802.11i 认证协议可验安全性形式化分析

宋宇波，胡爱群，姚冰心
（东南大学信息科学与工程学院，南京 210096）

［摘要］ IEEE 802.11 标准组提出了 802.11i 标准以增强无线局域网的安全性能。在 802.11i 标准中采用了 802.1X 标准实现无线局域网用户的认证和接入控制过程。针对 802.1X 认证协议的三方交互结构提出一种扩展 Bellare－Rogaway 模型，对 802.11i 认证和密钥交换机制进行可验安全性分析。通过分析，证明802.11i 认证协议存在缺陷并给出了相应的中间人攻击方法。

［关键词］ 802.11i；Bellare－Rogaway 模型；可验安全性；形式化分析
［中图分类号］ TP393.17 ［文献标识码］ A ［文章编号］ 1009－1742(2010)01－0067－07

1 前言

由于无线环境的开放性，无线局域网与有线互联网相比更容易受到安全威胁。802.11[1]标准的制定者将标准中的安全机制称为有线同等保密（wired equivalent privacy，WEP）协议。但研究表明，WEP 标准并没有实现预期的安全[2~5]。IEEE 组织于 2004 年 6 月提出安全增强标准 802.11i[6]以增强无线局域网安全性能。该标准采用 IEEE 802.1X[7]基于端口的接入控制协议，实现了申请者（Supplicant）、认证者（Authenticator）和认证服务器（authenticate server，AS）的接入控制模式。新标准的提出增强了无线局域网的安全性能，但如何对 802.1X 协议进行可验安全分析是笔者等最关心的问题。

对安全协议的可验分析都是基于计算复杂度理论进行的，采用多项式归约技术对安全协议的安全性进行有效的转换，将对密码体制的任何有效攻击归约到解一类已知 NP 问题的一个实例。近年来，这种分析方式被广泛接受，成为分析和设计安全机制的一种重要手段。

GoldWasser 和 Micali 最先提出加密机制安全性的形式化分析的概念[8]。他们提出了："语义安全"（semantic security）和"多项式安全"（polynomial security）两个概念，并证明在多项式时间归约情况下这两种安全性是等价的。Micali，Rackoff 和 Sloan[9]证明了这两种安全性同样可以和 Yao[10]提出的其他概念的安全性等价。在此基础上，Goldreich[11]和 Luby[12]分别提出了非对称加密算法以及对称加密算法的一致计算复杂度理论。上述文献的工作表明在多项式时间归约的情况下，不同概念的安全机制安全性是可以等价的，如果存在某个在多项式时间归约下的难解的问题，我们可以宣称基于该问题的安全机制是可验证安全。Bellare 和 Rogaway 最先使用计算模型方法证明认证和认证的密钥交换机制的安全性[13~16]。在他们具有开创性的研究中，模型化了对认证和认证的密钥交换协议的攻击，设计了几个简单的认证和密钥交换协议，并证明了这些协议是正确的。他们的证明把对协议的所谓成功攻击转化为伪随机性的失败，即可以用一个多项式时间的分辨器将伪随机函数的输出同真随机函数的输出分辨开来。但 Bellare－Rogaway 模型只适用于双方认证协议，在无线局域网环境下，针对 802.1X 认证协议的三方交互结构，提出了扩展的 Bellare－Rogoway 模型，并利用该模型进行了可验安全性分析，以便验

［收稿日期］ 2007－12－22；修回日期 2008－02－20
［基金项目］ 国家 242 信息安全计划（2007A04）；江苏省自然科学基金资助项目（BK2006108）
［作者简介］ 宋宇波（1977－），男，江苏无锡市人，东南大学信息科学与工程学院副教授，研究方向为无线网络和信息安全；E-mail：songyubo@seu.edu.cn

证 802.1X 协议是否能够提供足够的安全性。

2 扩展 Bellare – Rogaway 模型

在计算模型下安全性的形式化证明包括以下 3 步：

1）形式模型化协议参与者和攻击者行为：该模型化通常是以攻击者和攻击目标之间进行攻击游戏的形式给出的。

2）安全性目标的形式化定义：这里定义攻击者在攻击游戏中的成功，通常以（不可忽略的）概率和（可承受的）时间复杂度公式的形式给出。

3）形式化证明一个多项式时间的归约，把对给定目标的所谓攻击归约到计算复杂性理论中的一个认为不可能解决的难题；该归约的形式化证明是数学上证明一个定理成立。

在公共无线局域网环境下，假设所有的通信都在攻击者的控制下。攻击者除了可以访问通信双方交互的信息外，还可以向通信者发送自己的信息、篡改或重发通信者的信息，攻击者可以在任意时刻发起认证和密钥交换。公共无线局域网环境下的通信者将被形式模型化为攻击者可以使用的一个无限集合预言机。这些预言机之间不能交互，只能和攻击者相交互。一般情况下，攻击者可以利用重发攻击破坏认证和密钥交换协议，但是这种行为并不会构成一次破坏性的攻击。这里考虑的认证协议安全性定义如下：当且仅当攻击者只能通过重放通信者的消息才能完成认证过程的时候，认为该认证协议是安全的[14]。密钥交换过程除了考虑上述情况以外，还需要考虑协议的鲁棒性，当攻击者掌握其中的一个会话密钥时，并不影响其他会话密钥的安全性。在这里，将这个安全要求模型化为允许攻击者在需要的时候可以获得会话密钥，一旦攻击者获得该会话密钥时，该会话密钥将不在“新鲜”（fresh），通信者手里的密钥也将宣布为不新鲜。新鲜的密钥必须确保是受到保护的。笔者将把攻击者获得有用信息的能力形式模型归约化为对概率加密的安全形式化上。

2.1 认证参与者的的形式化

三方认证协议包含一个用户集 I_c、一个认证者集 I_a 以及认证服务器集 I_s。I_c，I_a 和 I_s 中都是可参与协议执行的用户、认证者或认证服务器的符号。每个用户、接入点或服务器都是某个安全参数 k 的多项式函数。攻击者不属于这三个集合。

形式上，三方认证议可以由一个四元组 $P=(\Pi,\Phi,\Psi,LL)$ 描述。Π 定义了一个诚实用户的行为；Φ 定义了一个诚实的认证者的行为；Ψ 定义诚实的认证服务器的操作；LL 为认证服务器分发给用户和无线接入点的初始会话密钥。

Π 函数定义为：$(m,\delta,\alpha)=\Pi(1^k,i,j,SK_i,PK_i,PK_s,conv,r)$

Φ 函数的定义为：$(m_i,m_s)=\Phi(1^k,i,j,K_j,conv,r)$

Ψ 函数定义为：$(m,\delta,\alpha)=\Psi(1^k,i,j,SK_s,PK_s,PK_i,K_j,conv,r)$

其中输入参数 1^k 为安全参数；i 和 j 分别表示用户和认证者的身份标识；SK_i 和 PK_i 为 i 的私钥和公钥，若用户使用对称密钥，则 $PK_i=\phi$；PK_s 为认证服务器的公钥；$conv$ 为当前对话比特流，随着协议的运行新的会话级联在它的后面；r 为一随机输入；K_j 为认证者和认证服务器间共享的密钥。

输出函数 m 为下一步要发送的消息；$\delta\in\{Accept,Reject,No-decision\}$ 为用户作的判决；α 为用户交互得到的秘密信息。m_i 和 m_s 分别为发送给用户 i 和认证服务器 s 的消息。

假设攻击者拥有黑盒形式预言机 $\Pi^s_{i,j}$，$\Phi^s_{i,s}$ 以及 $\Psi^s_{j,s}$，攻击者可以通过向这些预言机输入预定的质询并从预言机那里获得应答。在 Dolev – Yao 的威胁模型下，所有的通信都在攻击者的控制中，他指定预言机何时开始，并且获得所有的传输；攻击者可以从中选择自己所需要的传输，从而发送给其他的预言机。当攻击者通过预言机的应答可以获知他发送的质询是否被接受或者被拒绝。如果预言机 $\Pi^s_{i,j}$ 接受了攻击者的质询，它将生成一个私有会话密钥 $\sigma^s_{i,j}$，攻击者可以获得该密钥。这里主要考虑会话密钥一旦被攻击者获得的情况下，该安全协议是否还能保证以后会话密钥的安全。一个更加严重的情况是攻击者获得了协议参与者的最终状态，这种情况多半发生在攻击者本身就是协议交互的参与者。在这种情况下，攻击者可以获得参与者的内部状态，并且用自己的密钥替代参与者拥有的密钥。如果认证协议足够安全的话，即使攻击者为参与者之一，其他参与者的密钥将不会被泄漏。

2.2 认证协议安全目标的形式化

定义 1（良性攻击（benign adversery））：良性攻击用来描述一个可靠的网络，即这个网络是良性定义的（在一次协议运行结束时，两个通信的预言机

拥有完全相同的会话密钥)。而对于每一个 $(i,j,s,t) \in I_c \times I_s \times N \times N$,存在一个确定的攻击者,在协议的每次运行时,能忠实得在 Π_{ij}^{s} , Φ_{ji}^{t} , Φ_{js}^{u} 以及 Ψ_{sj}^{v} 之间传送消息。

定义 2 (匹配的会话):固定奇数 $R = 2\rho - 1$,令 P 是一个 R 轮消息的协议。在攻击者存在的情况下执行 P。考虑预言机 Π_{ij}^{s} , Φ_{ji}^{t} , Φ_{js}^{u} 以及 Ψ_{sj}^{v} ,会话序列分别用 C1, $C1'$,C2 和 $C2'$ 表示。

1) 如果存在 $\tau_0 < \tau_1 < \cdots < \tau_{R-1}$ 和 $\alpha_1,\beta_1,\alpha_2,\beta_2,\cdots\beta_{\rho-1},\alpha_\rho$,使得 C1 的前缀是 $(\tau_0,\lambda,\alpha_1),(\tau_2,\beta_1,\alpha_1),\cdots,(\tau_{2\rho-2},\beta_{\rho-1},\alpha_\rho)$, $C1'$ 的前缀是 $(\tau_1,\alpha_1,\beta_1),(\tau_3,\alpha_2,\beta_2),\cdots,(\tau_{2\rho-3},\alpha_{\rho-1},\beta_{\rho-1})$,则 $C1'$ 被称为是 C1 的匹配会话。

2) 如果存在 $\tau_0 < \tau_1 < \cdots < \tau_{R-1}$ 和 $\alpha_1,\beta_1,\alpha_2,\beta_2,\cdots\beta_{\rho-1},\alpha_\rho$,使得 $C1'$ 的前缀是 $(\tau_1,\alpha_1,\beta_1),(\tau_3,\alpha_2,\beta_2),\cdots,(\tau_{2\rho-3},\alpha_{\rho-1},\beta_{\rho-1}),(\tau_{2\rho-1},\alpha_\rho,*)$。C1 的前缀 $(\tau_0,\lambda,\alpha_1),(\tau_2,\beta_1,\alpha_1),\cdots,(\tau_{2\rho-2},\beta_{\rho-1},\alpha_\rho)$,则 C1 被称为是 $C1'$ 的匹配会话。

3) 如果存在 $\tau_0 < \tau_1 < \cdots < \tau_{R-1}$ 和 $\gamma_1,\delta_1,\gamma_2,\delta_2,\cdots\delta_{\rho-1},\gamma_\rho$,使得 C2 的前缀是 $(\tau_0,\lambda,\gamma_1),(\tau_2,\delta_1,\gamma_1),\cdots,(\tau_{2\rho-2},\delta_{\rho-1},\gamma_\rho)$, $C2'$ 的前缀是 $(\tau_1,\gamma_1,\delta_1),(\tau_3,\gamma_2,\delta_2),\cdots,(\tau_{2\rho-3},\gamma_{\rho-1},\delta_{\rho-1})$, , 则 $C2'$ 被称为是 C2 的匹配会话。

4) 如果存在 $\tau_0 < \tau_1 < \cdots < \tau_{R-1}$ 和 $\gamma_1,\delta_1,\gamma_2,\delta_2,\cdots\delta_{\rho-1},\gamma_\rho$,使得 $C2'$ 的前缀是 $(\tau_1,\gamma_1,\delta_1),(\tau_3,\gamma_2,\delta_2),\cdots,(\tau_{2\rho-3},\gamma_{\rho-1},\delta_{\rho-1}),(\tau_{2\rho-1},\gamma_\rho,*)$。C2 的前缀是 $(\tau_0,\lambda,\gamma_1),(\tau_2,\delta_1,\gamma_1),\cdots,(\tau_{2\rho-2},\delta_{\rho-1},\gamma_\rho)$,则 C2 被称为是 $C2'$ 的匹配会话。

如果 C1 是 $C1'$ 的匹配对话, $C1'$ 也是 C1 的匹配会话;C2 是 $C2'$ 的匹配对话, $C2'$ 也是 C2 的匹配会话,就称预言机 Π_{ij}^{s} , Φ_{ji}^{t} , Φ_{js}^{u} 以及 Ψ_{sj}^{v} 之间有匹配的会话。

定义 3 (不匹配会话):当一个协议 P 在攻击者的控制下执行时,如果存在一个没有变坏的预言机呈接受状态,但没有一个与它有匹配会话的预言机存在的时候,称这样的会话是不匹配的。

由此笔者等给出增强 Bellare – Rogaway 模型下三方认证协议的安全定义。

定义 4:如果满足下列要求,则认为协议 $P = (\Pi,\Phi,\Psi,LL)$ 是安全的,

1) 良定义的协议:在一个良性攻击存在的情况下,预言机 Π_{ij}^{s} , Φ_{ji}^{t} , Φ_{js}^{u} 以及 Ψ_{sj}^{v} 在协议结束时都处于接受状态,且拥有同样的会话密钥。

2) 对任意的攻击者,如果两个没有变坏的预言机有匹配的会话,那么他们都应处于接受状态,且拥有相同的会话密钥。

3) 对消息的认证,不匹配会话的概率是可忽略的。

4) 会话密钥的破解概率是可忽略的。模型中所有实体间的相互通信都受攻击者的控制。攻击者可以读、插入、修改、删除、延迟和重放任何消息,也可以在任何时候重新发起任何参与者的新会话。而且这个模型也模拟了攻击者发起重定向攻击、篡改攻击和劫持攻击的可能。

3 802.1X 协议的可验安全分析

802.1X 协议使用 EAP 认证标准,EAP 本身并没有定义具体的认证方法协议,它利用上层的认证交互进行身份认证。不失一般性,就最常用的 EAP – TLS 协议进行可验证安全性分析。

在 EAP – TLS 协议中,假设客户与服务器之间常用的密钥交换方法为 DH 密钥交换。认证服务器 AS 拥有一对密钥 (PK_{AS},SK_{AS}) ,其中 PK_{AS} 是认证服务器的公钥, SK_{AS} 是认证服务器的私钥。无线接入点 AP 和认证服务器之间共享一个长期的密钥 K,他们两者之间的通信都由该密钥保护,记 E_{K_x} 。每个用户拥有一对长期的秘密 α。秘密的可信度由证书权威机构颁发的证书证明,证书权威机构把 g^{α} 作为用户的公钥进行签名,则用户端证书和服务器证书分别为: $Cert(S) = < ID_S,g,p,q,g^{\alpha},\{ID_S,g,p,q,g^{a}\}_{sig_{CA}} >$, $Cert(AS) = < ID_{AS},PK_{AS},\{ID_{AS},PK_{AS}\}_{sig_{CA}} >$ 。

形式化后的 EAP – TLS 协议如图 1 所示。

定理 1:假设 TLS 协议中使用的公钥加密方案、数字签名方案以及抗冲突的单向散列函数是可验证安全的,则 TLS 协议也是具备可验证安全性的。

要证明定理 1,只需要证明它满足定义 4 的每个条件就足够了。这里笔者等只考虑 DH 密钥交换问题。

1)按照定义 1 中良定义协议的概念,在 Φ_{js}^{u} 和 Ψ_{sj}^{v} 之间,存在一个良性攻击。那么攻击者只是忠实的转发线路上的各种信息,而不会对线路中的信息进行破坏。根据 TLS 协议的描述,在通信结束的时候, Φ_{js}^{u} 和 Ψ_{sj}^{v} 能够获得同样的会话密钥,并且预言机都处于接受状态,所以 TLS 是一个良定义的

协议。

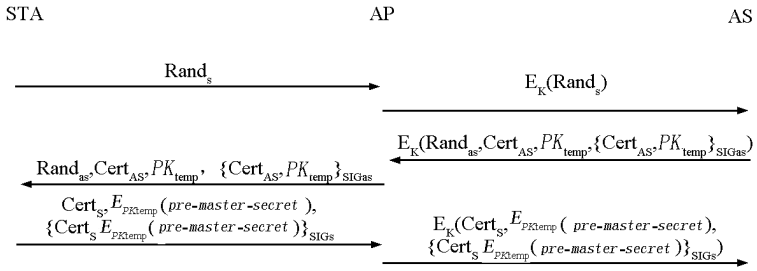

图 1　EAP – TLS 协议交互

Fig. 1　The interaction of EAP – TLS protocol

2)由 Π_{ij}^{s}，Φ_{ji}^{t}，Φ_{js}^{u} 以及 Ψ_{sj}^{v} 为没有变坏的预言机,他们具有匹配的会话。按照协议的描述,会话的发起者 Π_{ij}^{s} 在传送第一个消息给 Φ_{ji}^{t} 后,预言机 Φ_{ji}^{t} 能根据这些计算算出给 Φ_{js}^{u} 的内部输出，Φ_{js}^{u} 根据预言机 Φ_{js}^{u} 的内部输出计算出要发送给 Ψ_{sj}^{v} 的输出，Ψ_{sj}^{v} 预言机收到 Φ_{js}^{u} 的消息后计算出要返回给 Φ_{js}^{u} 的输出，Φ_{js}^{u} 根据返回消息计算出给 Φ_{ji}^{t} 的内部输出，Φ_{ji}^{t} 预言机根据 Φ_{js}^{u} 内部输出得到返回给预言机 Π_{ij}^{s} 的输出。预言机 Π_{ij}^{s} 能根据返回的消息判断协议处于的状态,并发送相应的值。如果 Π_{ij}^{s}，Φ_{ji}^{t}，Φ_{js}^{u} 以及 Ψ_{sj}^{v} 忠实地执行协议,那么最后一定可以正常终止,并且拥有相同的会话密钥。

这表明,在可靠的无线网络环境中,如果协议参与者忠实地执行协议,那么 TLS 协议是正确的。下面证明协议具有可相互认证的性质。

引理 1：TLS 协议能够认证发送者的身份,即它是一个可相互认证的协议。

证明:引理 1 的证明将分两个部分进行,先证明服务器向用户提供了正确的身份认证,然后再证明用户页向服务器提供认证。802.1X 本身并不提供无线接入点和用户之间的相互认证,这两者的认证过程在四步握手交换协议中完成。

命题 1：如果存在安全的数字签名方案,那么认证服务器可以向客户端提供认证。

证明:令攻击者的一次试验为 E。这里使用反证法,假设不匹配会话的概率是不可忽略的。,如果 E 攻击使得一个没有变坏的预言机 Π_{ij}^{s} 呈接受状态,而没有一个 Φ_{ji}^{t} 与它有匹配的会话。这种情况称为 E 成功攻击了 Π_{ij}^{s}。令 E 成功攻击的概率为 $Pr_{E_{success}}$,根据假设 $Pr_{E_{success}} = n(k)$,其中 $n(k)$ 是一个不可忽略的函数。

从 E 构造数字签名方案的模仿者 F，使得其成功的概率是不可忽略的。首先,F 为算法 G 和 Sig 抛硬币。然后，利用算法 G 为 F 构造签名用的密钥对 (PK_{temp}, SK_{temp})。最后用 PK_{temp} 作为输入调用伪造者 F。现在,F 开始调用 E,从 I_s 中选择实体 $j \in I_s$，并进行猜测;对于某个特定的 j 和 s,E 能成功攻击 Π_{ij}^{s}。F 再抛硬币,并用 G 为除 j 外所有的实体构造密钥对;将自己的输入 PK_{temp} 作为 j 的公钥。此时 F 已获得 E 要运行的全部输入,开始调用 E。F 利用签名预言机 Sig 帮助实体 j 回答对它的查询,以完成协议中要求的对 E 的所有查询。

假设 E 成功攻击了预言机 Π_{ij}^{s},那么在某时刻 τ_0,E 用 λ(空信息)查询了 Φ_{ji}^{t},故当 $\tau_1 > \tau_0$，Π_{ij}^{s} 必然会收到某个 PK_{temp} 的签名。如果这个信息的数字签名以前没有被查询过,那么 F 可把它作为这次试验的输出。如果这个信息 F 以前代表 j 签过,则意味着 PK_{temp} 以前已经被查询过。如果产生信息的时刻 $\tau_1 < \tau_0$,那么 F 放弃,即不是这个攻击的有效预言机查询。同时,信息也不能在 $\tau_1 > \tau_0$ 时刻产生,因为按照假设，Π_{ij}^{s} 和 Φ_{ji}^{t} 之间没有匹配的会话。若 E 没有成功攻击 Π_{ij}^{s} 的时候,则 F 放弃。

于是 F 利用 E 成功赢得自己的试验的概率至少是 $n(k)/q(1-\lambda(k))$,其中 $\lambda(k) = \Pr(\tau_0 < \tau_1)$ 是可忽略函数,这显然与数字签名是安全的假设矛盾。所以 $n(k)$ 是可忽略的,即 E 攻击 Π_{ij}^{s} 成功的概率不大。

命题 2：假设存在一个 E 可以在不破坏认证服务器向客户端提供认证的前提下,在时间 t 和 q 次预言机查询后,能以概率 π 违背客户端向认证服务器提供认证,那么 DH 问题可以在大致相同的时间内解决,且成功的概率为：$\pi' \geqslant \pi - (\frac{q}{2^l} + \frac{q}{q'})$。

证明:如果用 $NoAuth_{CS}$ 表示在攻击者存在的情

况下存在一个认证服务器实例 Ψ_{sj}^{v}，在协议执行的最后，它处于接受状态而没有和它有匹配的会话的用户实例 Π_{ij}^{s} 存在。那么这个事件定义了破坏用户向认证服务器提供认证的情况。同样也可以用 $NoAuth_{CS}$ 表示破坏认证服务器向用户提供认证的情况，即在攻击者存在的情况下，存在一个用户实例 Π_{ij}^{s}，在协议执行的最后处于接受状态，而没有一个和它有匹配的会话的服务器实例 Ψ_{sj}^{v} 存在。

服务器发送了 PK_{temp} 和 $(PK_{\text{temp}})_{sig_{AS}}$ 之后接收到 $\alpha = E_{PK_{\text{temp}}}(pre\_master\_secret)$，如果这时认证服务器验证接受，但这个 α 实际上不是客户发送的，那么这个信息可能是攻击者自己猜测出来的。假设共进行了 q' 次预言机查询，且 $E_{PK_{\text{temp}}}$ 的输出长度为 l_1，那么攻击者猜测正确的概率不超过 $\frac{q}{2^{l_1}}$。

或者 PK_{temp} 是以前某个预言机查询时已经问过的。假设以前一共查询了 q' 次，现在一共查询了 q 次，那么 PK_{temp} 被问过的概率不超过 $\frac{q}{q'}$。

或者攻击者能计算出 PK_{temp}，并由此计算 $E_{PK_{\text{temp}}}(pre\_master\_secret)$ 产生正确的回答。令攻击者能产生 $E_{PK_{\text{temp}}}(pre\_master\_secret)$ 的事件为Event，那么：

$$\Pr(NoAuth_{CS} \mapsto NoAuth_{SC}) \leqslant \Pr\{Event + \frac{q}{2^{l}} + \frac{q}{q'}\}$$

由此，命题得证。

根据上述推断，定理 1 成立。

下面进一步考虑 EAP－TLS 协议，首先考虑 EAP－TLS 协议是否是良定义的。按照定义 1 中良定义协议的概念，在 Φ_{js}^{u} 以及 Ψ_{sj}^{v} 之间，如果存在一个良性攻击。那么攻击者只是忠实的转发线路上的各种信息，而不会对线路中的信息进行破坏，但攻击者可以选择任意顺序和任意次数发送信息。根据 EAP－TLS 协议的描述，如果无线接入点和客户端都和一个良性攻击者相连，那么由 $\tau_0 < \tau_1 < \tau_3 < \tau_4 < \tau_5$，当客户端会接受下面的对话：

$$\begin{aligned} conv_{STA} = {} & (\tau_0, "", \text{Rand}_S), (\tau_2, \text{Rand}_{AS} \,||\, Cert_{AS} \,||\, PK_{\text{temp}} \,||\, \{Cert_{AS} \,||\, PK_{\text{temp}}\}_{sig_{AS}}, \\ & Cert_S \,||\, E_{PK_{\text{temp}}}(pre\_master\_secret) \,||\, \{Cert_S \,||\, E_{PK_{\text{temp}}}(pre\_master\_secret)\}_{sig_S}), (\tau_4, EAP - success, "") \end{aligned} \quad (1)$$

而无线接入点会接受下面的对话：

$$\begin{aligned} conv_{AP} = {} & (\tau_1, \text{Rand}_S, \text{Rand}_{AS} \,||\, Cert_{AS} \,||\, PK_{\text{temp}} \,||\, \{Cert_{AS} \,||\, PK_{\text{temp}}\}_{sig_{AS}}), \\ & (\tau_3, Cert_S \,||\, E_{PK_{\text{temp}}}(pre\_master\_secret) \,||\, \{Cert_S \,||\, E_{PK_{\text{temp}}}(pre\_master\_secret)\}_{sig_S}), \\ & EAP - success) \end{aligned} \quad (2)$$

显然根据定义 1，$conv_{STA}$ 和 $conv_{AP}$ 并不是两个匹配对话。并且笔者发现当无线接入点接受对话(2)时，客户端还会接受下面的对话：

$$\begin{aligned} conv_{STA} = {} & (\tau_0, "", \text{Rand}_S), (\tau_2, \text{Rand}_{AS} \,||\, Cert_{AS} \,||\, PK_{\text{temp}} \,||\, \{Cert_{AS} \,||\, PK_{\text{temp}}\}_{sig_{AS}}, \\ & Cert_S \,||\, E_{PK_{\text{temp}}}(pre\_master\_secret) \,||\, \{Cert_S \,||\, E_{PK_{\text{temp}}}(pre\_master\_secret)\}_{sig_S}), (\tau_4, EAP - success, ""), \\ & (\tau_5, Disassociate, "") \end{aligned} \quad (3)$$

显然会话(2)和(3)也不是匹配对话。因此 EAP－TLS 不是一个良定义的认证协议，同样，它也不可能具备可验安全性。综上所述，笔者有如下推断。

推断：即使 TLS 协议中使用的公钥加密方案、数字签名方案以及抗冲突的单向散列函数是可验证安全的，EAP－TLS 协议不具备可验证安全性。

4 中间人攻击

根据以上关于 EAP－TLS 可验安全性分析可以推得一个中间人攻击。该攻击如下：攻击者在无线接入点和客户端间进行 802.1X 协议认证时，当无线接入点向客户端发送 EAP－Response 帧后，无线接入点和客户端都处于认证成功状态。此时攻击者冒充无线接入点向客户端发送 Disassociate 帧，由于该帧没有任何的安全措施，攻击者很容易伪造，而同时客户端处于认证成功状态，会接受该帧而断开连接。此时攻击者即可以冒充用户获得无线网络的访问。

由于攻击者发送的是 802.11 协议帧，跟 TLS 协议本身并没有关联。因此，上述的中间人攻击适用于 EAP 认证的各个认证机制。即它是 802.11i 协议中的 802.1X 本身的一个漏洞，而跟采用什么认证机制无关。802.11i 协议中的 802.1X 之所以存在这样的漏洞，跟它的协议设计有关。无线接入点和客户端的状态机并不是对称的，根据 802.11i 标准，无线接入点的控制端口只有在认证成功后打开。但对于客户端来说却不是这样。客户端的端口始终处于打开状态。这种单向的认证方式导致了中间人攻击发生的可能性。攻击者很容易找到机会冒充无线

接入点向客户端发送伪造的信息。

如何解决这个攻击,最好的方法是修改无线接入点和客户端的认证状态机,提供无线接入点和客户端的双向认证。但这无疑要修改协议栈本身,对于公共无线局域网环境来说,修改通信协议将会影响不同厂商设备间的互通,虽然从安全性的角度考虑这是最好的解决方法,但从应用的角度考虑这并不现实。

现重新考虑 EAP – TLS 协议的分析,笔者发现引理 1 结论对于 EAP – TLS 协议来说仍然适用。也就是说攻击者获得会话密钥的概率是可忽略的。如果在 802.1X 协议里笔者做如下强制限制:即在认证过程结束后,客户端和无线接入点之间只接受 4 步握手密钥交换协议的帧,其他的 802.11 帧都将拒绝。4 步握手交换协议结束后,随后传送的任何 802.11 帧都必须受使用密钥交换协议生成的会话密钥保护,以确保 802.11 帧的安全性和可靠性,则可以消除上述的中间人攻击。

5 结语

笔者针对 802.1X 认证协议的三方交互结构提出一种扩展 Bellare – Rogaway 模型,对 802.11i 认证和密钥交换机制进行可验安全性分析。通过分析,证明 802.11i 认证协议存在缺陷,攻击者可以利用中间人攻击方法达到冒充用户获得无线网络的访问。

参考文献

[1] IEEE 802.11. 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[S]. America, ISO/IEC, 1999,17 – 21

[2] Nikita Borisov, Ian Goldberg, David Wagner. Intercepting mobile communications: the insecurity of 802.11[A]. MobiCom'01: Proceedings of the 7th Annual International Conference on Mobile Computing and Networking[C]. New York: ACM Press,2001:180 – 189

[3] Arbaugh W A, Shankar N, Wan Y J. Your 802.11 wireless network has no clothes[EB/OL]. http://www.cs.umd.edu/~waa/wireless.pdf,2001,3

[4] Arbaugh W A. An inductive chosen plaintext attack against WEP/WEP2[N]. IEEE Document 802.11 – 01/230,2001,5

[5] Walker J R. Unsafe at any key size; an analysis of the WEP encapsulation[N]. IEEE Document 802.11 – 00/362,2000,10

[6] IEEE802.11i. 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: Medium Access Control (MAC) Security Enhancements[S]. America, ISO/IEC, 2004:1 – 341

[7] IEEE802.1x. IEEE Standard for Local and Metropolitan Area Networks – Port – Based Network Access Control[S]. America, ISO/IEC, 2001,1 – 167

[8] GoldWasser S, Micali S. Probabilistic encryption[J]. Journal Computer and System Sciences,1984,4(28):270 – 299

[9] Micali S, Rackoff C, Sloan R. The notion of security for probabilistic cryptosystems[J]. SIAMJ. of Computing, 1988,4:412 – 426

[10] Yao A C. Theory and applications of trapdoor functions[A]. In Proceedings of the 23rd Symposium on Foundations of Computer Science[C]. IEEE, 1982

[11] Goldreich O. A uniform complexity treatment of encryption and zero – knowledge[J]. Journal of Cryptology, 2003,6:21 – 53

[12] Luby M. Pseudorandomness and Cryptiographic Applications[M]. New York: Princeton University Press, 2006

[13] Bellare M, Rogaway P. Entity authentication and key distribution[A]. In Cryptology – Crypto 03 Proceedings[C]. Lecture Notes in Computer Science, 2004:232 – 249

[14] Bellare M, Rogaway P. Provably secure session key distribution: the three party case[A]. Proc. 27th Annual Symposium on the Theory of Computing[C]. ACM, 2005:57 – 66

[15] Bellare M, Canetti R, Krawczyk H. A modular approach to the design and analysis of authentication and key exchange protocols[A]. Proc. 30th Annual Symposium on the Theory of Computing[C]. ACM, 1998: 419 – 428

[16] Bellare M, Pointcheval D, Rogaway P. Authenticated key exchange secure against dictionary attacks[A]. Cryptology – Eurocrypt 2000 Proceedings[C]. Lecture Notes in Computer Science, 2000:135 – 155

The provable security formal analysis of 802.11i authentication scheme

Song Yubo, Hu Aiqun, Yao Bingxin
(Research Center of Information Security, Southeast University, Nanjing 210096, China)

[**Abstract**] 802.11i standard is proposed by IEEE 802.11 Standard Group to improve the security of the WLAN. In 802.11i, 802.1x standard is used for the authentication and access controll. How to analyze the security of the new protocol to prove its validity is the most interesting problem we are concerned. In order to solve this problem, an expanded Bellare-Rogaway model is established to give a provable security formal analysis on this protocol. By utilizing the expanded Bellare-Rogaway model, a flaw has been found in 802.1X authentication protocols and the corresponding man-in-the-middle attack is given here.

[**Key words**] 802.11i; Bellare-Rogaway model; provable security; formal analysis