基于状态机的802.1X协议攻击检测方法

朱加伟[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802.1X协议存在一定漏洞且易受重放、拒绝服务等攻击，结合802.1X协议的认证过程，抽象出802.1X协议认证的状态转移过程，同时针对802.1X协议的功能性攻击，构造出一套攻击状态转移机制：分析802.11报文和基于局域网的扩展认证协议(EAPOL)/扩展认证协议(EAP)报文的结构；剔除出重传的报文，逐个字段解析出关键字并存入链表中；将根据EAPOL/EAP报文格式取得检测所需的EAP报文存入缓存.据此，设计出基于状态机的802.1X的攻击检测方法.实验结果表明，在实际组网环境下的重放/DoS等802.1X功能性攻击能够得到准确的检测，并具有有效、统一的检测结果.

关键词：协议攻击；状态转移；检测方法
中图分类号：TP393.06 **文献标志码**：A **文章编号**：0253-987X(2010)04-0052-05

Detection Methods for 802.1X Protocol Attacks Using State Machine

ZHU Jiawei[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. Province Key Laboratory of Software in Computing and Communication, Hefei 230027, China)

Abstract: There are some loopholes in 802.1X protocol such as replay attacks, DoS (Denial of Service) attacks and so on. The paper presents an state transition process for certification of 802.1X, and designs an attack state transfer mechanism for functional attacks. The architecture of 802.11 frames, EAPOL frames and EAP frames are analyzed. The replay frames are deleted and keywords are abstracted and saved from the list of remaining frames one by one. Then the EAP frames which are required for detection are saved in the cache. The security detection method of 802.1X is designed based on the state transition mechanism. Experimental results show that functional attacks of 802.1X such as replay/DoS attacks can be detected accurately in real network environments, and the detection is effective and consistent.

Keywords: protocol attack; state transition; detection method

随着手机、PDA、笔记本等无线产品的广泛使用，无线局域网(WLAN)得到了广泛的应用，其可移动性也受到了更多的重视，但由于信道的开放性，使得无线网络的安全问题成为一个束缚其发展的重要因素.

802.1X协议[1](下面简称为802.1X)是一种基于端口的网络访问控制协议，能够增强WLAN的安全性，其自身具有可扩展性、易用性，所以在很多领域得到了广泛的应用.但是，802.1X还存在一定的漏洞，容易受到重放、拒绝服务等攻击.当前的一般漏洞检测机制都是针对特定攻击进行特定的检测，即根据新发现的攻击，分析其攻击特点，然后制

收稿日期：2009-09-03. 作者简介：朱加伟(1987—)，男，博士生；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)；国家高技术发展计划资助项目(2007AA01Z428，2009AA01Z148)；安徽省自然科学研究计划重大项目(ZD2008005-2，ZD00904，JK2009A013，JK2009A025).

定相应的检测策略.

本文基于 802.1X 的功能性漏洞，提出了一套统一的基于状态转移的检测机制，并对该机制进行了有效性验证.

1　802.1X 分析

1.1　802.1X

802.1X[2-3]由申请者、认证方和认证服务器 3 部分组成，如图 1 所示. 客户端 STA 是申请者，接入点 AP 是认证方，认证服务器可以是 RADIUS 服务器. 802.1X 使用了扩展认证协议（EAP）[4]进行 STA 和 AP 之间的报文传送. EAP 允许上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，它们包括了 4 种基本报文：EAP-Req（认证请求）、EAP-Resp（认证响应）、EAP-Success（认证成功）和 EAP-Failure（认证失败）.

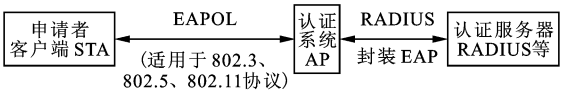

图 1　802.1X 结构

802.1X 的认证过程如图 2 所示，其中 STA 通过基于局域网扩展认证协议-启动（EAPOL-Start）开启认证过程，然后通过一系列的 EAP-Req/EAP-Resp 报文进行信息和报文的互相匹配，最后由 AP 返回 EAP-Success/EAP-Failure，提示认证成功或者失败.

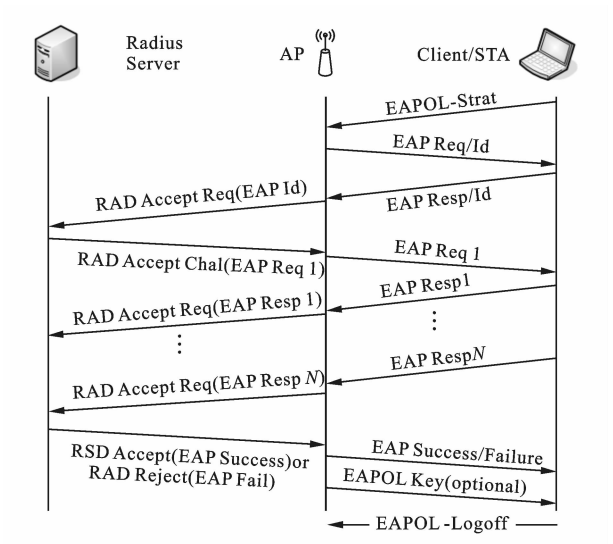

图 2　802.1X 认证过程

1.2　漏洞

由于无线网络特殊的开放性以及 802.1X 自身的特点，所以 802.1X 同时存在如下的一系列漏洞[5].

（1）重放攻击：重放 EAP-Success/EAP-Failure 等报文，造成了 802.1X 验证的失败或者连接状态发生变化，属于功能性攻击.

（2）洪泛攻击：AP 对所有合法的 EAPOL-Start 报文都会进行处理，攻击者发送大量的此类报文可以消耗 AP 资源，使得 AP 无法响应新的认证请求，属于性能性攻击.

（3）字典攻击：攻击者窃听 STA 与 AP 的通信，截取报文，即在获取了足够的数据之后，经离线再通过异或操作等算法计算，得到密钥，属于安全性漏洞攻击.

（4）其他攻击：包括中间人攻击[6]、APOL-Logoff 报文攻击等.

2　基于状态转移的检测机制

2.1　正常和被攻击状态分析

端口进入认证状态后，802.1X 的正确认证情况（见图 3）为状态匹配正确的情形：①在每一个 EAP-Req 报文之后一定匹配一个 EAP-Resp 报文；②在每一个 EAP-Resp 报文之后不可能匹配一个 EAP-Resp 报文；③每一个 EAP-Success/EAP-Failure 报文一定是独立的（独立是指在每一个 EAP-Success/EAP-Failure 报文之后不可能紧接着 EAP-Success/EAP-Failure 报文）.

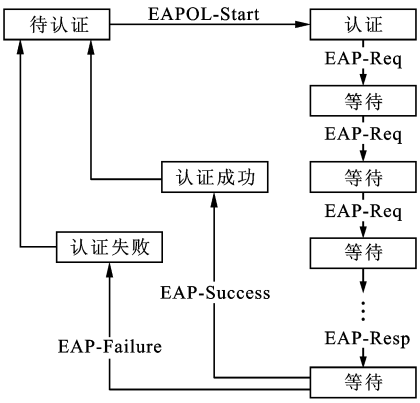

图 3　正常状态

现实的网络环境会出现一定的丢包现象，丢包时存在如下 2 种情况.

（1）报文重传成功：服务器/客户端对丢失的报文会进行重传，如果重传成功，验证过程可以继续进行，是一次合法的验证过程.

（2）报文重传失败：进行若干次重传直至超时，

服务器/客户端仍未收到重传的报文,则为报文传送失败.此时,验证过程因为没有正确状态的匹配而无法继续进行,802.1X 的验证失败.这是一次非法的验证过程,可被认定为攻击.

排除了丢包的影响,从而只有图 3 所示的验证状态才是一个唯一合法的 802.1X 认证过程,除此之外的所有不正常的状态都被认为是攻击.图 4 抽象出了所有不正常的报文匹配和状态匹配,其中添加了一个等待状态,表示根据当前报文的下一个报文来判断攻击的状态(图 4 中的等待状态为同一个状态).

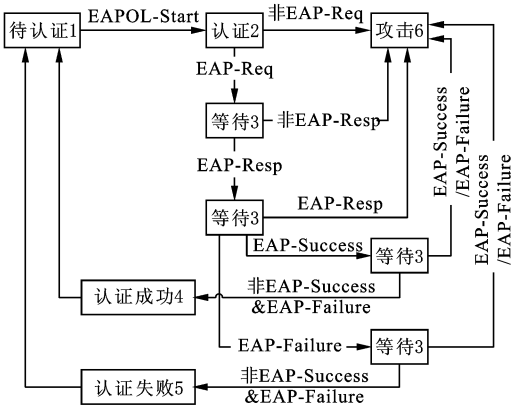

图 4 攻击状态

2.2 检测机制及分析

本文采取的是基于状态转移的检测方法[7],因此需要缓存一系列的 EAP 报文序列,以用于状态转移的判断.

2.2.1 检测机制 重传报文有一个重传标识位.首先分析 802.11 报文和 EAPOL/EAP 报文的结构,从获取到的 802.1X 报文中剔除出重传的报文,再将逐个字段解析出的关键字存入链表中.根据 EAPOL/EAP 的报文格式[4](见图 5),可从大量的 WLAN 报文中取得检测所需的 EAP 报文,并存入缓存.

如果解析出一个新的 EAP 报文,再从缓存中取出一定数量的当前 EAP 报文对应 AP 和 STA 的 EAP 报文序列.通过判断一系列报文的状态迁移的合法性可判断是否发生了攻击.

上述监测方式可以满足无线局域网 802.1X 安全性实时监控的需要,该检测机制对于所有的涉及 802.1X 连接报文的功能性攻击具有通用性.

2.2.2 时空性能分析 性能分析如下.

(1)报文解析.该解析是顺序地对报文的各个部分进行关键字判断,单条报文的长度是固定的,因此解析的时间复杂度为 $O(1)$.此处不进行报文的存储,所以不需要存储空间,故空间复杂度为 0.

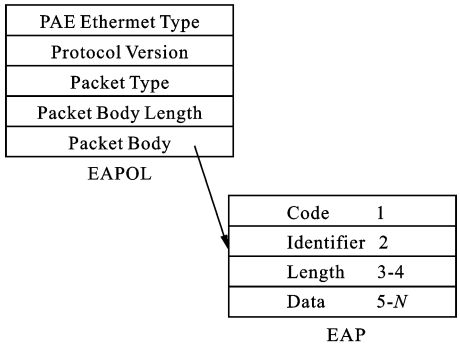

图 5 EAPOL/EAP 报文格式

(2)报文存储以及状态判断(假设链表长度为 m).当报文存储时,需要对已有的和新接收的报文采用插入排序算法按照发送时间进行排序,所以每单个报文的处理时间复杂度为 $O(m)$,空间复杂度为 $O(m)$.

因此,对于 n 条报文做处理时的整体时间复杂度为 $n(O(1)+O(m))=O(nm)$,空间复杂度为 $O(m)$.

2.3 几种已有漏洞的状态分析

下面是对几种 EAP 报文攻击的状态分析.

(1)EAP-Success 报文攻击:①构造 EAP-Success 报文攻击,即攻击者对正在进行 802.1X 认证的客户端发送自己构造的 EAP-Success 报文,使得客户端的认证状态发生变化;②EAP-Success 报文重放攻击,即攻击者通过特定方式抓取网络中的 EAP-Success 报文,在合适的时机(当 802.1X 认证时)将该报文发送给客户端.

此类攻击会出现多个连续的 EAP-Success 报文(见图 6),可被判定为图 4 中的攻击状态.

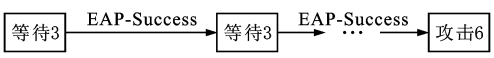

图 6 EAP-Success 报文攻击状态

(2)EAP-Failure 报文攻击:①构造 EAP-Failure 报文攻击,即攻击者对正在进行 802.1X 认证的客户端发送自己构造的 EAP-Failure 报文,使得客户端的认证状态发生变化;②EAP-Failure 报文重放攻击,即攻击者通过特定方式抓取网络中的 EAP-Failure 报文,在合适的时机(当 802.1X 认证时)将该报文发送给客户端.

此类攻击会出现多个连续的 EAP-Failure 报文（见图 7），可被判定为图 4 中的攻击状态.

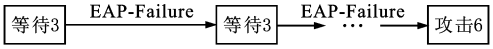

图 7　EAP-Failure 报文攻击状态

3　检测系统

3.1　系统结构

检测系统如图 8 所示，它是一个实际的组网环境，各部分说明如下.

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

（2）管理服务器（Server）. 管理服务器可基于攻击进行主动测试，同时也可对 Agent 接收到的数据进行处理，进行攻击检测或者将数据存入相关的存储模块.

（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的命令，同时显示测试结果等.

（4）802.1X 环境（STA-AP-Radius Server）. 本文使用的 802.1X 攻击环境是基于 PEAP-MS-CHAP v2 协议[8]搭建的，是一个实际的可使用的 802.1X 环境，因此攻击结果和检测结果具有一定的现实意义.

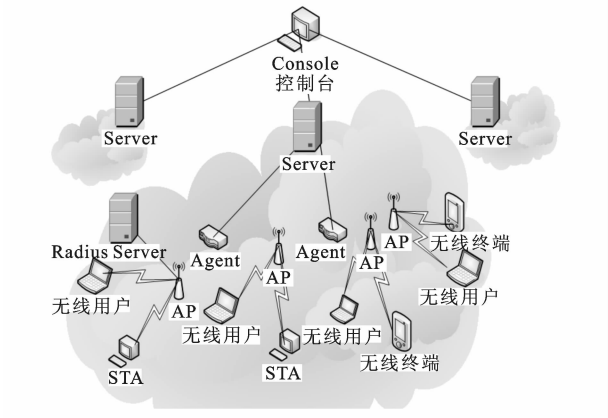

图 8　检测系统结构

3.2　检测结果

攻击结果是根据实际的 802.1X 连接状态和获取网络中对应的被攻击 STA 和 AP 之间的报文来判断的，实验采用 TP_LINK TL_WR641G＋的 AP，测试结果如表 1 所示. 从表中可以看出，文中分析的功能性攻击均能完成，说明 802.1X 有一定的安全隐患.

在攻击的同时，开启检测模块，通过检测模块在 Console 端的响应来判断是否检测到了攻击. 802.1X 正常连接过程应预先启动，并通过检查检测模块对正常的 802.1X 连接过程的响应来判断检测模块的误报情况，结果如表 2 所示.

由表 2 可以看到，本文提出的检测机制对于 802.1X 的功能性攻击的检测比较准确，与现存一般的检测机制相比，具有一定的通用性.

表 1　TP_LINK TL_WR641G＋的 AP 攻击结果

攻击方式	测试例名称	攻击结果
EAP_Success 攻击	802.1X_Dos_EapSuccess	攻击完成
EAP_Failure 攻击	802.1X_Dos_EapFailure	攻击完成
EAP_Success 重放攻击	802.1X_Re_EapSuccess	攻击完成
EAP_Failure 重放攻击	802.1X_Re_EapFailure	攻击完成

表 2　攻击检测结果

攻击方式	攻击结果	检测结果
EAP_Success 攻击	攻击完成	攻击
EAP_Failure 攻击	攻击完成	攻击
EAP_Success 重放攻击	攻击完成	攻击
EAP_Failure 重放攻击	攻击完成	攻击
正常 802.1X 连接	无攻击	无攻击

4　结束语

本文基于 802.1X 的认证过程抽象出了状态转移过程，在此基础上结合 802.1X 的某些功能性漏洞提出了一套统一的基于状态转移的检测机制. 同时，针对实际的组网环境进行了攻击测试和检测，以用来验证该机制的有效性. 下一步的工作是，在本文基础上尝试改进状态机，从而进一步完善本文机制[9-10]，使其更加完备，并能够检测出更多的 802.1X 攻击，以增强 802.1X 的安全性.

参考文献：

[1] BRAWN S K, KOA R M, CAYE K. Secure in an insecure world: 802.1X secure wireless computer connectivity for students, faculty, and staff to the camp-

us network [C]// Proceedings of the 32nd Annual ACM SIGUCCS Conference on User Services. New York, USA: ACM, 2004:273-277.

[2] CROW B P, WIDJAJA I, KIM J G, et al. IEEE 802.11 wireless local area networks[J]. IEEE Communications Magazine, 1997, 35(9):116-126.

[3] JEFFREE T, CONGDON P, SALA D, et al. P802.1X/D11-2001 IEEE standard for local and metropolitan area networks: standard for portbase network access control [S]. Piscataway, NJ, USA: IEEE, 2001.

[4] ABOBA B, BLUNK L, VOLLBRECHT J, et al. RFC 3748-2004 Extensible authentication protocol (EAP)[S]. Piscataway, NJ, USA: IETF, 2004.

[5] MISHRA A, ARBAUGH W A. An initial security analysis of the IEEE 802.1X standard [R]. Maryland, USA: University of Maryland. Department of Computer Science, 2002.

[6] HWANG H, GYEOK J, SOHN K, et al. A study on MITM (man in the middle) vulnerability in wireless network using 802.1X and EAP[C]// Proceedings of the 2008 International Conference on Information Science and Security. Los Alamitos, CA, USA: IEEE Computer Society, 2008:164-170.

[7] MCFALL R, DERSHEM H L. Finite state machine simulation in an introductory lab[C]// 25th SIGCSE Technical Symposium on Computer Science Education. New York: USA: ACM, 1994:126-130.

[8] Microsoft Corporation. Protected extensible authentication protocol (PEAP) specifi-cation [EB/OL]. [2009-07-27]. http://msdn.microsoft.com/en-us/library/cc238354(PROT.13).aspx

[9] DING P, HOLLIDAY J, CELIK A. Improving the security of wireless LANs by managing 802.1X disassociation[C]// Proceedings of the IEEE Consumer Communications and Networking Conference. Piscataway, NJ, USA: IEEE, 2004:53-58.

[10] PACK S, CHOI Y H. Pre-authenticated fast handoff in a public wireless LAN based on IEEE 802.1X model [C]// Proceedings of the IFIP TC6/WG6.8 Working Conference on Personal Wireless Communications. Deventer, Netherlands: Kluwer, 2002:175-182.

(编辑 苗凌)