CRYPTOGRAPHIC SOFTWARE SOLUTION FOR INFORMATION PROTECTION IN A CORPORATE INTRANET

Veselin TSELKOV

1. INTRODUCTION

The development of the Internet as the world's biggest network lays the foundation of the Information Society. The number of corporate systems based on the Internet technologies is gradually increasing. This leads to a rise in the threats and attacks to corporate Intranets. As a consequence, the security problems become imminent and have potentially greater impact.

The architecture of a corporate Intranet consists of nodes (local networks from workstations, servers, and communications devices) and internode communications.[3]

A number of technologies have been developed to protect these communications:

- firewalls
- virtual private networks (VPNs)
- traffic management;
- network management and audit;
- applications management and audit;
- intrusion detection systems;
- identification and authentication;
- encryption.

Cryptographic algorithms and mechanisms (symmetrical and asymmetrical) are the basis of almost all defensive technologies. However, for a significant part of commercially distributed products and technologies there are either government restrictions on the use of cryptographic mechanisms (for example, there are restrictions to the length of the keys in the United States) or necessity to receive special licenses allowing their purchase.[5,6]

Corporations dealing with top secret data have specific requrements towards their own cryptographic systems. The CSSW is a solution for cryptographic software to protect the information in a corporate Intranet.

2. BASIC CSSW SERVICES

CSSW is a Windows based software system for cryptographic protection. CSSW uses symmetrical and asymmetrical algorithms and provides the following services [1,2,7]:

- identification and authentication of users;
- identification and authentication of applications;
- cryptographic protection on file and block data levels;
- digital signature;
- access control to cryptographic functions;
- logs;
- cryptographic application program interface (CAPI).

3. ARCHITECTURE OF CSSW

CSSW consists of the following modules (figure 1):

- Crypto Machine (CM);
- Crypto Application Program Interface (CAPI);
- Local Crypto Server (LCS);
- Global Crypto Server (GCS);
- Security Administration and Control Center (SACC);
- Crypto Keys Distribution and Management Center (CKDMC);
- Security Applications.

Descriptions

Crypto Machine

The Crypto Machine is a system process, working on all workstations and servers. It is an OLE Automation Server providing access control and CAPI.

Crypto Application Program Interface

Crypto Application Program Interface is included in Crypto Machine. It provides a set of cryptographic functions to user applications, which must be developed as an OLE Automation Client.

Local Crypto Server

There is a Local Crypto Server in every node. LCS consists of:

- Crypto Container (CC). CC is a storage for cryptographic keys, system tables end logs of all users in its node;
- Crypto Requests and Keys Exchange (CRKE). CRKE realizes interactions in processes of key requests and exchange.

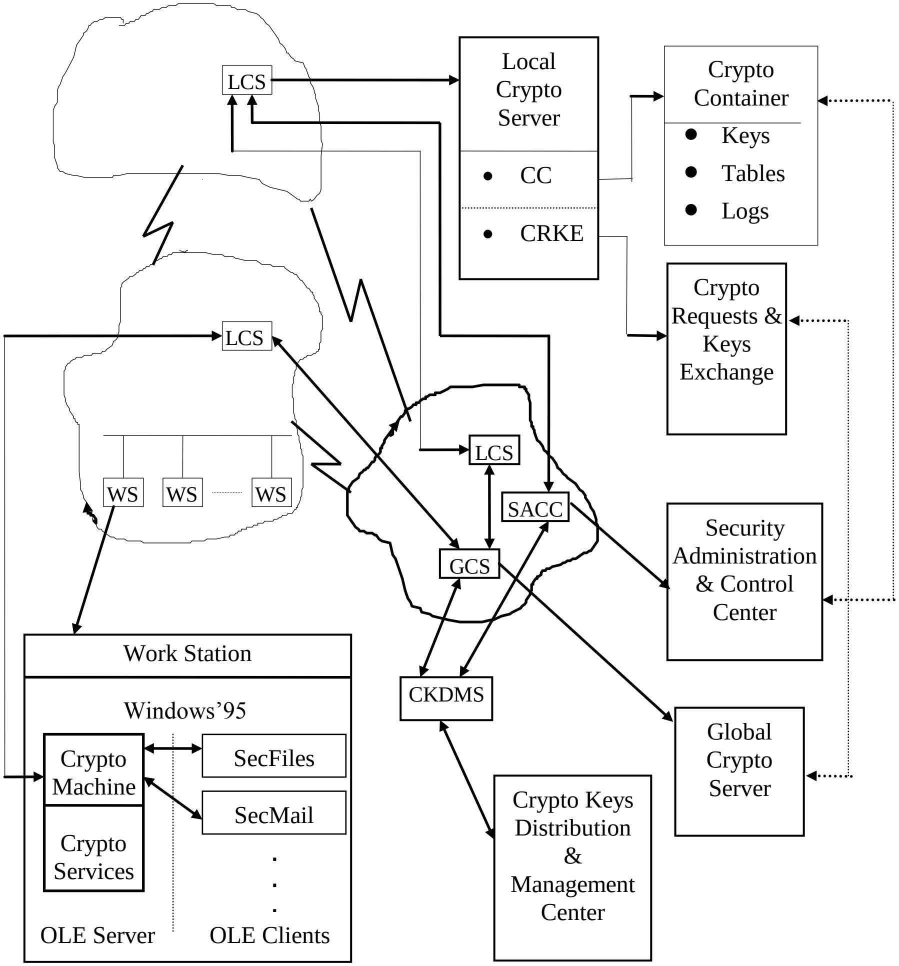

Figure 1: Architecture of CSSW

Global Crypto Server

The module Global Crypto Server executes requests for cryptographic keys and manages their distribution. It is only one for the whole corporate Intranet and controls all Local Crypto Servers.

Security Administration and Control Center

The module Security Administration and Control Center administers and controls the executed tasks with the CSSW system. Connected with all LCS, SACC summarizes and analyzes the information of all the logs.

Crypto Keys Distribution and Management Center

Crypto Keys Distribution and Management Center generates, distributes and manages keys and passwords. It is connected with GCS.

Security Applications

CSSW is an open system for designing and developing information security applications. Some of its typical applications are disk, directory, file, e-mail, clipboard, or data base protection. Based on Microsoft standards, all applications of CSSW can be integrated with Microsoft products, i.e., MS Office.

4. ORGANIZATIONAL STRUCTURES

CSSW supposes implementation of organizational structure including

- Administration and Control Center (ACC);
- Key Distribution and Management Center (KDMC);
- Security administrators (SA).

Administration and Control Center

SACC works in the ACC. SACC executes:

- definition of users, resources, and access rights;
- definition of schemes for information interactions;
- correspondence with the Key Distribution and Management Center;
- control of the state of CSSW;
- detection and reaction to destructive events;
- control of logs and audit.

Key Distribution and Management Center (KDMS)

KDMC generates keys and passwords according to the definitions by SACC.

Security Administrators

SA supports LCS (GCS) in the node by:

- defining users, resources, and access rights in the node;
- defining schemes for information interactions;
- configuring LCS;
- supporting cryptographic tools;
- installing and administrating both user's and LCS's software;
- communicating with ACC;
- detecting and reacting to destructive events;
- controlling logs and auditing.

5. CSSW DESCRIPTION

CSSW description includes description of nodes, workstations (users), applications, and groups of keys for each application. For each workstation the description covers the applications, which will use the cryptographic functions of the Crypto Machine module and the accessible (to this application) groups of keys.

The main nodes are described through Node.Name and Node.Id.
Main workstations are described through WS.Name and WS.Id.
The main application descriptions are Appl.Name and Appl.Id.
The main group descriptions are Group.Name and Group.Id.

Each workstation needs:

- a list of security applications working on this workstation;
- a list of available groups of keys for each security application.

System files

The system files for each workstation or server are:

- CryptoMachine.GFG - configuration file for the Crypto Machine;
- SysTbl - system table;
- ApplTbl - application table, containing a list of security applications working on this workstation;
- For each security application there is a ApplGrTbl - group table, containing a list of available groups of keys for each security application.

CSSW tools

Depending on its use, CSSW tools are separated as follows:

- software tools for a workstation;

- software tools for a security administrator;
- software tools for the Key Distribution and Management Center;
- software tools for the Administration and Control Center.

Software tools for a workstation

The software tools for a workstation include:

- Crypto Machine;
- Security Applications.

Data exchange between Crypto Machine and security application is based on the standard Windows interface - Object Linked and Embedded (OLE). The Crypto Machine is an OLE Automation Server and security applications are OLE Automation Clients.

A password is required to start the Crypto Machine. If the password is incorrect, the system function ShutDown will be executed.

A user, who does not know the password still may use the workstation without access to any cryptographic functions and encrypted data.

Each application, which uses the Crypto Machine, is identified and authenticated. If this is done successfully, the application receives a list of available groups of keys and continues to work normally.

Every Crypto Machine writes the executed tasks in a log file. The record of the log file contains:

- workstation's IP address;
- application name;
- date and time;
- cryptographic service;
- key;
- error code.

The log files can be accessed from the Administration and Control Center or the security administrator.

Software tools for a Security Administrator

The software tools for a security administrator include:

- LCSConfig - for configuration of LCS;
- LCSActual - to support keys and passwords;
- LCSInstall and CMInstall - to install software on the LCS and workstations;

- LCSConfig and CMConfig - to configure software on the LCS and workstations;
- CSSWView - to audit the use of Crypto Machines.

Software tools for KDMC

Software tools for Key Distribution and Management Center include:

- a tool for definition of the architecture;
- a tool for definition of security applications and groups of keys;
- a tool for definition of relations between workstations, applications, and groups;
- a tool for generation, distribution, and management of keys and passwords;
- a tool for audit and control.

Software tools for Administration and Control Center

Software tools for Administration and Control Center include:

- a tool for administration;
- a tool for audit and control.

There are two modes of work:

- reporting all records in the logs;
- filtered reporting.

The CSSW, described in this article, was designed on DELPHI, v.3 –5,[4] and based on DBMS ORACLE. It was applied in projects of the Institute for Advanced Defense Research of the "G.S. Rakovski" Defense Academy in Sofia, Bulgaria.

References:

1. Veselin Tselkov, *et.al.*, “A software security tools for information protection in PCs – “CS_SECURE_TOOLS,” in *Proceedings of the First National Conferences “INFORMATIC’94”* (Sofia, Bulgaria: SAI, 1994), 235-240.

2. Dragomir Pargov, Veselin Tselkov, Rusin Petrov and Iliya Kraytchev, “Security in Computer Systems,” in *Information Aspects of Security and Development of Modern Societies*, Velizar Shalamanov and Todor Tagarev, editors (Sofia: AFSEA-Sofia, 11 - 13 September 1996), 93-98.
3. Veselin Tselkov and Dragomir Pargov, “Security of Information System on Internet,” in *Proceedings of 1997 AFCEA-Sofia Seminar* (Sofia: 4-5 December 1997), 40-48.
4. M. Cantu, *Mastering Delphi 5* (Sofia: Softpress, 2000).
5. Br. Schneir, *Applied Cryptology* (John Wiley, 1996).
6. *RSA*, Available at http://rsa.com.
7. Deborah Russell and G.T. Gangemi, *Computer Security Basics* (O’Reily & Associates, 1991).

VESELIN TSELKOV see page 59.