Investigation of Methods Providing Information Security in SWIFT System

Sergii Budzherak, Lviv Polytechnic National University
(01.12.2010, Postgraduate Student Sergii Budzherak, Lviv Polytechnic National University)

Abstract

Methods, program software as well as organizational events, providing information security at the commercial banks during money transfers using SWIFT system, have been investigated. Cryptographic protection using in the system during sending electronic messages and external payments have been analyzed. Based on the obtained results present protection of the system interface has been illustrated as well as perspectives of its development in the future have been estimated.

1. SWIFT

Paper is dedicated to the external bank payments security using system SWIFT. The fact that more than 120 Ukrainian commercial banks became participants of this system (as well as the National Bank of Ukraine) increases the importance of the information security level of such payments.

S.W.I.F.T. (Society for World-wide Interbank Financial Telecommunications) is a leading international organization in the sphere of financial telecommunications. The main directions of SWIFT activities are: providing operational, serviceable, effective, confidential and protected from an unauthorised access telecommunication service for banks as well as providing work connected with standardization of forms and methods of financial information exchanging.

SWIFT provides its participants with number of unique facilities:

- increasing of the effectiveness of the commercial bank work due to using standardization and modern methods of information transfer;
- providing serviceability during transferring messages (coding and special order of sending and receiving);
- direct access of banks-participants SWIFT to their correspondents, branches or departments all over the world (ordinary message could be obtained during 20 minutes, urgent — till 5 min.);
- using standard messages helps in breaking language barriers and eliminate differences in practice of using international bank operations;

- guarantee of secure transfer, that means protection from false representation, loosing information as well as obligated reply for all payment orders and financial messages (during all the period of SWIFT work there was neither any case of sending fraudulent, nor case of users losses due to SWIFT fault).

Now SWIFT has about 8300 users (credit and financial organizations) from 208 countries all over the world. All of them, despite their geographical situation, have an opportunity to cooperate twenty-four-hour one with each other during 365 days in a year. Every day more than 12 millions financial messages have been transferring with total cost more than 6 trillions US dollars. Totally traffic volume in 2009 was 3,8 billions messages.

Based on SWIFT more than 50 national payment systems were established.

2. Cryptographic protection

Leading role in the security of SWIFT-payments belongs to cryptographic information protection [4] — type of protection connected with the way of information transformation using special (key) data for hiding/restoring sense of information, confirmation of originality, completeness, authority etc.

Investigated in the work X.25 [2] — is the family of protocols of the tunnel level of the network model OSI. X.25 provides a number of Permanent Virtual Circuits (PVC) and Switched Virtual Circuits (SVC)) at the same connection line, identified at the X.25-network according to the Logical Channel Identifier (LCI) or Logical Channel Number (LCN)).

Due to the serviceability of the protocol and its working over general using telephone networks X.25 was widely using in SWIFT, however now X.25 was driven out by the other tunnel level technologies (Frame Relay, ISDN, ATM) and by IP protocol, leaving, however, widely spread in the countries and territories with undeveloped telecommunication infrastructure.

X.25 determines telephone network characteristics for data transferring. To begin
connection, one computer apply to other concerning session. The other computer can accept or reject the connection. In the case of request acceptance, both systems can begin information transfer with total duplicating. Any side in any time can stop connection.

Advantages of X.25 network:
- either analog or digital canal data transferring could be used;
- connection all round the world — with any point in any country;
- possibility of connection with any producer equipment, coincident with OSI standard;
- possible connection between products IBM, DEC, Unisys, HP, Prime, Wang, Tandem, NCR and other main producers in the same network (therefore X.25 is the general standard protocol data transferring; most of the manufacturers support X.25 with built-in direct access facilities in host-computers, controllers or communication processors);
- complete data, high serviceable, security, network administration;
- Network disadvantages: significant delay burst transfer, therefore it cannot be used for voice or video information transfer.

Public Key Infrastructure [1, 3] (PKI) – authentication technology using open keys. This is a complex system, connecting open keys with user authentication with certification center.

PKI is a modern authentication technology using open keys with such mechanisms:
- assurance mechanism based on the assurance model;
- mechanism of using names unique at the environment;
- mechanism of spreading information, characterizing correctness connection of the appropriate pair of keys (open and secret) with the appropriate subject name in determined environment.

Base of PKI is a system with certification center and users as the main components.

Reliability service is based on PKI, it provides only electronic evidence for time of signing or data transfer and authentication of data sources, which in the conflict case between the sides could be taking into account in the court.

Program-technic protection methods in SWIFT are:
- codes of evidence of the original messages, which are generating during entering by special algorithms and a basing on the messages content. Though all know algorithm, the appropriate key know only sender and receiver;
- sequence messages control.

SWIFT messages have unique entrance and exit numbers during every session. Entrance sequence is estimated by slice-processor, while exit sequence - by receiver. These numbers are verified during sending and receiving and when they are not in the appropriate sequence, the messages are not only blocked, but the user terminal is switching off also. This mechanism guarantee, that no one message could be deleted and not duplicated.

There is also strict sharing responsibility for supporting security at SWIFT system. Bank, connected to system, is responsible for correct using and physical protection of terminals, modems and connection lines to the regional processor, for correct message during sending it into network as well as for working terminals. All other responsibility for sending messages takes administration of system. Protection control is providing after random time periods for checking the appropriate level of security. Responsibility of company begins in the moment of receiving digital message to the SWIFT access point and finishes at the moment of its leaving of the access point. Company is not responsible for security, connection facilities and connection lines between SWIFT access point and users terminals. Moment, from which SWIFT is not responsible for delivery, is confirmation of the receiver about receiving of the message.
3. Architecture of SWIFT network

Architectures of SWIFT network is multilevel (fig.1). At the first (lowest) level are clients and financial institutions with installed interface systems (IS). Regional SWIFT processors are at the second level. Any number of different interface systems can be connected to one regional processor (RP). Main computer SWIFT centers are at the third level (so called slice-processors - SP). SP are responsible for routing and saving messages. At the highest (fourth) level there are processors of system control, SCP, for providing monitoring of system functioning. SCP is constantly controlling and managing all the active system elements as well as all the access to the whole system.

SWIFT is more safe than any system of strategic defense of any country. There are four processing centers in the world at different continents and connected with duplicated canals, which are working synchronized.

4. Conclusion

Investigation of the connection to the SWIFT system has been carried out, management-administrative, technic-engineering as well as security policy at SWIFT system have been examined. Cryptographic protection, provided by protocols X.25, IP and open key infrastructure PKI have been analyzed.

Bibliography


Authors:

Mr. Sergii Budzherak
Lviv Polytechnic National University
vul. Knyazya Romana 1/3
79008 Lviv
tel.+380 (68) 184 00 16
email: budzik19@gmail.com