Research for the SECURITY systems-design of information application-systems

Masaru Makino *

Abstract

The author asserts that the most important technology for development of information systems is "systems-design". The author also asserts that the systems-design of information application-systems has two sides of view which are main object-activity and keeping "SECURITY".

In this paper the author puts force his power of technologies for design of keeping SECURITY rather than design of main object-activity.

In these days digital society has frequently destructive invasion from computer-network to computer-network. As shown in the body of this paper, we have many sort of technology for keeping security. However we have not appropriate and simple means for the systematic defense against much type of invasion.

In this paper the author presents synthetic systems-design and systems-approach for keeping SECURITY of information application-systems.

1. Introduction

The purpose of this study is keeping "SECURITY" in information application-systems. Keeping security is countermeasure against attack. Both of countermeasure and attack has many sides of stages.

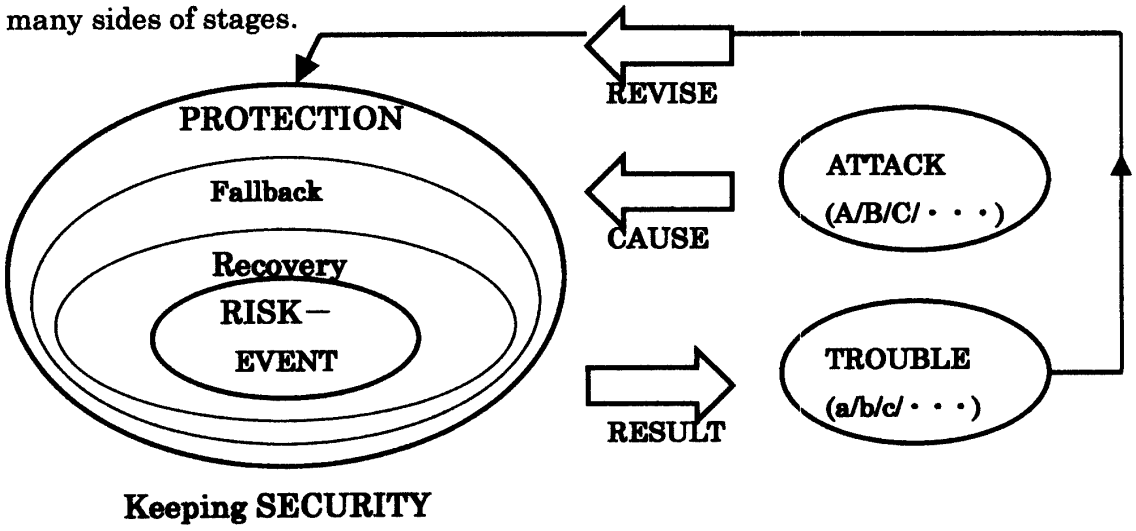


Fig. 1 Risk Management

Countermeasure for keeping security has a tendency to be similar to playing game.

* Department of Management Science

However it has much serious and complicated scene on both of technology and economy.

As shown in Fig. 1 keeping security for information systems needs much elements of technology which are protection against attack, fallback and recovery systems to risk-event.

2. Information systems-design

On abstract in this paper, the author asserts that the systems-design of information application-systems has two sides of view which are main object-activity and keeping security.

As shown in Table 1. we have four domains A,B,C,D. In this case, the table is composed of two dimensions those are systems-design (SD) and technology. Systems-design for main object-activity (A,B) is obverse and systems-design for security (C,D) is reverse.

We can see other part of dimensions which has systems-technology (A,C) and software technology (B,D).

Table 1. Systems-design

SD / Tech.	Main object-activity Systems-design	SECURITY Systems-design
System-Technology	A	C
Software-Technology	B	D

Each of these domain (A,B,C, D) has two sides respectively, those are general design and detail design.

And then we have eight domains (A_G,A_D,B_G,B_D,C_G,C_D, D_G,D_D).

3. Security systems-design

The author asserts that systems-design for main object-activity is obverse and systems-design for security is reverse in information systems-design.

Table 2. Risk Management

Attack (Offence)	Contingency: Disaster /Obstacle /Accident /Mistake /Privacy
	Crime: A /B /C /D / · · · · ·
Protection (Defense)	Prior Countermeasure: Inspection /Prevention
	Post- Countermeasure: Fallback /Recovery

However leading part of study in this paper is keeping security, therefore in table 1. C&D are obverse and A&B are reverse in the following description.

As shown in Table 2., risk management has attack (offence) side and protection (defense) side.

Attack side is composed of contingency and crime.

Protection side is composed of prior countermeasure and post-countermeasure.

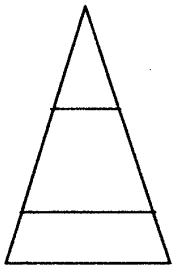
Detail elements of each side are shown in above Table 2.

4. Security systems-approach

4. 1 Systems-approach for systems-design

Systems approach is a direction of systems design for the information systems-development. As shown in Fig.2, information system is generally composed of three layers those are application/ middle/ base layers.

To give a few examples of each layer, application layer has EC (Electronic Commerce), online trade of stock by i-mode, and internet banking, middle layer has inter/ intra/ extra-network, database and cipher, base-layer has OS (Operating System) and many sorts of servers those are firewall/ proxy/ www / E-mail etc..



Ⅰ. Application Layer
Ⅱ. Middle Layer
Ⅲ. Base Layer

Fig. 2 Three layered Approach

Systems approach for systems design has two directions those are top-down(Ⅰ - Ⅱ - Ⅲ) and bottom-up (Ⅲ - Ⅱ - Ⅰ).

4. 2 Systems-approach for the SECURITY systems-design

In case of large system, for example big business systems we must adopt top-down approach(Ⅰ - Ⅱ - Ⅲ). However in case of small or middle systems we may adopt bottom-up approach (Ⅲ - Ⅱ - Ⅰ) or random approach.

In each case systems-approach for security systems-design depends on scale of system and other special reason for example saving cost or being in a hurry for starting the operation of the system. However in case of random approach the author consider that base layer(Ⅲ) is more important than other layers.

5. Technology of the SECURITY systems-design

5. 1 Security technology

The author presents security technology for information systems-design in Table 3..

The author has splitted items of SECURITY technology (C,D) in Table 1. to computer and network.

Table 3. Security Technology

	Computer	Network
System	Security Policy /Security Level /Security Agent /Server /EC /B to B /Cipher (DES /RSA) / Hacking /Virus /Electronic Money / SET / CERT-CC / Secure ID / Gateway	Internet / Firewall /Hacker /VPN /Provider / Proxy / Virus / CERT-CC / DNS / IPv6 /Switching HUB / FTTH / TCP-IP / Mobile /
Software	Distributed Object Oriented System /Anti-Virus /Penetration Attack /Security Agent / Web Server /DHCP Server /VPN /Logging	Firewall /IP-masquerade /SSL /SMTP /MIME /IO Port /BIND /Authentication/ Packet Filtering /Spam /Access Control

5．1．1 Attack operation

Attack operations in Table 3 are " Hacking, Virus, Penetration Attack, Spam ".

In classification of virus there are file infection, system domain infection, compound Infection, macro virus, VBS virus(Script virus).

5．1．2 Defense operation

Defense operations in Table 3 are " Cipher, CERT, Secure ID, Firewall, VPN, Proxy IPv6, Anti-Virus, Authentication, Packet Filtering, Logging ".

In these operation we have technologies those are application-dependent or application-independent. For example CERT or authentication is application-dependent.

The author presents example of defense operation in 5.2.2.

5. 2 Cipher SYSTEM

5．2．1 Algorithm of public key encryption

The computer makes cipher by algorithm of pseudo-random number. The formula is as shown in Table 4. In this formula X is original text. Y is cipher of X. R and n are public keys, S is private key.

Table 4. Formula

$X^R \equiv Y \pmod n$
$Y^S \equiv X \pmod n$

Example of digits for each variable is following.

X =2, Y =326, R =13, S =61, n =437

(Referred by Ref.[16])

5．2．2 Example of cipher system

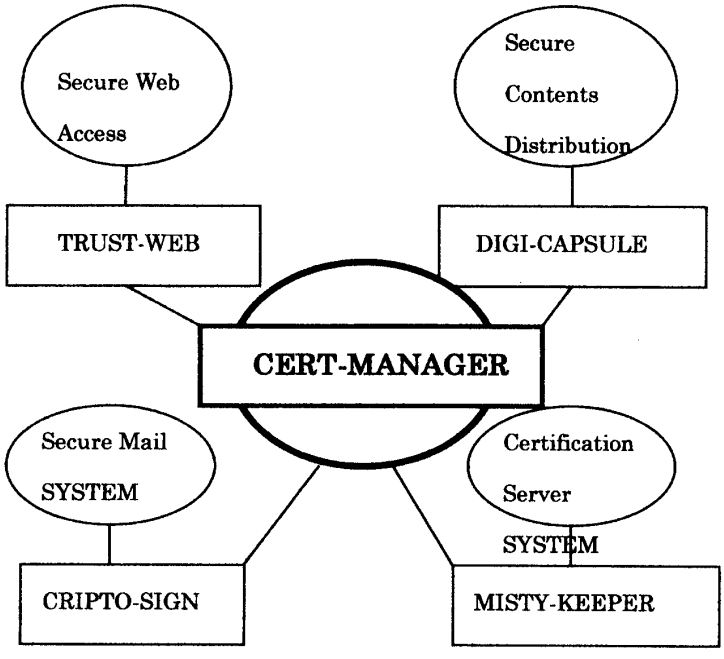


Fig. 3 MISTY Guard referred by Ref.[14]

MISTY is encryption algorithm developed by Mitsubishi Electric Corporation. The software based by this algorithm has been officially adopted as next-generation cellular-phone standard(3GPP project ／W-CDMA working group in Europe, the U.S., South Korea). Mitsubishi says that with electronic commerce and banking becoming a function of cellar phones, safe encryption technology for cellar phones is being regarded as an important issue.

5．3 SECURITY in Electronic commerce (EC)

5．3．1 Electronic money

The author asserts that the most important action-item in electronic commerce is accounting of sales. As shown in Table 5. we often use electronic money which has much style of currency.

Table 5. Electronic Money Referred by [17]

Account Method		Example
E-Account	E-Cledit	SET (VISA／Master Card)
	E-Check	E-Check (FSTC)
	E-Transfer	SECE (Cf. SET)
E-Money	IC-Card	Geld Karte／Debit Card／Web Money
	Network	E-Cash／Cyber Cash
	IC-Card／Net	MONDEX／VISA C ash／NTT E-Cash

Electronic account method has two groups those are E-account and E-money.

Representative example in E-account is SET(Secure Electronic Transaction).

Representative examples in E-money are debit card and Web-money.

5．3．2 Electronic commerce (B to B)

Electronic commerce (B to B) is commercial transaction from business company to business company by computer-network.

As shown in Fig. 4 EC server-computer supervises business transaction with seller and buyer. In this transaction seller and buyer generally do not see face to face mutually.

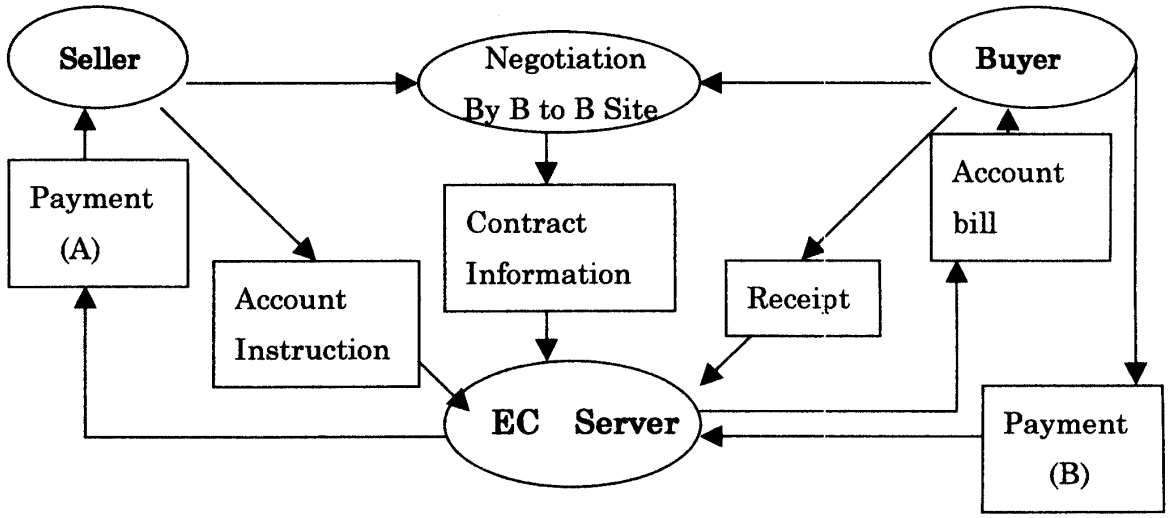


Fig. 4 Electronic Commerce (B to B) Referred by Ref.[15]

Therefore security information for seller and buyer is exceedingly important in electronic commerce(B to B) mutually. Especially payment(B) is most important in Fig.4. In payment we must be careful to sorts of electronic money as shown in Table 5. We should select carefully sort of electronic money in Table 5 or from other method.

6. Discussion

The author has asserted in introduction that the purpose of this study is keeping "SECURITY" in information application-systems.

6. 1 General case

The invader into home-page through internet is criminal against row. The sender of spam mail is hatefully social enemy. The spoof in authentication is robber.

The author presented technologies of many sorts of server (Proxy/ HTTP/ Firewall/ etc.) in the Memories of Fukui University of Technology(No.30). Therefore I hope that if you want to consider about more cases of security you see the reference [2].

6. 2 Business case

We must be careful of business virtual company, virtual mall and so forth. Non-existent company has no power of payment towards buying goods.

In business society there are planned bankruptcy or self- bankruptcy and other trouble. We should be aware of these troublesome occurrence in business transaction. We need special security technology for business information-application systems. For example in case of Fig.4 or incase of SET(Table 5) authentication or certification by organization or special company guarantees their business operations.

7. Conclusions

We can see many stages of security for information application-systems. We must be careful of ill will action with so much complex condition in all of the world.

(1) We must take great care of the security systems design for information application systems.

(2) We have open information systems and private information systems. The former is more dangerous than latter . Therefore we must be more careful of open systems.

(3) Systems approach of systems design has two directions that are top-down and bottom-up in three layered approach(Fig. 2).

(4) We have much technology for the design of information security(Table 3). However we should not make a wrong application.

(5) Security policy has a little inconsistency towards business operation, however the author does not treat these theme in this paper. The author asserts that security policy should be concrete and connected to the design technology.

8. Residual theme

The author intends to research security systems design for information application systems. There are many theme for information security systems design.

The author considers that all components of technologies for security should be connected one synthesis system.

The author would like to make a chance to present information application system connected with security innovation.

References

[1]Masaru Makino : Security systems design for MIS/OA related with computer network, Society of Korea MIS, 2000, pp.205-208.

[2]Masaru Makino : Research for the theory of information systems design(Series 1), Memories of Fukui University of Technology(No.30),2000,pp.293-300.

[3]Masaru Makino : A new scheme for information systems design, Memories of Fukui University of Technology(No.29),1999,pp.265-271.

[4]D.Brent Chapman, Elizabeth D.Zwicky: Building Internet FIREWALL, O'Reilly, 1996.

[5]Symantec : Norton Anti-Virus(Manual), 1998.

[6]David Kosiur : Electronic Commerce(Japanese language edition), ASCII Corporation, 1997.

[7]Suguru Yamaguti, Hironobu Suzuki : Information security, Kyohritsu shuppan, 2000.

[8]Net Technology Laboratory : Internet Protocol Version 6, Gizyutsu-hyohronsha, 1999.

[9]J.Millecan, J.Higgins, etc. : IIS(Internet Information Server, Japanese language edition), Impress Corp.&Prentice Hall Japan, 1997.

[10]Rik Farrow : UNIX System Security, Addison-Welsey Publishingcompany Inc., 1991.

[11]Yohichiroh Koga : Apache(Construction of HTTP Server, Japanese language edition), ASCII Corporation, 1998.

[12]Hironobu Suzuki : Practice Linux Security(Japanese language edition), Impress Corp., 2000.

[13]IEEE Computer Society : COMPUTER October 2000, IEEE, 2000.

[14]Mitsubishi Electric Corporation : Power MISTY (Cipher Software), Mitsubishi Electric corporation, 2000.

[15]CRC Sohgoh Kenkyuusyo : CRC Communication Sep/Oct 2000, CRC, 2000.

[16]Hideki Sawada : Cipher theory and algebra, Kaibundo, 1997.

[17]Japan Society for the Study of Office Automation : Office Automation October 1997, Japan Society for the Study of OA, 1997.

(Receiver December 8, 2000)