Basic principles for data protection for decision-making and control systems

O V Dudareva¹, A I Alchinov² and M Yu Vakhrusheva³

¹ Irkutsk National Research Technical University, 83, Lermontov str., Irkutsk, 664074, Russia
² Institute of Control Sciences of the Russian Academy of Sciences
³ Bratsk State University, Makarenko Str., 40, Bratsk, 665709, Russia

E-mail: odudareva@istu.edu

Abstract. Today, computers are firmly integrated into our daily lives. Work at any level without large volumes of information transfer seems impossible in modern society. This all makes it necessary to protect information at all levels. Once in the hands of attackers, this data can cause irreparable harm. In this regard, information protection as a whole is seen as a very important aspect of modern network security. The content of this paper will be useful both to specialists in the field of information security and to ordinary users.

1. Introduction
Information in the modern world is the main valuable resource. There are many different approaches to its protection. However, there are several standard approaches to protecting information and information systems from attacks. Let us analyze them in more detail [1-3].

2. Theoretical approach
We close all interfaces, and at the seventh level we scan what is available (for example, the Nmap program), close ports, at the web application level we scan directories, identify what we do not know, find suspicious files in directories. Next, we restrict access to such files, create temporary users, i.e. application components must work from an account with limited rights. We use standard operating system tools that limit the capabilities of an attacker, and the use of a virtual machine is also a good option, i.e. even if we lose the content of a web server, then the adjacent components will remain safe. Virtual machine practices reduce the potential for any kind of attack [4, 5].

Thus, it can be concluded that the general principles of data protection against attacks are the following:
1) Close interfaces and enable authentication;
2) Create dedicated users;
3) Ensure sandbox configuration (or virtual machine usage).

3. Fighting potentially dangerous files
How to deal with files that are potentially dangerous? In the Linux console, you can use commands to search for such files, for example:
In this case, we go to the directory/html and look for files that have such file extension as .bak or .old, view their content, if we understand that there should not be one, delete them.

Most frameworks have built-in security mechanisms.

For example:

- **PHP**: safe_mode (the mode in which PHP works, while administrative commands are not available to it), magic_quotes (the mode in which quotation marks are shielded so that certain parameters cannot be set and ensure SQL injection), open_basedir (this setting allows limiting the visibility and availability of parts of the file system);
- **JEE**: SecurityManager (a protection manager that allows restricting access to classes), AccessController (a class that is used after the protection manager, i.e. it is the second line of protection) [6, 7].

### 4. Protection when setting up cross-domain interaction

In terms of protection, the following is used when setting up the cross-domain interaction:

1) CORS (cross-origin resource sharing) – a technology of modern browsers, which provides the web page with access to resources of another domain.

   The technology itself is quite simple. There are three domains that want to download resources from server Z. In order to make this possible, the web server Z that gives content shall only specify a list of trusted domains in the header of the Access-Control-Allow-Origin response: A, B, C. Then, for the pages of these domains, restrictions of the same origin policy on the requested pages will not apply:

   Access-Control-Allow-Origin: A, B, C

   After that, the pages of A, B, C servers will be able to download content from server Z.

2) Cryptography Service Provider (CSP) is an independent module that allows cryptographic operations on Microsoft operating systems, which are controlled using the CryptoAPI functions. Simply said, this is a mediator between the operating system, which can control it using standard CryptoAPI functions, and the executor of cryptographic operations (this can be both a software and a hardware complex).

   One of the main objects is the key container. The container has its name, is created (or requested if already created) by the CryptAcquireContext function (...). There can be no more than one signature key pair, one exchange key pair, and one symmetric key in the container. If several symmetric encryption algorithms are supported, then there can be several symmetric keys, one key of each algorithm.

   Key pairs and symmetric keys can only be in a container. Only the public key of the pair can be outside the container.

   Private keys of key pairs are exported only in encrypted form. Some crypto providers fundamentally do not allow exporting private keys, even in encrypted form. Symmetric keys during export are also necessarily encrypted on the public key of the recipient or the negotiation key. Hashing objects are created to calculate the hash functions. You do not need to create a container to create hash objects.

3) If we also have Flash, in this case the file “crossdomain.xml” will help.

   Crossdomain is a special xml file that allows the loading of data between domains (the player and data are located on different domains).

   This file must be placed at the root of the site from which the data is downloaded (not the player, but the data).

   Permission is required for the following cross-domain operations:

   - loading styles, playlists and any other text data (JSON, XML, subtitles, etc.);
   - loading plugins in SWF format;
   - reading mp3 ID3 tags;
• smoothing loaded images when zooming.

A servlet is a Java interface, the implementation of which extends the functionality of the server. The servlet communicates with clients through the request/response principle.

When configuring different servlets, the “web.xml” file serves the key file, which is used to determine which URLs will be sent to a specific servlet, which URLs require authentication, etc. It will help to set up sessions and security flags for cookies. For example, as follows:

```xml
<session-config>
    <session-timeout>15</session-timeout>
</session-config>
<cookie-config>
    <secure>true</secure>
    <http-only>true</http-only>
</cookie-config>
<tracking-mode>COOKIE</tracking-mode>
```

In this case, we see the setting of the session timeout after 15 minutes of inactivity.

5. Conclusion

In addition to a wide variety of options for protecting against the actions of attackers, there are a number of standard recommendations, subject to which you can effectively protect any system from a large number of external attacks. Nevertheless, do not forget that the techniques described in the paper are not the only ones and by relying on them solely it is impossible to achieve the maximum security.

References

[1] Balanovsky A E, Shtayger M G, Kondrat’Ev V V, Van Huy V and Karlina A I 2018 Plasma-arc surface modification of metals in a liquid medium. *IOP Conference Series: Materials Science and Engineering* **411**(1) 012013

[2] Kondratiev V V, Karlina A I, Guseva E A, Konstantinova M V and Kleshnin A A 2018 Processing and Application of Ultra disperse Wastes of Silicon Production in Construction *IOP Conference Series: Materials Science and Engineering* **463**(3) 032068

[3] Gura D A, Gura A Y, Volkova T A and Lipilin D A 2020 Recreational space as a factor of sustainable development of coastal geosystems of the Krasnodar region *IOP Conference Series: Earth and Environmental Science* **579**(1) 012007 doi:10.1088/1755-1315/579/1/012007

[4] Buryanina N, Korolyuk Yu, Koryakina M, Lesnykh E and Suslov K 2019 Algoritom of Current Protection Based on Three Instantaneous-Value Samples *Proceedings of IEEE PES Innovative Smart Grid Technologies Europe* 890542

[5] Suslov K V, Solonina N N and Smirnov A S 2011 Smart meters for distributed filtering of high harmonics in Smart Grid *International Conference on Power Engineering, Energy and Electrical Drive*, 603652

[6] Balanovskiy A E, Karlina A I, Kolosov A D, Karlina Y I 2021 Study of the effect of nanomodifiers from silicon production wastes on morphological form of gray cast iron graphites. *CIS Iron and Steel Review* **21** 64–69

[7] Sivtsov A V, Elkin K S, Pan’kov V A, Karlina A I 2021 Specific Features of the Electric Mode of the Technological Process of Smelting of Commercial Silicon. *Metallurgist* **64**(9-10) 923–930