Development of secure automated management systems based on web technologies

Dmitry Kononov and Sergey Isaev

Institute of Computational Modelling of the Siberian Branch of the Russian Academy of Sciences, Akademgorodok 50/44, Krasnoyarsk, 660036, Russia

E-mail: ddk@icm.krasn.ru

Abstract. This paper discusses security problems of developing municipal management information systems for Department of Municipal Procurement of the Krasnoyarsk City Administration (Russia). Authors describe the problem, goals, and tasks to be solved. Some security aspects are given, as well as original extended role-based security access control model for web applications and web services. This work describes two information systems developed by specialists of the Institute of Computational Modelling of the Siberian Branch of the Russian Academy of Sciences using described approaches. The systems have been in production for several years. The methods used to protect information are given, the structure of software is presented.

1. Introduction

Currently, information and telecommunication systems, including those based on Internet technologies, are actively developing. Internet systems expand their areas of application and are used in management systems of state and regional authorities which use modern technology to provide their services to citizens [1]. Since these services are designed for a wide range of users, they operate in public networks which exposes them to information security risks. Every year, more and more security incidents occur in the world, resulting in both financial and reputational losses [2]. It is also not uncommon when restricted users databases with personal information are leaked into public access. Obviously, systems operating on the Internet should to be carefully protected. Ensuring information security is a complex task which is solved by a set of measures aimed at reducing information security risks. Using partial measures is insufficient for safe operation of the system on the Internet.

The basis of a modern protected information system is a properly designed access control to information resources. To do this, it is necessary to develop a strict security policy and use adequate access control models. In addition, it is necessary to ensure the security and integrity of data exchange processes both within the system and with external sources. The above tasks were solved successfully during the development of information systems to support municipal management of the Department of Municipal Procurement of the Krasnoyarsk City Administration (Russia).

2. Goals and tasks

The aim of creating secure information management systems is to increase Krasnoyarsk municipal management efficiency, and ensure high availability of local government services, as well as reduce paper workflow with replacement by electronic documents with digital signatures.

In connection with the active development of information technologies, many state and municipal authorities widely put into operation software systems that collect and process information related to the their activity. One of such systems in Krasnoyarsk is the Automated Information Support System for Municipal Procurement (AIS MP) [3]. The system's tasks include collecting and compiling a register of municipal needs, coordinating procurement documentation flow, posting procurement documents on the Russian official procurement website, data exchanging with federal trading platforms, and maintaining a register of municipal contracts.

In this paper, we consider 2 systems that are developed within the AIS MP. Developed systems solve the following tasks:

- conducting electronic competitive bidding for the right to dispose of municipal property;
- data exchange between municipal organizations and the Procurement Authority (Department of Municipal Procurement of the Krasnoyarsk City Administration) for budget and procurement reconciliation;
- ensuring the information security at all levels both within systems and during their interaction.

3. Web services protection

An important role in the development of web services is to ensure information security to protect the data transmitted through public networks. According to Kaspersky Security Bulletin 2018 [4], 30% of computers on Internet users at least once underwent a web attack. The main source countries of web attacks for 2018 are: USA (45.65%), Netherlands (17.53%), and Germany (11.7%). According to Symantec Internet Security Threat Report 2018 [5], 1 out of 10 URLs were identified as malicious in 2018, while in 2017 it was 1 out of 16.

According to the Top Ten Open Web Application Security Project (OWASP) statistics for 2017 [6], the most dangerous threats to web applications are: code and data injection, authentication problems, sensitive data disclosure, XML processing errors, access control errors, configuration errors, cross-site scripting (XSS), insecure deserialization, use of vulnerable components and libraries, insufficient monitoring and logging.

Currently, systems designed for enterprise use are being developed using Internet technologies for better scalability and flexibility. The main problem of such systems is insufficient security policy restrictions, since their operation is assumed in a safe environment. In reality, it turns out that in enterprise networks there are the same threats and risks as in the external networks. Therefore, before developing such systems, it is necessary to create a strict security policy and provide for all possible scenarios of user activities.

The following security components of web-based systems can be distinguished:

- *System software security (operating system).* The operating system is a set of software that provides control over the computer hardware and application programs, as well as their interaction between themselves and the user. The operating system security is very significant for the whole system security. Here, one of the main security tools is a network filter (firewall) which should limit packets and services provided for users.
- *Web server security.* The web server security is affected by some settings defined in configuration files. Errors in web server configuration can lead to potential security breaches and leaks of protected data.
- *Database security.* The database is often a target of interest for hackers because it may contain personal data, confidential, and other sensitive information. Database protection is one of the most important tasks in ensuring integrated information security.
- *Programming language security.* One of the most popular languages are interpreted languages (PHP, Perl, Python, Java) which have built-in high-level data types and libraries. Often programming languages and related components have vulnerabilities that should be fixed as soon as possible.

- *Components Security.* Using third-party components with an unknown reputation can increase the risk of successful breaking. Proprietary closed source software can contain spyware that collects and transmits sensitive information. Many software solutions are delivered without source code, which complicates identifying malicious tools and components.
- *Program code security.* An important part of protecting software code is filtering data and forms. Semantic attacks are common when revealing internal data structures. Running databases queries with insufficient data filtering can lead to SQL injections. As a result of data processing errors, it is possible to inject program code executed in the environment of the calling script.

4. Security model

Web applications security is a complex problem with several aspects. Security policy allows specifying necessary restrictions for access control which is accomplished by imposing restrictions described in security model. Applying appropriate security model leads to reducing risks of successful attacks. Modern applications and services use a role-based security model due to the possibility of flexible access control [7]. The classical role-based model does not take into account web applications features, for example, requests and links hierarchy. Below there is a brief description of the extended role-based security model for web applications and web services developed by the authors [8].

The original role-based access control model (RBAC) is described in [9]. We added new elements to RBAC model: "token", "request", "request parameter". Token (*Tk*) is a set of user attributes that allow him to carry out authentication in a system. Request (*Rq*) is a set of information sent by the client to HTTP server. The inclusion relation on top of requests set *Rq* defines non-strict partial order and allows to organize requests according to specified hierarchy. Next, we define a function *RqA()* mapping permissions to multiple requests $RqA: P \rightarrow 2^{Rq}$. For all the requests from *Rq* the request hierarchy *RqH* is introduced. Let's define a function *requests()* mapping a session to requests allowed in this session: $requests: S \rightarrow 2^{Rq}$. To accomplish access control based on HTTP request parameters, new element "request parameter" and functions were added to the model. Request parameter *(RqP)* is a set of pairs key/value of HTTP request which belongs to request *Rq* and used to transfer additional data to a specified location. Let's define two new functions: *RqPA()* mapping permissions to multiple parameters: $RqPA: P \rightarrow 2^{RqP}$; *params()* mapping requests to multiple parameters: $params: Rq \rightarrow 2^{RqP}$. The new model defines a set of elements:

<U, R, P, S, Tk, Rq, RqP, UA(U), PA(R), RqA(P), RqPA(P), user(S), roles(S), token(Tk), requests(S), params(Rq)>.

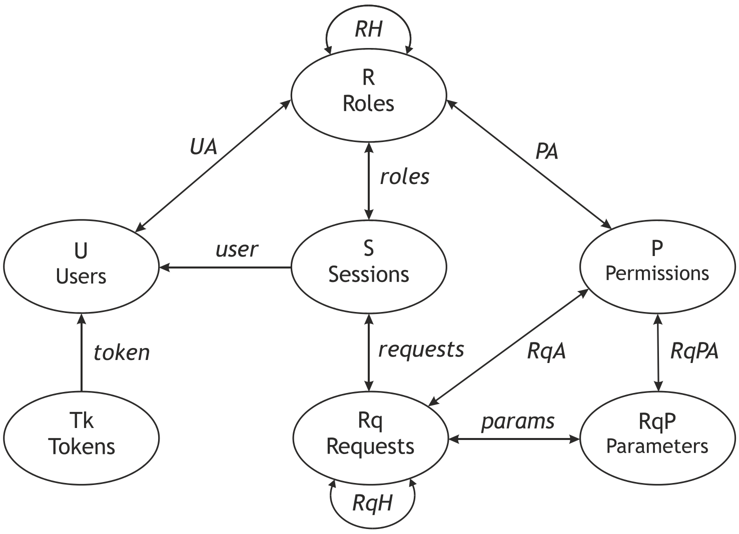

Figure 1. Elements of security model.

Figure 1 shows elements of new extended role-based access control security model. The resulting security model allows access control using not only the request path (URI), but also the request parameters. Additional parameters restrictions can be made using explicit function mapping and filtering language rules. This approach allows implementing complex access control policies in information systems in which permissions to perform an operation are carried out based on context including a set of parameters and their values. Often requests have a fixed set of parameters which are described by a specific format. It should be noted that the created model is not limited to a fixed set of parameters, but provides for a dynamic set of parameters depending on specified conditions. Imposing restrictions on parameters reduces the risk of information systems being compromised using the described security model.

5. Information systems in municipal management

The following systems have been successfully implemented with described requirements and put into production in the Krasnoyarsk City Administration: Electronic Trading Platform, Web Transport Packet System.

5.1. Electronic Trading Platform

The purpose of Electronic Trading Platform (torgi.admkrsk.ru) is to organize open bidding in the form of an electronic auction with price increase. The auction winner acquires a right to conclude a rent agreement of municipal property. The Electronic Trading Platform solves a number of tasks related to the organization of electronic auctions, including:

- publication of electronic auction documentation for public access;
- accepting and approving participation requests from business and individuals;
- conducting electronic auctions;
- automated generation of auction results with winners;
- service maintaining procedures;
- data storage protection.

As an external data source, Document Library system is used (as a part of AIS MP [3]). The system data storage includes the following components: a registry of electronic auctions with a full set of documentation for each auction, a registry of electronic auctions participants, information about participation requests with documents submitted by participants, information about auctions results, service data for operator (journals, notifications), reference registries, working days schedule, regulatory information.

5.2. Web Transport Packet System

The Web Transport Packet System is used to coordinate the budget of Krasnoyarsk municipal organizations. The system organizes data exchange between the Procurement Authority and budget managers with municipal organizations. Additionally, the system ensures integrity through the digital signatures and information protection according to specified security policy. The system also provides consistency and chronological accuracy of the data. The developed system allows to exchange information on municipal procurement, registry and software updates. The system operates within the Automated Information Support System for Municipal Procurement (AIS MP) [3].

6. Methods of information protection

There are various methods and approaches to ensuring information security for web applications and web services. One important note is to protect a server-side part of the system [10]. The developed information systems have tools to grant access control for authorized users implemented using the described security model. In the program code part, the following information protection methods are used:

- authentication and authorization of registered users;
- access control using extended RBAC model;
- restrictions on user passwords;
- using digital signatures to certify legal user actions;
- using filtering tools for user-entered data to prevent injections [11];
- traffic encryption when interacting with users via the HTTPS protocol;
- access control based on IP addresses;
- access control based on geo-targeting (user country);
- access control for internal services;
- logging of all significant operations for detecting abnormal situations;
- blocking suspicious requests that are not typical for normal operation.

7. Structure of software and functions

The software was created using modular principles and object-oriented approach which provides flexibility to add new functions for subsystems. The server software runs under the Microsoft Windows Server operating system. The scheme of software is presented in figure 2.

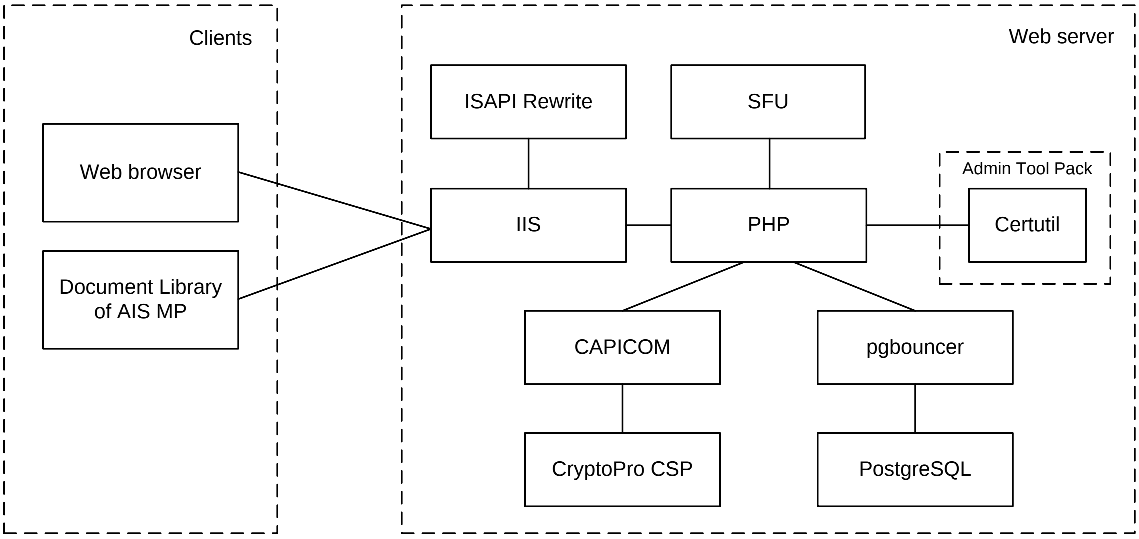

Figure 2. Scheme of software components.

Tools that extend operating system capabilities are:

- Windows Services for Unix (SFU) – includes POSIX tools for Windows.
- ISAPI Rewrite – a module for IIS that provides URL rewrite (similar to Apache mod_rewrite).
- Admin Tool Pack – a set of tools for administering the Windows Server operating system; in particular, includes a utility for managing certificates Certutil.
- CryptoPro CSP – cryptographic software that provides encryption and digital signature processing to certify legal user actions according to Russian cryptographic standards GOST 34.10-2001, 34.10-2012, 34.11-94, 34.11-2012, 28147-89, 34.12-2015 (analogues of NIST security standards).
- CAPICOM – ActiveX component for interaction application with system cryptographic providers.

The server software includes: PHP – server programming language; PostgreSQL – relational database management system; Pgbouncer – query balancer for PostgreSQL as an intermediate layer for accessing data, creating a pool of connections.

8. Conclusion

The developed information systems for municipal management support have been tested and successfully solve the tasks of the Department of Municipal Procurement of the Krasnoyarsk City Administration. Using described information protection techniques and security model, it was possible to protect sensitive data and ensure uninterruptible operations. During the operation, attempts of unauthorized access were recorded and analyzed, which made possible to improve system functions under high load conditions.

Currently, the Electronic Trading Platform works in production mode and available at https://torgi.admkrsk.ru. During the period from 2012 to 2018 of system operation, 2531 electronic auctions were held, as a result the Krasnoyarsk city budget received additional funding in the amount of 1.58 billion rubles.

Web Transport Packet System works in production mode since 2012. In 2018, the system successfully conducted 2631 purchases in the amount of 16.396 billion rubles for municipal organizations of Krasnoyarsk city. Several years of system operating revealed no problems with ensuring integrity and chronological accuracy of the data.

Despite the growing risks of information security, the developed systems successfully accomplish all the tasks, which confirms the efficiency of the approaches used.

References

[1] Leonova M 2009 New Index for Measuring Feedback and e-Participation Effectiveness of e-Government in Russia *9th European Conf. on e-Government* 29-30 June (London: Academic Conferences Ltd) pp 445–50

[2] Chowdhury A 2016 Recent Cyber Security Attacks and their Mitigation Approaches – an Overview *7th International conference on applications and techniques in information security* 26–28 October Cairns, Australia (Singapore: Springer) pp 54–65

[3] Sherbenin V F, Luzan N F, Nozhenkova L F, Isaeva O S and Zhuchkov D V 2007 Integrated Automated Support for Planning, Placement and Control of Municipal Orders *Proc. of the 10-th all-Russian scientific practical conference Problems of Informatization of the region* (Krasnoyarsk: Sib. Feder. Un-t, Politech. in-t) pp 3–11

[4] 2018 Kaspersky Lab. Kaspersky Security Bulletin 2018 Statistics Available from: https://securelist.com/kaspersky-security-bulletin-2018-statistics/89145/

[5] 2019 Symantec Corporation. Symantec Internet Security Threat Report 2019. Available from: https://www.symantec.com/security-center/threat-report

[6] 2017 The OWASP Foundation. OWASP Top Ten 2017 Available from: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_2017_Project

[7] Li Fr and Wu Ht 2015 Design and Implementation of Authorization System Based on RBAC *7th International conference on intelligent human-machine systems and cybernetics IHMSC* 26-27 August Hangzhou, China (Piscataway: IEEE) pp 502-4

[8] Kononov D and Isaev S 2018 Improving Web Applications Security Using Path-Based Role Access Control Model *3rd Russian-Pacific Conference on Computer Technology and Applications* AUG 18-25 Vladivostok (NY: IEEE) pp 1-3

[9] Sandhu R S, Coyne E J, Feinstein H L and Youman C E 1996 *Role-Based Access Control Models* (*IEEE Computer* vol 29-2) pp 38–47

[10] Xiaowei Li, Yuan Xue 2014 A Survey on Server-Side Approaches to Securing Web Applications (*ACM Computing Surveys* vol 46-4) (New York: ACM) p 1-29

[11] Deepa G and Thilagam P S 2016 Securing Web Applications from Injection and Logic

Vulnerabilities: Approaches and Challenges (*Journal Information and Software Technology.* vol 74) (MA USA: Butterworth-Heinemann Newton) pp 160-80