第43卷 第10期 西 安 交 通 大 学 学 报 Vol. 43 №10
2009年10月 JOURNAL OF XI′AN JIAOTONG UNIVERSITY Oct. 2009

无线局域网802.1X协议安全性分析与检测

薛雨杨[1,2,3]，周颢[1,2,3]，赵保华[1,2,3]
(1.中国科学技术大学计算机科学与技术系，230027，合肥；2.网络与交换技术国家重点实验室，100876，北京；
3.安徽省计算与通讯软件重点实验室，230027，合肥)

摘要：针对无线局域网(WLAN) 802.1X协议易受重放、拒绝服务等攻击的问题，采用非形式化方法，根据攻击者的能力，从攻击者扮演的协议角色，即模仿正常的协议行为和破坏正常的通信出发，分析了802.1X协议的安全性，并对攻击行为进行了分类，据此提出了一种基于攻击的无线局域网主动测试方法.通过构造协议报文序列、模拟攻击者的攻击行为对协议运行主体进行攻击，从而判断协议是否存在安全漏洞.测试结果表明，所提方法有效地结合了攻击者和测试者的特点，在一定程度上覆盖了针对802.1X协议的已知安全漏洞，并具有发现潜在问题的能力.

关键词：无线局域网；安全性分析；主动测试
中图分类号：TP393 **文献标志码**：A **文章编号**：0253-987X(2009)10-0052-04

The Security Analysis and Detection of 802.1X Wireless Local Area Network

XUE Yuyang[1,2,3], ZHOU Hao[1,2,3], ZHAO Baohua[1,2,3]
(1. Department of Computer Science and Technology, University of Science and Technology of China, Hefei 230027, China; 2. State Key Laboratory of Networking and Switching Technology, Beijing 100876, China; 3. Anhui Province Key Laboratory of Software in Computing and Communication, Hefei 230027, China)

Abstract: Aimed at the problem that the vulnerable wireless local area network (WLAN) 802.1X protocol is not susceptible to replay and DoS (denial of service) attacks, etc, an informal method is introduced to analyze the security properties of 802.1X protocol. The method classifies attack behaviors according to the ability of attackers, and from the aspect of the role which attackers can play in the protocols (i.e., imitating normal protocol behavior or breaking normal communication). Then a new method, WLAN active testing, is proposed. Attacks to the protocol running mainbody are implemented by simulating the actions of the attacker which can be used to make up protocol messages. The results are used to determine whether the protocol security vulnerabilities exist or not. Testing results show that the method combines characteristics of both the attacker and the tester to cover some known protocol security vulnerabilities, and has the ability to reveal some potential problems.

Keywords: wireless local area network; security analysis; active testing

无线局域网(WLAN)是计算机和无线通信技术结合的产物，它避免了有线网络对用户的束缚，具有强有力的市场竞争力，发展迅速.同时，无线空间传播信道的开放性导致了多种不安全因素，包括假冒攻击、网络欺骗、信息窃取等，使得WLAN网络运营和通信信息的安全受到了极大的威胁.

认证是实现WLAN安全的重要组成部分.802.1X[1-2]协议是一种基于端口的网络访问方案，可用于WLAN的身份认证.802.1X协议提供了用户认证和密钥分发的框架，控制用户只有在认证通

收稿日期：2009-03-02. 作者简介：薛雨杨(1985—)，女，硕士生；赵保华(联系人)，男，教授，博士生导师. 基金项目：国家自然科学基金资助项目(60872009，60602016)；国家高技术研究发展计划资助项目(2007AA01Z428，2009AA01Z148)；安徽省自然科学研究计划重大资助项目(ZD2008005-2，ZD200904，JK2009A013，JK2009A025).

过以后才能与网络连接，从而达到了接受合法用户接入、保护网络安全的目的. 由于 802.1X 协议实现简单、易于运营，由此得到了广泛的使用，但它在设计上仍存在一些缺陷，易受到重放、拒绝服务等攻击. 因此，在实际应用环境中需要对系统的安全性进行测试，以检测系统抵御攻击的能力.

本文从攻击者的角度对 802.1X 协议的安全性进行了分析，并在实际环境中针对 802.1X 协议应用主动测试方法检测 WLAN 抵御安全漏洞的攻击的能力.

1　协　议

802.1X 协议由申请者、认证方和认证服务器 3 部分组成，其结构如图 1 所示. 客户端 STA 是申请者，访问点 AP 是认证方，认证服务器可以是 RADIUS 服务器.

为了能够在申请者和授权机构之间使用认证算法，802.1X 协议引入了可扩展认证协议(EAP)[3]. EAP 只是一种封装协议，允许高层使用多种不同的认证方法，包括 MD5-Challenge、TLS 和 TTLS 等常用的高层认证方法. STA 和 AP 之间的认证通话通过 EAP 报文来传递. EAP 包括 4 种基本报文：EAP-Request(认证请求)，EAP-Response(认证响应)，EAP-Success(认证成功)和 EAP-Failure(认证失败). EAP-Request 与 EAP-Response 消息有 6 种类型，其中最重要的是 Identity 消息. AP 发送 EAP-Request/Identity 请求消息，申请者返回的 EAP-Response/Identity 消息包含了用户名和认证服务器能识别的其他信息.

802.1X 协议制定了基于局域网的 EAP(EAPOL)，用于承载 EAP 报文和执行其他管理任务. EAPOL 报文共有下面 5 种类型.

(1)EAPOL-Start：802.1X 协议为认证方保留了某一专用的组播媒体访问控制(MAC)地址，申请者向此地址发送此报文，判断认证方是否存在.

(2)EAPOL-Key：认证方在允许申请者接入网络时，用此报文向申请者发送加密(或其他)密钥.

(3)EAPOL-Packet：承载 EAP 报文.

(4)EAPOL-Logoff：申请者向认证方发送此报文，希望离开网络.

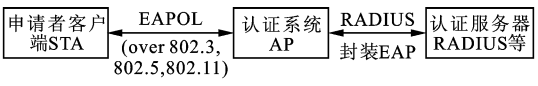


图 1　802.1X 协议结构

(5)EAPOL-Encapsulated-ASF-Alert：允许一个未授权设备向系统发送管理警告.

802.1X 协议认证过程如图 2 所示.

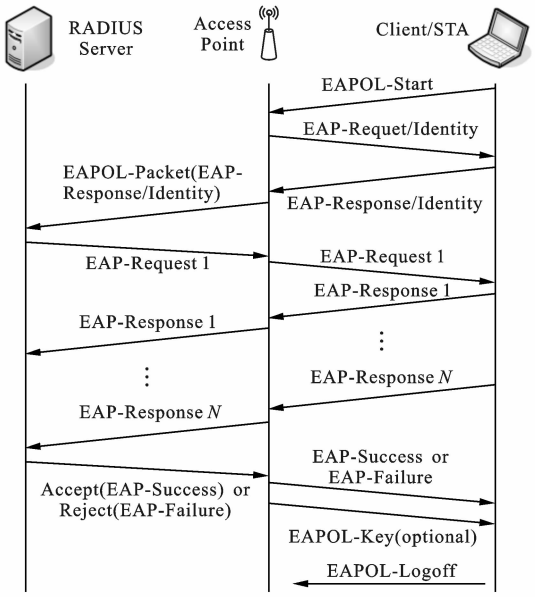


图 2　802.1X 协议认证过程

2　攻击驱动的安全性分析

协议的安全性分析有形式化与非形式化 2 种方法. 非形式化方法根据已知的各种攻击方法对协议进行攻击，以攻击是否有效来检验协议是否安全.

本文采用非形式化方法，根据攻击者的能力，从攻击者可以扮演的协议角色出发分析了 802.1X 协议的安全性[4]，并对攻击行为进行了分类，但只考虑无线环境中的安全性，即 STA 与 AP 通信交互的部分.

2.1　攻击者能力

要想实现攻击，攻击者需要具备一定的知识和能力. Dolev-Yao 模型[5]是著名的攻击者模型，其假设攻击者拥有足够的知识和能力实现网络中所有可能的攻击. 攻击者具有如下能力：可窃听所有经过网络的消息；可阻止和截获所有经过网络的消息；可存储获得或自身创造的消息；可根据存储的消息伪造消息、发送消息；可作为合法主体参与协议的运行.

2.2　基于攻击者角色的攻击分类

在 STA 与 AP 之间通信，攻击者可以扮演 STA 与 AP 这 2 种角色，模仿正常的协议行为，破坏二者间正常的通信，达到攻击目的.

2.2.1　STA 角色　攻击者扮演 STA，对 AP 攻击. 攻击行为如下.

(1)发送 EAPOL-Start 报文. AP 对所有合法的

EAPOL-Start 报文都会进行处理，攻击者发送大量此报文可消耗 AP 资源，使 AP 无法响应新的认证请求，导致网络瘫痪，属于 DOS(拒绝服务)攻击.

(2)发送 EAPOL-Logoff 报文. 由于 AP 接收此报文但并不对发送者进行身份认证，因此攻击者可以伪装成合法用户，潜在地欺骗 AP，使 AP 注销该用户. 合法用户被注销时并不知情，直到它稍后试图通过 WLAN 进行通信时才会有所察觉. 一般而言，用户会发现中断连接的状态并自动重新关联和认证，以重新获取无线连接. 攻击者可以连续传输欺骗性 EAPOL-Logoff 报文，从而实现有效攻击.

2.2.2 AP 角色 攻击者扮演 AP，对 STA 攻击. 攻击行为如下.

(1)发送 EAP-Success 报文. ①对合法 STA 发送 EAP-Success 消息，由于 802.1X 协议缺乏客户身份认证机制，使得 STA 以为认证成功，其状态转为认证完成，从而把攻击者当作 AP 进行数据传输；②在 STA 的认证阶段，攻击通过重放一个正确的、伪造 STA 和 AP MAC 地址的 EAP-Success 报文，来影响 STA 对认证成功性的判断. 理论上，STA 如果接收到 EAP-Success 报文，会停止 802.1X 协议初始链接的验证过程，而此时如果正常的验证过程未停止，就会出现验证失败的状况.

(2)发送 EAP-Failure 报文. ①合法 STA 在与 AP 的认证过程中，当收到 AP 发送的 EAP-Failure 报文时会认为认证失败；②在 STA 的认证阶段，攻击通过重放一个正确的、伪造 STA 和 AP MAC 地址的 EAP-Failure 报文，来影响 STA 对认证成功性的判断. 攻击效果如同 EAP-Success 报文重放.

2.2.3 独立攻击者 802.1X 协议可用于密钥(EAPOL-Key 报文)分发，攻击者不扮演任何协议角色，只窃听 STA 与 AP 的通信，截取报文. 在获取到足够的数据之后，通过异或操作等算法离线计算得到密钥. 它属于字典攻击.

3 安全性检测

实际使用中为保证 WLAN 的安全性，需要对其协议安全性进行分析，并采取相应的安全管理措施. 安全性分析包括主动分析和被动分析. 后者基于入侵检测方法，监测、分析网络数据与已知攻击特征的匹配情况，判断是否存在针对已知漏洞的攻击. 本文主要研究主动分析，即基于攻击的主动测试.

3.1 测试方法

基于攻击的主动测试方法通过构造协议报文序列，模拟针对 WLAN 安全漏洞的网络攻击，并与待测设备(STA 和 AP)交互，检测待测设备的防御能力，从而判断设备是否存在安全漏洞.

测试方法结合攻击者和测试者特点，可模拟任意情景下的网络攻击行为，攻击行为如 2.2 节所述. 模拟攻击行为需编写测试例，测试例中应包括：网络信息收集、判断是否可以进行攻击及选定攻击对象；执行攻击脚本；分析结果，判断攻击是否成功.

本文使用 Tcl 脚本语言编写测试例. 用 Tcl 的 C/C++接口将编写的低层网络通信函数扩展为命令. 基于这些命令，根据实际需要组合数据包，编写控制命令.

3.2 测试环境

测试环境如图 3 所示，主要功能描述如下.

(1)无线安全分析终端(Agent). 它可以部署在 WLAN 中的任何位置，主要功能是执行脚本，按脚本配置组合攻击所需报文，并将采集到的网络信息进行预定的本地处理，然后再将处理后的数据发送到管理服务器.

(2)管理服务器(Server). 它是整个系统的核心，其包含数据处理模块，以接收来自各个 Agent 的信息，并将处理后的数据根据数据类型存储到存储模块或者网络信息库之中.

(3)控制台(Console). 它是管理员交互界面，用于发布网络分析和网络管理命令，显示测试结果等.

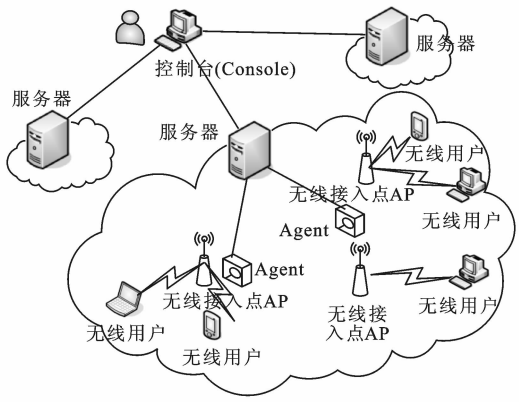


图 3 测试环境

3.3 测 试

主动测试作为安全分析与管理系统的一个功能模块，可以帮助分析 WLAN 的机密性、完整性、可用性及用户验证等内容，指导管理员配置安全策略，建立防御机制.

主动测试模块主要包括 3 部分，如图 4 所示，功能描述如下.

(1)脚本分发. 管理员由控制台发送控制命令，

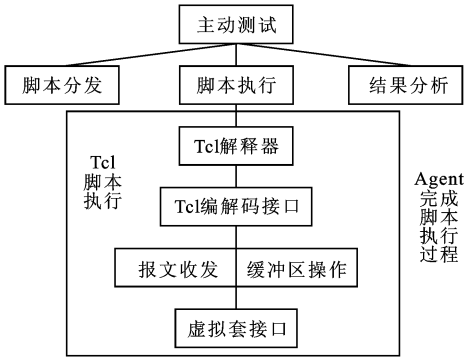


图 4　主动测试基本结构

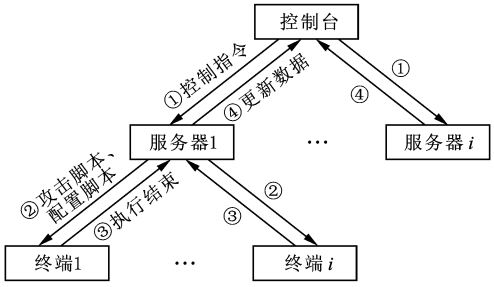
Server 根据配置将脚本分发给各个 Agent.

(2)脚本执行. 在接收到从 Server 发送来的脚本之后，Agent 执行测试脚本. Server 与 Agent 间的控制命令、测试脚本等均通过 Tcl 命令解释器解释、实现. 图 4 中的虚拟套接口、报文收发、编解码接口都是通过 C++语言扩展实现的.

(3)结果分析. Agent 执行脚本进行主动测试，并将采集到的数据结果发送给 Server，Server 再将结果回送到控制台显示.

3.4　测试流程

测试流程如图 5 所示.



①、②表示用户控制 Server，其将测试用例的参数配置脚本和攻击脚本发送给 Agent；③表示 Agent 执行攻击脚本，对待测设备进行攻击测试，并将执行结果返回到 Server；④表示从 Agent 到 Console 的数据更新

图 5　测试流程

3.5　测试结果

测试结束后，在控制台显示测试结果，如表 1 所示. 实验使用型号为 TP-LINK TL-WR641G+的 AP，基于 STA 和 AP 角色扮演的攻击均成功得以实现，说明 WLAN 中确实有这些安全隐患，需安全管理员采取安全措施进行防护. 字典攻击与 EAP 采用的具体加密算法有关，针对不同的加密方式需要有不同的破解方式，具有一定难度，需进一步研究.

表 1　802.1X 协议测试结果①

攻击方式	测试例名称	测试结果
字典攻击	同具体 EAP 算法有关	
Eapol_Start Dos 攻击	802.1X_Dos_EapStart	攻击成功
Eapol_Logoff 攻击	802.1X_Dos_EapLogoff	攻击成功
Eap_Failure 攻击	802.1X_Dos_Failure	攻击成功
Eap_Success 攻击	802.1X_Dos_EapSuccess	攻击成功
EAP_Success 重放攻击	802.1X_Re_EapSuccess	攻击成功
EAP_Failure 重放攻击	802.1X_Re_EapFailure	攻击成功

①：对 TP LINKTL WR641G+型号 AP(MS-Chap2-Peap)的测试.

4　结束语

本文主要讨论无线局域网 802.1X 协议的安全性，并采用基于攻击者角色扮演的方法对 802.1X 协议安全性进行分析，对可能受到的攻击进行分类. 在实际环境中，采用基于攻击的主动测试方法对 802.1X 协议安全性进行了测试，以此印证了安全分析下的可能的攻击行为. 下一步工作是针对无线局域网其他安全协议进行分析、测试.

参考文献：

[1] Institute of Electrical and Electronic Engineers. ANSI/IEEE 802.1X－2001　Standard for local and metropolitan area networks port-based network access control [S]. Piscataway, NJ, USA: IEEE, 2001.

[2] ABOBA B. IEEE 802.1X network port authentication [EB/OL]. [2008-12-20]. http://www.drizzle.com/~aboba/IEEE/.

[3] ABOBA B, BLUNK L, VOLLBRECHT J, et al. RFC3748　Extensible authentication protocol (EAP) [S]. Reston, VA, USA: Internet Society, 2004.

[4] WILLIAM M, ARBAUGH A. An initial security analysis of the IEEE 802.1X standard [EB/OL]. [2008-12-10]. http://www.cs.umd.edu/~waa/.x.pdf.

[5] DOLEV D, YAO A. On the security of public key protocols [J]. IEEE Trans on Information Theory, 1983, 29(2):198-208.

(编辑　苗凌)