Security of Information Systems – User's Attack Inside of Organization

Martin Hanzal
martin@sodatsw.cz

SODAT software spol. s r.o.
Sedlakova 33
Brno, Czech Republic

Abstract

A person is one of the biggest threats to information systems, a person can attack a system from the outside or inside of an organization. A person (employee) attacking an information system from within an organization is an aggressor who has the biggest chance to obtain protected data from information systems. Current operating systems can assign many permissions to allow access to individual parts of information systems and they provide access control for specific operations such as reading, writing, creating, deleting etc. Then they can audit all user's operations within an information system. User's (employee's) security tests and internal rules are inseparable parts of a security policy of information systems. Strong cryptography will protect all transmitted and stored data. All of these permissions and restrictions can be sufficient for data protection. But a trustworthy internal user (employee) can become a non-trustworthy one (e.g. he leaves organization). We are not sure, if the data from the information system was taken by him because this user (employee) had permission to work with specific data. After leaving the organization he has no permission to work with the data any more but we are not sure, if the data was copied to somewhere else where he still has a permission to work with it. The solution is to set a protected local or remote area where the data is transparently encrypted and decrypted and privileged applications can be assigned and are allowed to work with the data normally. These privileged applications can't save data or its parts, export or move it to another area, which is not protected. This is a technical solution how to protect data which users commonly work with and have the possibility to steal them electronically. The development of the AreaGuard system can solve this situation in the operating systems MS-WINDOWS NT/2000.

Keywords: information system, security, data of information systems, employee, access control, inside of organization, outside of organization, protected area, privileged application, client, server.

1. Introduction

Security is one of the most important parts of information systems. It is necessary to make the risk analysis of an information system before it will be used in practice. We must know all risks which can occur in releasing our information systems in practice. Every information system must guarantee confidentiality, availability and integrity. The risk analysis must verify that the information system guarantees all of the three before mentioned properties. This paper will describe one of many threats to the information system. This threat is a person who wants to get confidential data from the information system. This person can attack an information system from:

- The outside of organization – an attacker has no legal access to the information system, he is not authorized to use the data from the information system and he is not inside the computer network of the organization.
- Within the organization – an attacker has legal access to the information system, he is authorized to use the data from the information system and he is inside the computer network.

Both of these two attacks have the same target for the attacker. The attacker wants to get sensitive data from the information system. The attack from within the organization is the main topic of this paper. Current protective mechanisms of information systems, current threats to information systems from the user's side and mainly new methods of data protection against the attacks from authorized users will be presented in this paper.

2. The Protective Mechanisms Against User's Attack

There are many rules and technical solutions how to protect data against unauthorized access. Every unauthorized access can violate the confidentiality of data. The most protective mechanisms solve internal and external attacks. We can divide these mechanisms into two groups:

- The prevention against any attack – these mechanisms prevent attacks. (e.g. user's training, user's authentication, access control, cryptography).
- Proof of an attack – these mechanisms prove performed attacks (e.g. audit and monitoring performed access of the user in a part of the information system).

User's training – it is a very important part of security. Every user must know that he will be punished when some sensitive data of the information system is disclosed. It means a financial penalty or punishing the user in same way. The user must be informed how to work with sensitive data. He must cooperate in working with the security of the information system and he must adhere to all rules of the security policy.

User's authentication – it verifies the authorized user's access to the information system. The hardware token is used for safer user's authentication. This token transmits the user's password or certificate.

Access Control – it is the most used method how to defend unauthorized access in specific parts of the information system because every user has permission, which defines enabled and disabled access in parts of the information system. It also defines operations, which can be executed (e.g. reading, writing, creating, deleting). This protection is used as a sufficient method for data security in most operation systems and applications.

Cryptography – nobody can use data without the knowledge of the encryption key. Modern information systems use encryption in the user's authentication and in data encryption.

Audit – it stores all operations, which were executed by users. It can prove the user's time of access to data, operations executed with data etc.

3. The Model of Client and Server Architecture in Information System

Modern information systems are mostly divided into two parts:

- The server – server applications are run here and work with all the stored data of the information system and provide communication between the server and clients.
- The client – it means the user's computer. The client provides the server data to the user. The client sends commands to server applications, which answer and send the results back.

The basic structure of client and server is the same and is made up of three parts:

- The user's interface – it receives the commands from a user and sends it back.
- The application – it executes the user's commands.
- The data – it is a disk storage where all data is stored and applications access this data.

All protective mechanisms must be included in the client and in the server. The user can execute only specific operation with data and they can access only specific data. It is very important to protect the communication between the client and the server. This communication is performed via LAN or WAN computer networks and the data transmitted via network must be encrypted. Many protocols are used for data communication and these protocols have their own protective cryptography mechanisms.

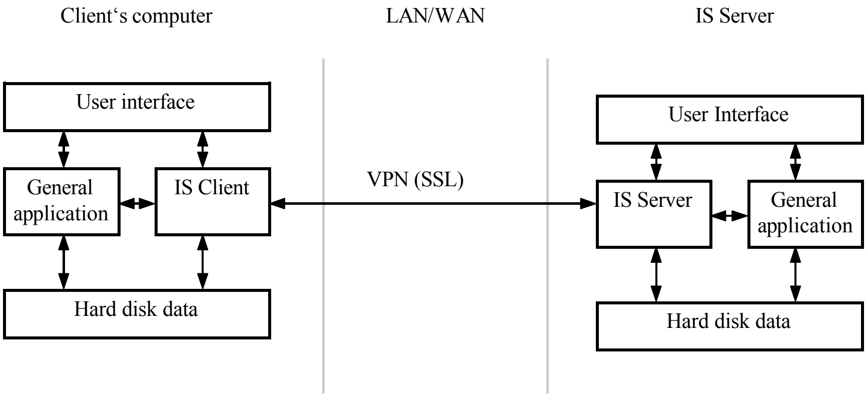

Figure 1. The architecture of the client and the server in an information system

Let’s have a look in greater detail at the threats to the information system, which can occur at the client’s side. The application part of the client is divided into two basic types of applications:

- The IS client – this is an application which communicates with the server of the information system. The IS server reads and writes server data and sends it back to the IS client as answers to the client’s questions.
- The general application – e.g. a text or a table processor, which works directly with stored local or shared data (direct access to files).

There is one big difference between the client and general application and it is the access to the data. The application can only access data, which is accessible by the authorized user. The application provides data for the user via the user’s interface and the user controls the application via the user’s interface. The applications can exchange data themselves (e.g. using a clipboard). It enables application X to send data to application Y and application Y can write data to the disk or can work with it.

The architecture of the server is very similar to the client architecture. A user usually cannot access the server directly but the IS Server application can be used as a service provider. One type of user is an administrator who administrates information systems and has more privileges than a usual user. Administrators have different permissions to access data. They work directly with IS Server applications and control the server data. The administrator can use another general application too but the general application is used on the server side. The general and server applications can exchange data themselves as well.

4. The Most Frequent Causes of Data Leakage from Information Systems

An employee (user) of an organization needs sensitive data for his work. The organization owns valuable data. A loss of data means a loss of finance for the organization. The employee is trusted because he has been tested. The employee has access to sensitive data and knows encryption keys only to data he needs for his work. He can only execute specific operations (e.g. reading, writing…). All protective mechanisms are sufficient while the employee is still the trusted by the organization and he adhere to all the security policy rules. But the employee can resign or be fired and can be employed with another organization. He is not considered as trustworthy anymore. He can copy the organization's data and take it to another organization and harm the organization.

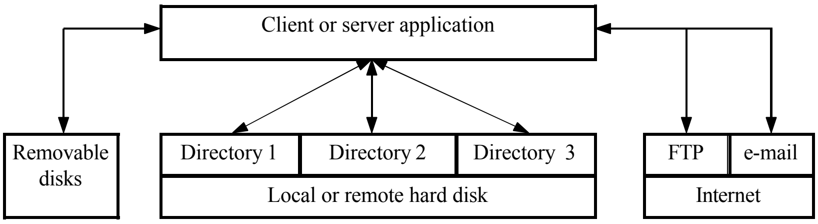

Figure 2. The access of application to data files

All protective mechanisms, written above, protect data against unauthorized access adequately. But the employee has authorized access to the data. All applications which a user uses for work can access data which is accessible by the user working with the applications. The applications can be of a general application type (e.g. file manager) and a user can copy or remove the source of sensitive data to a new target which can be removable disks (e.g. CD-R, CD-RW, ZIP, diskette…) or another local or remote directory. Besides these targets the user can send data via e-mail or transmit it to another server (e.g. FTP server). A new place (a new data source) usually has other permissions and data is mostly decrypted during the data transmission. When the employee finishes his work in the organization all permissions are taken away. But the employee still has the permission to work with copied or transmitted data from the new target.

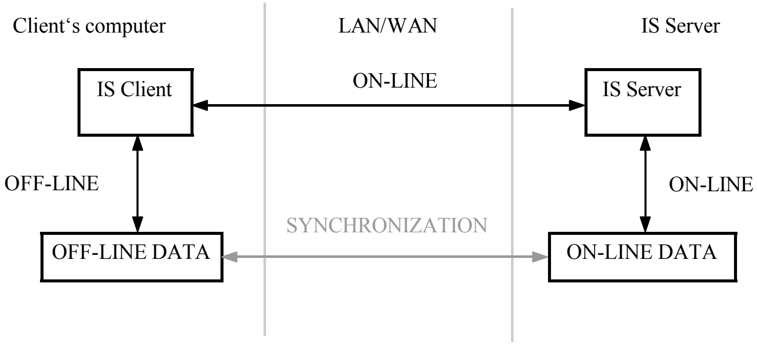

Figure 3. Data synchronization in the information system

This problem seems to connect general applications, which use files from local or remote disks and are able to copy them to another place. The IS client gets only answers from the IS server but these ones can be transmitted to another application or stored on a local or remote disk. The most dangerous are synchronous processes because users working with mobile computers need accessible data from the server with them. It is solved by synchronization on the client's and the server side. The client's and the server data (or their parts) are the same and are stored on the client's disk. A big possibility of copying it without any other organization control.

Besides copying the data there is another possibility of taking the data by printing. The most valuable form is data in electronical form because copying the data is not suitable.

5. A New Protective Method - Firmwall

Only threats and methods how authorized users can get sensitive data from the information system were presented. Today's information systems have no chance to define the data location (data files) without any possibility of copying it to another target place and loose control over it. They can audit these operations, they are able to find out what data was copied (transmitted) and to find out the person who did it. This audit does not protect other data copying.

There is a solution to work with data without any other possibilities of copying them to another target place. Only authorized users can access locations (directories) from the application with permission to work with data from this *protected area*. The term is called *privileged application.*

The protected area can be on a local or remote disk and is exactly defined by the directory path with sensitive data. The system should be able to defend against creating a new protected area by an unauthorized user as well as making it impossible to copy data to a newly created protected area. Every protected area has its own encryption key and algorithm which are all data encrypted. N-applications can be generally defined for working with a specified protected area. When accessing privileged applications from a protected area, read data is transparently decrypted and written data is transparently encrypted. The privileged application can read data from any area (directory) or from its protected area. The privileged application can only write the data to its own protected areas. All stored data is transparently encrypted.

There are three applications and data areas in figure 4. Application 1 is a standard application which can read and write data to unprotected areas. There is no possibility to read or write data to protected areas. Application 23 is a privileged application for protected areas 2 and 3. Application 23 can read data from any unprotected area and from protected areas 2 and 3. The application can write to protected areas 2 and 3 only. The last mentioned privileged application, 3, can write to protected area 3.

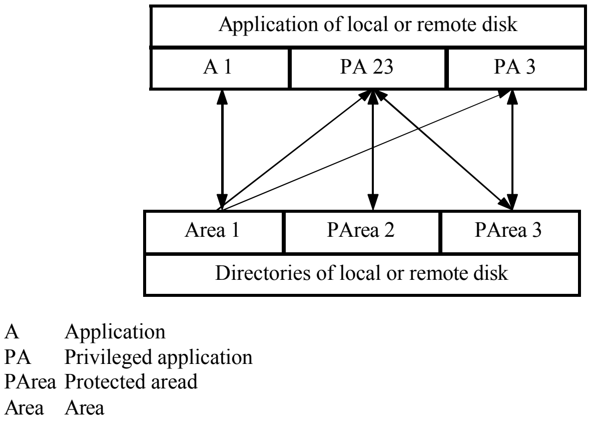
Application of local or remote disk
A 1
PA 23
PA 3
Area 1
PArea 2
PArea 3
Directories of local or remote disk
A Application
PA Privileged application
PArea Protected aread
Area Area

Figure 4. Reading and writing data from areas to applications

There is a possibility of exchanging the data themselves in an operating system (e.g. using a clipboard). Transmitting the data is possible only between applications which are privileged for the same protected area. If there is a difference between privileged applications then they can work with read data only within this application. Privileged applications must be exactly defined to disable the creation of a new privileged application to a user. The privileged application is exactly defined by a specific path to the executing program which creates system processes. There are three applications in figure 5, they can exchange data themselves using tools of the operating system (e.g. clipboard). Application 1 is not a privileged application. The data from this application can be transmitted to another application (also privileged) or the data can be exchanged itself (also for a privileged one). Privileged application 23 can receive data from any other and at the same time they can exchange data 3 with privileged application 3 because the data belongs to the same protected area.

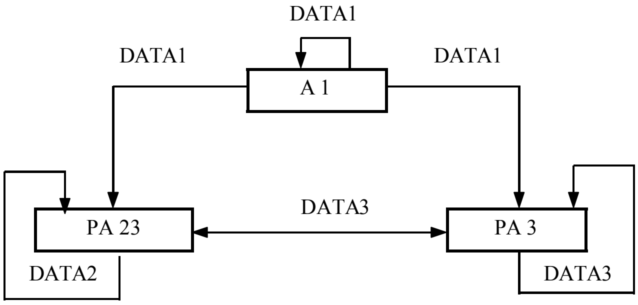

Figure 5. The possibility to transmit data between applications

All extended features of directories (areas) and applications must be protected against unauthorized access and must be accessible for the security administrator. Every client computer working with protected areas and privileged applications needs to control the access of privileged applications to protected areas and to know encryption information about the protected area (algorithm and key). This information can be stored in local or shared databases including the information about each property. Every user must be authenticated himself and then he is able to use encryption keys, protected areas and privileged applications. There is a bigger risk of attacking and loosing information by local storing and at the same time there is less possibility to change this information by the administrator. On the other side, shared information on the server reduces the possibility of attack to this database and that's why the administration is easier because information is stored on a shared server and all users access this information at one place.

The above-mentioned problems concerning data protection – *firmwall*, which are owned by an organization and should be protected against unauthorized users are solved by AreaGuard project which operates in an MS-WINDOWS NT/2000 environment. This project is under laboratory testing at present and will be released into the users' environment as a very effective way of protecting an organization's data. AreaGuard is integrated into the kernel of the operating system where it monitors all accesses of each process to a file system and compares if it is a privileged process. Only with AreaGuard can you enter a protected area and encrypt or decrypt data in this area. Encryption of a protected area is progressed by a special encryption engine which is integrated inside the kernel of the operating system. It reduces the possibility of data damaging.

6. Conclusion

Problems of information system security are rather big and wide and the above-mentioned threat of a user attack within an organization is only a part of all possible threats. According to analyse, 70-80% of known attacks are done by internal users (employees). The possibility which has been described is not the only threat which is involved with information systems by an employee. Nobody, who is responsible for the security of information system, can exclude this possibility and has certainly come across, whether it be a personal experience or by hearing about it, data being lost or taken. We are forced to think about data protection in a technical way because protecting data by law and believing in the confidentiality and loyalty of employees is not suitable for data protection.