电子采购系统动态身份认证策略研究

罗 东[1]，秦志光[2]，马新新[2]

(1. 电子科技大学管理学院 成都 610054; 2. 电子科技大学计算机科学与工程学院 成都 610054)

【摘要】分析了电子采购系统身份认证的常用方式及应用；结合P2DR模型及其体系结构，得出动态身份认证P2DR安全模型；针对电子采购系统的安全需求，提出了基于P2DR的电子采购系统身份认证策略模型。该策略模型根据不同用户在电子采购不同阶段的不同安全需求，综合考虑政策、成本、业务范围等因素，动态调整电子采购系统身份认证形式，实现“安全、成本、效率”的动态平衡。

关 键 词 电子采购系统； 身份认证； 信息安全； 策略
中图分类号 TP389.1 文献标识码 A

Dynamic Identity Authentication Policy of E-Procurement System P2DR Research

LUO Dong[1]，QIN Zhi-guang[2]，MA Xin-xin[2]

(1. School of Management，University of Electronic Science and Technology of China Chengdu 610054;
2. School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu 610054)

Abstract The modes and applications of identity authentication in common used E-Procurement System (EPS) are analyzed in this paper firstly. Then, the dynamic identity authentication policy model is acquired according to Policy, Protection, Detection, and Response (P2DR) model and architecture. Finally, the identity authentication policy model based on P2DR is proposed for the security requirement of EPS. Considering all kinds of factors such as policy, cost, working scope and so on, this policy model can adjust the modes of EPS dynamically and realize the homeostasis among “security, cost and efficiency” for different security requirements and users in each stage of e-procurement.

Key words e-procurement system; identity authentication; information security; policy

电子采购是利用计算机技术或系统代替传统的文书系统，通过网络传输完成采购工作的一种业务处理方式，也称网上采购。它的基本特点是网上寻找供应商和商品、网上洽谈贸易、网上订货甚至网上支付货款，包括目录采购、网上竞价、网上招投标、在线磋商等。电子采购具有交易费用低、时间短、适用范围广、过程透明等传统采购方式无法比拟的优势，已经广泛地应用于企业、政府、国际组织等各种采购主体的各类产品采购中，覆盖了B2B、B2C、B2G、C2C等电子商务模式，在全球范围内呈现逐步取代传统采购方式的趋势。

在传统采购方式向电子采购系统转变的过程中，面对的首要问题是安全问题。安全问题主要来源于两个方面：(1) 互联网本身的不安全；(2) 参与电子采购各方交易数据安全如何保证。安全需求的主要内容包括，参与电子采购各方在网络环境下身份的确认、信息安全传输、采购过程不可抵赖，以及如何保证各采购环节的可靠与可信、有效防范黑客和病毒的攻击、系统安全审计、容灾备份等。

安全策略是为保护信息系统安全而制订的规则和措施的总和，是系统安全的框架和依据。目前，对电子采购系统安全性问题的研究主要集中在如何利用信息安全技术实现系统的安全或防护，而以安全策略为核心来规划、指导系统安全体系建设的研究相对较少。P2DR模型体现了以安全策略为核心，根据安全需求动态调整系统安全措施的指导思想。身份认证作为信息系统安全防护体系的第一道防线，其安全策略对保证电子采购系统的整体安全至关重要。因此，本文拟通过基于P2DR模型的电子采购系统动态身份认证策略的研究，对以安全策略为核心指导信息系统安全体系规划和建设的模式进行探讨。

收稿时间：2007 – 07 – 28
作者简介：罗 东(1972 –)，男，博士生，主要从事信息管理与电子商务方面的研究。

1 电子采购系统身份认证方式及应用

1.1 信息系统主要的身份认证方式及其利弊分析

1.1.1 基于静态口令的认证方式

传统的身份认证技术主要采用基于静态口令的认证方法。这种认证方法由系统事先保存每个用户的用户名、口令。进入系统时用户输入用户名和口令，系统根据保存的用户信息与用户输入的信息相比较，从而判断用户身份的合法性。

基于口令的认证方式是目前普遍使用的身份认证技术，但它存在严重的安全隐患和漏洞：(1) 基于口令的认证是一种单因子的认证，口令一旦泄露，用户即可能被冒充；(2) 用户往往选择简单、容易被猜测的口令，因而不能抵御口令猜测攻击；(3) 口令在传输过程中可能被截获；(4) 系统中所有用户口令以文件形式存储在认证方，攻击者可以利用系统存在的漏洞获取系统的口令文件，即使口令经过加密后存放在口令文件中，口令文件被窃取后也能对系统进行离线字典式攻击；(5) 只能进行系统认证用户的单向认证，攻击者可能伪装成系统骗取用户的口令；(6) 口令对重放攻击无抵抗能力。

1.1.2 基于动态口令的认证方式

为解决基于静态口令认证方式存在的安全问题，特别是解决针对重放攻击的防范，安全专家提出一次性口令(OTP)的动态口令密码体制。OTP认证是一种摘要认证，单向散列函数在其中起着重要作用。OTP的主要思路是在登录过程中加入不确定因素，使每次登录过程中传送的信息都不相同，以提高登录过程的安全性。例如，登录密码=MD5(用户名+密码+时间)，系统接收到登录口令后以同样的算法做一个验算即可验证用户的合法性。

OTP较基于静态口令的方式安全性有较大的提高，但OTP认证只支持服务器对用户的单方面鉴别，无法防范假冒服务器欺骗合法用户。另外，如果客户端与服务器端的时间或次数不能保持良好的同步，就可能发生合法用户无法登录的问题。

1.1.3 基于物理证件的认证方式

基于物理证件的认证方式采用硬件的方式对用户身份的合法性进行认证。目前常采用的物理证件有智能卡、USBKey等。基于物理证件的物理安全性验证用户的身份，没有管理中心发放的物理证件则不能访问系统资源，即使物理证件丢失，入侵者仍然需要猜测用户口令。

基于物理证件的认证方式是基于PIN+物理证件的双因子认证，PIN或物理设备被窃取，用户仍不会被冒充，比基于口令的认证方式具有更好的安全性。但由于每次从IC卡中读取的数据是静态的，通过内存扫描或网络监听等技术，用户的身份验证信息还是很容易被截取，安全隐患依旧存在。

1.1.4 基于数字证书的认证方式

基于数字证书的认证方式通过认证中心(CA)事先为客户签发数字身份证明，当客户和服务器彼此需要进行身份验证时，可分别从CA获取对方的数字证书。在会话和通信时首先交换身份证明，其中包含将各自的公钥交给对方，然后才使用对方的公钥验证对方的数字签名，交换通信的加密密钥等。在确定是否接受对方的身份证明时，还需检查有关服务器，以确认身份证明是否有效。这种身份认证方式基于CA的双向、双因子认证，交易双方需同时具备私钥、身份数字证书。相对于传统用户名加密码的身份认证方式，以CA为中介的身份认证的安全性明显增强。

1.1.5 基于生物特征的认证方式

基于生物特征的认证方式以人体惟一的、可靠的、稳定的生物特征(如指纹、虹膜、脸部、掌纹等)为依据，利用计算机和网络技术进行图像处理和模式识别。该方式具有很好的安全性、可靠性和有效性。但采用这种方式系统的研制和开发费用高昂。

以上五种身份认证方式中，基于生物特征认证方式安全性最高，其次是基于数字证书和物理证件的认证方式，然后是基于一次性口令的认证方式，最不安全的是基于静态口令的方式。但安全性越高，实施成本也越高。

1.2 电子采购系统目前主要的身份认证方式及应用

目前电子采购系统根据面向客户对象服务的类型分为三种模式，分别为：卖方一对多(主要基于卖方目录，如网上书店、网上商城等B2C网站)、买方一对多(主要基于买方竞价、招标采购，如中石化、台塑、摩托罗拉、HP等B2B网站)、电子社区(主要基于第三方、买方或卖方联盟建立的网上交易社区，如Covisint、能源一号网等B2B企业联盟社区、中国采购与招标信息网、韩国在线电子采购系统等B2G电子采购社区)。各种电子采购系统目前主要采用的身份认证方式为基于静态密码和基于数字证书的两种方式。

1.2.1 基于静态密码方式

目前大多数的电子采购系统都采用基于静态密

码的身份认证方式，特别在PKI/CA认证体系尚不普及的国家。目前，我国大多数企业建立的一对多电子采购系统及多对多电子交易社区，基本都采用这种方式，如长虹、海尔、华为等企业的电子采购系统，以及中国化纤网、能源一号网等电子社区。

1.2.2　数字证书方式

在PKI体系相对成熟的国家，如美国、加拿大、澳大利亚、韩国等，企业、政府的电子采购系统普遍采用基于数字证书的身份认证方式。韩国电子化政府采购规则规定，交易中心必须采用电子签名和印鉴技术，推动了韩国的政府采购从电子招标、电子商城、电子合同到电子支付的采购全过程的电子化。自2005年我国电子签名法正式实施以来，基于数字证书的身份认证方式逐步得到发展，建立了部分行业和区域CA中心，但由于缺乏通用PKI标准等原因，在技术、管理、观念等方面都滞后于PKI/CA体系相对成熟的国家，总体仍处于市场孕育期之中，基于数字证书的身份认证方式仅在少量的企业和政府电子采购系统中采用。

其他身份认证方式目前也有应用，如国内网上采购支付目前采用的基于USBkey的认证，以及英国、新加坡政府电子招标系统中采用基于智能卡进行身份认证等，但应用范围目前尚不及前两种。

因此，尽管目前已存在相对成熟、安全的身份认证技术，但出于成本、系统需求等方面的考虑，电子采购系统实施者往往需要在安全、成本、效率之间进行权衡和决策。为适应不同系统实施主体在电子采购系统不同阶段安全需求的动态性特点，可利用动态安全策略来指导系统的规划和建设。

2　动态身份认证P2DR安全模型

2.1　P2DR模型及体系结构

P2DR模型是动态安全模型的代表性模型，模型包含Policy(安全策略)、Protection(防护)、Detection(检测)和Response(响应)四个主要部分。P2DR模型是在整体安全策略的控制和指导下，在综合运用防护工具(如防火墙、身份认证、加密等手段)的同时，利用检测工具(如漏洞评估、入侵检测等系统、Honeynet等)了解和评估系统的安全状态，通过适当的响应(如策略调整、系统备份、灾难恢复等)将系统调整到“最安全”和“风险最低”的状态。安全策略是P2DR安全模型的核心，围绕安全策略，防护、检测和响应组成了一个完整的、动态的安全循环。

P2DR模型和体系结构分别如图1和图2所示。

图1　P2DR模型

Response	策略调整、系统备份、灾难恢复			
Detection	入侵检测系统	Honeynet	病毒检测	漏洞扫描
Protection	防火墙	加密		身份认证
Policy	策略			

图2　P2DR的体系结构

2.2　动态身份认证P2DR安全模型

根据P2DR的体系结构，不同的安全应用和安全需求会形成不同的安全模型。表1围绕信息系统身份认证策略，将静态身份认证防护技术与入侵检测系统、Honeynet、系统日志等检测技术结合起来，识别非法入侵，动态地调整身份认证方式，形成动态身份认证P2DR安全模型。

表1　动态身份认证P2DR安全模型

P2DR模型	实现方式和作用
Policy	制订信息系统身份认证策略
Protection	基于静态口令的身份认证
Detection	利用入侵检测系统、Honeynet、系统日志等，识别非法入侵
Response	对发现的身份认证安全问题，在安全策略指导下，动态调整身份认证方式

3　电子采购系统动态身份认证策略

表1中，Policy(制订信息系统身份认证策略)是动态身份认证P2DR安全模型的核心，将表1模型应用于电子采购系统，制订电子采购系统身份认证策略就成为电子采购系统动态身份认证P2DR安全模型的核心，而制订可行的身份认证策略需要了解电子采购系统安全的需求。

3.1　电子采购系统安全需求

电子采购按业务流程分为信息发布(通过网络发布买方采购信息或卖方产品目录)、网上采购(通过买卖双方在线招投标、在线竞价、目录采购、网上磋商等形式进行)、电子合同(买卖双方在线签订电子合同)、电子支付(买方通过网络向卖方支付货款)四个阶段。从目前具体的应用来看，能实现四个阶段的电子采购系统并不多，大部分电子采购系统处在第一或二阶段，我国国内现在基本还没有能完整实现四个阶段的电子采购系统。

因此，结合实际需求，电子采购系统可分阶段实施，前面的流程是后面的基础，系统安全需求随着实施阶段逐级提高，对系统身份认证技术的安全性要求也逐步提高，如图3所示。

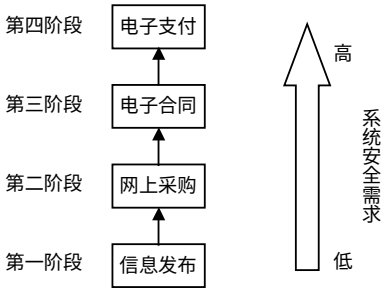

图3 电子采购系统流程及安全需求示意图

3.2 基于P2DR的电子采购系统身份认证策略模型

电子采购安全除了由于网络攻击技术等的发展而引起的网络环境相对变化外，主要是伴随着电子采购实施阶段变化而呈现明显的动态性特点。不同电子采购系统在实施电子采购的不同阶段甚至同一阶段，由于系统知名度、被保护信息资源价值、系统安全防范措施等方面的差异，存在的安全风险也有所不同，需要通过入侵检测系统、Honeynet、系统日志等检测工具来发现风险，动态调整身份认证方式。

表2为电子采购各阶段存在的主要安全风险以及为保证系统安全需求可采取的身份认证方式。

表2 不同电子采购阶段对应的身份认证方式

电子采购阶段	存在的主要安全风险	可采取的身份认证方式
信息发布	假冒发布虚假信息、篡改或删除商务信息	静态口令
网上采购	窃听或截获传输数据、插入或修改传输中的数据、抵赖	静态口令、动态口令、基于物理证明和数字证书
电子合同	窃听或截获传输数据、插入或修改传输中的数据、抵赖	基于物理证明或数字证书
电子支付	窃取信用卡或购物卡	基于物理证明、数字证书或身份特征

制订电子采购系统身份认证策略还需考虑政策法律环境(如一个国家是否颁布了电子签名法，对该国电子采购系统是否采用基于数字证书的身份认证方式影响较大)、业务范围(针对国内用户、全球用户面对不同的安全需求，需采用不同的认证方式)、实施成本(身份认证方式安全性越高，成本越高)、实现方式(包括企事业单位自主开发、外包开发、第三方服务三种系统身份认证实现方式)等方面的综合因素。

本文提出的基于P2DR的电子采购系统身份认证策略的模型如图4所示。

电子采购系统身份认证策略(P)可视为身份认证方式(X)、电子采购实施阶段(Y)、综合因素(Z)三个子集组成的三维空间集合，即$P=\{X, Y, Z\}$。不同的YZ组合，在三维空间集合中将对应不同的X。

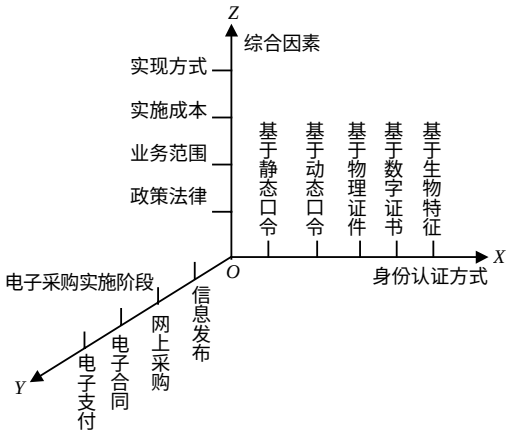

图4 电子采购系统动态身份认证策略模型

4 结 束 语

基于P2DR的电子采购系统身份认证策略根据不同用户在电子采购不同阶段的不同安全需求，综合考虑法律政策、实施成本、业务范围、实现方式等因素，根据“成本效益”、“适度安全”等信息系统安全基本原则，动态调整身份认证形式，实现了“安全、成本、效率”的动态平衡。本文为即将或正在实施电子采购的政府有关部门、企事业单位进行电子采购系统建设时，避免系统规划和设计的盲目性提供了一种制订动态安全策略的参考模式。

参 考 文 献

[1] 杨永川, 李冬静. 信息安全[M]. 北京: 清华大学出版社, 2007.
[2] 薛 质, 苏 波, 李建华. 信息安全技术基础和安全策略[M]. 北京: 清华大学出版社, 2007.
[3] 方 勇, 刘嘉勇. 信息系统安全导论[M]. 北京: 电子工业出版社, 2003.
[4] 戴尔·尼夫. 电子采购——从构想到实施[M]. 北京: 中信出版社, 2002.
[5] 孟学军, 石 岗. 基于P2DR的网络安全体系结构[J]. 计算机工程, 2004, 30(4): 99-101.
[6] 侯小梅, 毛宗源, 张 波. 基于P2DR模型的Internet安全技术[J]. 计算机工程与应用, 2000, (12): 1-2.
[7] 向华萍. 管理信息系统安全模型的研究[D]. 南昌: 华东交通大学, 2006.
[8] 杨 明. 韩国电子化政府采购系统成效显著[J]. 中国招标, 2007, (2): 13-16.
[9] 胡道元. 信息网络安全模型与安全平台[J]. 中国信息导报, 2000, (8): 48-49.
[10] 李章程, 王 铭. 英国电子政务建设进程概述[J/OL]. http://www.allwinners.info, 2006-06-18.
[11] 应可珍. 高安全性电子化采购系统的研究[D]. 杭州: 浙江工业大学, 2004.
[12] BENJAMIN P C Y, ELSIE O S. Migrating procurement onto the Internet[J]. Electronic Commerce Research, 2002, 2: 113-134.

编 辑 熊思亮