Transactions of the Korean Nuclear Society Autumn Meeting
Gyeongju, Korea, October 29-30, 2009

Survey of Cyber Security Methods for the Nuclear Power Plants

Yoo-Rark Choi [a*], Jae-Cheol Lee [a], Young-Soo Choi[a], Seok-Boong Hong [a]
KAERI, P.O.Box 105, Yuseong Daejeon Korea
yrchoi@kaeri.re.kr

1. Introduction

Cyber security includes the method of protecting information, computer programs, and other computer system assets. Hardware security, which is the security of computer assets and capital equipment, refers to computer location, access control, fire protection, and storage procedures. Such measures as badges, electronic identification keys, alarm systems, and physical barriers at entries are used for this purpose. Software security entails the protection of software assets such as Application Programs, the Operating System, and the Data Base Management System and stored information. Special user numbers and passwords are typically used to prevent unauthorized access to software and data. In addition to security for hardware and software, good internal control also requires that measures be taken to prevent loss or accidental destruction of data.

Cyber attacks create substantial threats to large enterprises, including federal systems and digital I&C of a NPP (Nuclear Power Plant) is one of them.

The cyber security policy for the digital I&C network of the NPP has been established for years by KINS, but its scope is very broad and conceptual.

We will propose a cyber security method based on cryptography and authentication that is developed for the digital I&C network of the NPP.

2. Cryptography and Authentication

Until modern times cryptography referred almost exclusively to encryption, which is the process of converting ordinary information (plaintext) into unintelligible ciphertext. Decryption is the reverse, in other words, moving from the unintelligible ciphertext back to plaintext. A cipher is a pair of algorithms which create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a key.

Authentication refers to the process where one entity verifies another entity's claim to holding a specific digital identity. Commonly one entity is a client (a user, a client computer, etc.) and the other entity is a server (computer). Authentication is accomplished via the claimant's presentation of an identifier and its corresponding credentials to the verifier. Examples of types of credentials are passwords, one-time tokens, digital certificates, and phone numbers.

The Data Encryption Standard (DES) is a block cipher. It is based on a symmetric-key algorithm that uses a 56-bit key. DES consequently came under intense academic scrutiny which motivated the modern understanding of block ciphers and their cryptanalysis.

DES is now considered to be insecure for many applications. This is chiefly due to the 56-bit key size being too small. The algorithm is believed to be practically secure in the form of Triple DES, although there are theoretical attacks. In recent years, the cipher has been superseded by the Advanced Encryption Standard (AES).

3. Triple DES and AES

The digital I&C network must satisfy Hard-Realtime constraint, so the processing time for encryption is a very important factor in the digital I&C network.

Table I: Digital I&C Network

Network	Data Len. (Byte)	Processing Capacity	Protocol
IPN	46~1,500	14.52 Mbps	100Mbps Ethernet
QIAN	1~246	178.43 Kbps	Profibus-FMS
CN	Over 72	19.75 Mbps	Token-Ethernet
PAIN/PBIN	1~246	341.89 Kbps	Profibus-FMS
PCIN/PDIN	1~246	238.72 Kbps	Profibus-FMS

The processing capacity of the IPN that requires the heaviest transfer capacity) is 14.52Mbps.

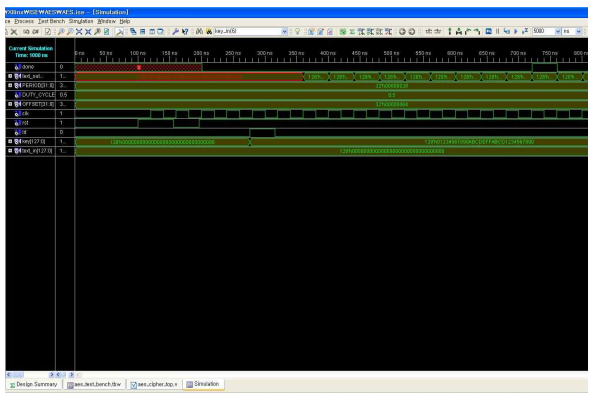

Fig. 1. Experiment of AES speed

AES algorithm takes 300ns to encrypt 128bits data with virtex-2(clock 40MHz). Its processing capacity is 427Mbps.

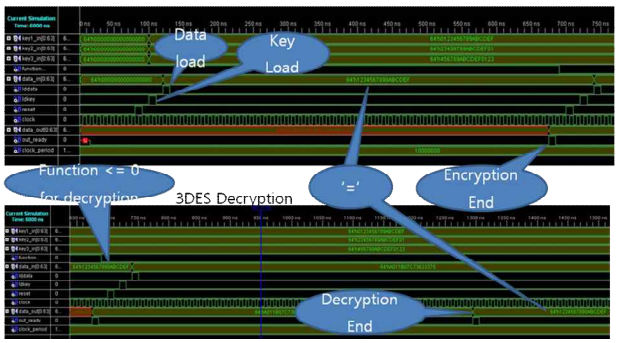

Fig. 2. Experiment of Triple DES speed

Triple DES algorithm takes 400ns to encrypt 64bits data with virtex-4(clock 100MHz). Its processing capacity is 160Mbps.

We can make conclusion that the processing time for encryption/ decryption is very short and harmless to the hard-Realtime constraint from the experiment results.

4. Increasing Security Grade

The data format of the digital I&C network is simple and short. These characteristics cause the week points in terms of Crypto analysis. We designed new methods of increasing security grade using the encryption and authentication with data reordering.

Table 2: Data Frame of the digital I&C network

	Bit offset								
Octet Offset	7	6	5	4	3	2	1	0	Definition
0 ~ 5	Destination MAC Address								Ethernet
6 ~ 11	Source MAC Address								Ethernet
12 ~ 13	Ethertype								Ethernet
14 ~ 15	Length								Ethernet
16 ~ 31	Reserved for security								NSCP
32 ~ 507	Payload								NSCP
508 ~ 511	FCS								Ethernet

To reordering the data:

$D = F_{(R)}[M \| n] \| R_{(o)} \| S$

Where

D = Data Field(476 Bytes)

M = Original Data, n = Random Number

$F_{(R)}$ = Reordering Function

$R_{(o)}$ = Reordering Sequence(43 Bytes)

S = Special Bytes(3 Bytes)

The data reordering yields confusion to analysis of the data. Random number is padding data(not 0 padding and not 1 padding). The reordering sequence $R_{(o)}$ includes the serial sequence number array and each byte of it will have the original sequence of the data(10Bytes data).

Encryption of data field(Payload):

$D = F_{(R)}[M \| n] \| R_{(o)} \| S$

$C_{(D)} = E_{(k)}[F_{(R)}[M \| n] \| R_{(o)} \| S]$

Where

$C_{(D)}$ = Cyper Text For Data D

E = Encryption Algorithm(Triple DES or AES)

k = Key

For authentication:

$C_{(D)} = E_{(k)}[F_{(R)}[M \| M_{(SM\|DM)} \| n] \| R_{(o)} \| S]$

Where

$M_{(SM\|DM)}$ = MAC(Message Authentication Code) value for (Source Mac Address || Destination Mac Address) : 12 Bytes

The authentication notation includes MAC of source-destination Mac address. It will be employed as a user authentication in the digital I&C network.

$M_{(D)}$ that is MAC value for original data(M) will be stored at the 'Reserved for security' field of data frame, and used as a message authentication.

5. Conclusion

Many kinds of cyber security technologies that are developed in the IT industry may be applied to the digital I&C network that is used in the nuclear industry.

All of the network systems and their components always have holes and they will act as a potential cause for cyber security disturbances. Cyber security activity for a NPP must be performed but we can't assure that it is sufficient for cyber security of the NPP.

Anyway, when the digital I&C network is attacked by invader, the control systems do not generate mul-function and the forged command must be rejected in it.

We proposed a new security methodology to accomplish the cyber security of the digital I&C network based on data reordering, data encryption and authentication.

REFERENCES

[1] Cyber security industry alliance, cyber security issues, CSIA, http://www.csialliance.org

[2] Y.R. Choi, S. B. Hong, I.S. Koo, and J.C. Lee, A state of art of IT secutiry technologies for cyber security, KAERI/AR-784/2007, 2009.

[3] Y.R. Choi, J. C. Lee, "Survey of Cyber Security Intrinsic for a Nuclear Power Plant", Proc. Of the Korean Nuclear Society Spring Meeting Jeju, May. 2009.

[4] ANSI X9.63(Draft), "Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Key Cryptography."