



专题：能源互联网技术与应用

一种基于 PKI 的能源信息系统多渠道统一身份认证方法

汤阳¹, 张翼英², 何业慎³, 王聪², 雷明³

(1. 广东电网有限责任公司佛山南海供电局, 广东 佛山 528299;

2. 天津科技大学计算机科学与信息工程学院, 天津 300457;

3. 深圳市国电科技通信有限公司, 广东 深圳 518109)

摘 要: 能源信息系统存在用户体验差、管理不统一、有安全隐患问题, 迫切需要从源头研究各种电子渠道之间的统一身份认证问题, 实现对多个电子服务信道的统一管理以及对各种电子信道的服务监督。提出了一种基于 PKI 证书的多维电子信道统一认证方法, 用于能源信息系统。用户可以通过所提出的方法直接访问每个应用系统, 并在没有多个认证过程的情况下在应用系统之间执行快速且安全的切换。该方法可以为用户提供从事复杂业务管理活动的便利性和安全性。

关键词: PKI; 多渠道认证; 能源信息系统; 能源互联网

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2019156

A PKI-based multi-channel unified identity authentication method for energy information system

TANG Yang¹, ZHANG Yiyi², HE Yeshen³, WANG Cong², LEI Ming³

1. Foshan Nanhai Power Supply Bureau of Guangdong Power Grid Co., Ltd., Foshan 528299, China

2. College of Computer Science and Information Engineering, Tianjin University of Science & Technology, Tianjin 300457, China

3. China Gridcom Co., Ltd., Shenzhen 518109, China

Abstract: There are problems of poor user experience, inconsistent management, and potential security risks in energy information system. It is urgent to study the issue of unified identity authentication between various electronic channels from the source to achieve unified management of multiple electronic service channels and service supervision of various electronic channels. A multi-dimensional electronic channel unified authentication method based on PKI certification was proposed for energy information system. Users could directly access each application system through the proposed method and perform fast and secure switching between application systems without multiple authentication processes. The approach provided users with the convenience and security of engaging in complex business management activities.

Key words: PKI, multi-channel certification, energy information system, energy internet

收稿日期: 2019-04-02; 修回日期: 2019-05-24

通信作者: 张翼英, winzyy@163.com

基金项目: 国家自然科学基金资助项目 (No.61807024)

Foundation Item: The National Natural Science Foundation of China (No.61807024)



1 引言

能源互联网是以电为核心,借鉴互联网模式,建设以信息—物理二元网络融合为基础的新型能源服务系统。其中,能源信息系统是能源互联网的智能化、信息化和互动化的重要支撑和主要内容。同时,能源互联网开放、互联、共享的特性,为能源信息化系统的可靠运行带来新的挑战^[1]。多业务、多渠道、大规模接入能源信息系统为客户提供便捷服务,但同时也带来各种问题,如多渠道接入、多身份认证、分别注册等。例如,国家电网公司营销系统建立了丰富的电子服务渠道,包括 95598 网站、电 E 宝、掌上电力、国网商城、E 充电、微信;而随着各电子渠道的丰富应用,在逐步方便用户使用的同时,出现了用户需要分别注册、查询服务不共享等体验不佳的问题,缺乏对多种电子服务渠道的统一管理,对各电子渠道的服务监管有所欠缺,因此,急需从源头着手,对用户在多种电子渠道间的统一身份认证等进行具体研究^[2]。

多维电子服务渠道通常是各业务应用系统相互独立,用户不能一次登录就获得多系统业务应用所提供的服务,虽然部分业务之间做了超链接,但需要再次登录,才能享受下一业务系统的应用服务,使用繁琐,体验很差;另外,由于各电子服务渠道各自为政、独立运营,公司无法整合各个电子服务渠道的客户资源优势,实施针对性的营销运营;同时,缺乏对各个电子渠道进行统一管理和监测的平台,目前的管理较为分散、支撑手段较为欠缺^[3-4]。

因此,本文面向能源信息系统,从源头着手建立用户的统一身份认证管理系统(unified identity authentication system, UIAS),用户登录一次就可以访问其他电子渠道,即实现所谓的“一点登录,多点漫游”功能,保证了多维电子渠道的安全接入,以便优化各互联网电子渠道用户体验,

增强能源互联网公司的互联网服务竞争力。

2 研究现状

身份认证技术发展历程是由软件认证到硬件认证、由单因子认证到多因子认证、由静态认证到动态认证的过程。常见的基于口令的鉴别方法存在严重的安全问题,安全性依赖于口令,口令一旦泄露,用户即会被冒充;而基于智能卡的认证方式,由于智能卡具有硬盘加密功能,有较高安全性,每个用户有一张智能卡,智能卡存储用户的秘密信息,同时验证服务器也存放该秘密信息^[5]。基于公钥数字证书认证方法有较好的安全性,但是认证时延较长。基于生物特征认证方式,以人体可靠和稳定生物特征(指纹、虹膜、脸部、掌纹等)为依据,采用计算机的强大功能和网络技术进行图像处理和模式识别,该技术具有较好的安全性、可靠性和有效性,与传统身份确认手段相比,无疑产生了质的飞跃^[6]。目前,国内身份认证技术以弱身份认证为主,主要包括用户名/口令认证技术、动态口令认证技术等。用户名/口令的认证方法是最简单也是最常用的认证技术之一,动态口令认证是一种在传统用户名/口令基础上发展起来的,让用户的密码按照时间或者使用次数不断动态变化,实现一次一密的身份认证技术^[7]。参考文献[8]中提出了一种基于智能城市新型公钥加密方案的轻量级相互认证协议(LMA),实现了 ECN 与新 AP 之间的直接相互认证和密钥协商,无需第三方参与。尽管 LMA 已经简化了认证过程,但由于公共密码操作和数字签名验证的开销,它在 CPS 通信中仍然不够有效。

根据应用程序登录方法不同,传统的单点登录(single sign-on, SSO)^[9]方法分为两类:基于脚本和基于访问权限的 SSO 解决方案。基于脚本的 SSO 方法通过脚本自动化登录过程来实现,该方法实现简单,并且兼容多种目标系统,可以直接在目标系统中加入基于脚本的 SSO 方法。但是

基于脚本的 SSO 方法安全性不高,单点登录与自动登录不同,需要考虑的安全因素很多,并且需要安装客户端软件。由于没有修改目标系统,单点注销、集中管理用户身份、安全交换目标系统间用户数据等除 SSO 登录外的其他功能比较难以实现。基于访问票据的 SSO 方法要求目标系统通过升级访问权限来实施 SSO,SSO 服务器负责用户的认证,目标系统通过 SSO 服务器验证访问票据的有效性^[5-6]。目标系统必须遵守基于访问权限的 SSO 标准,比如访问票据的表示、目标系统与 SSO 服务器通信方式、用户与 SSO 服务器通信方式等。该方法实现完整功能的 SSO,并且安全性高,但是需要修改目标系统,把用户身份的验证修改成对访问票据的验证。尤其重要的是该 SSO 标准必须得到软件供应商的广泛接受。

在国内,许多门户网站建立统一认证管理,比如阿里集团将旗下的淘宝、天猫、阿里巴巴、阿里旅游等平台进行统一认证,实现一站式登录;千橡互动集团将人人网和糯米网等进行统一认证;百度将旗下的百度文库、百度贴吧等实现统一认证。在国外,也有很多实际运用 SSO 的案例,比如微软提出的 passport 方法、SUN 公司提出的 Identity Server、麻省理工学院提出的 Kerberos 协议以及耶鲁大学提出的 CAS 协议等,为实现统一认证提出了很好的解决方案。

国外许多大型网络公司已经实现了统一认证系统,比如 Facebook 发布的新移动平台策略以及 Google 旗下的各平台^[10]。

随着信息化技术的不断发展以及对服务水平及质量的不断追求,能源信息系统各自建设起丰富的电子服务渠道,需要建立用户的统一身份认证管理系统,保证多维电子渠道的安全接入,以便优化各互联网电子渠道用户体验,增强能源互联网服务竞争力。

3 统一身份认证系统

为了解决能源信息系统缺乏对各个电子渠道进行统一管理和监测的问题,本文设计了一个基于 PKI 的统一身份认证系统,以 PKI 的证书申请、证书审核、证书签发和证书发放机构为基础,通过随机数应答挑战机制,实现为电子服务渠道中的各种应用提供统一的身份认证服务。图 1 描述了 UAIS 的逻辑结构,即 UAIS 包含认证客户端、认证服务器、票据服务器和需调用的轻量级目录访问协议(lightweight directory access protocol, LDAP)目录服务器。初次进入系统的用户,主动完成一次身份认证过程,就能访问其他授权的电子渠道的所有资源,而不需要主动参与后续的身份认证过程,减少了认证时间,实现了所谓的“一点登录,多点漫游”功能。

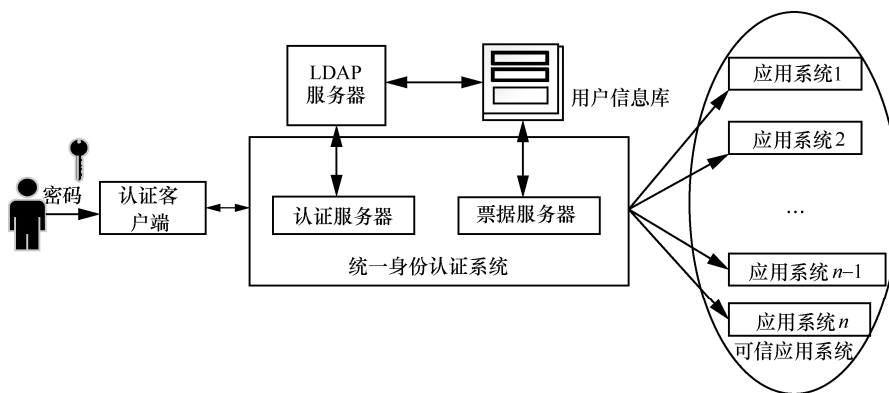


图 1 UAIS 逻辑结构



在 UAIS 中, 用户使用密码登录认证客户端, 认证客户端将用户信息发送给身份认证服务器。身份认证服务器连接 PKI 和 LDAP 服务器以完成与用户的双向认证, 如果通过认证, 则进入票据服务器, 票据服务器实现“一点登录, 多点漫游”。认证客户端提供简洁可操作的交互界面, 管理用户登录。身份认证服务器的主要功能是验证客户端证书的有效性, 进而实现与客户端的安全交互。验证证书的有效性包含验证证书链、证书的有效期、证书黑名单和证书持有者。CRL (证书吊销列表) 和证书链存储在本地, 并定期将新 CRL 下载到 LDAP^[11]。身份验证成功后, 系统将进入票据服务器, 如果失败, 则返回用户登录界面。UAIS 的认证方法符号描述见表 1。

表 1 UAIS 需要的符号描述

符号	描述
$A \rightarrow B : M$	A 发送消息 M 给 B
N_A	由 A 生产的随机数
$E_K(M)$	公共密钥 K 加密消息 M
$\{M\}_K$	对称密钥 K 加密消息 M
$\text{Sig}_A(M)$	A 创建的对消息 M 的数字签名
C_A	A 的证书

认证协议工作流程如图 2 所示, UAIS 交换信息见表 2。首先, 用户发送认证请求, 认证请求消

息包含用户证书、用户产生的随机数、安全属性, 并使用 Rivest、Shamir 和 Adleman (RSA) 等方法实现对随机数签名, 从而确保证书请求消息的真实性。

表 2 UAIS 交换信息

过程	信息
认证请求	$U \rightarrow AS : \text{Cert}(U), N_U, \text{Capabilities}, \text{Sig}_U(N_U)$
认证回复	$AS \rightarrow U : \text{Cert}(AS), N_U, N_{AS}, E_U(AK), \text{Lifetime}, \text{SID}, \text{Sig}_{AS}(N_U, E_U(AK))$
密钥确认	$U \rightarrow AS : N_{AS}, \text{ID}_U, \{N_{AS}, \text{ID}_U\}_{AK}$

认证服务器接收到认证请求消息后, 验证用户证书的合法性, 包括以下步骤。

(1) 验证证书是否由受信任的证书颁发机构 (CA) 颁发, 该 CA 涉及整个证书链的身份验证。如果无法直接信任证书, 它将继续搜索查找, 直到找到其信任的 CA 或根 CA。

(2) 如果查找到用户证书由受信任的 CA 颁发, 则解析证书以获取证书的内容, 证书内容包含服务器证书结构、服务器名、序列号、CRL、用户公共密钥等。

(3) 验证证书的序列号是否有效, 检查 CRL 以查看证书是否无效。

(4) 查询 LDAP 服务器的用户列表以确定用户是否是注册的合法用户。

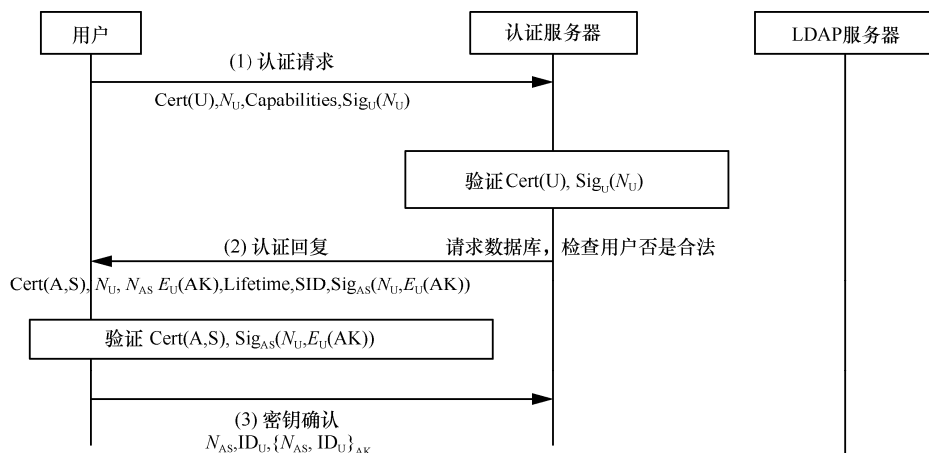


图 2 认证协议工作流程

如果证书验证失败,则服务器拒绝用户登录。如果证书验证成功,服务器验证认证请求消息的签名,签名验证后,认证服务器确定了与用户共享的加密算法和协议,并为用户激活认证密钥(AK);然后,使用用户公钥对其进行加密,并在认证回复消息中将其发送回用户。认证回复消息包括AS证书、用户公钥加密的AK,用于区分连续AK的AK序列号、AK有效时间、AS生成的随机数以及用户的随机数及RSA的签名,以确保认证回复消息的真实性。

最后,用户发送密钥确认,密钥确认包括用户的身份证号、认证回复消息中接收的随机数以及AK对这两个值的加密,以保证消息的真实性。AK是用户和AS的新会话密钥,用于进一步的通信。该过程采用随机数应答挑战机制,可以有效解决网络应用系统中通信方的双向身份认证问题,避免虚假网站、恶意服务器伪装、中间人攻击、重放攻击、SVM(support vector machine,支持向量机)扰动攻击以及移动系统恶意应用安全等安全问题^[12-14]。

票据服务器包含票据发行模块和票据解析模块。当用户与认证服务器完成双向认证后触发票据发行,票据发行即票据发行模块生产用户的认证凭证(即票据),存储在用户信息库中,票据包含用户的基本信息、登录信息、权限属性和其他可访问的电子渠道列表。而票据解析模块分析用户的登录票据并确定其特定的专用电子渠道,保障只有相应的电子渠道才能对其进行解密,防止用户信息泄露。

4 BAN 逻辑正确性分析

使用BAN逻辑验证UAIS方法的正确性。BAN逻辑是用于推理信任、加密和协议的形式化逻辑。BAN逻辑由Burrows、Abadi和Needham^[9]提出。BAN逻辑用于证明协议的执行是否可以实现预期目标并找到协议设计缺陷。BAN逻辑有特

定的逻辑符号和逻辑规则,并把所有的消息转换成相应的形式语言。采用BAN逻辑分析特定协议,首先根据逻辑符号理想化协议、做出合理的假设,然后运用逻辑规则,把协议进行理想化,通过假设推断具体协议能否达到预期目标。使用BAN逻辑验证UAIS方法的目标是经过认证协议的执行,通信双方能完成相互认证,并确保共享一个新的会话密钥。

为简便起见,A代表用户,B代表认证服务器AS。所提出的统一认证方法的目标如下:

$$A \models A \leftrightarrow B, B \models A \leftrightarrow B$$

UAIS方法的理想化协议如下所示:

认证请求: $A \rightarrow B: E_{CA^{-1}}(\overset{K_A}{\rightarrow} A, A), \text{Sig}_A(N_A)$;

认证回复: $B \rightarrow A: E_{B^{-1}}(\overset{K_B}{\rightarrow} B, B), E_A(AK), \text{Sig}_B(N_A, E_A(AK))$;

密钥确认: $A \rightarrow B: \{N_B, A\}_{AK}$ 。

在理想化协议中去掉了没有加密的部分,即对验证过程没有意义的部分。用户证书主要包含用户的公共密钥和身份证号,并使用CA对其加密。假设每个角色都知道CA的公钥和自己的私钥,并相信自己产生的随机数是最新的,而AK是由B生成的。做出的假设如下:

$$A \models \overset{K_A}{\rightarrow} A, B \models \overset{K_B}{\rightarrow} B, A \models \overset{K_{CA}}{\rightarrow} CA, B \models \overset{K_{CA}}{\rightarrow} CA,$$

$$A \models \overset{K_A}{\rightarrow} A, A \models \#(N_A), B \models \#(N_B),$$

$$A \models (B \Rightarrow \overset{AK}{(A \leftrightarrow B)}), B \models (B \Rightarrow \overset{AK}{(A \leftrightarrow B)})$$

UAIS方法的形式化分析如下所示。

在认证请求中,利用消息含义规则以及假设得出式(1):

$$B \models \overset{K_A}{\rightarrow} A, B \triangleleft N_A, B \models (A \sim N_A) \quad (1)$$

在认证回复中,利用消息含义规则以及假设得出式(2):



$$A \models \xrightarrow{K_B} B, A \triangleleft (AK, N_A) \quad (2)$$

N_A 是 A 发送给 B 的, 并且只发送给 B, 所以当 A 接收到 N_A 时, A 使用随机数 N_A 相信认证回复消息是 B 发送的, 即得出式 (3):

$$A \models (B \sim (A \leftrightarrow B))^{AK} \quad (3)$$

利用新鲜规则以及 $A \models \#(N_A)$, 得出式 (4):

$$A \models \#(A \leftrightarrow B)^{AK} \quad (4)$$

使用随机数验证规则以及式 (3) 和式 (4), 得出式 (5):

$$A \models B \models (A \leftrightarrow B)^{AK} \quad (5)$$

根据管辖规则和假设 $A \models (B \Rightarrow (A \leftrightarrow B))^{AK}$, 得出式 (6):

$$A \models (A \leftrightarrow B)^{AK} \quad (6)$$

在密钥确认中, 利用消息含义规则, 得出式 (7):

$$B \triangleleft A, N_B \quad (7)$$

由于 B 只发送 N_B 给 A, 将接收到的 N_B 与之前发送出的 N_B 进行对比, 如果相同, 则表示 B 确认 A 接收到了 AK, 所以得出式 (8):

$$B \models A \models (A \leftrightarrow B)^{AK} \quad (8)$$

使用 N_B 和管辖规则, 得出式 (9):

$$B \models (A \leftrightarrow B)^{AK} \quad (9)$$

得出了式 (6) 和式 (9), 即 UAIS 认证协议的目标, 如式 (10) 所示:

$$A \models A \leftrightarrow B, B \models A \leftrightarrow B^{AK} \quad (10)$$

在 UAIS 方法中, 用户和认证服务器不仅完成了相互认证, 同时也完成了密钥确认。

5 UAIS 的安全性分析

本节将根据用户相互认证、重放攻击和中间人攻击来分析 UAIS 方法的安全性能。在分析过程中, 假设用户和认证服务器 AS 在两个不同的会话中生成相同随机数的概率非常小; 只有证书所有者拥有相应的私钥, 其他实体拥有公钥, 但是获得私钥的可能性很小。

5.1 相互认证

UAIS 方法的主要目标是协议完成后, 用户和 AS 达到相互认证。首先, AS 和用户交换证书, 验证证书后获得彼此的公共密钥, AS 只授权给拥有合法证书的用户。在认证请求和认证回复消息中加上签名以保证消息的真实性。在认证回复时, 用用户公共密钥加密的 AK 以确保只有拥有对应私密的用户才能获得 AK、AS 产生的随机 N_{AS} 以及对认证回复消息的签名。当 AS 接收到从用户发送的密钥确认消息, 用 AK 解密获得 N_{AS} , 如果接收的 N_{AS} 和发送的 N_{AS} 相同, 则 AS 确定此消息是由用户发送的, 因此 AS 认证用户, 并且确认用户已经获得了 AK。用户通过同样的方法来认证 AS。通过随机数挑战一应答机制, AS 和用户完成相互认证, 阻止潜在的恶意攻击。

5.2 重放攻击

攻击者通过恶意地重传或重放以前发送过的消息来实现重放攻击, 是常见网络攻击的一种。在 UAIS 方法中, 通过使用随机数挑战一应答机制, AS 和用户产生随机数确保消息是最新的, 在不同的会话中, 产生的随机数不一样。在认证请求消息中, 用户发送新产生的随机数 N_U , 并用私钥加密消息, 即对消息进行签名以保证消息的真实性。在认证回复消息中, 用户接收到随机数 N_U , 比较接收到的随机数 N_U 与发送的随机数 N_U , 如果一致, 则判定接收到的消息是最新的。在密钥确认阶段, AS 通过比较发送的随机数 N_A 和接收到的随机数 N_A 是否一致来确认此消息是否是最

新的, 并且判定此消息是由用户发送的。所以, UAIS 能够抵抗重放攻击。

5.3 中间人攻击

主动拦截攻击之一就是常见的 MITM (man-in-the-middle, 中间人) 攻击。在 MITM 攻击过程中, 通过拦截正常的网络通信数据, 并进行数据篡改和嗅探, 而通信的双方却毫不知情。攻击者可以接收两个受害者之间交换的所有消息, 并在他们之间添加新消息。在 UAIS 方法中, 发送者对认证请求消息和认证回复消息进行签名, 以确保消息的真实性。在认证请求阶段, 攻击者无法改变用户的签名消息, 同样地, 在认证回复阶段, 由于攻击者没有 AS 和用户的私钥, 攻击者不能改变 AS 的签名消息以及解密所有用户利用公共密钥加密的消息; 通过验证签名消息, 用户能判断认证回复消息是否是由 AS 发送的。同样地, AS 通过由 AS 颁发的一次性对称密钥加密的密钥确认消息验证用户的身份。因此, UAIS 能够抵抗 MITM 攻击。

6 UAIS 的性能分析

本节从加密操作数和认证时延两个方面比较 UAIS 和 LMA^[11]方法的性能。基本加密操作数包括以下 6 种: 证书验证 (CERT)、对称密钥加密和解密 (SED)、RSA 公共密钥加密 (RSE)、RSA 公共密钥解密 (RSD)、数字签名 (SIG)、数字签名验证 (VER)。在这 6 种基本加密操作中, 由于公钥解密算法的复杂度低、公钥加密算法的复杂度低, 而签名算法复杂度低、验证签名算法复杂度低, 所以公钥解密操作和数字签名操作花费的时间比其他加密操作长。表 3 描述了 UAIS 方法的各个加密操作个数以及基本加密操作花费的时间, 根据参考文献[10], 模拟环境使用 Windows Vista 32 bit, 处理器是 VC2005 SP1, Intel Core 2 1.83 GHz, 用 C++ 编写算法。

表 3 UAIS 方法加密操作

	UAIS		LMA		时延	
	AS	UE	AS	UE	AS	UE
CERT	1	1	1	1	0.07 ms	0.13 ms
SED	1	1	2	2	1.074 μ s	0.546 μ s
RSE	1	0	2	2	0.07 ms	0.13 ms
RSD	0	1	2	2	1.52 ms	3.01 ms
SIG	1	1	1	1	1.42 ms	3.02 ms
VER	1	1	1	1	0.07 ms	0.13 ms

接下来分析在没有攻击的情况下, UAIS 方法的认证过程的时延指在客户端或 AS 端完成认证计算所需的时间 T_{auth} 。 T_{auth} 由所有加密操作所花费的时间决定, 包含证书验证、公钥加密/解密、数字签名和签名验证以及对称密钥加密/解密所花费的时间。

T_{auth} 由式 (11) 决定:

$$T_{\text{auth}} = T_{\text{CERT}} + T_{\text{SED}} + T_{\text{RSE}} + T_{\text{DEC}} + T_{\text{SIG}} + T_{\text{VER}} \quad (11)$$

由表 3 和式(11)可以得出 UAIS 方法和 LMA 的认证过程所花费的时间大约是 7.92 ms 和 14.3 ms, 即式 (12) 和式 (13):

$$T_{\text{auth}}^{\text{UAIS}} = t_{\text{CERT_AS}} + t_{\text{CERT_UE}} + t_{\text{SED_AS}} + t_{\text{SED_UE}} + t_{\text{RSE_AS}} + t_{\text{RSE_UE}} + t_{\text{SIG_AS}} + t_{\text{SIG_UE}} + t_{\text{VER_AS}} + t_{\text{VER_UE}} = 7.92 \text{ ms} + 1.62 \mu\text{s} \quad (12)$$

$$T_{\text{auth}}^{\text{LMA}} = t_{\text{CERT_AS}} + t_{\text{CERT_UE}} + 2t_{\text{SED_AS}} + 2t_{\text{SED_UE}} + 2t_{\text{RSE_AS}} + 2t_{\text{RSE_UE}} + 2t_{\text{RSD_AS}} + 2t_{\text{RSD_UE}} + t_{\text{SIG_AS}} + t_{\text{SIG_UE}} + t_{\text{VER_AS}} + t_{\text{VER_UE}} = 14.3 \text{ ms} + 3.24 \mu\text{s} \quad (13)$$

然后, 在恶意攻击可能出现的前提下分析 UAIS 方法的性能。认证过程不能被认证方法抵抗的攻击 (如重放攻击和中间人攻击等) 中断, 但是可能被一些未知的或者新的恶意攻击中断。新的且不可预测的恶意攻击被称为未知攻击; 能够通过安全分析防止的常见攻击被称为已知攻击。如果已知攻击攻击 UAIS 和 LMA 认证过程, 则成功的 UAIS 和 LMA 的认证时延是固定的; 否则成功的 UAIS 和 LMA 的认证时延是随机的。UAIS



和 LMA 可能在任何验证阶段被一个未知攻击所中断。改变未知攻击的比例来分析 UAIS 和 LMA 认证方法的性能。并执行这 3 种方法 10 000 次, 即 $\text{Time}_{\text{ALLATTACK}} = 10\,000$, 衡量性能的参数是平均成功认证时延, 定义如式 (14) 所示:

$$\text{Delay}_{\text{AVG}} = \frac{\text{Delay}_{\text{UNKNOWN}} \times \text{Times}_{\text{UNKNOWN}} + \text{Delay}_{\text{KNOWN}} \times \text{Times}_{\text{KNOWN}}}{\text{Times}_{\text{KNOWN}}} \quad (14)$$

其中, $\text{Times}_{\text{UNKNOWN}} = \text{Ratio}_{\text{UNKNOWN}} \times \text{Times}_{\text{ALLATTACK}}$ 。

图 3 显示了仿真结果。由于 UAIS 方法可能不能抵抗未知攻击, 所以一个成功的认证过程所花的时间是随机的, 即随着未知攻击比例的增大, 平均成功认证时延也会增大。但是在未知攻击比例的情况下, UAIS 平均成功认证时延只有 LMA 的一半。

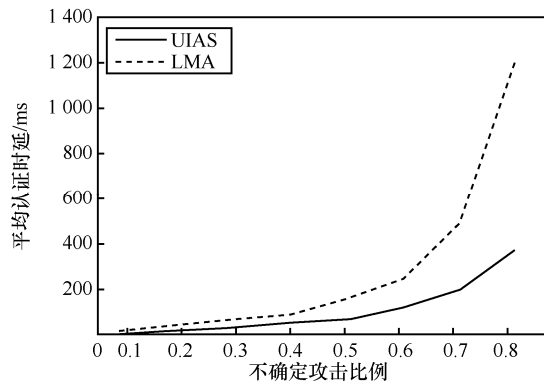


图3 未知攻击情况下的平均认证时延比较

7 结束语

本文提出了一种基于 PKI 的统一身份认证方法, 有效地解决了能源信息系统各电子渠道统一管理的问题, 分析结果表明 UAIS 在完成相互认证和保持会话密钥一致性的同时, 能够抵抗重放攻击和中间人攻击。用户可以利用该认证方法直接访问每个应用系统, 并在没有多个认证过程的情况下在应用系统之间执行快速且安全的切换。该方法可以为用户开展从事复杂业务信息化的安

全访问认证提供便利性和安全性。

参考文献:

- [1] 刘林, 张运洲, 王雪, 等. 能源互联网目标下电力信息物理系统深度融合发展研究[J]. 中国电力, 2019, 52(1): 1-9.
LIU L, ZHANG Y Z, WANG X, et al. Research on deep integration of power cyber physical system under energy internet goals[J]. Electric Power, 2019, 52(1): 1-9.
- [2] 王继业, 孟坤, 曹军威, 等. 能源互联网信息技术研究综述[J]. 计算机研究与发展, 2015, 52(3): 1-18.
WANG J Y, MENG K, CAO J W, et al. Research on information technology for energy internet: a survey[J]. Journal of Computer Research and Development, 2015, 52(3): 1-18.
- [3] 陈国慧, 谭海波, 吕波, 等. 基于 CAS 和 Liferay 门户的统一身份认证系统[J]. 计算机技术与发展, 2018(12): 106-110.
CHEN G H, TAN H B, LV B, et al. Unified identity authentication system based on CAS and Liferay portal[J]. Computer Technology and Development, 2018(12): 106-110.
- [4] 王栋, 陈传鹏, 颜佳, 等. 新一代电力信息网络安全架构的思考[J]. 电力系统自动化, 2016, 40(2): 6-11.
WANG D, CHEN C P, YAN J, et al. Pondering a new-generation security architecture model for power information network[J]. Automation of Electric Power Systems, 2016, 40(2): 6-11.
- [5] WANG Z Z, WANG Y. Research and design of campus network unified identity authentication system based on Kerberos[J]. Advanced Materials Research, 2012(4): 546-547.
- [6] FENG F, LI X, WANG L. Design and implementation of identity authentication system based on fingerprint recognition and cryptography[C]//IEEE International Conference on Computer & Communications, August 11-13, 2017, Chengdu, China. Piscataway: IEEE Press, 2017.
- [7] KIM N Y, PARK K Y, PARK J H. DOTP-AaaS: dynamic one time password matching-based authentication as a service[Z]. 2017.
- [8] LI N, LIU D, NEPAL S. Lightweight mutual authentication for IoT and its applications[J]. IEEE Transactions on Sustainable Computing, 2017(2): 359-370.
- [9] BURROWS M, ABADI M, NEEDHAM R. A logic of authentication[J]. ACM Transactions on Computer Systems, 1989, 23(5): 1-13.
- [10] 黄飞飞. 基于 SOA 架构的企业统一用户身份认证平台研究[J]. 中国管理信息化, 2016, 19(19): 56-58.
HUANG F F. Research on enterprise unified user identity authentication platform based on SOA architecture[J]. China Management Informatization, 2016, 19(19): 56-58.
- [11] DANIEL E, VASANTHI N A. LDAP: a lightweight

deduplication and auditing protocol for secure data storage in cloud environment[J]. Cluster Computing, 2017(4): 1-12.

- [12] ZENG K, GOVINDAN K, MOHAPATRA P. Non-cryptographic authentication and identification in wireless networks[J]. IEEE Wireless Communications, 2010, 17(5): 56-62.

- [13] 钱亚冠, 关晓惠, 吴淑慧, 等. 一种基于贪心算法的 SVM 扰动攻击方法[J]. 电信科学, 2019, 35(1): 81-89.

QIAN Y G, GUAN X H, WU S H, et al. A SVM perturbation attack method based on greedy algorithm [J]. Telecommunications Science, 2019, 35(1): 81-89.

- [14] 陈铁明, 项彬彬, 吕明琪, 等. 基于字节码图像和深度学习的 Android 恶意应用检测[J]. 电信科学, 2019, 35(1): 9-17.

CHEN T M, XIANG B B, LV M Q, et al. Android malicious application detection based on bytecode image and deep learning [J]. Telecommunications Science, 2019, 35(1): 9-17.

[作者简介]



汤阳 (1988-), 男, 广东电网有限责任公司佛山南海供电局工程师, 主要研究方向为电力通信技术、信息安全、用电管理。



张翼英 (1973-), 男, 博士, 天津科技大学计算机科学与信息工程学院特聘教授, 主要研究方向为物联网及其安全、安全密钥、智能电网、信息安全等。



何业慎 (1979-), 男, 博士, 深圳市国电科技通信有限公司营销总监、科学技术部总经理, 主要研究方向为智能电网通信技术、系统集成技术、物联网及安全技术、智能安防技术等。



王聪 (1988-), 女, 博士, 天津科技大学计算机科学与信息工程学院讲师, 主要研究方向为物联网、信息安全、边缘计算安全等。

雷明 (1985-), 男, 深圳市国电科技通信有限公司助理工程师, 主要研究方向为电力线通信技术、用电管理、项目管理。