2005 年 9 月
第 7 卷第 9 期

中国工程科学
Engineering Science

Sep. 2005
Vol.7 No.9

研 究 报 告

无线接入点 WAPI 认证机制的研究与实现

宋宇波，胡爱群，杨晓辉，王质礼
（东南大学信息安全研究中心，南京 210096）

[摘要] 随着无线局域网技术的广泛应用，新的无线局域网安全标准被提出以增强无线局域网的安全性能。在分析 WAPI（WLAN Authentication and Privacy Infrastructure）标准的技术特征和基本架构的基础上，介绍了无线接入点对 WAPI 认证机制的实现机理和具体流程，并对 WAPI 认证机制的性能进行测试分析。

[关键词] 无线局域网；WAPI；测试分析
[中图分类号] TP393.17 [文献标识码] A [文章编号] 1009－1742（2005）09－0065－05

1 前言

随着公共无线局域网（PWLAN，public wireless LAN）的日趋普及与大量应用，无线传输的安全性已经成为个人用户和运营商关注的焦点。802.11 无线局域网标准[1]采用开发系统认证和共享密钥认证两种方式提供用户认证。但 802.11 标准的认证协议存在极大的安全问题，因此 IEEE 正在制定新的安全增强标准 802.11i[2]，针对无线网络原有的安全弱点进行改进。由于 IEEE 802.11i 的标准尚未制订完成，在 WIFI 的推动下，制订了 WPA（WIFI Protected Access）标准[3]，以 IEEE 802.11i 草案为蓝图，去建构出一个符合现今需求、具备更进一步安全性的无线网络环境。我国也提出了自己的无线局域网国家标准，国家标准在 IEEE802.11 的基础上提出了新的一种无线局域网媒体访问控制和物理规范，其中增加了类似于 IEEE802.1X[4]的认证模型——无线局域网鉴别与保密基础结构 WAPI。该结构利用椭圆曲线密码（ECC，elliptic curve cryptosystem）算法实现数字签名和身份认证。

WAPI[5]（WLAN Authentication and Privacy Infrastructure）由无线局域网鉴别基础结构 WAI（WLAN Authentication Infrastructure）和无线局域网保密基础结构 WPI（WLAN Privacy Infrastructure）组成。笔者在分析 WAPI 标准的技术特征和基本架构的基础上，介绍了东南大学信息安全研究中心开发的无线接入点对 WAPI 认证机制的实现机理和具体流程，并对 WAPI 认证机制的性能进行测试分析。

2 WAPI 机制

WAPI 的鉴别过程采用 WLAN 鉴别基础结构（WAI：WLAN Authentication Infrastructure），用于实现 STA 与 AP 之间的相互鉴别，它建立在链路验证过程和关联过程之上。只有鉴别成功后，STA 才能安全接入 AP。WAI 鉴别基础结构采用公钥密码技术，用于 STA 与 AP 之间的相互身份鉴别。该鉴别建立在关联过程之上，是实现 WAPI 的基础。

AP 提供两种访问 LAN 的逻辑通道，定义为两类端口，即受控端口与非受控端口，AP 提供 STA 连接到鉴别服务单元（ASU）的端口（即非受控端口），确保只有通过鉴别的 STA 才能使用

[收稿日期] 2004－07－19；修回日期 2004－09－18
[基金项目] “八六三”高技术计划资助项目（2002AA143010）
[作者简介] 宋宇波（1977－），男，江苏无锡市人，东南大学博士研究生

AP 提供的数据端口（即受控端口）访问网络。在基于端口的接入控制操作中定义了 3 个实体：鉴别器实体 AE（authenticator entity）、鉴别请求者实体 ASUE（authentication supplicant entity）和鉴别服务实体 ASE（authentication service entity）。

非受控端口允许鉴别数据在 WLAN 中传送，该传送过程不受当前鉴别状态的限制。对于受控制端口，只有当该端口的鉴别状态为已鉴别时，才允许协议数据通过。图 1 给出了鉴别请求者、鉴别器和鉴别服务实体之间的关系及信息交换过程。在图 1 中，鉴别器的受控端口处于未鉴别状态，鉴别器系统拒绝提供服务，鉴别器实体利用非受控端口和鉴别请求者通信。

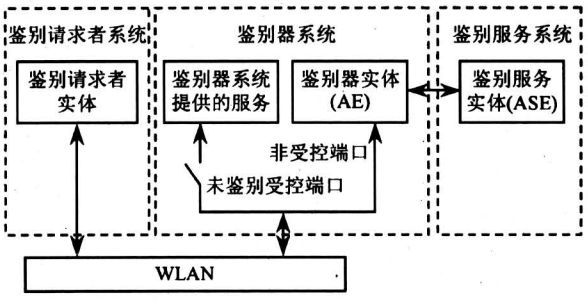

图 1 鉴别系统结构

Fig.1 Authentication system architecture

当 STA 关联或重新关联至 AP 时，必须进行相互身份鉴别。若鉴别成功，则 AP 允许 STA 接入，否则解除其关联。整个鉴别过程包括证书鉴别与会话密钥协商，如图 2 所示。

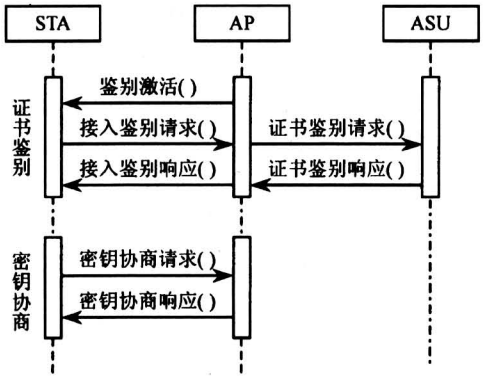

图 2 接入鉴别流程图

Fig.2 Access authentication process

证书鉴别具体过程如下：当 STA 关联 AP 时，AP 向 STA 发送鉴别激活以启动整个鉴别过程。STA 向 AP 发出接入鉴别请求，将 STA 证书与 STA 的当前系统时间发往 AP。AP 收到接入鉴别请求后，将 STA 证书、接入鉴别请求时间、AP 证书及 AP 的私钥对它们的签名构成证书鉴别请求发送给 ASU。ASU 收到证书鉴别请求后，验证 AP 的签名、AP 证书和 STA 证书的有效性。验证完毕后，ASU 将 STA 证书鉴别结果、AP 证书鉴别结果和 ASU 对它们的签名构成的证书鉴别响应返回 AP。AP 对 ASU 返回的证书鉴别响应进行签名验证，得到 STA 证书的鉴别结果，根据此结果对 STA 进行接入控制。AP 将收到的证书鉴别响应回送至 STA。STA 验证 ASU 的签名后，得到 AP 证书的鉴别结果，根据该鉴别结果决定是否接入该 AP。至此 STA 与 AP 之间完成了证书鉴别过程。STA 与 AP 证书鉴别成功之后进行会话密钥协商，密钥协商过程如下：STA 产生一串随机数据 STA_random，利用 AP 的公钥加密后，向 AP 发出密钥协商请求。AP 收到 STA 发来的密钥协商请求后，利用本地的私钥解密协商数据，得到 STA 产生的随机数据，然后产生一串随机数据 AP_random，利用 STA 的公钥加密后，再发送给 STA。STA 与 AP 将自己与对方产生的随机数据进行模 2 和运算生成会话密钥 Session_Key = AP_random⊕STA_random，利用协商的会话算法对通信数据进行加、解密。

3 WAPI 机制的实现

支持 WAPI 机制的无线接入点是在基于 Motorola 的 POWERPC 处理器 MPC852 硬件平台的嵌入式系统上实现的。如图 3 所示，天线部分从无线媒介中截获到相应的 2.4 GHz 频段上的无线信息，通过低噪声放大等信号调理后送到射频处理单元，然后在中频变频，AD 采样后送到基带处理单元 HFA3863 进行解扩和其他相关处理。为了保证实时性和可扩展性，MAC 层的功能以 2 种方式实现：数据的接收和发送、数据的加密和完整性校验、载波监听多路访问（CSMA/CA）以及和物理层的交互通信等实时性要求比较高的功能在 LINUX 嵌入式系统的内核中实现；而 MAC 层的管理模块、WAPI 机制认证模块以 LINUX 嵌入式系统的用户空间程序形式实现。

在无线局域网中，WAPI 的端口是一个逻辑概念，确定何时允许数据从 IEEE802.11 链路经过。每个 WAPI 端口都映射一个连接。其流程如图 4 所示。

WAPI 端口包括一个授控端口和一个非受控端

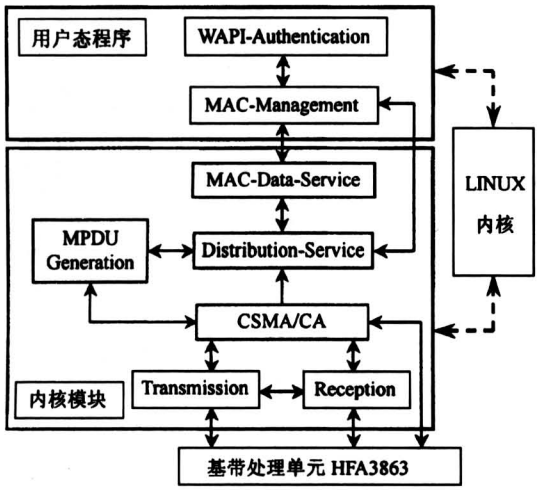

图 3　支持 WAPI 机制的无线接入点框架图

Fig.3　WAPI access point architecture

口。其 WAPI 认证过程通过非授控端口进行，同时受控端口将阻止 2 个 STA 间数据通信。一旦认证执行成功，授控端口将打开以允许通信数据通过。WAPI 请求者和认证者通过 WAPI 非受控端口交换协议信息。授控端口在 Mac-Data-Service 模块中实现。当收到新站点的连接请求后，先建立物理连接，接着初始化授控端口，过滤所有的数据通信。当数据类型为 WAPI 认证帧时上传到用户态空间的 WAPI-Authentication 模块进行处理，其他数据包则作丢弃处理。

WAPI 认证模块流程以状态机的形式实现。笔者设计了符合 WAPI 认证协议的认证者状态机，如图 5 所示。

WAPI 认证模块流程以状态机的形式实现。笔者设计了符合 WAPI 认证协议的认证者状态机，如图 5 所示。

Authenticator 状态机有以下的状态：

1）INITIALIZE：Authenticator 状态机处于初始化状态。当 portControl 为 Auto 并且 portMode 不等于 portControl 时进入此状态，并且置 portMode 为 Auto。当 INITIALIZE 结束后，无条件地进入 DISCONNECTED 状态。

2）DISCONNECTED：Authenticator 状态机处于未连接状态。由 INITIALIZE 状态无条件转换进入此状态，或者由 FAILURE 状态无条件转换进入此状态，此时向用户发送激活数据包，并且置 portStatus 为 Unauthorized。当收到用户发送的接入鉴别请求时进入 SERVER-REQUEST 状态。

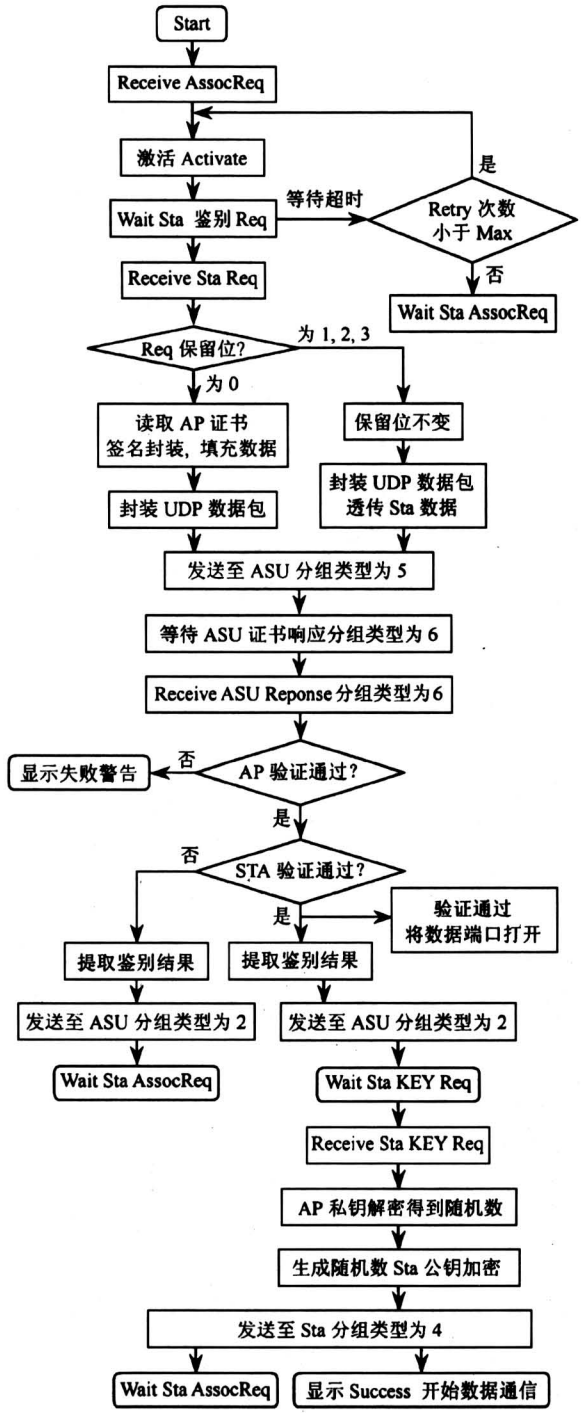

图 4　支持 WAPI 机制的接入点流程图

Fig.4　WAPI access point flow chart

3）SERVER-REQUEST：Authenticator 状态机处于向认证服务器请求状态。由 DISCONNECTED 状态收到用户的接入鉴别请求进入此状态，此时向认证服务器发送证书鉴别请求数据包，并且置 rxAuthResp，authSuccess，authFailure 为 FALSE。当收到认证服务器发送的证书

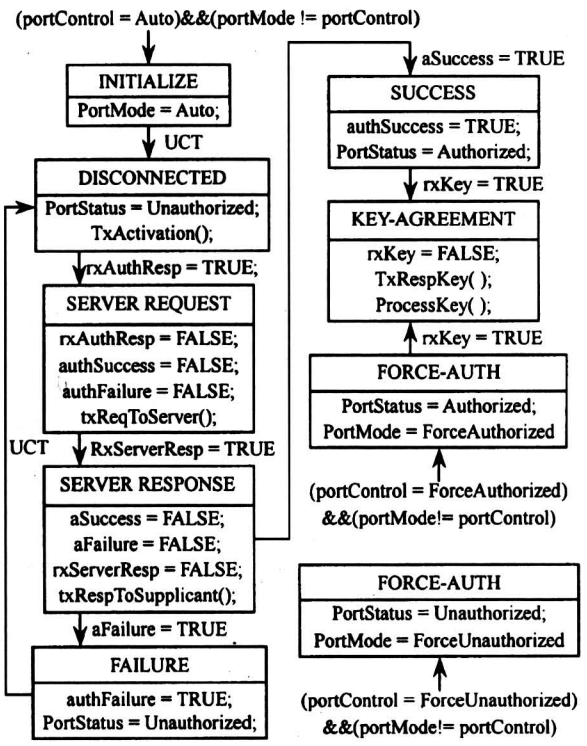

图 5 WAPI 鉴别状态机

Fig.5 WAPI authentication state machine

鉴别响应时进入 SERVER-RESPONSE 状态。

4) SERVER-RESPONSE: Authenticator 状态机处于向认证服务器响应状态。由 SERVER-REQUEST 状态收到认证服务器发送的证书鉴别响应进入此状态，此时向用户发送接入鉴别响应数据包，并且置 rxServerResp, aSuccess, aFailure 为 FALSE。当认证服务器认证成功时进入 SUCCESS 状态，当认证服务器认证失败时进入 FAILURE 状态。

5) SUCCESS: Authenticator 状态机处于用户认证成功状态。由 SERVER-RESPONSE 状态置 aSuccess 为 TRUE 时进入此状态，置 authSuccess 为 TRUE，portStatus 为 Authorized。当收到用户的密钥协商的数据包时进入 KEY-AGREEMENT 状态。

6) FAILURE: Authenticator 状态机处于用户认证失败状态。由 SERVER-RESPONSE 状态置 aFailure 为 TRUE 时进入此状态，置 authFailure 为 TRUE，portStatus 为 Unauthorized。无条件转换到 DISCONNECTED 状态。

7) KEY-AGREEMENT: Authenticator 状态机处于与用户密钥协商的状态。由 SUCCESS 状态得到用户的密钥协商请求数据包时进入此状态或由 FORCE-AUTH 状态得到用户的密钥协商请求数据包时进入此状态，置 rxKey 为 FALSE，并且发送密钥协商响应数据包，处理密钥。

8) FORCE-AUTH: Authenticator 状态机处于强制认证通过状态。当 portControl 为 Force-Authorized 并且 portMode 不等于 portControl 时进入此状态，并且置 portMode 为 Force-Authorized，portStatus 为 Authorized。当收到用户的密钥请求数据包转换到 KEY-AGREEMENT 状态。

9) FORCE-UNAUTH: Authenticator 状态机处于强制认证不通过状态。当 portControl 为 ForceUnauthorized 并且 portMode 不等于 portControl 时进入此状态，并且置 portMode 为 ForceUnauthorized，portStatus 为 Unauthorized。

4 结语

目前的 WAPI 提供相对于过去 WEP 加密机制而言，采用基于证书的认证协议和对称加密算法提供无线网络保护，随着目前无线网络的日趋普及，对于企业与注重安全性的运营商而言，具备 WAPI 机制的无线网络设备，在未来将会发挥比较重要的作用。在讨论 WAPI 的技术特征和基本架构的基础上，笔者提出了支持 WAPI 机制的无线接入点实现方案，详细描述了 AP 的软件实现框架结构和端口控制的流程图。最后通过状态机的方式实现了 WAPI 认证的具体流程。

参考文献

[1] LMSC of the IEEE Computer Society. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications [S]. IEEE Standard 802.11, 1999

[2] LMSC of the IEEE Computer Society. Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security [S]. IEEE STD 802.11i/D10.0, April 2004

[3] Wi-Fi Alliance. Wi-Fi Protected Access (WPA) Version 1.2 [S]. C Brian Grimm, Wi-Fi Alliance, December, 2002

[4] LMSC of the IEEE Computer Society. IEEE Standard for Local and Metropolitan Area Networks-Port-Based Network Access Control [S], IEEE Std 802.1X-2001, June, 2001

[5] 信息技术—系统间远程通信和信息交换局域网和城域网—特定要求—第 11 部分：无线局域网媒体访问控制和物理层规范 GB 15629.11-2003 [S]. 宽带无线 IP 标准工作组. http://www.chinabwips.org/, 2003

The Research and Implementation of WAPI Authentication on WLAN Access Point

Song Yubo, Yang Xiaohui, Hu Aiqun, Wang Zhili

(*Research Center of Information Security, Southeast University, Nanjing* 210096, *China*)

[**Abstract**] With the wireless LAN technologies being widely applied, new WLAN security standards have been proposed to enhance the WLAN security. In this paper, through discussing the technology characteristic and the basic framework of the WAPI standard, the detail of the application of the WAPI authentication procedure on the WLAN access point was given. Furthermore, the performance of the authentication procedure was discussed.

[**Key words**] WLAN; WAPI; test analysis

(上接第 64 页)

The Risk Analysis of Liquefied Petroleum Gas Leak and the Consequence Assessment Method

Chen Sining, Sun Jinhua, Wang Qingsong

(*State Key Laboratory of Fire Science, University of Science and Technology of China, Hefei* 230026, *China*)

[**Abstract**] The liquefied petroleum gas (LPG) has multifarious risks associated with fire or explosion in the traffic and storage process. The leak of LPG can induce disasters including flash fire, unconfined vapor cloud explosion (UVCE), boiling liquid expanding vapor explosion (BLEVE), etc. In this paper, occuring condition and risk of those disasters are analyzed. Quantified risk analysis (QRA) is used in consequence assessment. The assessment method for the hazards to the environment by UVCE and BLEVE is researched.

[**Key words**] fire; liquefied petroleum gas leak; risk analysis; consequence assessment