Distr.
GENERAL

CES/AC.71/2001/17
5 December 2000

ENGLISH ONLY

STATISTICAL COMMISSION and ECONOMIC COMMISSION FOR EUROPE

COMMISSION OF THE EUROPEAN COMMUNITIES (EUROSTAT)

CONFERENCE OF EUROPEAN STATISTICIANS

Joint ECE/Eurostat Meeting on the Management of Statistical Information Technology
(Geneva, Switzerland, 14-16 February 2001)

Topic (ii):Challenges and opportunities for statistical offices working in a network environment

THE PROBLEMS CONNECTED WITH SECURITY OF DATA TRANSFER VIA NETWORK AND THE SOLUTIONS IMPLEMENTED IN THE CSO OF POLAND

Submitted by Polish Central Statistical Office [1]

CONTRIBUTED PAPER

I. INTRODUCTION

1. The term “security policy" covers all tasks of management, administration, technical personnel, users and all other members of the organization involved in maintaining the necessary level of security of the statistical information system. This safety level is illustrated by the number of security features used. It serves to control access to resources (equipment, software, documentation, raw data), data confidentiality, authentication and data integrity.

2. The aim of this paper is to describe the methods used to solve problems connected with security of data transfer throughout the developed network of the Central Statistical Office (CSO). Government regulations, current technical means, and actions to be taken in the near feature will be considered.

[1] Prepared by Halina Agnieszka Stegawska.

II. GOVERNMENT REGULATIONS

3. Steps taken to ensure an adequate level of security for collected data, which is sent through the computer networks, processed, and made available, are based on the following legal acts:

- Public Statistics Act of June 29, 1995
- Protection Non-public Data Act of January 22, 1999
- Secret Chambers Directive of February 9, 1999
- Directive on Basic Requirements of Teleinformation Systems and Networks of February 25, 1999
- Directive on the Standards of Labeling of Confidential Materials, and on Assigning of Classification Level, of February 26, 1999.

4. Based on the above-mentioned acts and directives, the following guidelines for working in the computer network at the CSO were developed:

- Corporate network guidelines for STAT-GUS;
- Scheme network guidelines for LAN-US (LAN-VSO);
- Scheme network guidelines for LAN_GUS (LAN-CSO);

These guidelines were approved by the Head of CSO on November 27, 1997. A team was created to develop a set of organizational, technical and financial requirements for data security sector supervised by the Head of CSO.

III. THE PROBLEMS AND SOLUTIONS

III.1 Classification of possible data security problems

5. Possible problems in the breach of security of data processed by computer networks can be divided into three main categories:

- Intentional breach of security – the theft of an inscription key, or tapping of a network connection. If the data is encrypted using one of the commonly used algorithms, it is possible to break the code by systematic checking of all possible character combinations that make up the inscription key; this is know as a brute force attack. It may also be possible to steal an inscription key, which is sent over the network.

- Unauthorized data access - by logging in using a stolen or guessed password. Unauthorized access is also possible if there is a lack of a proper authentication procedure.

- Denial of service – due to the breach of security system, users can not use a given or all services of the equipment connected to the network or server.

III.2 Basic network security services

III.2.1 Identification

6. Users are identified by applications through a password (UserID). The user may have different passwords for all applications, but optimally should have a single, common password. In CSO all users have their own private UserID. Because of the cooperation between users, system administrators and the

network administrators, it is possible to assign one password to access different resources and services.

III.2.2 Authentication

7. Authentication is the process of a user's identity verification. This requires an exchange of secret information between the user and the application. The information exchange can be in the form of a password known only to the user or to dedicated equipment - of the challenge-response type, for example.

8. All users of information services, and especially those using network connection, are required by the CSO to give a password. This password and how it is entered must meet the following requirements:

- the password must be hard to guess or steal. New passwords are automatically checked and ones that are deemed to be too easy to guess are rejected. There is a procedure in the network use guidelines on how to store the password, depending on the level of the user – from network PCs to main administrators;
- the password should not be visible when it is being entered;
- the number of unsuccessful attempts to enter the correct password is limited. After the limit is reached, the system blocks the user's account, and suspends the login procedure for the user. The block on the account can be removed after the user is verified by the system administrator, or after a given amount of time;
- the password aging is taken into account. The user is informed by the system that on a given date the password will become invalid;
- the administrator has the ability to change, or to oblige the user to change, a password at any given moment;
- the user can change a password at any given time;
- to obtain access to some systems the user may be required to enter double passwords;
- the passwords can be assigned by the system. For example, access to some internet services is made available after the user enters their firewall assigned password.

III.2.3 Authorization and access control

9. Authorization is the process of assigning access rights to a user. Access rights determine the level at which the person is authorized to enter data, whether they can only read it, or can change the content of the file by adding their information.

10. CSO has many levels of authorization. Users can assign authorization level to files created on their working stations. When making discs available on the network, the user can also assign authorization level for files on the disc.

11. Access level to information on the servers is assigned by the server administrator, in accordance with the needs of the clients, only at the necessary level.

12. The corporate network administrator gives Internet access to users for the required services. The most popular access is to e-mail, limited access is given to telnet and ftp. Access to files is controlled to ensure that the usage of network services complies with the above-mentioned guidelines. In order to protect the data from hackers, access is limited strictly to users who are both authenticated and authorized.

III.2.4 Confidentiality of information

13. Confidentiality is concerned with protecting the information from being made public when it is not intended to do so. Classified information must be protected when it is stored and when it is being sent. When data is stored locally, its protection can be assured by following guidelines for access, or by encrypting. Data sent over the network should be encrypted or sent over connections, which guarantee the necessary level of security.

14. A high security level of information on CSO servers is accomplished by strictly following the procedures for assigning user access rights by administrators of the operating systems (SCO UNIX, HP-UX, and Windows NT), and by administrators of the file servers and data bases (for example INGRES, SQL server). In addition, access to certain information is monitored. The rights and responsibilities of administrators and users are clearly defined in the guidelines for using the networks.

15. The corporate network of the statistical department (WAN) ensures data transfer through Permanent Virtual Connection (PVC), in a network based on a Frame Relay protocol. Sending the data in this protocol makes it possible to achieve a high level of data security. The operator of the WAN network Telekomunikacja Polska (Polish Telecommunication) ensures a high level of data security on their nodes. In an effort to improve security between the nodes of the FR network and those of the Statistical Offices, double connections are utilized. Currently, some of the transferred data is encrypted using a public key, which is publicly available from the certificate authority, in accordance with the X.509 standard.

16. Connections between smaller offices and their supervisory statistical offices are made through a telephone line. A call-back method is used to increase the security level of the transfer, and the server.

III.2.5 Data Integrity and Digital Signatures

17. When sending confidential documents through the computer network, it is very important to check data integrity. This ensures that the document was not modified during transfer. The data integrity check most commonly consists of creating a message digest using an appropriate mathematical algorithm. Using the message digest, it is then possible to detect whether the document was modified, but this does not guarantee the authenticity of the document. Therefore, there is no effective way to determine beyond doubt who sent the document, when using just the message digest. The authenticity check is accomplished by also including an electronic signature with the document. The electronic signature can be made by encrypting the message digest with a key known only to the sender. The receiving party can then use a publicly known encryption key made available by the sender to decode the message digest. If this procedure produces a correctly decoded message digest, then the receiving party can be sure that the encryption was done using the sender's private key, and thereby verifies the origin of the transfer.

18. CSO is currently preparing to implement the data integrity and digital signature procedures into confidential document transfers.

IV. INTERNET ACCESS

19. The subject of secure Internet access, as well as access from Internet to the corporate WAN-CSO network, requires a separate discussion. All data processing resources inside CSO’s Intranet are closed by the "firewall system" to external users. Only www servers with public databases, connected in front of the 'firewall system" with proxy functions, are accessible via Internet. Users working in regional statistical

offices and in CSO LAN have access to the Internet only through a central firewall system. Use of the Internet services requires user authentication, and authorization for services such as email, www, telnet, and ftp. The system firewall is assisted by two additional routers, which make any hacking attempt into the system much harder.

V. STATISTICAL CONFIDENTIALITY – RELATED PROJECTS.

20. A data security system needs to be constantly modified to make use of newer techniques, which ensure a higher level of safety. With this under consideration, CSO is working on improvements in the areas of:

- determining weak points in the currently used firewall system, it's modifications, or possible replacement;
- changing the operating system to WINDOWS 2000 Servers and Windows 2000 PC;
- replacement of part of the equipment working in Local Area Networks and CSO Corporate Network with equipment of higher security level- e.g. Switch L3, new generations of the routers;
- implementation of the cryptography of data on the server and WAN levels;
- updates to the "Rules and Regulations for the Users of Computer Networks" and their implementations.

VI. CONCLUSION

21. In closing I would like to stress the importance with which security of the collected, processed and user available statistical information is treated by everyone in the statistical office. It is undoubtedly true that a system with unbreakable security in all areas is not possible. In practice, we find that some degree of risk must be accepted, because, as security systems are becoming more and more sophisticated, so are hacking techniques. In order to effectively protect confidential information it is necessary to find possible weak areas, which might become a cause of loss of confidentiality, integrity or availability of that information. For each area at risk, it is necessary to determine all realistically possible ways in which security can be broken, and develop methods to prevent such events. It can be helpful to use the services of a firm specializing in detecting and correcting weak points in a data security system.