Computer Science and Application 计算机科学与应用, 2016, 6(6), 347-353
Published Online June 2016 in Hans. http://www.hanspub.org/journal/csa
http://dx.doi.org/10.12677/csa.2016.66043

Hans汉斯

A Study on Security Strategies of Educational Electronic Identity Authentication System

Qinghua Zhou, Lei Liu, Yongjun Wen, Junlong Tang, Lijun Tang

Department of Physics and Electronics, Changsha University of Science and Technology, Changsha Hunan
Email: qqted@qq.com

Received: Jun. 2nd, 2016; accepted: Jun. 19th, 2016; published: Jun. 23rd, 2016

Abstract

The authentication system of educational electronic identity covers various aspects in daily operations of educational application system in which authentication is served by e²ID. Therefore, its security assurance and steady operation are extremely important. This paper analyzes a variety of security risks in the educational electronic identity authentication system, and puts forward safety strategies from both the management and technical measures.

Keywords

Educational Electronic-ID, Network Security Strategy, Secure Transmission of Data

教育电子身份认证系统的安全策略研究

周庆华，刘　磊，文勇军，唐俊龙，唐立军

长沙理工大学，物理与电子科学学院，湖南　长沙
Email: qqted@qq.com

收稿日期：2016年6月2日；录用日期：2016年6月19日；发布日期：2016年6月23日

摘　要

教育电子身份认证系统涵盖了以e²ID提供认证服务的教育应用系统日常运行的方方面面，因而保障其安

文章引用: 周庆华, 刘磊, 文勇军, 唐俊龙, 唐立军. 教育电子身份认证系统的安全策略研究[J]. 计算机科学与应用, 2016, 6(6): 347-353. http://dx.doi.org/10.12677/csa.2016.66043

全、稳定地运行显得尤为重要。本文分析了教育电子身份认证系统存在的各种安全隐患，从管理和技术两方面提出了保障教育电子身份认证系统安全、稳定运行的安全策略。

关键词

教育电子身份号，网络安全策略，数据安全传输

1. 引言

目前电子身份认证技术有 eID 认证技术、OpenID 技术等，其性能品质较优。其中，杨明慧[1]等论述的德国 eID 机制，目前由公安部第三研究所根据我国国情进行研发，现处于初步发展、试点应用阶段。沈保全[2]分析运用的 OpenID 技术，它是一个去中心化的网上身份认证系统，实现了网络用户方便、安全的身份认证，但是也存在一些不足：任何人都可以建立一个网站提供 OpenID 验证服务，而网站性能参差不齐，导致 OpenID 的验证过程不是很稳定；且存在较严重的中间人攻击安全风险。而目前我国网络身份认证更多的是采用用户名/密码组合、动态口令、智能卡等，前者容易遭到各种攻击，后者适用范围狭小，不利于推广。基于此湖南省推出了教育电子身份号(Education Electronic Identity)，简称为 e^2ID。e^2ID 是根据个人基础信息(身份证号)的散列值和随机数字生成的标识码，用于标识网络空间中的个人身份，通过非对称加密技术由身份证号单向生成，共 12 位[3]。e^2ID 与身份证号一一对应，个人凭 e^2ID 登录网络空间，而 e^2ID 本身是公开的身份标识号，并不涉及个人隐私，可以有效保证个人信息隐私安全[4] [5]。由于网络安全隐患日益突出，教育电子身份认证系统也面临着越来越多的安全问题。例如在教育电子身份认证系统，需要单位管理员单条或批量录入个人基础信息，通过 e^2ID 引擎，得到包含 e^2ID 的个人信息列表文件，由于互联网环境的开放性，使得经由教育电子身份认证系统的用户隐私数据面临着外界的威胁。如何保证教育电子身份认证系统安全稳定运行以及实现数据的保密性、完整性和有效性成为了重要的研究内容[6]。本文从技术和管理两个方面探讨了教育电子身份认证系统的安全隐患，并提出了教育电子身份认证系统的安全防范策略。

2. 教育电子身份认证系统中存在的安全隐患分析

目前教育电子身份认证系统根据系统功能划分，系统的参与者共有如下五类：个体、单位管理员、居民服务中心、系统管理员、第三方应用系统。系统顶层用例如图 1 所示。其中四类用户对系统的访问权限有较大区别：系统管理员对数据库系统拥有绝对访问权限，除了读、写和修改数据库的权限，还能为其他系统用户分配权限；居民服务中心只对特定数据拥有读权限或者少量的写权限，并且只能对数据库系统内有限的特定资源进行访问；然而个体和单位管理员处在不同的地域，他们只能通过互联网进行访问，这就决定了其在地理上可以是分散的，终端环境得不到有效控制。这就要求系统有较高的可靠性、安全性和稳定性，并且在高并发、重负载下具有良好的安全性能。

2.1. 物理层安全隐患分析

(1) 系统工作环境的安全隐患

系统工作环境的安全隐患包括：因地震、火灾、雷击、静电、温度、湿度等非人为灾害性事故导致的软硬件设备故障或损坏；因电磁泄漏、剩磁效应、网络设备老化、机房屏蔽性能差等引起静电干扰或外界的电磁干扰使系统软硬件不能正常工作等。

(2) 系统工作设备的安全隐患

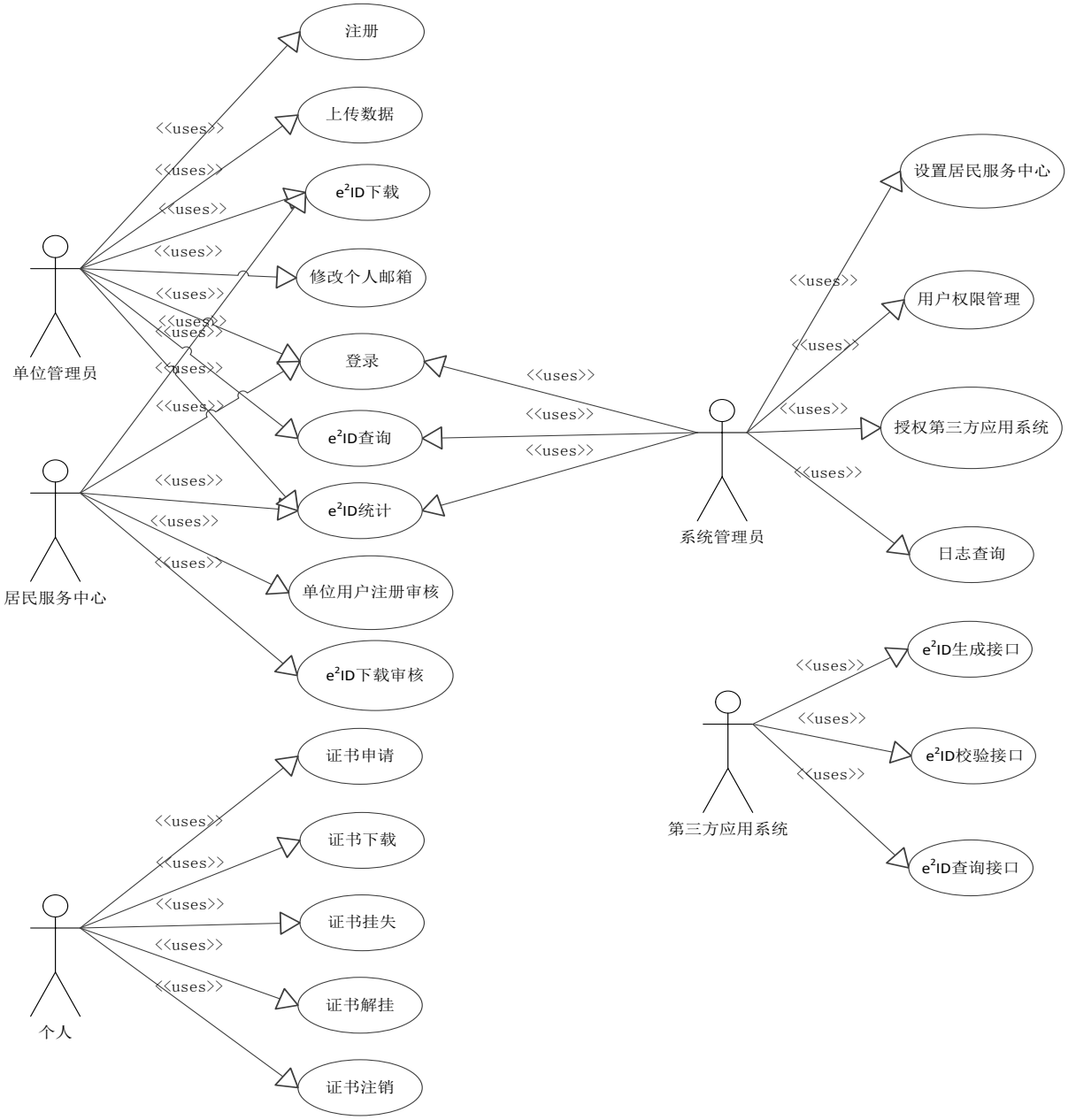

Figure 1. Use case diagram: educational electronic identity authentication system
图 1. 电子身份认证系统顶层用例图

系统工作设备的安全是网络应用系统安全运营的前提，其工作设备包括服务器、通讯组件等硬件设备。其自身的稳定性、安全性将直接或间接地影响教育电子身份认证系统能否稳定有序地工作。例如，路由设备信息泄漏，服务器主机端口配置隐患等。

2.2. 管理层安全隐患分析

教育电子身份认证系统涉及各个级别、各个权限且身份不同的用户，通过系统管理员分配不同的权限进行相应操作。在日常使用过程中，经常出现这样的现象：用户帐号或密码由于设置过于简单、遭到泄露、没有安全退出应用系统等都将直接影响到数据安全；教育电子身份认证系统工作人员利用职务之

便而越权操作、窃取信息、非法获得密文密钥等；部分内部人员有非法企图，向系统中投放木马病毒等，对数据进行破坏；由于部分新进管理员，出现操作不当或失误，导致系统崩溃、数据损坏。而上述这些现象在管理上却没有相应的制度来约束。因此，要将制度管理和技术方案相结合来保障系统数据安全。

2.3. 应用层安全隐患分析

(1) 身份认证与授权控制的安全隐患

目前教育电子身份认证系统登录和服务器主机登录使用的是用户名和密码结合的方式，这种静态口令单一、形式固定，且其通过数据库进行存储。这种形式存在的口令很容易被网络窃听、非法访问、穷举攻击等手段截获。使用截获的口令可以轻易登录管理系统，可能导致用户的基础信息泄漏或系统的破坏。

(2) 信息传输的完整性隐患

目前通过教育电子身份认证系统申请 e^2ID 的流程是由单位管理员整理区域用户信息进行单条或批量申请。该过程首先由单位用户组织区域用户基础信息(包括身份证号、姓名、性别等)形成 xls 表格，上传至教育电子身份认证系统，系统通过 e^2ID 引擎，生成 e^2ID 并入原始 xls 表格，并返回给单位管理员。xls 表格在互联网上进行传输时，互联网本身的特性决定了这些包含用户隐私信息的 xls 表格在传输过程中存在被窃听或被篡改的可能性。

3. 教育电子身份认证系统的安全防御策略与实现

3.1. 环境和设备的安全策略与实现

环境和设备安全是为了保障硬件设备安全稳定运行免受自然灾害、人为盗窃、恶意窃听等攻击。同时，要定期对数据进行备份，出现这些不可避免的破坏时，使用备份数据可以快速恢复受损数据，减少损失。在数据备份的同时需要考虑备份库的数据能不能完全替换生产库，两库的数据是否能够实现实时共享，备份的频率是否能符合预期的设计。数据备份的方式有很多种，像教育电子身份认证系统，数据量大、分布集中、需要备份的数据库服务器比较多，采用增量备份与完全备份相结合的异地备份策略实现数据安全预期设计的目标。同时为了实现数据请求零误差，在系统部署上线之前需要制定数据恢复应急预案[7]。

3.2. 管理层安全策略与实现

安全防护如果仅仅从技术方面进行考虑，很难充分保障系统绝对安全，还需要从系统维护管理人员方面进行考虑，只有在保证技术安全的同时建立和完善管理策略，才能最大限度实现系统的安全稳定运行。

在管理上提升现有教育电子身份认证系统管理人员的计算机应用能力。要求其不仅懂得 e^2ID 生成管理的相关业务知识，还应懂得计算机网络的专业知识。要求系统运维人员能不定期对上述安全策略的实施过程与结果进行数据采集与分析，并根据分析结果对安全策略进行实时调整和优化。

3.3. 应用层安全策略与实现

身份认证与授权控制的安全策略包括：(1) 用户口令安全策略：增加认证因子，结合 USBKey，同时对用户的口令进行检查，且对于口令强度不够的，强制要求用户进行更改，同时要求用户定期更换新的安全口令；在用户拥有 USBKey 操作权限及正确口令的情况下，方可允许用户正常登录。(2) 用户权限访问控制策略：采用基于角色权限访问控制策略，减少用户有意或无意的操作给系统带来的破坏。

数据安全传输策略可以考虑根据 PKI 公钥基础设施建立基于 SSL/STL 虚拟专用网，通过构建加密传输通道的方式来消除数据或文件在传输过程中的安全隐患。

3.3.1. 身份认证与授权控制的安全策略实现

当系统面向互联网用户时，用户环境比较复杂，如果此时用户处理重要数据(如居民身份证号、姓名等 xls 文件)，系统的资源将直接展现给用户，将可能带来重大安全隐患，因此这种场景下，需要对用户加强身份认证。其具体流程如图 2 所示。

用户安全访问的具体过程如下：

(1) 在客户端：digest_X = QUERY_X (硬件序列号+数据)，以硬件序列号和标识用户权限的数据为因子根据存储在 USBKey 中的私钥 KeyID 返回算法计算结果摘要；

(2) 在服务端：根据接收到的硬件序列号和标识用户权限的数据，取出存储在服务器数据库中的公钥 KeyID；根据 digest_Y = QUERY_Y (硬件序列号+数据)得到新的摘要信息；

(3) 如果在客户端生成的消息摘要和在服务器端生成的消息摘要一致，即：digest_X = digest_Y；则说明验证通过。

(4) 通过 USBKey 的验证之后，方可对系统资源进行访问。否则不能进行数据访问或修改等操作。

用户进行访问操作前，首先需要确定用户的角色，根据角色提供相应的访问权限。然后提供相应的菜单，让其对相应权限进行操作。

3.3.2. 信息传输的完整性的安全策略实现

采用 PKI 公钥基础设施[8]主要基于以下考虑：由于上传和下载的 xls 文件大，不能运用复杂耗时的加密算法，基于对称加密和非对称加密算法考虑，应该采用对称加密算法，节约加密时间成本；而仅仅依靠对称加密的方式安全级别不够，因此，在设计数据传输安全时，本文考虑使用对称加密算法和公钥加密算法相结合的方式，图 3 清晰地描述了加密过程。

结合对称加密和公钥加密两种算法，一则可通过公钥来加密对称加密密钥保证了密钥传输过程的安全，二则在对称加密密钥完好无损的情况下，将密文被破解的隐患降到了最低。从而完成了数据安全传输的任务，其具体过程如下：

(1) 首先在客户端完成两步加密过程：第一步通过脚本生成对称加密密钥，将原文和生成的对称加密

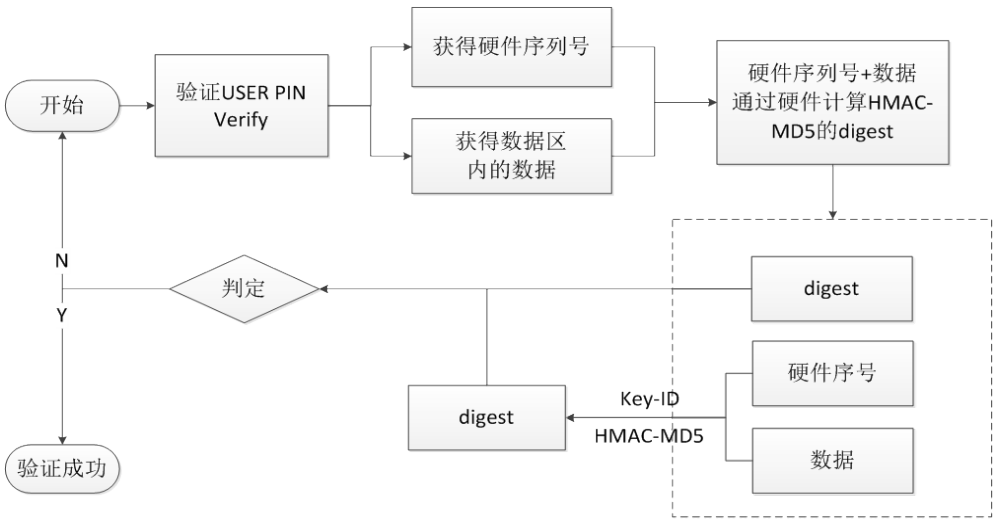

Figure 2. Flowchart: Secure assessment for users
图 2. 用户安全访问流程图

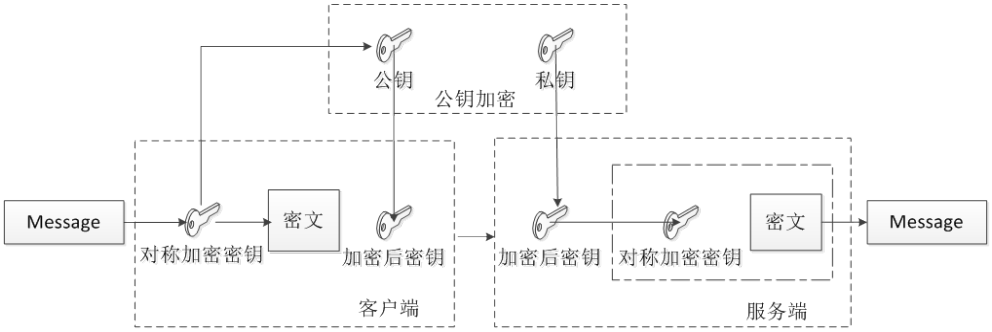

Figure 3. Conceptual drawing: Secure transmission with two encryption schemes combined
图 3. 两种加密方式结合的安全传输方案图

密钥作为输入，得到密文；第二步通过从 CA 得到的公钥将对称加密密钥进行加密，得到加密后的对称加密密钥。然后将加密后密钥附着在密文后面传输给服务端。

(2) 同样在服务端完成两步解密过程：首先将传输过来的密文和加密后的密钥分离，通过 CA 提供的私钥将加密后的密钥进行解密，得到对称加密密钥原文；接着将对称加密密钥和密文作为输入，得到信息原文，完成加密工作。

该方法很好地实现了要求文件加密且达到一定加密效率的场景下的加密需求，对于解密对称加密密钥，必须要拥有私钥的服务器才能得到对称加密密钥原文，从而解密加密原文。但是该方案中因为公钥是公开的，所以问题在于，任何一方客户端都可以通过公钥来加密对称加密密钥，伪装成真正意义上的客户端，此时可以采取两套防范措施：1、实现传输之前完成用户身份认证；2、通过公钥证书实现客户端和服务端的双向认证。

4. 结束语

本文根据目前教育电子身份认证系统可能存在的安全隐患，从环境和设备、人员管理及系统应用层面等三个方面着手，不仅在系统管理人员方面提出相关建议；且探讨分析了系统在不可抗力损害的情况下，如何利用灾备快速恢复系统正常运行；同时重点探究了应用层的安全风险，通过基于 USBKey 的安全登录模型和利用 PKI 公钥基础设施实现对称加密和公钥加密相结合的高效文件加密方法，有效地预防和控制各类不利于教育电子身份认证系统安全、稳定运行的风险，具有普遍的适用性。

文中提出的安全策略不仅适用于教育电子身份认证系统，也适用于各种 B/S 结构的数据管理系统，对解决各种网络安全问题以及应对教育信息化建设进程中面临的各种挑战，提供了一定的技术支持。

基金项目

国家科技支撑计划课题资助(2014BAH28F04)。

参考文献 (References)

[1] 杨明慧, 刘孟占, 邹翔, 汪志鹏, 饶洁. 德国 eID 机制对我国网络身份管理的启示[J]. 计算机技术与发展, 2014(7): 157-161.

[2] 沈保全. OpenID 第三方认证的应用实践分析[J]. 图书馆建设, 2015(4): 18-20.

[3] 转发关于开展湖南省教育电子身份号应用工作的通知[EB/OL]. http://www.csedu.gov.cn/news/77799.html, 2015-11-05.

[4] 咸立亭. 积极稳妥地开展教育认证系统的建设与应用[J]. 中国教育信息化, 2009(9): 16-20.

[5] 文勇军, 刘磊, 周庆华, 王键, 唐立军. 实名制教育阳光服务平台研究[J]. 中国教育信息化, 2015(5): 73-75.

[6] 吴江, 李太勇, 刘洋洋. 高校教务系统的安全策略研究[J]. 中国教育信息化, 2011(9): 64-66.
[7] 李学刚. Oracle 安全审计技术在教学管理信息系统中的应用研究[D]: [硕士学位论文]. 长沙: 湖南大学, 2011.
[8] 马高扬. 构建安全可信的移动办公系统[J]. 信息安全与通信保密, 2015(12): 90.