UDC: 681.324
Original scientific paper

WORKSTATION SECURITY ENSURANCE

Alenka Hudoklin, Alenka Stadler

University of Maribor, Faculty of Organizational Sciences, Kranj, Slovenia
E-mail: alenka.stadler@fov.uni-mb.si

A methodology for the ensured security of a workstation connected in a computer network within an organization is presented. A technique for the determination of the required security level for a workstation's tangible and intangible components is described. A set of security measures for each security level of the workstation's tangible and intangible components is selected. The methodology is applied to workstations in the computer network of a Slovenian state agency. The required security levels for the workstation's tangible and intangible components are determined. Two sets of security measures corresponding to security levels determined for both types of the Agency's workstation components are listed.

Keywords: workstation, computer network, security, physical threats, logical threats, countermeasures.

1. INTRODUCTION

Nowadays, computer networks have become an integral part of business. A security breach of a computer network within an organization can result in loss of revenue, loss of productivity, the cost of new hardware or software, loss of customer confidence, legal and contractual fees, etc. Workstation security is an essential part of the overall security of the network. Unauthorized access to the system through a workstation represents one of the biggest security threats to the computer network.

In the literature, workstation security is usually treated as a part of network security. Possible security risks presented by the workstations and those features of security protection which address those risks are discussed, sometimes in detail (see e.g. [2], [3]). However, these authors do not allow for disparity among the sensitivity of assets within the different networks which result in the different consequences of potential security threats. We must bear in mind that workstations connected to different networks require a different level of security protection.

In principle, specific security measures for any particular workstation can be defined in the framework of conventional risk analysis (see e.g. [9]). Risk analysis involves the definition and evaluation of sensitive system assets, the identification and evaluation of possible security threats, and an assessment of asset vulnerability to a given security threat. Usually, it is very difficult to collect all the data needed for an efficient risk analysis. Data on the likelihood of a threat occurring, and data on the potential losses following such an occurrence are often not available. Therefore, recommendations for choosing the security measures corresponding to different classes of sensitivity of system assets would be of great help.

It is desirable to define the number of different security levels of a workstation according to the different sensitivity levels of system data. Each level of workstation security requires a different set of protective measures. Such an approach was used in the American military publication Department of Defence Trusted Computer System Evaluation Criteria known as the "Orange Book" [5]. The "Orange Book" states that the lower the discrepancy between the maximum sensitivity level of activities on a system and the minimum clearance of any user of the system, the lower the level of security required. The rationale behind this is that the threat of users with a low security clearance gaining access to highly sensitive information is more serious than any other threat. Bhaskar (see [1]) adapted these concepts to be applicable in the office environment and developed a method for the determination of workstation security levels. For each workstation security level, he presented the guidelines for workstation security protection. Among possible security threats, he took into account only unauthorized access to the workstation.

In this paper, we will describe a methodology for defining measures against security threats to the workstation connected to the computer network within an organization. Our methodology represents a modification of Bhaskar's methodology. Apart from logical security threats, physical threats were also taken into account. The methodology will be applied to the workstations of the computer network within a Slovenian state agency.

2. DESCRIPTION OF A WORKSTATION AND ITS COMPONENTS

A workstation is defined as a computer (an intelligent terminal or personal computer) connected to a computer network (local area network (LAN), wide area network (WAN) or metropolitan area network (MAN)). Apart from workstations, a computer network contains a mainframe or a number of computers providing specific services called servers (e.g. file server, security server, communication server, etc.).

A workstation's function includes:

- ❑ Interacting with the user through a graphical interface
- ❑ Preparing the user's request through standard interfaces for accessing the server
- ❑ Communicating with the server over a communication interface
- ❑ Performing analysis on the data received from the server to be presented to the user

Workstation components can be divided into two categories: tangible and intangible components. Tangible components are used to contain or to support intangible components. Tangible components include physical storage devices (disks or tapes), and other computer hardware (processors, memory boards, video screens, etc.). Intangible components are the following logical entities: the main memory contents (operating system and currently executing program with its working data), the user profile or account and the contents of the physical storage devices (files and directories).

3. THREATS TO WORKSTATION SECURITY

We have used the following definition of a security threat [12]: A security threat is any potential event or act that could cause one or more of the following to occur: unauthorized disclosure, destruction, removal, modification or interruption of sensitive information, assets or services, or injury to people. Threats to computer security can be grouped into two broad categories: physical threats and logical threats. Physical threats affect the actual existence and physical conditions of the computer facilities, and (indirectly) the data stored in the affected facilities. A logical threat is an intentional or unintentional activity affecting data stored or transmitted by the computer system.

Physical threats can damage or destroy only workstation components (tangible and intangible), while logical threats can affect the intangible components of the whole computer network within an organization. Through a workstation an intruder can access and misuse sensitive information stored in other computers in the network.

Workstation components should be protected against security threats by the implementation of adequate protective measures. Protective measures serve four basic purposes: avoidance, prevention, detection and recovery. Avoidance means simply not exposing workstation components to threats. Tasks should be organized so that threats can be avoided. Prevention includes hardware and software security functions, management controls as well as setting up and enforcing security policies. Detection seeks to discover misuse while it is occurring or after the fact. It serves four purposes: it deters misuse, allows the detection of a threat occurrence in time to reduce the damage, allows the identification of the perpetrators and reveals the vulnerabilities. Recovery includes restoring the damaged resources and trying to remove the vulnerabilities that allowed a security breach.

The selection of cost-effective protective measures against logical threats to a workstation's intangible components, and against physical threats to a workstation's tangible components depends on the sensitivity of the data stored in the system. Higher sensitivity data requires a stronger logical as well as a stronger physical protection. When a workstation is adequately protected against physical threats, logical threats cannot take place.

4. A METHODOLOGY FOR WORKSTATION SECURITY ENSURANCE

We will determine a number of security levels for a workstation connected to the computer network within an organization using the technique described in [1]. For each security level, we will analyze security requirements and select a set of appropriate protective measures against physical and logical threats to workstation components. We will not consider cabling and communication channels.

4.1. Security level for a workstation's intangible components

The process of determining the proper security level for the intangible components of a workstation within a given network (system) is divided into two distinct steps:

1. The sensitivity levels of all activities on the system and the clearance levels of any user of the system are defined. Then the maximum sensitivity level and the minimum clearance level are determined.
2. The maximum sensitivity level and the minimum user clearance level assigned in Step 1 are used to determine the required security level for the intangible workstation components.

Step 1

The sensitivity levels for system activities and user clearance levels are expressed on the same scale as shown in Table 1.

Table 1. Sensitivity and user clearance levels

SENSITIVITY/CLEARANCE	DESCRIPTION
U	Unrestricted
R	Restricted
C	Confidential
S	Secret
TS	Top Secret

The meaning of the sensitivity levels of system activities from Table 1 is:

U - applies to activities involving data that is not sensitive or classified;

R - applies to activities (usually of a routine or non-strategic nature) involving data which has a definite requirement for non-disclosure, the destruction or corruption of which may cause losses, inconvenience or embarrassment to the organization;

C - applies to activities involving low or medium level strategic information or information on significant sums of money, the unauthorized disclosure of which could reasonably be expected to cause damage to the business;

S - applies to activities involving information on large sums of money or high level strategic information, the unauthorized disclosure of which could reasonably be expected to cause serious damage to the business;

TS - applies to activities involving information that is of crucial importance to organization strategy or security, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the business.

The meaning of user clearance levels from Table 1 is:

U - applies to persons with no clearance or authorization, access would only be permitted to information for which there are no specified controls;

R - applies to persons who have authorized access to certain sensitive information of a routine non-strategic nature, for official use only;

C - applies to persons who are allowed access to certain low or medium level strategic information or to other information the knowledge of which might, if divulged, cause increased security threats;

S - applies to persons who are allowed access to high level strategic information, on a need to know basis;

TS - applies to persons with the need to know information of crucial importance to either strategy or security.

Step 2

Determination of the required security level for a workstation's intangible components depends on the result of Step 1 and on whether the system is an open or a closed one. The classification of a system as either open or closed depends on whether it is adequately protected against the introduction of malicious logic (virus, Trojan horse, etc.). Malicious logic is created mainly by application developers or maintainers. In a closed system these persons have sufficient clearance and authorization to justify the presumption that they have not introduced malicious logic. They should have the same clearance level as the most sensitive data, where the maximum data sensitivity level is confidential or below, or at least a secret clearance, where the maximum data sensitivity level is secret or top secret. The system is open, when the clearance levels of application developers and maintainers are lower than those described above.

In Tables 2 and 3, security levels for intangible workstation components in open and closed systems are given for all possible combinations of minimum clearance and maximum sensitivity levels.

Table 2. Sensitivity/clearance matrix for open systems

		Maximum sensitivity level				
		U	R	C	S	TS
Minimum user clearance	U	1	4	5	6	7
	R	1	3	4	5	6
	C	1	2	3	4	5
	S	1	2	2	3	4
	TS	1	2	2	2	3

Table 3. Sensitivity/clearance matrix for closed systems

		Maximum sensitivity level				
		U	R	C	S	TS
Minimum user clearance	U	1	3	4	5	6
	R	1	2	3	4	5
	C	1	2	2	3	4
	S	1	2	2	2	3
	TS	1	1	1	1	2

4.2. Security level for a workstation's tangible components

When determining the required security level for a workstation's tangible components, only the sensitivity level of system activities has to be considered. Countermeasures against physical threats do not depend on the clearance levels of authorized users or on whether the system is open or closed one. The security level for a workstation's tangible components corresponds to the maximum sensitivity level of system activities (see Table 4).

Table 4. Security levels for a workstation's tangible components

Maximum sensitivity level	U	R	C	S	TS
Workstation security level	1	2	3	4	5

4.3. Security measures

Security measures for a workstation's tangible components were grouped according to the type of physical threat. We used this categorization because the occurrence of any physical threat causes damage or destruction of the tangible component affected, independently of the tangible component type. Therefore, it is the type of physical threat that determines the protective measures required. We have considered the following types of physical threat: fire, rising water, falling water, hardware and software failures, lightning or power defects and physical malicious acts by an intruder. In order to find appropriate measures against each physical threat, we examined abundant literature on computer physical security (see e.g. [3], [6], [7], [8]). For each security level determined previously, we selected a set of measures against a given physical threat to a workstation's tangible components.

Security measures for intangible components were grouped according to the type of intangible component because logical threats affect different types of intangible component differently. In formulating of the sets of countermeasures corresponding to each security level for intangible components, we relied on guidelines published in [1] and the literature from [2], [4] and [10].

5. APPLICATION OF THE METHODOLOGY TO A WORKSTATION IN THE COMPUTER NETWORK WITHIN A SLOVENIAN STATE AGENCY

The security methodology described in the previous section was applied to the workstations of a Slovenian state agency (in the following text "Agency") working in the field of social security. The Agency consists of the headquarters and 12 off-site branches. There are over 400 workstations at the Agency's headquarters and 25 - 30 workstations at each of the Agency's branches. Workstations at the headquarters are connected to the host computer via a LAN, while workstations at the off-site branches use the X.25 network.

The Agency's computer network handles personal data about a great number of Slovenian citizens. Unauthorized disclosure of this data could affect citizens' privacy, which is protected by Slovenian law (see [11]). Therefore, aside from the confidentiality of strategic business information, the confidentiality of citizens' personal data must also be ensured. On the other hand, the unavailability or corruption of citizens' data can influence their incomes and burden the Agency with the cost of restoration of data lost or damaged. Consequently, the availability and integrity of citizens' data are also important.

In the following text we will determine security levels for the tangible and intangible components of a typical workstation in the Agency's computer network and propose a set of safeguards against physical and logical security threats.

5.1. Determination of security levels for workstation components

Step 1 of the methodology described in section 4 comprises the determination of the Agency's main activities, a definition of the users of the Agency's computer network, and the assignment of respective sensitivity and clearance levels. The results of Step 1 are shown in Tables 5 and 6.

It can be seen from Tables 5 and 6 that for the system observed, the maximum sensitivity level is C and the minimum clearance level is U.

In Step 2, we derived the security levels for both types of workstation components. The Agency's computer network was classified as a closed system because application programmers and maintainers have sufficient clearance (see Tables 5 and 6). Taking into account the results of Step 1 and Tables 3 and 4, the security levels were determined to be 3 for the workstation's tangible components, and 4 for the workstation's intangible components.

5.2. Security measures for a workstation's tangible components

At security level 3, we have recommended the following measures against security threats to a workstation's tangible components:

Protection against fire

- ❑ The building should be constructed of fire-resistant materials or protected by a fire-suppression system.
- ❑ The computer room should be equipped with clearly visible fire extinguishers.
- ❑ The personnel should be trained and drilled in the use of fire extinguishers.
- ❑ There should be sufficient fire and smoke alarms appropriate to the environment.
- ❑ Exits and evacuation routes should be clearly marked.
- ❑ All unnecessary sources of ignition should be eliminated or identified and accepted.
- ❑ Ready access for fire-fighting personnel should be ensured.

Table 5. Sensitivity levels of main Agency activities

Activity	Sensitivity Level
1 Clerk training	U
2 Document editing	U
3 Printed document acceptance or posting	R
4 Customer data backup	R
5 Statistical data analysis	R
6 Executing basic agency functions	R
7 Program testing	R
8 Program development and upgrading	C
9 Program distribution	C
10 Program maintenance	C
11 Data base administration	C
12 System analysis	C
13 Assignment of user access privileges	C
14 Control data verification	C
15 Central control of the data for executing basic agency functions	C
16 Computer system maintenance	C
17 Collecting temporary data for strategic decision making	C
18 Department management	C

Table 6. Clearance levels of different users

User	Clearance Level
1 Clerk	U
2 Registrar	U
3 Courier	U
4 Technician	R
5 Project manager	R
6 Operator	R
7 System analyst	C
8 Application programmer	C
9 Program maintainer	C
10 Data base administrator	C
11 Computer system maintainer	C
12 System programmer	C
13 System manager	C
14 Department manager	C

Protection against rising and falling water

- The computer room should be located on high ground or high in the building.
- Cut-offs for any water in the ceiling should be identified, labelled and accessible.
- The ceiling should be free of holes or defects.
- Plastic sheeting should be available.
- Provisions should be made for fast removal of water from the computer room.

Protection against hardware and software failures

- There should exist firm contracts concerning hardware and software purchasing and maintenance.
- A safety stock of critical hardware components should exist.
- Software backup should be available.
- Preventive maintenance of hardware should be undertaken according to an accepted policy.
- Corrective maintenance of hardware and software should be performed regularly.
- Any physical storage device should be checked daily for disk errors, bad sectors, etc.
- Appropriate operating conditions should be ensured.

Protection against lightning or power defects

- Lightning protection devices should be installed.
- Power conditioning equipment should be installed.

Protection against any physical malicious acts by an intruder

- The workstation should be kept in a dedicated room.
- The room should be lockable by a smart card with a PIN.
- All windows to the computer room should be inaccessible from the outside.

5.3. Security measures for a workstation's intangible components

For a workstation's intangible components at security level 4, we have recommended the following countermeasures:

Main memory contents

- An uninterruptible power supply should be installed.
- The workstation power supply should be separated from the power supply for other electrical equipment.
- Each user should be allowed to use only a specifed amount of the main memory of the system.
- The system break-in keys should be disabled.
- There should be a system manager who can manage and monitor the use of the operating system.

- There should be an access log, recording who has accessed the system and at what time, what has been printed out and which remote devices have been mounted, as well as all accesses to the system and to individual files and applications.
- A detailed audit trail should record all important transactions.
- Different classes of users should be given different privileges to perform operating systems' functions, depending on their need to do so and on their security clearance.
- Interactive system monitoring should be introduced. A "superuser" (security manager, auditor, etc.) should be able to monitor system activities in real time.
- The ability to write command language procedures should exist to enable greater control and security to be programmed into the operating system.

User profile or account

- A username and a password should be used.
- The minimum number of characters in the password should be six.
- Passwords should be able to expire.
- There should be an auto log-off facility.
- Access to the system should be restricted by preventing users from logging-on between certain hours.
- Remote access to the system should be controlled by a pass-code.

Contents of physical storage media

- Fixed or removable disks should be given read-only status when necessary.
- Fixed disks should be partitioned so that certain users are only allowed to address certain areas.
- Users must be prevented from being able to read (or write onto) the disk directly.
- Full backup of disk contents should be taken at least weekly.
- Incremental backup of disk contents should be taken at least twice daily.
- Old files should be erased with multiple overwriting.
- It should be possible to attach "create", "read", "write", "execute" and "delete" attributes, in any combination, to a file. These capabilities should be attached on the basis of "system manager", "owner", "group" and "world".
- Sensitive data should be encrypted.

The list of security measures presented enables an assessment and eventual improvement of the existing security level of each Agency's workstation. Special attention must be paid to protection against logical threats. An inadequate level of logical security at a single workstation in the Agency represents a serious security risk for the entire Agency's computer network.

6. CONCLUSION

The security of workstations connected to the computer network is a very important part of the overall security of the information system within an organization. An adequate security level of the workstation could be achieved by introducing appropriate measures against security threats. Selection of cost-effective protective measures depends on the sensitivity of the data stored or processed by the computer network. Higher sensitivity data requires stronger logical as well as stronger physical protection.

A methodology for workstation security ensurance has been presented. Workstation components have been divided into tangible and intangible components. Tangible components are vulnerable to physical threats, while intangible components are vulnerable to logical threats. We have defined five different security levels for tangible workstation components, and seven security levels for intangible workstation components. The security level for a workstation's tangible components depends on the sensitivity levels of activities on the system, while the security level for a workstation's intangible components depends on the sensitivity levels of activities on the system and on the clearance levels of the system users.

We have selected a set of appropriate security measures for each security level of a workstation's tangible and intangible components. Security measures for a workstation's tangible components have been grouped according to the type of physical threat, while security measures for the intangible components have been classified according to the type of intangible component.

The methodology described has been applied to workstations in the computer network of a Slovenian state agency working in the field of social security. It has been found that security level three for tangible components of a typical Agency workstation is required, while security level four is needed for a workstation's intangible components. We have listed a set of security measures for both types of workstation components.

REFERENCES

[1] K. Bhaskar. *Computer Security, Threats and Countermeasures*. NCC Blackwell, Manchester, 1993.

[2] S. Cobb. *PC and LAN Security*. Computing McGraw-Hill, New York, 1996.

[3] P. H. Corrigan. *LAN Disaster Prevention and Recovery*. PTR Prentice Hall, Englewood Cliffs, 1994.

[4] P. T. Davis. *Complete LAN Security and Control*. Windcrest. McGraw-Hill, New York, 1994.

[5] DOD 5200.28-STD, Department of Defence Trusted Computer System Evaluation Criteria. USA Department of Defense,1985.

[6] L. J. Fennelly. *Effective Physical Security*. Butterworth Publishers, Stoneham, 1992.

[7] R. P. Fisher. *Information Systems Security*. Prentice-Hall, New Jersey, 1984.

[8] M. E. Kabay. *The NCSA Guide to Enterprise Security Protecting Information Assets*. McGraw-Hill, New York, 1996.

[9] A. Reed and S. Watt. *Computer Risk Manager: A Manager for EDP Contingency Planning*. Elsevier, Oxford in association with Alkemi, Berkshire, 1989.

[10] R. C. Summers. *Secure Computing*. Computing McGraw-Hill, New York, 1997.

[11] Zakon o varstvu osebnih podatkov. *Uradni list Republike Slovenije*, No. 8/90, 1990.

[12] A. C. L. Zemler. *Guidelines for Computer Security at CQU*. Central Queensland University, CQU Computer Security Committee, Rockhampton Queensland, Australia, 1996.

Received: 7 June 1998
Accepted: 3 September 1998

Alenka Hudoklin
Alenka Stadler

ZAŠTITA SIGURNOSTI RADNIH STANICA

Sažetak

U članku je prikazana metodologija zaštite radne stanice od prijetnja koje utječu na sigurnost računalne mreže u organizaciji. Komponente radne stanice podijeljene su na opipljive i neopipljive. Opipljive komponente radne stanice uključuju eksternu memoriju (diskove, magnetne trake, itd.) i ostali računalni hardver (procesore, ulazno-izlazne jedinice, itd.). Neopipljive komponente radne stanice su sljedeći logični resursi: sadržaj primarne memorije (operativni sustav, aplikativni softver s pripadajućim podatcima), profil korisnika računalne mreže i sadržaj eksterne memorije (datoteke i direktoriji). Opipljive komponente izložene su fizičkim prijetnjama, dok su neopipljive komponente izložene logičnim prijetnjama. Definirano je pet različitih nivoa sigurnosti za opipljive komponenete i sedam nivoa sigurnosti za neopipljive komponente radne stanice. Nivo sigurnosti opipljivih komponenata radne stanice ovisi o nivou osjetljivosti aktivnosti u računalnom sustavu, dok nivo sigurnosti neopipljivih komponenata ovisi o nivou osjetljivosti aktivnosti na sustavu i o nivou ovlaštenja korisnika računalnog sustava. Predložen je niz zaštitnih mjera za svaki nivo sigurnosti opipljivih i neopipljivih komponenata radne stanice. Zaštitne mjere za opipljive komponente radne stanice grupirane su s obzirom na tip fizičke prijetnje, dok su zaštitne mjere za neopipljive komponente klasificirane prema tipu neopipljive komponenete. Opisana metodologija aplicirana je na radnu stanicu u računalnoj mreži jedne od državnih institucija u Sloveniji. Određeni su potrebni nivoi sigurnosti i navedene primjerene zaštitne mjere za oba tipa komponenata radne stanice.

Ključne riječi: radna stanica, računalna mreža, sigurnost, fizičke prijetnje, logične prijetnje, zaštitne mjere.