第32卷 第23期 计 算 机 工 程 2006年12月
Vol.32 No.23 Computer Engineering December 2006
·安全技术· 文章编号：1000—3428(2006)23—0135—02 文献标识码：A 中图分类号：TP309

一种新的无线局域网认证机制

张浩军[1,2]，祝跃飞[1]
(1. 信息工程大学网络工程系，郑州 450002；2. 河南工业大学计算机工程系，郑州 450052)

摘 要：分析了无线局域网的安全标准 IEEE 802.11i 和 WAPI 在安全与效率上存在的缺陷。提出了一种基于哈希链构造认证令牌，实现无线网络快速实体认证机制 FWAI。与 802.11i 和 WAPI 比较，新机制使用较少的交互，无需数字签名，实现在“第一时间”对实体 STA 的认证，并高效产生会话密钥。新机制不仅能有效防范 STA、AP、ASU 的假冒、消息重放等攻击，还具有很强的抗击拒绝服务攻击的能力。
关键词：无线局域网；WAPI 802.11i；认证；FWAI

Novel Authentication Scheme for WLAN

ZHANG Haojun [1,2], ZHU Yuefei [1]
(1. Department of Network Engineering, Information Engineering University, Zhengzhou 450002;
2. Department of Computer Engineering, Henan University of Technology, Zhengzhou 450052)

【Abstract】 Several shortcomings of two security standards in WLAN: IEEE 802.11i and WAPI are analyzed on efficiency and security. A fast/efficient authentication scheme for WLAN (FWAI) is proposed, which is based on tokens derived from Hash chains. Compared with 802.11i and WAPI, the proposed scheme needs fewer messages to authenticate STA in the foremost time, as well as session keys are negotiated efficiently. The scheme canot only against personating STA, AP and AS and messages replay attacks, but also can against DoS attacks effectively.
【Key words】 WLAN; WAPI 802.11i; Authentication; FWAI

1 概述

无线局域网(WLAN)固有的开放性，存在以下安全弱点：无线通信信息易被窃听、截获、篡改，非授权用户非法使用网络资源，网络更容易受到敌手攻击等。本文讨论扩展服务集(Extended Services Set)网络或称基础架构 WLAN 的安全服务协议，实现：(1)实体的认证。即工作站 STA(Station)、访问节点(Access Point，AP)和认证服务器(Authentication Server，AS)的相互认证，阻止任何非法实体的欺骗和假冒；(2)数据保密通信。在实体认证的基础上，STA 和 AP 间协商产生会话密钥，加密无线通信信道。

目前WLAN安全的两大标准为IEEE 802.11i[1]和我国具有自主知识产权的无线局域网认证与保密基础设施 (WLAN Authentication and Privacy Infrastructure，WAPI)[2]。802.11i 集成了多种成熟的有线网络安全协议标准，它们往往有较广泛的安全分析，有广泛的软、硬件开发与应用支持。但同时，这种协议集成，并未针对WLAN环境进行优化，增加了系统配置的复杂性，如RADIUS服务器本身并不支持数字证书管理服务；实现 802.11i 中STA-AS双向认证与密钥协商的事实标准协议EAP-TLS[3]，会话交互多，AS工作负荷高。

WAPI针对WLAN环境独立设计，基于数字证书(独立设计的数据结构[4]，不兼容X.509 证书格式)的公钥体制实现实体认证，其认证协议简洁，易于部署。但其存在以下不足：证书鉴别阶段，STA只提供公钥证书(公开的)，AS只是验证该证书的有效性，并未真正认证STA合法性。密钥协商结束，AP通过判定STA是否拥有合法会话密钥验证其——合法性“隐性认证”。同时，WAPI中AP需要数字签名操作构造“证书鉴别请求”消息，AP计算负载重，易成为通信瓶颈及攻击对象。

WAPI和 802.11i中认证协议存在不足：(1)不具备在“第一时间”对WLAN的主要认证对象STA的认证。802.11i的EAP-TLS认证协议需执行多轮握手协议[3]；WAPI实现隐性认证。因此，AS(及WAPI中的AP)容易受到诸如拒绝服务的攻击，而这种攻击可以通过构造合法握手消息实施。(2)基于数字证书进行实体认证，两个协议中证书对应的一对公/私钥需要同时支持加密和签名操作，这是不提倡的应用。(3)实体认证协议中数字签名和验证操作需要实体具有较强的计算能力，AP或AS都易成为计算瓶颈，易受拒绝服务攻击。 (4)认证消息冗余，如传递数字证书这样公开信息。

本文借鉴了 802.11i 和 WAPI 安全协议设计中好的思想，优化实体认证方案，提出了一种新 WLAN 认证机制——快速无线局域网认证基础架构(Fast WLAN Authentication Infrastructure，FWAI)。

2 高效 WLAN 认证机制

高效的 WLAN 认证协议应该尽量在“第一时间”实现对 STA 认证，即在认证握手协议的第一个消息中 STA 应该给出明确的、可以证明身份的认证信息，同时认证协议应尽量简洁，计算要求低。

2.1 令牌的构造

本文引入可认证的令牌概念实现对 STA 的第一时间的认证，令牌的构造基于哈希链技术。

基金项目：国家自然科学基金资助项目(90204015，60473021)；河南省科技攻关基金资助项目(0524220044) 河南工业大学科研基金资助项目(0401009，050215，050211)
作者简介：张浩军(1969－)，男，副教授、博士生，主研方向：信息安全理论与技术；祝跃飞，教授、博导
收稿日期：2006-06-09 **E-mail：**zhj@haut.edu.cn

构造一个哈希链，首先确定一个密码学安全的哈希函数h，其安全参数记为k，有h: $\{0,1\}^* \mapsto \{0,1\}^k$，随机选择一个秘密种子$s$，迭代执行哈希函数$N$次，得如下哈希链：

$$T_0 = h^N(s) = h(h^{N-1}(s)) = \underbrace{h(h(h(...h}_{N}(s))))$$

其中链尾为$T_0 = h^N(s)$，称为验证“公钥”。一个STA按上述过程选择参数，构造认证哈希链，并计算令牌集合，链尾作为该链的验证公钥，记为$Token^0_{STA}=h^N(s)$，STA第i次(i从1到N)出示自己的认证令牌为$Token^i_{STA}=h^{N-i}(s)$。

AS可以通过计算$h^i(Token^i_{STA})$(其中i应大于AS记录的该STA哈希链已释放的“链节”的指针)，并与其验证公钥比较，相等表示该令牌有效，更新链节指针为当前i值。实际上AS只需记住最新验证节点的指针p并更新该链验证公钥为$Token^p_{STA}$；下一次验证，计算$h^{i-p}(Token^i_{STA})$并与当前验证公钥比较即可。正常情况下，i每次加1，AS只需执行1次哈希函数计算。

2.2 高效 WLAN 认证机制 FWAI

FWAI 机制中，假设 AS 与 AP 已完成相互认证并预共享对称密钥，记为：AS_AP_SK；STA-AS 之间结合令牌和公钥证书实现相互认证和密钥协商。FWAI 认证协议如下所示：

S1: STA->AP: (ID_{STA}, $Token^{2i-1}_{STA}$, TS, $E_{AS\_pk}(Token^{2i}{}_{STA}, TS, R1)$)

S2: AP->AS: (ID_{AP}, ID_{STA}, $Token^{2i-1}_{STA}$, TS, $E_{AS\_pk}(Token^{2i}{}_{STA}, TS, R1)$)

S3: AS->AP: $E_{AS\_AP\_SK}(ID_{STA}, TS, SUCC, MAC1, PMK, E_{STA\_pk}(ID_{AP}, R2))$ or $E_{AS\_AP\_SK}(ID_{STA}, TS, FAIL)$

S4: AP->STA: (ID_{STA}, TS, ID_{AP}, $E_{STA\_pk}(ID_{AP}, R2)$, $E_{PMK}(MAC1, R3)$)

S5:STA->AP: $E_{PMK}(MAC2, R4)$)

FWAI 认证协议中符号含义如表 1 所示。

表 1 FWAI 认证协议中符号含义

符　号	含　义
ID_{STA} ID_{AP}	STA/AP 惟一标识，可以使用介质访问控制 MAC 地址、或便于目录管理的惟一编码
$Token^{2i-1}_{STA}$ $Token^{2i}_{STA}$	STA 的第 i 次释放的两个认证令牌
TS	时间戳
AS_pk	AS 的公钥
STA_pk	STA 的公钥
PMK	Pairwise Master Key，AS、STA协商产生主会话密钥$PMK=PRF(ID_{SAT}, ID_{AP}, R1, R2)$
PTK	Pairwise Transient Key，短暂会话密钥，用于 STA-AP 间保密通信(意义与用法同 802.11i) $PKT=PRF(PMK, R3, R4)$
R1/R2 R3/R4	各实体产生随机数，用于构造会话对称密钥
$E_k(x)$	使用密钥 k 加密数据 x

其中 PRF(Pseudo-random function)表示伪随机数生成函数。此外，FWAI 中包括 2 个消息鉴别码，用于实现对会话的鉴别与认证。

$MAC1=h(ID_{STA}, Token^{2i-1}_{STA}, TS, E_{AS\_pk}(Token^{2i}{}_{STA}, TS, R1))$

$MAC2=h(ID_{STA}, TS, ID_{AP}, E_{STA\_pk}(ID_{AP}, R2), E_{PMK}(MAC1, R3))$

STA 第 i 次登录无线网络，构造认证消息 S1，包括 2 个有效认证令牌，明文发送令牌 $Token^{2i-1}_{STA}$，保密发送令牌 $Token^{2i}_{STA}$。AS 收到 S2，验证 2 个令牌，并使用 2 个随机数 R1/R2 构造主会话密钥 PMK，并安全转发给 AP。消息 S4、S5 用于 STA 与 AP 间协商短暂会话密钥 PTK，实现它们之间信息的保密通信。

实体数字证书定义参考WAPI[2]及其改进方案[4]。FWAI协议中不需要证书交换，保留证书定义，可支持AS的分布式部署和证书漫游。

3 性能分析

3.1 安全性分析

(1)基于令牌的安全认证。合法 STA 拥有有效的令牌。哈希链是按逆序发布的，密码学安全哈希函数的单向性保证了令牌的不可伪造。令牌的每次释放是新鲜的，保证了令牌不可重复使用，不能重放，即保证了协议消息的鲜活性。对于敌手劫持会话，可以通过时间戳有效窗口及多因子认证(参见安全属性(3))发现重放。

(2)STA对AS/AP隐性认证。FWAI机制中STA对AS的认证是隐性的(不是通过AS的数字签名)，因为只有合法的AS才能获得正确的(使用其公钥加密的)R1，并构造正确的PMK，STA在收到认证响应后，STA通过解密$E_{PMK}(MAC1, R3)$，并验证MAC1 可验证AP合法性，即合法的AS构造出正确PMK并转发给AP。

(3)对 STA 的多因子认证。FWAI 机制实现了对 STA 的双因子认证，即一方面通过判断 STA 是否拥有合法、新鲜的令牌认证其有效性；另一方面通过密钥 PMK 协商，“隐性”认证 STA 合法性，即合法 STA 拥有合法私钥，能够获得 R2 并构造合法的 PMK。

(4)会话密钥的安全性。虽然敌手容易截获甚至修改消息内容$E_{AS_pk}(TS, R1)$和$E_{STA_pk}(ID_{AP}, R2)$，但其无法获得正确的R1、R2(敌手不拥有解密私钥)，因此无法伪造PMK、PTK。

(5)实体不可伪造性。STA 不可伪造性：非法用户无法出示正确的与自己 ID 绑定的示证材料——令牌(哈希链节点值)，因此无法通过 AS 的认证；同时非法用户不拥有合法的公钥证书对应的私钥。

AP 不可伪造性。AP 与 AS 事先基于有线网安全协议共享了通信密钥，基于对称密码算法实现相互认证和保密通信。

AS 不可伪造性。伪造的 AS 没有与 AP 共享的正确密钥；且不具有合法 AS 的私钥，无法生成合法的 PMK，无法通过整个协议认证。

(6)消息认证码应用。机制中引入 2 个消息认证码(Message Authentication Code，MAC) ——MAC1、MAC2，这 2 个认证码都被保护在使用 PMK 加密的密文中。MAC1 允许 STA 验证响应消息及其对应的请求消息的完整性；MAC2 允许 AP 认证 STA 返回的响应消息及其对应消息 S4 的完整性。

(7)抵抗拒绝服务攻击。FWAI 系统中，AS 可以通过一个哈希函数计算，快速验证 STA 令牌的合法性，从而在“第一时间”内验证 STA 实体的有效性。对非法请求，无需解密 S1 的加密部分，直接返回给 AP 认证无效的响应，AP 可以采取地址过滤/阻塞等方法，降低非法(攻击)消息对资源的占用。

3.2 效率分析与提升

(1)对 STA 第一时间认证。通常情况下，AS 对 STA 的认证通过一次哈希函数计算在第一条消息内即可完成。进而才对第一个消息中的密文进行解密操作，做进一步合法性验证。

(2)密码操作计算量小。整个验证过程各参与实体均不需要数字签名和签名验证操作。

(3)构建认证“先头哨所”——AP预认证功能。根据WLAN部署与网络管理策略，AP 可以周期性地从 AS 下载、更新、

（下转第 142 页）