

基于动态口令的 WiFi 身份认证方案研究

王增光, 陈立云, 卢 昱

(军械工程学院 信息工程系, 河北 石家庄 050003)

摘 要: 针对日益严重的无线网络安全问题, 从安全性和移动终端负载能力考虑, 提出了一种 WiFi 环境下的轻量级双向身份认证方案. 该方案基于挑战/应答机制, 用户对认证服务器的认证通过基于异或运算的身份认证方式来实现; 认证服务器对用户的认证通过基于公钥加密的身份认证方式实现. 通过性能分析可知, 该方案认证简洁, 减轻了客户端的运算量和存储量, 同时又能抵抗重放攻击、小数据攻击、网络窃听和冒充攻击, 适合应用到对安全性要求较高的 WiFi 环境下.

关键词: 无线网络; 身份认证; 动态口令; 轻量级

中图分类号: TP393

文献标识码: A

文章编号: 1000—7180(2016)06—0078—04

Research on WiFi Identity Authentication Scheme Based on Dynamic Password

WANG Zeng-guang, CHEN Li-yun, LU Yu

(Department of Information Engineering, Ordnance Engineering College, Shijiazhuang 050003, China)

Abstract: A lightweight authentication scheme of WiFi environment is raised from the perspective of security and the load capacity mobile terminal according to the increasing serious of wireless network security. The new scheme is based on the challenge/response. The authentication of user to authentication server is realized by lightweight authentication. The authentication of authentication to user is realized by identity authentication based on public key encryption. Through the analysis of performance, the scheme is simple and the computation and storage of the client are reduced. What's more, the scheme can resist replay attack, network eavesdropping and posing as attack, which is suitable for the application to the WiFi environment with high security requirements.

Key words: wireless network; authentication; OTP; lightweight

1 引言

随着互联网技术以及移动终端的迅速发展, WiFi 已经普遍使用在众多公共场合, 是当前应用极为广泛的无线网络接入方式. 但是, WiFi 本身的开放性给网络带来了很大的风险. 身份认证是网络安全的基础和前提, 一旦身份认证系统受到破坏, 网络将无安全可言. 当前, WiFi 身份认证主要通过服务集标识符(SSID)、物理地址过滤(MAC)、有线对等保密(WEP)/WiFi 保护接入(WPA)、端口访问控制技术(IEEE802. 1X)等弱认证方式实现^[1], 认证功

能主要由各无线接入点实现, 加密方式简单、管理不便、安全性不高. 因此, 构建一个安全的身份认证方案对无线网络的普及具有重要意义.

目前, 无线网络环境下的身份认证方案已经有一些研究成果. Ye Xi^[2] 提出基于 S/Key 的移动智能终端认证方案. 该方案通过前后相关的口令序列来实现认证, 通过迭代和加密运算来抵抗常见攻击手段. 但 S/Key 认证过程中采用 Hash 链式加密, 计算量大, 用户口令使用到一定的次数后, 需要重新进行初始化. Longyang Gong 等人^[3] 基于 Hash 函数和伪随机函数相结合生成一次性动态口令, 实现用

户和认证服务器之间的双向认证. 但该方案中用户的身份标识以明文的形式在网络上传输,带来了一定的安全隐患,并且该方案中客户端需要生成和存储高质量的伪随机数序列,没有考虑移动终端的负载能力. Torben Tuseler 等人^[4]提出基于移动终端地理位置作为认证因素的身份认证方案. 但客户端的定位效果有一定的局限性,导致密钥空间受限,方案实施难度较大.

本文提出了一种 WiFi 环境下的轻量级身份认证方案. 区别于传统 WiFi 环境下的单向身份认证,该方案采用双向身份认证,即考虑移动终端计算存储能力有限的特点又兼顾认证的安全性,适合应用到部分对安全性要求较高的 WiFi 环境中.

2 身份认证系统结构

本文设计的 WiFi 环境下的身份认证系统结构如图 1 所示.

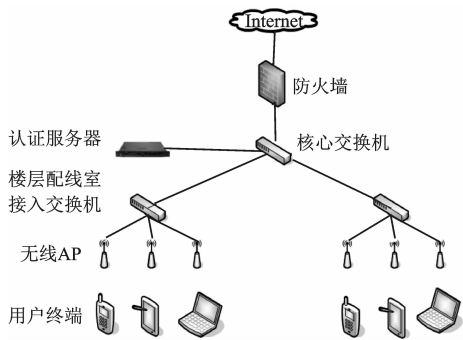


图 1 身份认证系统结构

用户终端通过无线接入点 AP 接入网络,同一楼层的无线 AP 通过网线连接到该楼层配线室的接入交换机,核心交换机将系统中的认证服务器、防火墙及不同楼层配线室的接入交换机互连. 用户第一次未经过认证而提出访问互联网资源请求后,无线接入点 AP 将用户的认证请求通过 HTTP 重定向到认证服务器,由认证服务器和用户进行双向身份认证,认证成功后才能对资源进行访问和操作.

3 身份认证方案设计

3.1 身份认证方案设计思想

本方案应用于部分对安全性要求较高 WiFi 环境中,移动智能终端通过无线接入点重定向到认证服务器进行身份认证,需要遵循以下原则:(1)为了提高身份认证的安全性,避免伪造服务器攻击,用户和认证服务器之间进行双向身份认证;(2)考虑到移动终端的运算能力有限,要尽量减少客户端的计算

量,客户端对服务器的身份认证采用轻量级身份认证;(3)为了满足对高安全性的需要,服务器对用户的身份认证通过基于公钥加密结合伪随机数来实现;(4)尽量简化认证过程以减少网络中的通信量.

身份认证方案的总体设计思想如下所示.

(1)双向认证的实现:通过基于挑战/应答的身份认证机制来实现认证双方的双向身份认证. 用户对服务器的认证通过 Hash 函数结合异或运算来实现;服务器对用户的身份认证通过求解椭圆曲线离散对数的困难性结合 OTP 认证技术来实现.

(2)Hash 函数的选择:选择 SHA-1 作为认证方案中的 Hash 函数. SHA-1 在移动终端上的能耗仅略高于 MD5,但 SHA-1 的安全性要高于 MD5,所以 Hash 函数选择 SHA-1^[5].

(3)加密算法的选择:选择 ECC 作为认证方案的加密算法. 在当前常用的公钥密码体制中,ECC 具有计算量小,处理速度快,存储空间小,密钥单位安全强度高的优点,所以加密算法选择 ECC^[6].

3.2 身份认证方案描述

身份认证方案分为注册和认证两个方面,所涉及到的符号及描述如表 1 所示.

表 1 本文涉及的符号及描述

符号	描述
U	用户
AP	无线接入点
AS	认证服务器
DS	数据库服务器
Internet	互联网资源
ID_x	X 的身份标识
M	用户认证服务器合法身份的依据
P_w	用户登陆口令
K_{UR}	用户公钥
K_{US}	用户私钥
K_{SR}	服务器公钥
K_{SS}	服务器私钥
ECC	安全椭圆曲线密码系统的参数集
IMEI	移动设备唯一身份标识
$E(K, m)$	用密钥 K 对明文 m 进行加密
$Sign_y(x)$	用 y 对 x 进行签名
SHA()	SHA-1 加密
$x y$	级联 x 和 y
R	随机数据串

3.2.1 注册阶段

注册阶段主要完成用户口令和密钥的选择,用户和服务器通过安全信道交换身份证明以及公开密钥,整个注册阶段的流程如图 2 所示.

具体注册流程如下:

(1) 认证服务器 AS 选择合适的椭圆曲线进行

初始化,选取密钥对 K_{SR} 和 K_{SS} ;

(2) 用户 C 向认证服务器 AS 发起注册请求;

(3) 认证服务器 AS 将 ECC 连同 K_{SR} 发送给用户 C ;

(4) 用户 C 存储 K_{SR} 并根据安全椭圆曲线选取自己的密钥对 K_{UR} 和 K_{US} ;

(5) 用户输入 ID_U 和 P_W , 请求注册, 向认证服务器发送用 K_{SR} 加密的 ID_U 、 P_W 、 K_{UR} 、 $IMEI$ 、 M 令 $M = SHA(ID_U || P_W)$, 即发送 $E(K_{SR}, ID_U || K_{UR} || IMEI || P_W || M)$;

(6) 认证服务器 AS 收到消息后用其私钥解密消息, 验证数据库服务器中是否存在 ID_U , 如果存在, 则向用户 C 发送用户名已存在, 注册失败的消息;

(7) 如果 ID_U 验证成功, 则认证服务器将 ID_U 与 $IMEI$ 、 K_{UR} 、 M 、 P_W 绑定, 并存入数据库服务器, 向用户发送注册成功信息。



图2 注册阶段流程

3.2.2 认证阶段

认证阶段主要完成用户与认证服务器之间的双向认证. 在身份认证方案中, 用户提出认证请求后, 认证请求会被重定向到认证服务器, 由认证服务器完成认证后才能访问互联网资源. 由于无线接入点只进行数据包的转发, 因此在认证流程图中只体现用户与认证服务器的认证流程, 身份认证阶段流程图如图3所示.

身份认证的具体过程可描述如下^[7-9]:

(1) $U \rightarrow AP: ID_U || ID_{Internet}$ 用户搜索相对应的无线接入点, 通过浏览器提出访问资源的请求.

(2) $AP \rightarrow AS: ID_U || ID_{Internet}$ 无线接入点收到用户的 $http$ 请求后, 将用户的请求重定向到认证服务器, 进行相关的认证. 认证服务器查询数据库服务器检验用户是否注册. 如果数据库服务器中没有相关用户, 则拒绝认证, 用户不具有资源访问权限.

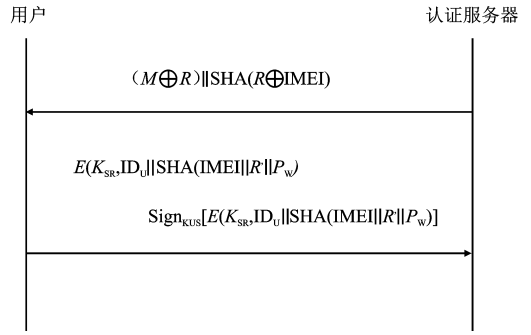


图3 身份认证阶段流程

(3) $AS \rightarrow AP: (M \oplus R) || SHA(R \oplus IMEI)$ 数据库服务器中查询到相关用户后, 认证服务器利用伪随机数发生算法产生 R , 向无线接入点发送 M , R , $IMEI$ 运算后的信息 $(M \oplus R) || SHA(R \oplus IMEI)$, 并保存副本.

(4) $AP \rightarrow U: (M \oplus R) || SHA(R \oplus IMEI)$ 无线接入点将收到的消息转发给用户. 用户通过字符串运算提取出 $M \oplus R$ 、 $SHA(R \oplus IMEI)$, 令 $P = M \oplus R$, $Q = SHA(R \oplus IMEI)$. 并计算 $M' = SHA(ID_U || P_W)$, $R' = M' \oplus P$, $Q' = SHA(R' \oplus IMEI)$. 如果 Q' 与 Q 不相等, 则用户对认证服务器认证失败, 认证服务器为伪造服务器, 向管理员反馈问题.

(5) $U \rightarrow AP: E(K_{SR}, ID_U || SHA(IMEI || R' || P_W)) || Sign_{K_{US}}(E(K_{SR}, ID_U || SHA(IMEI || R' || P_W)))$

如果用户对认证服务器认证成功, 用户输入 P_W , 对 P_W 、 R' 和 $IMEI$ 进行哈希运算, 令 $W = SHA(IMEI || R' || P_W)$, 用服务器公钥对 ID_U 和 W 加密, 使用用户私钥对消息进行签名后, 将结果发送给 AP .

(6) $AP \rightarrow AS: E(K_{SR}, ID_U || SHA(IMEI || R' || P_W)) || Sign_{K_{US}}(E(K_{SR}, ID_U || SHA(IMEI || R' || P_W)))$

无线接入点将消息转发给认证服务器, 认证服务器用其私钥解密消息得到 ID_U 和 W . 通过 ID_U 查找对应的 $IMEI$ 和 P_W , 若不存在则拒绝认证, 若存在则对 $IMEI$ 、 R 及 P_W 做哈希运算, 令 $W' = SHA(IMEI || R || P_W)$. 如果 W 与 W' 不相等, 则认证服务器对用户认证失败, 拒绝登录.

4 性能分析

4.1 有效性分析

(1) 认证过程简洁, 不需要第三方参与, 避免了

复杂的CA认证体系。

(2)区别于传统的单向WiFi身份认证方案,本方案采用双向身份认证。用户对认证服务器的认证采用轻量级身份认证,认证服务器对用户的认证采用基于公钥加密的身份认证。既考虑到移动终端存储、计算能力有限的问题,又保证了认证服务的安全。

(3)除去无线接入点转发认证信息过程,用户和认证服务器之间通过三次握手即可完成认证过程,通信量少。

(4)传统双向身份认证中用户和认证服务器都需要产生伪随机数才能实现相互认证,而本身份认证方案中只需要认证服务器才生成高质量的伪随机数,并且用户无需存储额外的认证信息,减轻了移动智能终端的负担。

4.2 安全性分析

4.2.1 抗重放攻击特性分析

通过加入高质量的伪随机数,保证每次认证消息不同,使得攻击者截获的认证信息无法通过认证方的认证,从而有效地避免了重放攻击。

4.2.2 抗伪造服务器攻击特性分析

区别于传统的单向WiFi身份认证方案,本方案采用双向身份认证。根据3.2.2节中对WiFi环境下的身份认证方案的具体描述可知,第4步中用户通过轻量级认证协议完成对认证服务器的认证,能够有效地避免伪造服务器攻击。

4.2.3 抗小数攻击特性分析

本身份认证方案没有采用前后相关的口令序列,动态口令根据伪随机数重新生成,与上次成功认证的用户口令无关,从根本上杜绝了小数攻击。

4.2.4 抗网络窃听特性分析

用户对服务器的认证消息通过SHA-1加密来保证安全性,攻击者截获消息后通过穷举法攻击,理论上不可行;认证服务器对用户的认证消息通过基于公钥的加密手段进行处理,只有认证服务器拥有相应的私钥能够解密消息。因此,第三方截获消息后无法还原出消息所对应的内容。

4.2.5 抗冒充攻击特性分析

根据3.2.1节对用户注册阶段的具体描述可知,用户通过安全信道与认证服务器交换身份认证和公开密钥。因此,只有认证服务器AS拥有用户认证服务器的合法身份的依据 M ,攻击者无法冒充认证服务器。即使攻击者获得了 M ,通过运算只能获得 R' 由于无法拥有用户唯一身份标识IMEI,仍不

得到 $Q' = \text{SHA}(R' \oplus \text{IMEI})$,无法通过认证。同理, C 拥有 M 以及通过运算后得到的认证服务器产生的随机数 R ,攻击者无法冒充用户。即使攻击者获得 M 及 R ,由于无法拥有IMEI,仍然得不到 $W' = \text{SHA}(\text{IMEI} || R || P_w)$,无法通过认证。

5 结束语

针对WiFi环境下身份认证的特点,结合部分场合对安全性要求较高的特点,提出了一种轻量级的双向身份认证方案。该身份方案中,用户对认证服务器的认证通过SHA-1加密和异或运算实现,减轻了移动智能终端的负担;认证服务器对用户的认证通过求解椭圆曲线离散对数的困难性结合OTP认证技术来实现,提高了认证的安全性。通过对认证方案进行相应分析可知,该方案能够实现用户与认证服务器的双向认证,同时能够有效抵抗重放攻击、伪造服务器攻击、小数攻击、网络窃听和冒充攻击,适合应用到对安全性要求较高的无线WiFi认证环境中。下一步将对认证方案进行仿真并对协议进行形式化分析,来证明认证方案的实用性和合理性。

参考文献:

- [1] 张婧. WiFi网络实名认证的方法研究和实现[J]. 计算机工程与科学, 2012, 34(10): 22-27.
- [2] Ye Xi. An improved OTP authentication system and its application in mobile commerce [C]// Intelligence Computation and Evolutionary Computation. Wuhan, China: IEEE, 2013: 615-624.
- [3] Gong Long-Yan, Pan Jing-Xin, Liu Bei-bei, et al. A novel one-time password mutual authentication scheme on sharing renewed finite random sub-passwords [J]. Journal of Computer and System Sciences, 2013, 79(1): 122-130.
- [4] Torben Kuseler, Ihsan Alshahib Lami. Using geographical location as an authentication factor to enhance mCommerce application on smartphones [J]. International Journal of Computer Science and Security, 2012, 5(4): 278-287.
- [5] Damasevicius R, Ziberkas G. Energy consumption of hash functions [J]. Elektrotechnika ir Elektrotechnika, 2012, 18(10): 81-84.
- [6] 路而红. 现代密码算法工程[M]. 北京: 清华大学出版社, 2012: 196-213.
- [7] 杨明星, 彭新光. 一种轻量级一次性口令认证方案[J]. 小型微型计算机系统, 2014, 35(8): 1808-1811.

制信号在波形中表现了相应的时序关系,通过 1553B 芯片手册确认其时序正确性。

(2) 时序仿真

SOPC 时序仿真与逻辑时序仿真差别在于, SOPC 逻辑代码的接口包含两部分:一部分为外部接口,另外一部分为 PPC 的接口。通过 SOPC 的时序仿真可以验证以下两方面。

① PPC 接口信号时序

验证 PPC 接口与内部逻辑交互时候是否存在时序不满足情况或者亚稳态情况。

② 时序仿真引起的功能表现是否正确

验证在实际网表层面典型功能场景是否正确,在行为级验证中已验证过行为表现的正确性,在网表层面如果验证不通过,可以通过波形追溯出哪些信号时序的不满足引起了功能层面的错误。

4 SOPC 仿真技术的应用

上述的 SOPC 仿真技术应用在了航天高可靠型号任务 SOPC 片上系统测试中,共测试验证了 5 个项目,发现了以下几类问题。

(1) 软件代码的线程优先级调度出现问题。

(2) 软件代码对于 GPIO 的某一位操作时,误操作了其他位,导致给逻辑代码发出的控制信号混乱,引起功能错误。

(3) 软件代码的进程安排不合理导致控制流信号混乱引发功能异常。

(4) 软件代码在使用需外部接口触发的中断时,由于中断处理方式不正确引发功能异常。

(5) 逻辑接口和 PPC 接口交互时由时序问题引起建立保持时间不满足导致功能异常。

(6) 逻辑采集数据存放在存储区,软件没有及时取走数据,导致数据上传出现故障。

测试发现,上述几类问题引发了许多重要功能的不满足,在传统板级测试或模拟软件功能的纯逻辑测试验证中很难定位问题的原因,基于软件和逻辑

联合仿真的 SOPC 验证技术则可以准确定位出问题,避免引发功能异常或风险。

5 结束语

本文对 SOPC 仿真技术进行深入剖析研究,提炼出了一套切实可行的基于软件和逻辑联合仿真的 SOPC 验证方法,阐明了 SOPC 仿真技术的具体实现方法,包括软件工具初始化文件的配置、处理器仿真库的配置、仿真环境的特殊配置。分析了 SOPC 的具体验证方法,包括 CPU 内核测试方法、内核对逻辑代码接口测试方法、SOPC 软件功能测试方法、SOPC 软件和逻辑联合测试验证的方法,并对其中常见的问题给予归类总结。这套验证方法可以作为 SOPC 仿真验证的一个标准,在工程实践中存有重要价值。

参考文献:

- [1] 陈叶富. 集成处理器仿真平台 SOPC 系统可测试性方法研究[D]. 哈尔滨:哈尔滨工业大学,2011.
- [2] 姚双武. 基于 SOPC 的集成处理器仿真平台研制[D]. 哈尔滨:哈尔滨工业大学,2010.
- [3] 刘景宁,舒芳,童薇,等. SOPC 光纤通道控制器 IP 核的仿真验证[J]. 华中科技大学学报,2008,36(10): 91-94.
- [4] 沈浩. 基于 SOPC 的短波 OFDM 通信信号仿真平台的研究[D]. 武汉:武汉工程大学,2011.
- [5] 魏子杰,许军,张磊,等. 基于 SOPCde 电力电子实时仿真系统设计[J]. 电测与仪表,2012 年,49(11):81-84.
- [6] 姚凤振. 基于 SOPC 技术的水声通信半物理仿真平台设计与实现[D]. 青岛:中国海洋大学,2013.
- [7] xilinx ISE help[EB/OL]. [2015-08-01]. <http://help.ubuntu.com/communtly/xilinxISE>. 2014.

作者简介:

周 珊 女,(1983-),硕士,工程师. 研究方向为高可靠软件,可编程逻辑测试. E-mail:zhoushan@csu.ac.cn.

王金波 男,(1978-),博士,副研究员. 研究方向为高可靠软件.

(上接第 81 页)

[8] 王秦. 基于 OTP 的移动商务身份认证协议研究[D]. 北京:北京交通大学,2010.

[9] 叶汝军. 校园网络身份认证技术平台研究[J]. 微电子学与计算机,2012,,29(3):155-158.

作者简介:

王增光 男,(1991-),硕士研究生. 研究方向为网络安全与信息对抗. E-mail:wang1223797579@163.com.