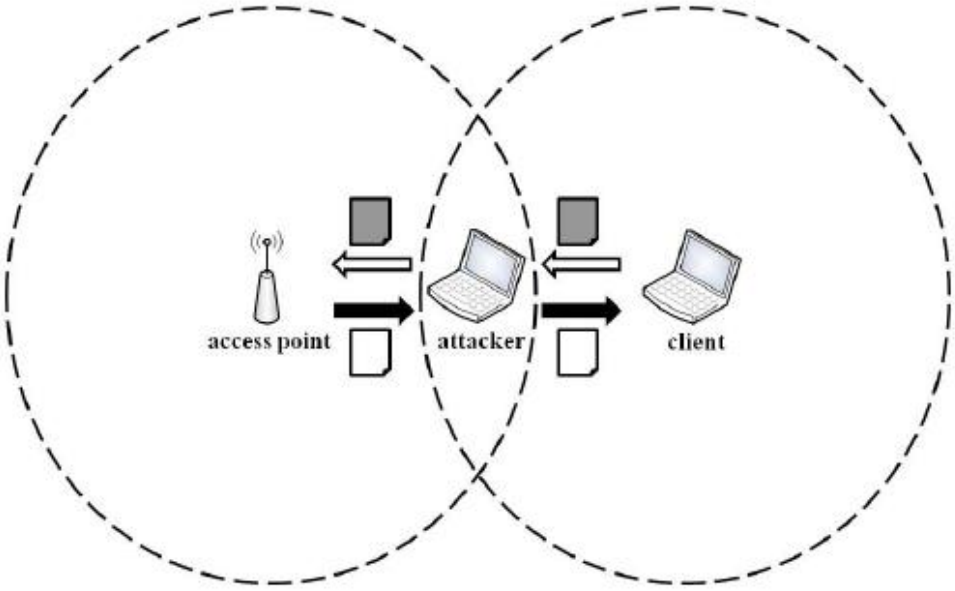

Fig. 4. A model of the man-in-the-middle attack

图四展示的是在无线局域网络中实现 MITM 攻击的方法，由于访问接入点与客户端之间的间隔很大，这两者不能够直接通信。攻击者作为中继器，即所有包含 SSID 的数据包都会在没有修改的情况下重新传递到接收器中，并且访问接入点/客户端的数据包传递给客户

端/访问接入点。如果攻击者想要伪造加密数据包，攻击者需要传递伪造的数据包。这种方法很难被用户发现。我们在图 5 中提供了一种更为有效的 MITM 攻击模式。在这种模式中，攻击者使用定向天线来发送数据包。由于攻击者的数据包不能到达发送器，攻击者不是那么容易能够被发送器察觉。

4.2 策略

在 MITM 攻击中，用户的通信被攻击者截获，直到 chopchop 攻击结束为止。假设攻击者使用加密数据包（IV = x）来执行 chopchop 攻击。如果加密数据包（IV=x+1）被传递给接收器，那么使用加密数据包（IV=x）实施的 chopchop 攻击就会失效，因为 TSC 计数器已经更新至 x+1。为了减少通信停止的影响，我们采用了三种以下的方式进行攻击：

中继器模式（Repeater mode）：攻击者将所有包含 SSID 信标的数据包（未做修改）传递给接收器，并且访问接入点/客户端的数据包传递给客户端/访问接入点。

MIC 密钥恢复模式：这种模式的目的在于获取 MIC 密钥。MIC 和校验和可以通过基于 MITM 攻击的 chopchop 来恢复，并且 MIC 密钥也随之被恢复。这种模式的执行时间大约为 12-15 分钟。

信息伪造模式：这种模式的目的在于使用 MIC 密钥伪造加密数据包。当目标是 ARP 数据包时，这种方法的执行时间为 4 分钟（3.3 提到过），我们将在 4.3 中讨论如何减少这种模式执行时间的方法。当攻击者不能执行 chopchop 攻击，攻击者就会执行中继器模式。在这种模式中，通信的中断并不会发生。当通信中断的影响很小时，MIC 密钥恢复模式就会被执行，例如无线局域网络的大部分数据包都是 ARP 数据包。当重要的数据包（例如交互应用程序的数据包等）通过 MIC 密钥恢复模式的方式被发送，这种模式就会被中断，攻击者就会执行中继器模式。当 MIC 密钥通过 MIC 密钥恢复模式恢复后，信息伪造模式就会执行，来在短时间内伪造加密数据包。

4.3 缩短攻击执行时间

使用这三种攻击模式，攻击造成通信中断的时间最好减少到 4 分钟。在本节中，我们将讨论如何为信息伪造模式的通信中断时间缩短。

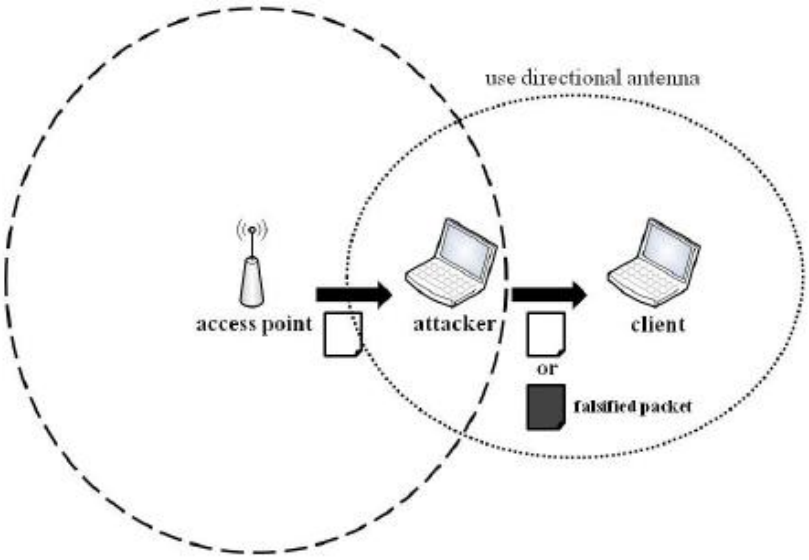

Fig. 5. A model of the man-in-the-middle attack with directional antennas

首先，我们集中在从 MIC 密钥恢复模式恢复的信息上。当 MIC 密钥恢复模式攻击成功后，攻击者可以知道访问接入点的 IP 地址。一般来说，访问接入点的 IP 地址是固定的，那么 ARP 数据包的未知字节缩减为 1 字节。其次，我们将提供缩短 MIC 错误等待时间的执行时间。Beck-Tews 攻击能够恢复所有校验和的 4 字节，并且校验和将会与从 ARP 数据包候选字节中计算出来的校验和进行比较。

比较这些校验和的 4 字节能够有效提高攻击的成功率，但是 MIC 错误等待时间至少需要 3 分钟。因此，我们采用的方法只是对校验和的部分进行比较以缩短 MIC 错误等待时间。在我们的攻击中，我们通过 chopchop 攻击只是恢复了校验和的部分字节。这个过程并不需要 MIC 错误等待时间。

因此，我们的信息伪造攻击模式的执行时间就比 Beck-Tews 攻击的时间少了 3 分钟，也就是说我们的攻击执行时间只需要 1 分钟。

我们还对我们的攻击成功率进行了评估。在我们的信息伪造攻击模式，ARP 数据包的未知字节候选字节数量为 28，而攻击者会做 ARP 数据包的 28 个候选字节。对于 ARP 数据包的每个候选，校验和都能够使用 MIC 计算出来。攻击者会将计算出来的校验和的最后字节与从 chopchop 攻击恢复的校验和的最后字节进行比较，假设 ARP 数据包的候选计算出来的 8 字节 MIC 与 MIC 密钥是统一分布的变量，那么这些校验和的最后字节不相同的可能性就是(28 - 1)/28。当所有的 28 – 1 个不争气的候选都被判断出来，我们的攻击就成功了。

ARP 数据包的 28-1 个不正确的候选字节的所有校验和不相同的可能几率如下：

$$\left(\frac{2^8-1}{2^8}\right)^{2^8-1} \sim 0.369.$$

因此约 37%的加密 ARP 数据包都能够在 1 分钟内通过我们的攻击被恢复。请注意，从我们的攻击中恢复的加密 ARP 数据包是可以区分的。

5 结语

本文提出了一种对所有 WPA 部署进行攻击的实质性信息伪造攻击方法。我们的攻击是将 Beck-Tews 应用到 MITM 攻击中，并且能够伪造加密小数据包（如 ARP 数据包）。

我们提出了 MITM 攻击的策略以及减少攻击执行时间的方法。最终，我们的攻击执行时间最少只需要 1 分钟，并且我们的攻击可以在所有 WPA 部署中实施。接下来的工作将会是对我们的这种攻击进行实验以及对攻击执行时间进行更详细的评估（完）。

注，本话题在 IT 专家网的讨论帖地址：

http://bbs.ctocio.com.cn/viewthread.php?tid=7888523&extra=

2009 年 9 月 2 日星期三

lisj@staff.chinabyte.com