第 38 卷 第 3 期
Vol.38 No.3

计 算 机 工 程
Computer Engineering

2012 年 2 月
February 2012

• 安全技术 •

文章编号：1000—3428(2012)03—0153—03 文献标识码：A 中图分类号：TP393

一种安全高效的 WAPI 改进策略

丁 清，朱 敏，闫二辉

(四川大学计算机学院，成都 610064)

摘 要：提出一种安全高效的 WAPI 改进策略。介绍 WAI 接入鉴别机制及其形式化描述，根据 RSA 算法与公钥认证框架方案改进密钥认证体制，讨论证书认证和密钥协商过程，分析改进 WAPI 的安全性和运行效率。结果表明，该策略可以将身份认证和密钥协商过程有机结合，能抵御重放攻击。

关键词：形式化分析；自验证公钥；身份认证；密钥协商

Safe and High-effective Improved Strategy of WAPI

DING Qing, ZHU Min, YAN Er-hui

(College of Computer Science, Sichuan University, Chengdu 610064, China)

【Abstract】This paper proposes a safety and high-efficiency improved strategy for WAPI. It introduces the WAI access identify mechanism and its formalization description. According to RSA algorithm and public key authentication framework, it improves the key authentication system, discusses the certificate authentication and key agreementconsultation process, and analyzes the security and efficiency of improved WAPI. Analysis results show that this strategy can realize authentication and key agreement process organic union, and resist the replay attack.

【Key words】formal analysis; self-certified public key; identity authentication; key agreement

DOI: 10.3969/j.issn.1000-3428.2012.03.052

1 概述

无线局域网鉴别与保密基础结构(Wireless LAN Authentication and Privacy Infrastructure, WAPI)主要包含 2 个方面，即无线局域网鉴别基础结构 WAI 和无线局域网保密基础结构 WPI。WAI 用于提供安全策略协商、用户身份鉴别、密钥协商、接入控制的功能。2009 年国家标准 WAPI 获得国际社会同意，重启国际标准流程[1]，WAPI 的研究异常火热。本文从密钥密码体制和协议的高效性 2 个方面考虑，提出一种安全高效的 WAPI 改进策略。

2 WAI 接入鉴别机制

WAPI 接入鉴别机制由证书鉴别过程、单播密钥协商过程和组播密钥/站间密钥通告过程 3 个部分组成。WAPI 机制鉴别过程如图 1 所示。

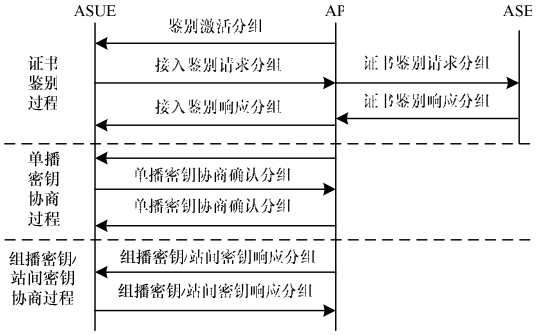

图 1 WAPI 机制鉴别过程

2.1 WAI 的形式化描述

设 $Cert_{\mathrm{ASUE}}$、$Cert_{\mathrm{AP}}$ 分别表示 ASUE 和 AP 的证书；P_{ASUE}、P_{AP} 分别表示 ASUE 和 AP 的身份；S 表示鉴别标志，R_{ASUE}、R_{AP} 分别表示 ASUE 和 AP 的挑战；$SIG_{\mathrm{ASUE}}(XX)$、$SIG_{\mathrm{AP}}(XX)$ 分别表示 ASUE 和 AP 用自身的私钥对消息 XX 的签名；N_{ASUE}、N_{AP} 为 ASUE 和 AP 产生的随机数；$HMAC(XX)$ 为作用于 XX 的消息鉴别码函数 $ADDID=(MAC_{\mathrm{ASUE}}\,||\,MAC_{\mathrm{AP}})$ [2]。AP、ASUE 实现双向认证和密钥交换的形式化描述如下：

(1) $\mathrm{AP}\rightarrow\mathrm{ASUE}: S, Cert_{\mathrm{AP}}$。

(2) $\mathrm{ASUE}\rightarrow\mathrm{AP}: S, R_{\mathrm{ASUE}}, \alpha=x\cdot P, P_{\mathrm{AP}}, Cert_{\mathrm{ASUE}}, SIG_{\mathrm{ASUE}}(S, R_{\mathrm{ASUE}}, \alpha=x\times P, P_{\mathrm{AP}}, Cert_{\mathrm{ASUE}})$，其中，$x\in_R[1,n-1]$。

(3) $\mathrm{AP}\rightarrow\mathrm{ASUE}: R_{\mathrm{ASUE}}, R_{\mathrm{AP}}, \beta=\gamma\cdot P, P_{\mathrm{AP}}, P_{\mathrm{ASUE}}, SIG_{\mathrm{AP}}(R_{\mathrm{ASUE}}, R_{\mathrm{AP}}, \beta=\gamma\cdot P, P_{\mathrm{AP}}, P_{\mathrm{ASUE}})$，其中，$\gamma\in_R[1,n-1]$。

(4) $\mathrm{AP}\rightarrow\mathrm{ASUE}: ADDID, N_{\mathrm{AP}}$。

(5) $\mathrm{ASUE}\rightarrow\mathrm{AP}: ADDID, N_{\mathrm{ASUE}}, N_{\mathrm{AP}}, HMAC(ADDID, N_{\mathrm{ASUE}}, N_{\mathrm{AP}})$。

(6) $\mathrm{AP}\rightarrow\mathrm{ASUE}: ADDID, N_{\mathrm{ASUE}}, HMAC(ADDID, N_{\mathrm{ASUE}})$。

文献[2-5]运用数学原理对国标 WAPI 形式化描述做了一系列的推导，证明其在安全性、效率等方面存在缺陷。

2.2 WAPI 密钥认证体制的现状

国家标准的 WAPI 在安全和性能上存在如下缺陷：

(1)单钥体制的可扩展性差且不能提供抗抵赖攻击。

(2)AKA 协议容易泄露 ASUE 的标识，使 ASUE 被追踪或是遭受伪 AP 攻击[1]。

(3)AP 和 HLR 之间的有线通信链路缺乏有效保护。

(4)当用户漫游至异地网络时，AP 和 ASUE 归属的 HLR 相距遥远，认证向量的传输将增加网络负载[6]。我国现阶段采用的公钥认证协议应用于 WAPI 存在以下缺陷：

作者简介：丁 清(1986－)，女，硕士研究生，主研方向：网络安全；朱 敏，教授；闫二辉，硕士研究生

收稿日期：2011-07-20 **E-mail：**D_XiYun@126.com

1)在 AP 和 ASUE 不知道彼此公钥的前提下，双方必须通过资源有限无线信道传送自己的公钥证书，并验证其合法性与有效性，严重增加网络负载、计算负担和传输时延。

2)现有的公钥认证协议，大部分都要 ASUE 做繁重的数字签名运算，影响用户接入的实时性[6]。

3 本文改进方案

3.1 密钥认证体制改进

本文改进方案是基于大整数分解难题的 RSA 加密算法，以及具有自验证性公钥认证密钥协商方案。在 SPA 中，存在一个可信的 CA(Certificate Authority)，CA 为 ASUE 和 AP 颁发具有可自验证性的公钥证书。CA 为 ASUE 和 AP 产生公钥的过程，系统密钥数据为 CA 生成 RSA 的密钥数据，具体说明如下：

(1)公开模数 $N=P\times Q$，其中，P、Q 是长度相等的大素数，如$|P|=|Q|=512$。

(2)公开指数与 $\Phi(N)$ 互素，其中，$\Phi(N)=(P-1)\times(Q-1)$。

(3)秘密指数 d 满足 $e\times d=1\bmod \Phi(N)$。

(4)公开元素 $g\in Z^*_N$ 具有最大的乘法阶，为计算 g，CA 找 g_P 作为模 P 的生成元，并找 g_Q 作为模 Q 的生成元，然后以用中国剩余定理来构造 g。

CA 公开系统参数(N, e, g)，并秘密保存系统私钥 d。

用户密钥数据：用户 A(ASUE 或 AP)随机选择一个长度为 160 bit 的整数 S_A 作为私钥，计算 $v\leftarrow g^{-S_A}(\bmod N)$，并把 v 发送给 CA。然后，用认证协议向 CA 证明知道 S_A 且不泄漏 S_A，并将身份 I_A 发给 CA。

CA 创建用户 A 的公钥，过程为：为 $v-I_A$ 计算 RSA 签名，$P_A\leftarrow(v-I_A)^d(\bmod N)$，CA 发送 P_A 给 A 作为其公钥的一部分。此时 $I_A\equiv P_A^e-v(\bmod N)$。

用户 A 能够证明其知道以 g 为底模 N 的离散对数，即值 $-S_A$，这就保证 P_A 是由 CA 发行的。

3.2 认证和密钥协商过程

证书认证、密钥协商过程分 2 种情况考虑：(1)当 ASUE 采用自验证公钥证书而 AP 采用传统的公钥证书；(2)ASUE 和 AP 均采用自验证公钥证书。

首先假设 ASUE 向 CA 申请的公钥数据 (S_U,P_U,I_U)(括号表示为一条数据流)，AP 采用传统公钥数据 $(PK_{\mathrm{AP}},SK_{\mathrm{AP}},I_{\mathrm{AP}})$，则单边自验证认证密钥协商过程如图 2 所示。

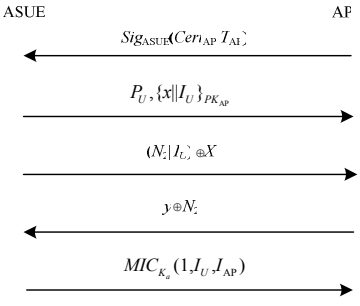

图 2 单边自验证认证密钥协商过程

图 2 的说明如下：

(1)由于 AP 使用传统公钥证书，因此要将 ASUE 对其证书的鉴定结果和签名值预先发送给 ASUE，此分组信息可用来充当鉴别激活分组。

(2)ASUE 用 AP 的公钥验证其签名合法后产生随机数 $N_1\in[0,A]$，得到 $x=H(g^{N_1}\bmod N)$，发送 $P_U,\{x\|I_U\}_{PK_{\mathrm{AP}}}$ 到接入点 AP。

(3)AP 用其私钥 SK_{AP} 解密收到的数据，获得 x 和 I_U，并产生随机数 $N_2\in[0,B]$，将 $(N_2\|I_U)\oplus x'$ 发送给 ASUE，这里的 x' 为 x 的低 128 位。

(4)ASUE 利用 x，还原出 N_2 和 I_U，判断收到的 I_U 和发出的 I_U 是否一致，如果一致，那么说计算 $y=N_1+N_2\times S_U$，发送 $y\oplus N_2$ 给 AP。

(5)AP 利用 N_2 还原出 y，判断 I_U 是否和在步骤(2)中接受到的一致，如果一致，那么判断以下条件是否同时成立：

$$H[g^y(I_U+P_U^e)^{N_2}]\bmod N=x \tag{1}$$

$$y\in[0,A+(B-1)(S-1)] \tag{2}$$

如同时成立，则 ASUE 通过证书认证。此时，AP 将 y 的低 128 位作为共享密钥 K_S，利用函数 $f(K_S)$ 生成会话密钥 K_C 和消息认证码密钥 K_v，向 ASUE 发送 $MIC_{K_a}(1,I_U,I_{\mathrm{AP}})$。

(6)ASUE 利用 y 生成对应的 K_S、K_C、K_v，用 K_v 验证 AP 发送的 $MIC_{K_a}(1,I_U,I_{\mathrm{AP}})$ 的真伪，如真则确定 AP 与自己协商好会话密钥。设 ASUE、AP 已经向 CA 申请的证公钥为 (S_U,P_U,I_U) 和 (S_A,P_A,I_A)，那么双边自验证认证密钥协商过程如图 3 所示。

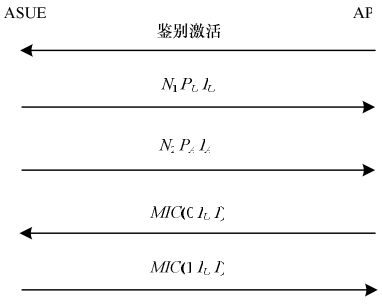

图 3 双边自验证认证密钥协商过程

图 3 的说明如下：

(1)ASUE 产生随机数 $N_1\in[0,A]$，并向 AP 发送数据 (N_1,P_U,I_U)。

(2)AP 产生随机数 $N_2\in[0,B]$，并向 ASUE 发送数据 (N_2,P_A,I_A)。

(3)ASUE 根据接收 AP 的公钥数据，以及自己的私钥，计算 $K_S=(P_A^e+I_A)^{S_U}\bmod N$，再用 K_S 计算 K_C 和 K_v，向 AP 发送 $MIC(0,I_U,I)$。

(4)AP 根据接收到 ASUE 的公钥数据和自己的私钥，计算 $K_S=(P_U^e+I_U)^{S_A}\bmod N$ 和 K_C，以及 K_v，用 K_v 检验 ASUE 发送过来的验证信息是否正确，正确则发送 $MIC(1,I_U,I)$ 给 ASUE。

(5)ASUE 用 K_v 验证 AP 发送过来的消息验证码，若通过验证，则确定与 AP 彼此之间的身份并协商好密钥。

4 改进后的 WAPI 协议分析

4.1 安全性

本文策略具有 GPS 的安全性，且可实现单纯 GPS 方案所不能完成的双向认证及密钥协商功能。具体体现在如下 5 个方面：

(1)双向认证

对于单边自验证认证密钥协商过程方式，只有当双方协

商一致的会话密钥 K_d 时，建立互信关系。双边自验证认证密钥协商过程方式，鉴于自验证公钥认证及密钥协商算法的安全性，只有当拥有正确私钥的 AP 时，才能可解密消息 $\{x \| I_U\}_{PK_{AP}}$ 获得 ASUE 身份 I_U 和 x。在 ASUE 确认收到的 I_U 合法时，才确定 AP 是合法的。AP 根据双边自验证认证密钥协商过程的步骤(5)判别 ASUE 身份的合法性。

(2)抵御重放攻击

对于双边自验证认证密钥协商过程认证方式，由于协议消息分别包含随机数 N_1、N_2，并由其构成后续的 K_S、K_C 和 K_v，保证消息具有新鲜性和不可预测性，因此 ASUE 和 AP 可以通过验证消息认证码的方式来检测重放攻击的发生。对于 Sin_SPA KA 认证方式，由于协议中各条消息分别包含随机数 N_1、N_2，以及由其构造的 x 和 y，因此所有消息均具有新鲜性和不可预测性。重放攻击可在协议执行至双边自验证认证密钥协商过程的步骤(3)，由 ASUE 检测出来，或在协议执行至双边自验证认证密钥协商过程的步骤(5)，由于条件式(2)不成立而被 AP 察觉。

(3)不可抵赖性

合法的自验证证书是无法由非法用户虚构的。非法用户即使知道一个合法用户的身份或是自己虚构的身份 I_A，要构造合理的证书还需要知道 S_A、P_A。如果随机选 P_A，则根据 $I_A \equiv P_A^e - v(\mathrm{mod}\, N)$ 无法计算出正确的 v，进而不能得到正确的 $-S_A$。

对于双边自验证认证密钥协商过程认证方式，由于改进的密钥交换协议是一个 DH 交换协议，只用拥有对应私钥的用户才可以计算出正确的共享密钥，因此只要双方协商了一致的会话密钥，就不能否认自己的证书信息。对于单边自验证认证密钥协商过程认证方式，由于计算 $|S| \geqslant 160$ bit 的短指数离散对数问题的困难性，现有算法无法在有效时间内依据等式 $x = H(g^{N_1} \bmod N)$ 从 x 推出 N_1，AP 也无法根据等式 $y = N_1 + N_2 \times S_U$ 由 y 算出 S_U，所以，一旦 ASUE 通过认证，则不能否认自己的证书信息。

(4)有机结合身份认证的密钥协商

在现有的 WAPI 标准中，身份认证以及密钥协商是作为 2 个独立的部分存在的，会导致严重的 DOS(Disk Operating System)攻击和中间人攻击，而本文策略将身份认证和密钥协商有机统一起来，实现 ASUE 和 AP 双向显式的密钥认证，并且 ASUE 和 AP 产生的密钥是新鲜、随机的、公平的，可防止因任何一方提供弱密钥而带来的安全隐患。

(5)可允许合法用户私钥相同

由于自验证公钥证书 (S_U, P_U, I_U) 是由 3 个部分组成，根据 CA 产生证书的原理，相同的 S_U 并不会产生相同的 P_U，因此不同的 ASUE 拥有相同的私钥在整个 WAPI 认证体系中并不会产生冲突。

4.2 效率分析

纵观 WAPI 体系，计算资源和网络带宽决定整个协议的效率，由于现阶段 ASUE 计算资源的限制，因此 ASUE 是整个 WAPI 协议运行效率的关键点所在。以下从 ASUE 的角度出发来分析认证协议性能，并与现有协议进行比较。SPA 认证及密钥协商方式与 WAPI 的比较如表 1 所示。其中，Trans 是否传递证书；PEX 是预指数运算次数；EX 是在线指数运算次数；KE 是加密次数；KD 是解密次数；Sig 是签名次数；Ver 是验证运算；Hash 是 Hash 运算次数；XOR 是异或次数。

表 1 SPA 认证及密钥协商与 WAPI 定性比较

协议名称	Trans	PEX	EX	KE	KD	Sig	Ver	Hash	XOR
WAPI	Y	0	0	1	1	1	2	1	1
Sin-SP	N	1	0	1	0	0	1	2	2
Dou-SPA	N	0	2	0	0	0	0	2	0

由表 1 可知，本文提出的 WAPI 认证策略相对于国际标准 WAPI 有以下优点：

(1)不需要传递证书便能进行分身认证和密钥协商，进而减小 ASUE 的信息传送量。

(2)由于 ASUE 进行指数运算和公钥运算的次数减少，因此减小了 ASUE 的计算量，从而提高了 WAPI 的效率。在 Sin_SPA KA 认证方式中，由于 ASUE 可通过离线方式预计算 x，并存储((N_1, x)，因此 ASUE 的计算量最轻。

(3)为进一步提高协议的效率，在实际应用中，可选择 $g = 2$ (并不减弱安全性)，其优点在于在使用“平方乘”算法做模指数运算时，平方运算无须做模约简，而且乘 g 的运算就是移位操作。

5 结束语

本文提出一种安全高效的 WAPI 改进策略。分析表明，该策略能达到双向认证和密钥协商的目的，具有安全性，与现有的 WAPI 认证协议相比，能减少 ASUE 的在线计算量和数据传输量，提高认证系统的整体性能。

WAPI 与诸多协议相似，在协议设计时更多强调的是安全性，而没有充分考虑方案的可用性。这种措施虽然能减少信息泄漏，防止产生进一步恶意攻击，但却增加潜在的 DOS 攻击。本文将在以后的工作中继续研究改进 WAPI 的失败恢复方案，保证每个 AP 能以最短的时间接入到网络中。

参考文献

[1] 史云志. 无线局域网安全机制研究与无线接入点 WAPI 协议实现[D]. 北京: 北京邮电大学, 2010.

[2] 吴柳飞, 张玉清, 王凤娇. 一种新的 WAPI 认证和密钥交换协议[J]. 计算机工程, 2008, 34(8): 164-166, 199.

[3] 李兴华, 马建峰. WAPI 实施方案中的密钥协商协议的安全性分析[J]. 计算机学报, 2006, 29(4): 576-580.

[4] Pang Liaojun, Li Huixian, Wang Yumin. Security Analysis of Newly Ameliorated WAPI Protocol[J]. Journal of Southeast University, 2008, 24(1): 25-28.

[5] 张 帆, 马建峰. CK 模型下的无线认证协议[C]//第九届中国密码学学术会议论文集. 北京: [出版者不详], 2006.

[6] 郑 宇, 何大可, 梅其祥. 基于自验证公钥的 3G 移动通信系统认证方案[J]. 计算机学报, 2005, 28(8): 1327-1332.

编辑 刘 冰