2-2002

Security Control in Inter-bank Fund Transfer

Dan Zhu
Iowa State University, dzhu@iastate.edu

Security Control in Inter-bank Fund Transfer

Abstract

Modern financial institutions have cashed in on the electronic business opportunities of the Internet by developing numerous payment systems to meet various payment service requirements. Advanced computer systems and telecommunications technology are being used to offer fast, convenient, and secure ways to conduct financial transactions at service and security levels that are hardly or never achieved by traditional payment systems. In this paper, we examine the function and operation flow of the electronic funds transfer process as well as its security control mechanism. To evaluate telecommunication and data security techniques, a standard-leading inter-bank payment system called the Society for Worldwide Inter-bank Financial Telecommunications System is introduced. Some important security features are investigated in detail.

Disciplines

Business | Communication Technology and New Media | E-Commerce | Finance and Financial Management

Comments

This article is published as Zhu, Dan. "Security control in inter-bank fund transfer." *Journal of Electronic Commerce Research* 3, no. 1 (2002): 15-22. http://www.jecr.org/node/288. Posted with permission.

SECURITY CONTROL IN INTER-BANK FUND TRANSFER

Dan Zhu
Department of Logistics, Operations and MIS
Iowa State University
E-mail: dzhu@iastate.edu

ABSTRACT

Modern financial institutions have cashed in on the electronic business opportunities of the Internet by developing numerous payment systems to meet various payment service requirements. Advanced computer systems and telecommunications technology are being used to offer fast, convenient, and secure ways to conduct financial transactions at service and security levels that are hardly or never achieved by traditional payment systems. In this paper, we examine the function and operation flow of the electronic funds transfer process as well as its security control mechanism. To evaluate telecommunication and data security techniques, a standard-leading inter-bank payment system called the Society for Worldwide Inter-bank Financial Telecommunications System is introduced. Some important security features are investigated in detail.

1. Introduction

Information security is considered one of the most critical concerns in today's competitive digital economy. Web technologies provide an amazing infrastructure for electronic data interchange (EDI), direct marketing, and information retrieval (Palmer and Griffith 1998). In particular, electronic banking and financial services have immense growth potential via the Internet. Some of the most important security issues involve electronic money and digital cash. As more and more companies jump onto the information superhighway with interactive web sites, information security becomes an important issue in digital economy (Wang, Lee and Wang 1998).

The intrinsic properties of the Web determine its vulnerability to failure and attack. Evidence of computer network insecurity is all around us. According to the CSI/FBI 2001 computer crime and security survey conducted by the Computer Security Institute (CSI), 85% of respondents (primarily large corporations and government agencies) detected computer security breaches within the last twelve months (Power 2001). The study also found that the most serious financial losses occurred through theft of proprietary information and financial fraud. The information loss incurred by web-based companies is almost double the losses incurred in the previous year. Unfortunately, the value of information security often is not adequately emphasized. This is partly because implementing security systems represents a cost burden that does not reflect an immediate return, and partly because organizations are sometimes unaware of security breaches.

A security mechanism is used to enforce a security policy. Security mechanisms for web servers and clients address vulnerabilities of the software, operating system, and communication channel. Mechanisms include correctly configuring the network and host, configuring the web application, authenticating and authorizing the Web service, using firewalls effectively, logging, and monitoring. Lack of Web security can pose a threat to an individual or a company. Valuable data can be stolen, altered, or even destroyed by cracking passwords, eavesdropping and impersonation. For example, credit card services that do not utilize proper security mechanisms jeopardize the security of their clients' credit card information. Unwanted changes may be made to individual or business web pages. Pranksters can also crash systems/networks, which businesses and individuals will have to rebuild at their own expense. In addition, organized crime and information warfare presents even greater threats to our society in general.

The main objective of this research is to examine the function and operation flow of the electronic fund transfer (EFT) system as well as its security control mechanism. Payment is the act of exchanging something of value for a product or service (Summers 1994). The major methods of payment used in a modern society include cash, check, credit card, electronic funds transfer, and so on. The essence of these mechanisms is the credit of participants in the payment process. Payment is achieved by transferring ownership of assets, often "money." To fully investigate an inter-bank EFT system (including its network architecture and operation interface), a custom-built, message-handling system called the international Society for Worldwide Inter-bank Financial Telecommunications (SWIFT) system is introduced as a case study. SWIFT is a system used to perform international funds transfer. It is owned by a company composed of more than 1400 share-holding member banks, which are located in more than 600 member countries in North, Central and South America; Europe; Africa; Australia; and the Far East (Davies and Price 1989). The network has been in operation since 1977.

The rest of this paper is organized as follows. Section 2 provides the background and introduces the mechanisms of inter-bank electronic fund transfer. Section 3 describes the system and network architecture of the SWIFT. Section 4 discusses security control and presents a proposed system to improve the security features. Finally, section 5 concludes the paper and points out directions for future research.

2. Background

Internet and client server computer networks often lack built-in security measures. Some of the security measures include a number of metrics along the following dimensions such as data confidentiality, data integrity, data availability, organization performance, impact on customers, and impact on suppliers (Johnson 1998; Pfleeger1997). Risk assessment of information security involves analyzing a system's information needs and vulnerabilities to attack as well as the costs of losing or recovering the system and its information. A brief review of the literature indicates that one of the major factors that make a network more vulnerable is due to its distributed nature in the configuration of client server networks. Firewall is commonly used by enterprises to safeguard their computer network systems from intruders (Goncalves 1998). Encryption and decryption provide the technology that transforms plain text into cipher-text. Thus, only those who know the decryption key can decrypt the cipher-text to obtain the original readable data.

Research in Internet security has primarily focused on resolving complex computer security problems by developing new encryption algorithms in cryptography (Mainwald 2001). A widely adopted implementation of secret-key cryptography is Data Encryption Standard (DES). Recent effort has been devoted to research and development of advanced encryption standard (AES) (Abdalla and Bellare (2000), Desai 2000, Bellare and Rogaway 2000, Nechvatal et al. 2000, Hikari-no-oka et. al. 2000, Ko et. al. 2000, Paillier 2000). Other researchers focus on cryptanalysis, that is, on how to break encryption algorithms. Biryukov and Shamir (2001) describe a surprising efficient attack on block ciphers that contain alternate layers of invertible S-boxes and affine mappings. The attack proposed in this paper could also be used on Rijndael, the winner of the AES competition. To find a more robust replacement for the DES, NIST announced the advanced encryption standard (AES) in January of 1997 (Nechvatal et al. 2000). In 1998, the NIST selected 15 candidates for the AES, which were then subject to preliminary analysis by the world cryptographic community. In August 1999, NIST selected five algorithms for more extensive analysis, and Rijndael had been selected as the proposed candidate for the AES. Rijndael is a block cipher that uses keys and blocks of 128, 192, or 256 bits. The algorithm consists of 10 to 14 rounds, depending on the size of the plaintext block and the size of the key. Rijndael should appear in many systems in the near future and should be considered as an appropriate alternative to TDES.

Encryption and decryption provides the secrecy of data communication, but intruders still can tap transmission media and falsify the message. Also, reneging and forgery from the two parties of the transaction may exist. Message authentication and electronic signatures are applications of encryption systems that provide verification of message integrity, data origin authentication, and protection against repudiation. Message authentication is a procedure that allows parties to verify that the received messages are authentic, i.e.; they are genuine and have come from their alleged sources. Before the message is sent, it is fed into an authentication code generator, which creates a code that accompanies the message to the receiver. Upon receipt of the message, the receiver performs an authentication code calculation and obtains another authentication code. If the message has not been altered, the same authentication code will be generated. Multiple algorithms can be used for authentication code generation. If there are no authentication keys, some kind of hashing function can be used, but this method suffers from collision problems, i.e., a falsified message generates the same authentication code with the original message. Encryption/decryption algorithms are often used for authentication. When the RSA cipher algorithm is used, the generated authentication code is called an electronic signature because it is from a proprietary private key and no one else can falsify his/her signature.

In addition, transport security (tunelling) is a technology that enables one network to send its data via another network's connections. Tunneling works by encapsulating a network protocol within packets carried by the second network. Layer Two Tunneling Protocol (L2TP) is an extension of the Point-to-Point Tunneling Protocol (PPTP) used by an Internet service provider (ISP) to enable the operation of a virtual private network (VPN) over the Internet. Vaults, such as data vaults, server vaults, and hardened OS vaults, can be used to protect not only business data and e-commerce applications, but security services as well. In this design, critical applications such as firewalls and PKI systems can be put in a vault. Many tools provide an access control and host-based intrusion prevention suite for Windows-based networks. Some use a distributed agent/console architecture to monitor inbound requests to designated applications, including Web, file and database servers, as well as desktop hosts. Agents control the application's ability to access file, network, registry and COM resources based on predefined policies. When resource requests are flagged as potentially malicious, the agent denies them and sends an alert to a centralized Web-based management console via SSL. The console then correlates alerts to provide a network-wide picture of attack or misuse patterns. Unlike network-based intrusion detection systems (Zhu et al. 2001), these

agents don't use signature-based scanning to detect potential attacks. Rather, each agent is configured at a specific threshold for suspicious events according to the purpose, sensitivity and placement of the application it's protecting

The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. SSL is included as part of both the Microsoft and Netscape browsers and most Web server products. Developed by Netscape, SSL also gained the support of Microsoft and other Internet client/server developers as well and became the de facto standard until evolving into Transport Layer Security. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate.

Inter-bank EFT uses on-line transactions carried out on private networks to transfer funds; the bank plays the role of both payer and payee. Such transfers occur between a bank and its customers, or a bank and another bank. In contrast to a check payment, which requires several actual cryptographic processing days and manual efforts like signature verification, check sorting, and information capture, EFTs are same-day, almost instantaneous payments. Figure 1 illustrates one method used for such transfers to conduct payments.

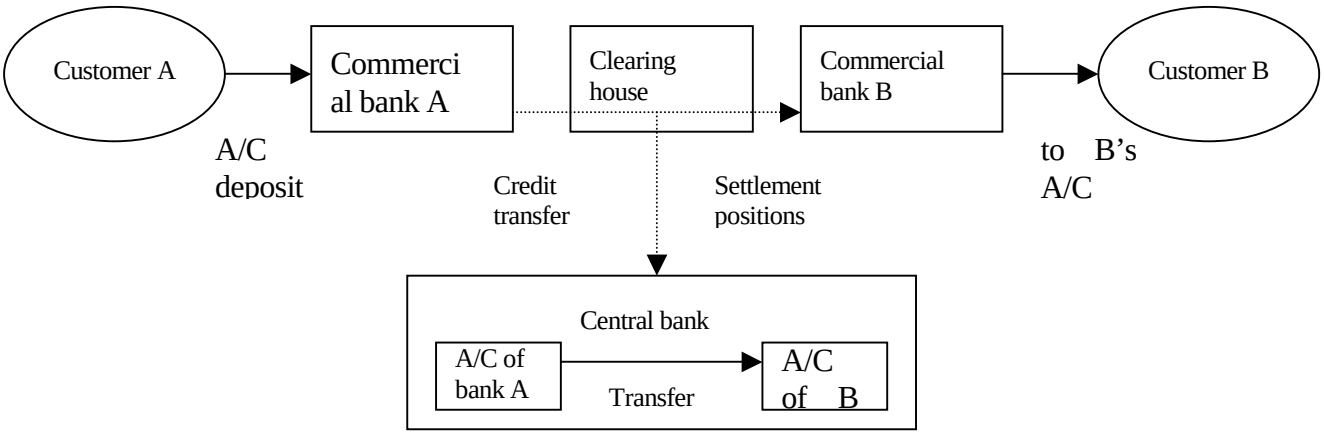


Figure 1. A method of funds transfer to conduct payment

As shown in Figure 1, customer A uses commercial bank A to remit a fixed amount of money to customer B and his/her commercial bank B. After receiving the remittance amount plus any fees, commercial bank A sends an electronic credit transfer message to commercial bank B through a clearinghouse. According to the credit instruction, commercial bank B credits the remittance amount to customer B's account (or advises customer B to pick up the check). After a fixed accounting period, the computer system at the clearinghouse will calculate the settlement positions for participating banks and send them to the central bank via telecommunication channels. The system at the central bank will use the accounts held by commercial banks to perform debit/credit operations for clearing the difference of transfer amount among banks, thus completing the funds flow of remittance process. EFTs can achieve immediate payment across two remote sites by the telecommunication facility under some credit line arrangement, but there must be some way to ensure the security of the remittance. Such protection should prevent the revelation of the information as well as illegal modification of it, by both external attackers and internal betrayers.

Large amounts of money are involved in everyday funds transfer transactions, therefore, the security of systems and the smooth of operation must be maintained. In general, there are five central requirements of network security (1) Confidentiality: Data should not be disclosed to unauthorized persons; (2) Access control: Operation of the system is under some control mechanism to prevent illegal access of data; (3) Integrity: Message information should remain original to carry designated transaction details. (4) Data origin authentication: Some way is used to prove the source of data; (5) Non-repudiation: System should provide some features to ensure that nobody can deny involvement in an electronic transaction so that the legal effect of an EDI transaction can be relied on.

Cryptography has been widely applied in data communication to meet the above security requirements. In the following sections, some key technologies of cryptography are introduced and the security features of SWIFT are studied.

3. System architecture

To further investigate the inter-bank EFT system, its network architecture, and operation interface, we introduce a custom-built, message-handling system -- the international Society for Worldwide Inter-bank Financial Telecommunications (SWIFT) system. The best way to identify security risks in a computer network is to examine its current configuration. In this section, we introduced the system architecture.

3.1. Network structure

Operating centers of SWIFT are located in the U.S., Belgium, and the Netherlands with store and forward procedures processing all messages. In member countries, there are regional processors connected to operating centers by leased lines. The connections are duplicated to cope with contingencies. All connections from member banks to the network are concentrated through regional processors, and there are emergency lines to let customers connect to alternative regional processors when one processor becomes corrupt. The SWIFT system can report statistics on messages sent and received. It has a 14-day backup, which allows it to retrieve messages up to two weeks after the original transmission dates. This helps banks check the status of messages when problem occurs in the content of messages or completeness of their traffic.

Network protocols used in Swift include TCP/IP and X.25. The X.25 protocol, adopted as a standard by the Consultative Committee for International Telegraph and Telephone (CCITT), is a commonly-used network protocol. The X.25 protocol allows computers on different public networks (such as CompuServe, Tymnet, or a TCP/IP network) to communicate through an intermediary computer at the network layer level. X.25's protocols correspond closely to the data-link and physical-layer protocols defined in the Open Systems Interconnection (OSI) communication model. The IP based SWIFT network connects financial institutions worldwide and extends from the SWIFT operating centers to the Customer premises. The major components of a Swift System consist of the Secure IP network (SIPN), Connection, SWIFTNet, SWIFTNet Link, SWIFT Interface, etc. The Secure IP Network (SIPN) is a private network of leased bandwidth owned by SWIFT. The SIPN is based on TCP/IP, a proven technology that provides a high level of technology, interoperability and openness. Connection can be made by through the Customer premises equipment (CPE) via a leased line or ISDN to a SWIFT Point-of-Presence (POP) system, or by PSTN or ISDN dial-up connection. The CPE is an optional IP routing and traffic-filtering device, provided by SWIFT and placed at the Customer premises. SWIFTNet Link is a software package provided by SWIFT and its installation is a pre-requisite to gaining access to the SWIFTNet services. It provides Application Programming Interfaces (APIs) to third party application vendors. As a third-party, SWIFT also offers two applications and services based on SWIFTNet Link. One is called SWIFTAlliance WebStation, which is a browser-based interface that is integrated with SWIFTNet Link to suit end user traffic. Another is called SWIFTAlliance Gateway, which is a server-based interface that is integrated with SWIFTNet Link to suit high volume application-to-application traffic.

SWIFT requires that each customer have a dedicated terminal with pre-accredited software. That dedicated terminal will include encryption, authentication, and data scrambling on it. The terminal (often referred to as a SWIFT) Interface Device or SWIFT Interface is what is connected to the network – via leased line, X.25, dial up or whatever. It is a trusted terminal and, once a message has been submitted. Once in the network the SWIFT formatted message (there are different formats for different purposes) will be carried to the designated counter party. The SWIFT Interface is typically located in members' offices. The nine primary categories of financial messaging supported include customer transfers, bank to bank instructions, foreign exchange and derivatives, documentary collections, securities, syndicated loans and precious metals, travelers checks, documentary credits, statements, advice, and general messages.

3.2. The message-passing payment process

Strictly format-defined messages are composed by SID and sent through the network to perform payment functions. Message types are divided into categories according to different types of transactions. Some examples of SWIFT message categories include (1) customer transfers; (2) bank transfers; (3) foreign exchange, loans/deposits; (4) documentary collections; (5) securities; (6) reserved for future use; (7) documentary credits; (8) special payment mechanisms; (9) special messages, and so on.

The names of the sending bank and receiving bank are contained in the header of the message, which directs the message text through the system. This type of message represents the simplest kind of transactions – a paying customer has an account with the sending bank and the beneficiary customer has an account with the receiving bank. The settlement position is cleared through an account held by one of these banks for the other. Whether this is the sender's account with the receiver's bank or the receiver's account with the sender bank depends on the transaction currency. If the transaction currency is that of the sender's country, the sending bank credits the account held by the receiving bank. If the transaction currency is that of the receiver's country, the receiving bank debits the account held by the sending bank. In other cases, messages are transmitted through intermediate banks and a third-party corresponding bank performs the settlement. Such payment involves more complex routing and accounting relationships. A sample SWIFT payment message with field labels is depicted as below.

Account	Transaction Ref#	ISIN#	Security Description	Opening Balance	T/ D	S/ D	Transaction Type	Amount	Status

Transaction Types

MESSAGE TYPE (MT)	DESCRIPTION
MT540	Receive Free
MT541	Receive Against Payment
MT542	Deliver Free
MT543	Deliver vs. Payment
MT544	Confirmation of Receive Free
MT545	Confirmation of Receive Against Payment
MT546	Confirmation of Deliver Free
MT547	Confirmation of Deliver Against Payment
MT548	Statement Status and Processing Advice
MT535	Statement of Holdings
MT536	Statement of Transactions
MT537	Statement of Pending Transactions

Figure 2. A Sample Swift Payment Message

3.3. Applications

For over twenty years, SWIFT has been used to support a large number of applications in financial industry. For example, CB Biochim Plc is one of the first Bulgarian banks that became a member of SWIFT in early 1990s. It has successfully transmitted large amount of financial messages in accordance with SWIFT program. Elink Transfer is another example application that utilizes SWIFT to process transfers from Germany to Finland banks. The Syllog SSB presents another application that can be used to connect any firm to the SWIFT network, and can send and receive any type of SWIFT message.

4. Security control of SWIFT

4.1. Security Risks and Planning

Some of the main risks involved in Swift may come from hackers, increased dependence of banks on IT, Open Technologies, and increased electronic access by customers. Attacks on the system are possible by the following means: (1) Readily available sophisticated hacking tools; (2) Packet/Address spoofing; (3) Stealth diagnostics; (4) Sniffers; (5) Sweepers; and (6) Backdoors

Current general security planning for Swift could include the following:

- Formulate Security Policy
- Allocation of responsibilities which includes separation of duties and dual control
- Assets Classification through assigning owners and business risk analysis to ensure confidentiality, integrity, and availability
- Personnel Security's major task is to create security awareness among employees
- Physical Security enforcement includes concentric security parameters, locks and identifications, and proper maintenance
- IT Security focuses on system access control (such as user identification, authentication and authorization), secure transmissions (such as message encryption, message authentication, message signature, non-repudiation, proof of origin, proof of delivery), and system integrity at both production (such as database integrity and Operating System security) and delivery level (quality assurance).

4.2. Security Control

The main security control features of the SWIFT system includes end-to-end authentication, sequence number control, user access control, and encryption between operating centers.

4.2.1. End-to-end authentication

SWIFT provides secret-key and end-to-end authentication; i.e. authentication between two banks detecting any bogus payment message. Bilateral keys are managed manually according to SWIFT-issued guidelines. Such manual procedure

suffers from key generation and transportation problems. To ensure the secrecy of transaction information, each bank is required to generate a unique key for every bank it does business with. This creates a severe key management problem for the large number of banks worldwide. Transportation of keys is another problem; if you could send the secret key from the sender to the recipient securely and in a tamper-proof fashion, you would not need the symmetric crypto-system because you would simply use that same secure channel to send the payment message. The end-to-end layer provides transaction-level capabilities secured through digital certificates as issued by the SWIFTNet Public Key Infrastructure (PKI). Features of the end-to-end layer include the following: (1) Provision of trust through non-repudiation, end-user authentication and access control; (2) Protection against fraud by supporting end-user access-control and end-to-end integrity and confidentiality; (3) The facility for applications to encrypt and sign individual transactions.

4.2.2 Sequence number control

Authentication control does not prevent a message from being replicated, deleted, or stored and retransmitted at a later date. The sequence numbering of messages handles these requirements. A payment message is transmitted with an input sequence number, output sequence number, and transaction reference number. They must be in order separately. The format and the input sequence number are checked by the SWIFT operating center and those messages with format errors or wrong sequence numbers are rejected by operating centers. The output from SWIFT operating centers contains an output sequence number that must be checked by the recipient. The transaction reference number provides an end-to-end sequence control for each pair of banks, and is included in the part of the message to which the authentication is applied. Since there is no authentication feature between end-banks and operating centers, input sequence numbers may be altered during the bank-center link and the order of message sending could be changed. Banks might lose interest difference.

4.2.3 User access control

Terminals logging into the system must verify their identity using a password issued by SWIFT. The password is sent in two parts in the form of a table. By sending each part separately, the interception of a complete password set is made less likely. Each password table contains a sequence of passwords listed against a sequence number. Each login employs the next password in the sequence so that the interception of passwords by line tapping gives no clue to the next password that will be needed. To avoid the trick of extracting passwords by impersonating the SWIFT system to the terminal, each password is given a response number that the user must receive from the SWIFT and check before beginning transactions.

4.2.4 Encryption between operating centers

To preserve the privacy of the banks' messages, the international lines that connect operating centers and join them to regional processors are protected by encryption. But encryption is not used on the line between banks and regional processors because it would prevent the useful role of SWIFT explain that privacy is not such a cardinal security factor as authentication. Then why do they offer an encryption function on international lines?

4.3. SIPN level core security solutions

4.3.1. IP Packet filtering

IP packet filtering protects the network nodes against denial-of-access attacks and against any other unauthorized access. The POP applies IP packet filtering through access control lists. This ensures that only the allowed combinations of source and destination IP addresses pass through the POP. Packet filtering prevents the following occurrences such as traffic from an unauthorized device passing through the POP or traffic from an authorized device passing to an unauthorized device. This prevents direct customer-to-customer traffic whilst allowing traffic between a customer and the SWIFT operating center. In addition, the IP packets are filtered on the protocol type and the destination port number. By blocking unauthorized protocols, the freedom for preparing attacks is limited.

4.3.2. IP Encryption Authentication and Integrity

Hardware encryptors are used within the network POPs and core domain to protect against traffic observation. These encryptors may be replaced when Ipsec ESP technology reaches maturity. The hardware encryptors also provide indirect IP traffic authentication, as bilateral keys are needed to correctly decrypt the IP traffic. In addition, an MD5-based MAC checksum guarantees the authenticity and integrity of the network-management data.

4.3.3. Router Authorization

IP packet filters are implemented on all Secure IP Network routers. This implementation counters IP-level attacks from within or outside the network at the first encountered router. Packets that have an external origin are filtered-out by IP packet filtering at the core routers. In addition, Network Address Translation (NAT) at the SWIFTNet boundaries hides the internal topology of the network in order to make attacks more difficult.

4.3.4. Firewalls

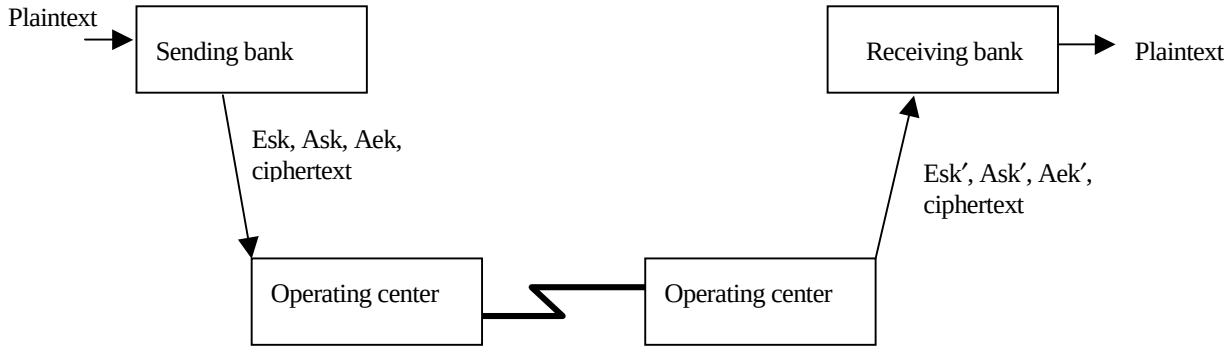
In order to contain the impact of attacks, SWIFTNet equipment is segregated into domains that are protected by firewalls and filtering-routers. POPs and CPEs also act as filtering-routers. The firewalls and filtering routers are configured to protect against the attempts to access unauthorized servers and routers, and denial of service attacks, including attacks through Ping of Death, SYN flooding, bursting-of-packets and LAN denial.

4.4 A proposed improvement model

Lack of encryption between banks and regional processors present serious risks to the system as transmissions may be intercepted and modified or even deleted. Attackers may subsequently divert, redirect, or cancel funds transfers. One of the countermeasures is to use public key cryptography to ensure proper authentication and privacy stealing vulnerability and other required compensating controls to secure cryptographic keys. The RSA cipher is a revolutionary invention in the cryptography field. It enables ciphering without leaking private key information. It deploys the public key scheme to modify the key escrow mechanism to be used in SWIFT system offering the following features for the above stated problems:

- Each bank owns its private key and public key, but different keys are used for authentication of different transactions, and these keys are unknown to SWIFT as before.
- Provide bank-to-center authentication.
- Provide link-by-link encryption from end-to-end.

Each bank has a securely stored private key and a public key. A SWIFT terminal generates a random number for every message transmitted as the end-to-end authentication session key, and encrypts this key with the receiver's public key. Using the same procedure to perform bank-to-center input sequence number authentication, it enables an operating center to verify the authenticity of the input sequence number from customer banks. The receiving bank to verify the output sequence number from the operating center uses the same method. Let us name this as link-by-link authentication. Finally, link-by-link encryption can be performed using a uniquely generated session key for message encryption and encrypting the session key with the public key of the code at the other side of the link. Figure 3 depicts this procedure.



Esk: Encrypted link-by-link encryption session key
Ask: Encrypted link-by-link authentication session key
Aek: Encrypted end-to-end authentication session key

Figure 3. Modified SWIFT network

The authentication code is encrypted and contained in the cipher text. The authentication verification can be performed by the decrypted plain text and the authentication code. Thus, every code only needs to store its private key and manage its public key. With its own private key, each bank or operating center can obtain required encryption and authentication session keys in an automatic way, and such critical information can not be eavesdropped. If a fast, public-key cryptography is developed, the mechanism of encryption and authentication will be greatly simplified.

5. Conclusion

This paper studies the functional and technical features of an inter-bank funds transfer system – SWIFT. There exist some flaws in the security of this system, which could lead to serious problem and have substantial financial impact. The practice of using both public-key and secret-key cryptography is blamed for the poor performance of the existing public-key cipher system. We present an initial proposal to improve its security level and operation performance.

The tremendous growth in the Internet and electronic commerce has created serious challenges to network security. A number of other practical attacks on such fund transfer systems have been outlined, and procedural vulnerabilities have been

listed as one of the main problems (Anderson 2001). The key factors in determining appropriate security measures include value of the data, the structure and interactions of the organization, complexity of the tools, etc. The usability of security mechanism and consumer trust issues present interesting directions for future research.

Acknowledgement
This research is partially supported by a NSF grant. We would like to thank S. Hong, Q. Meng and R. Venkata for their excellent research assistance. I also thank the three anonymous reviewers for their valuable and specific suggestions to improve the manuscript.

REFERENCES

Anderson, R. *Security Engineering: A Guide to Building Dependable Distributed Systems*, Wiley Computer Publishing, 2001.

Abdalla M. and Mihir Bellare, *Increasing the Lifetime of a key: A Comparative Analysis of the Security of Re-keying Techniques*, Advances in cryptology-ASIACRYPT 2000: 6th International Conference on the Theory and Application of Cryptology and Information Security, Kyoto, Japan, December 3-7, proceedings, pp546-557, 2000.

Bellare, M. and Phillip Rogaway, *Encode-Then-Encipher Encryption: How to Exploit Nonces or Redundancy in Plaintexts for Efficient Cryptography*, Advances in cryptology-ASIACRYPT 6th International Conference on the Theory and Application of Cryptology and Information Security, Kyoto, Japan, December 3-7, proceedings, pp317-330, 2000.

Biryukov, A. and Adi Shamir, *Structural Cryptanalysis of SASAS*, Advances in Cryptology: EUROCRYPT 2001 International Conference on the Theory and Application of Cryptographic Techniques, Innsbruck, Austria, May 6-10, proceedings, pp395-405, 2001.

Davies, D. W. and W. L. Price, *Security for Computer Networks*, John Wiley, NY, 1989.

Denning, D. E. and D. K. Branstad (1996), A Taxonomy for Key Escrow Encryption Systems, *Communications of the ACM*, Vol. 39, No. 3, 34-49.

Desai, A. *The security of All-or-Nothing Encryption: Protecting against Exhaustive Key Search*, Advances in cryptology, CRYPTO 2000 : 20th annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, proceedings, pp359-375, 2000.

Diffie, W., and Hellman, K. New directions in Crypotography. IEEE Trans. On Informatino Theory IT-22, 6 644-654, 1976.

Power, R. Computer Security: Issues and Trends, 2001 CSI/FBI Computer Crime and Security Survey vol. VII, No. 1, 2001 http://www.gocsi.com/prelea/000321.html

Goncalves, M., *Firewalls Complete*, McGraw Hill, New York, NY, 1998.

Johnson, J. Z. "Network Security Programs: Process and Metrics for the Real-World", White paper, Internet Security Systems, Inc, 1998.

Kalakota R. and A. Whinston, Frontiers of Electronic Commerce, Addision Wesley, MA, 1996.

Ki Hyoung Ko, Sang Jin Lee, Jung Hee Cheon, Jae Woo Han, Ju-sung Kang, and Choonsik Park, *New Public-Key Cryptosystem Using Braid Groups*, Advances in cryptology, CRYPTO 2000 : 20th annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2000 : proceedings, pp166-183.

Mainwald, E. *Network Security: A beginner's guide*, McGraw-Hill, 2001

Nechvatal J., E. Baker, L. Bassham, W. Burr, M. Dworkin, J. Foti, E. Robak (2000), *Report on the development of the Advanced Encryption Standard (AES), Oct. 2, 2000.* (http://csrc.nist.gov/encryption/aes/round2/r2report.pdf)

Okamoto, T, Keisuke Tanaka, and Shigenori Uchiyama, *Quantum Public-key Cryptosystems*, Advances in cryptology, CRYPTO 2000: 20th annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, proceedings, pp147-165. 2000.

Pascal Paillier, *Trapdooring Discrete Logarithm on Elliptic Curves over Rings*, Advances in cryptology-ASIACRYPT 2000: 6th International Conference on the Theory and Application of Cryptology and Information Security, Kyoto, Japan, December 3-7, proceedings, pp573-583, 2000.

Palmer, J. W. and Griffith, D. A. "An Emerging Model of Web Site Design for Marketing," *Communication of the ACM*, Vol. 41, No. 3., pp. 45-51, 1998.

Pfleeger, C. P. *Security in Computing*, second edition, Prentice Hall, NJ, 1997.

Stallings, W. *Data and Computer Communications*, Upper Saddle River, Prentice Hall, NJ, 2000.

Silberschatz, A. Operating System Concepts, Reading, Mass, Addison Wesley Longman, MA, 1998.

Summers, B. J. *The Payment System: Design, Management, and Supervision*, International Monetary Fund, Washington, D.C., 1994.

Zhu, D., Premkumar, G. X. Zhang and Chao-Hsien Chu, Data Mining for Network Intrusion Detection, A Comparison of Alternative Methods, *Decision Sciences* Journal, 32, 4, 635-660, 2001.