Empirical Approach to Enhance the Security of DNP3 Protocol in SCADA System using Low-latency Block Cipher*

HakJu Kim† , Kwangjo Kim‡
Dept. of Computer Science,
Korea Advanced Institute of Science and Technology

ABSTRACT

Critical infrastructures like Nuclear Power Plants (NPP), railroad networks, and water distribution / treatment systems are fundamentally important to human life. Failure of such structures endangers human lives, environment, and economy in world-wide scale. Supervisory Control And Data Acquisition (SCADA) system have been installed to operate those infrastructures efficiently and safely, but series of recent hacking incidents have stressed the importance to improve cyber-security of SCADA systems. This paper assesses basic differences between general IT systems and SCADA system, analyzes up-to-date technologies and approaches to secure the systems, and suggests cyber-security improvement of popular DNP3 protocol in SCADA system using authenticated encryption based on low-latency symmetric key cryptography and key management scheme.

Keywords: SCADA, authenticated encryption, key management, DNP3, GCM, CCM, PRINCE

I. Introduction

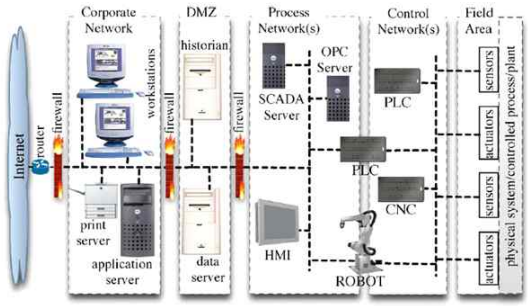
Critical infrastructures are those physical and cyber-based systems essential to the minimum operation of economy and government[1]. They are designed for energy, gas, and water distribution, transportation systems, and air traffic control[2]. Damage against those critical infrastructures will cost safety of human and environment as well as uncountable monetary loss nation-wide and also world-wide. Chernobyl disaster of Russian nuclear plant and Fukushima disaster of Japanese nuclear plant are the clear examples that show how failure of one critical infrastructure can impact our society, environment, and the world.

SCADA system or network that monitor and control individual analog and digital nodes of critical infrastructure has the different set of technologies and protocols like Modbus[3] and DNP3 (Distributed Network Protocol version 3)[4] from general-purpose IT systems or networks. Also, security requirements and approaches to protect SCADA system from cyber-threat are different from those of other general systems. Those protocols are not designed to consider cyber-security of SCADA systems. Several researches and documents like DNPSec[5] and DNP3 Secure Authentication (DNP3 SA)[4] have attempted to improve security of those protocols, but they have deficiencies in terms of performance or fundamental security requirements as known as CIA (Confidentiality, Integrity, and Availability).

* This research was supported by the KUSTAR-KAIST Institute, Korea, under the R&D program supervised by the KAIST.
† ndemian@kaist.ac.kr
‡ kkj@kaist.ac.kr

II. SCADA system

Many of critical infrastructures in a country have historically been physically and logically separate systems[1]. Physical safety measure of critical infrastructures from non-cyber threats has been well developed. As a result of advances in information technology (IT) and the necessity of improved efficiency, these infrastructures have become increasingly automated and interlinked[2] via SCADA networks. [Figure 1][2] shows typical connections of SCADA systems. Process and Control networks work as the SCADA network. In Korea, we believe that there is no physical connection to the Internet from SCADA networks. Some SCADA systems like ones in United States have connection to the Internet. Among elements of CIA, availability are the most important security requirements of SCADA systems. To ensure cyber-security of SCADA networks of critical infrastructures, they have been designed to be physically closed network from outside network like the Internet to eliminate the possibility of cyber-security breach. However, Stuxnet, an Advanced Persistent Threat (APT) attack on Iranian nuclear facilities in 2010[6] and its successors like Duqu, Flame, and Gauss demonstrate that the protection of SCADA systems using physically network isolation is not complete against cyber attack. Furthermore, there are increasing demands to interconnect separate SCADA systems and to efficiently and remotely monitor the systems from outside especially through the Internet. Many power plants in United States have been connected to outside networks for efficient remote maintenance. Therefore, the SCADA networks must be protected against cyber-threats like APT with new security measures.



[Figure 1] SCADA network[2]

2.1 Differences between ICS and other IT systems[2]

Current cyber-security technologies have focused on general-purpose IT systems like in desktop or business, and there are growing concerns focusing on developing cyber-security technologies also for Industrial Control Systems (ICS). The SCADA system is one of ICS. ICS and general-purpose IT systems both evolved from development of IT, but they have different characteristics. ICS system is directly interfaced to a physical system through its sensors and actuators, but general-purposer IT systems are not necessarily directly interfaced. ICS networks are responsible for field area consisting of sensors and actuators, and provide supervisory and management functions with specialized software modules for each different systems, while general-purpose IT systems typically use general-purpose technologies like TCP/IP. ICS systems require real-time constraints (often hard) and hard availability constraints. The traditional isolation of ICS from general-purpose IT systems and different characteristics of ICS have caused adoption of special-purpose

〔Table 1〕 Difference between ICS and general-purpose computing system〔2〕

	DBCS	IACS
	System Characteristics	
Average node complexity	high (large servers/file systems/databases)	low (simple devices, sensors, actuators)
Number of users	very high	limited
Multi-vendor environment	moderate	frequent
System lifetime (years)	some	some tens
Outage of system availability	often tolerable	rarely/never tolerable
Tolerability of time delays	medium/high	low/none (real-time)
Acceptable processing times	minutes÷days	milliseconds÷minutes
Tolerability of failures	medium/high	low/none
Communication protocol stacks	general purpose (i.e. TCP/IP, UDP)	special purpose/proprietary/real-time
Operating systems	general-purpose (i.e. Windows, Unix)	real-time, embedded, special-purpose
	System Maintenance and Upgrading	
S/w patches and upgrades	very frequent	rare or none
No longer supported s/w versions	rare	often in use
New s/w releases	frequent (extensive changes)	rare (small changes)
Frequency of h/w upgrades/changes	medium/high	very low/low
	Security Practices	
Security awareness	high/very high	usually low (rising)
Availability of security expertise	high/very high	very low/low
Adoption of security audits	frequent	very rare/rare
Online security checks	frequent	rare (often impossible)
	Security Countermeasures	
Use of anti-virus	heavy	rare/none (often impossible)
Physical protection	frequent (site protection and surveillance)	difficult (remote and not guarded sites)
Availability and adoption of firewalls and IDSs	frequent/very frequent	rare/sometimes impossible
	Impact of Negative Events (Cyber-Attacks)	
Losses	information, money	human lives, things, environment, money
Costs of successful attacks	bounded	unbounded
Pre-estimation of losses	possible	often impossible (i.e. human lives, environment damages)

proprietary hardware and software. The lifetime in ICS system spans tens of years, and hardware and software upgrades (or patching) are very difficult in order to keep the system available at all times. Because of the isolated nature of ICS, the access to the ICS is allowed to the legitimate personnel. The hardware requirement of ICS is minimal; most components of the ICS do not require intense processing or graphical calculations. Needless to say, the cost of failure is enormous. 〔Table 1〕〔2〕 summarizes the differences in various aspects. Many ICS include unmanned and small remote sites. Therefore, the ICS requires different cyber-security approach from general system approach in terms of cryptography, firewall, and others.

2.2 Popular SCADA protocols

Because hardware and software upgrade is very unfavorable for SCADA systems, many SCADA systems still operate on out-of-date technologies like serial communications and proven protocols like Modbus RTU (Remote Terminal Unit), RP-570, Profibus, and Conitel〔7〕. However, modern standardized protocols like DNP3, IEC 60870-5 (International Electrotechnical Commission), and IEC 61850 are getting popular. Modern protocols include various communications technology like serial communications and Ethernet. Also, they consider easy upgrades and security measures embedded within themselves. Modbus, DNP3, and IEC 60870-5 are very popular in the SCADA network protocols. Profibus〔8〕, Profinet〔9〕, and AS-i〔10〕 are examples of their contenders.

2.2.1 Modbus[3]

Modbus, first published by Modicon (www.modicon.com), is the industry's serial *de facto* standard since 1979〔11〕. Modbus is a royalty-free application layer protocol providing client-to-server

communication between devices connected on different types of networks. Variations of Modbus support various media like TCP/IP, Token Passing network, and serial communication. However, some of its variations and updates like Modbus Plus remain to be proprietary.

Modbus is based on request-and-reply mechanism and utilizes function codes to provide different services. It is very easy to be implemented and managed by the users. However, Modbus has functional insufficiency and structural incompetence for modern SCADA network. Due to a legacy protocol, Modbus does not support many data types. One master station can connect to at most 247 of field devices. Modbus is based on the inefficient mechanism in which master station routinely poll every slave devices. Furthermore, the designers of Modbus protocol did not consider security.

2.2.2 DNP3[4] and IEC 60870-5[12]

In 1994, Westronic Incorporated first published DNP3, which is intended to be first truly open SCADA network protocol. DNP3 and IEC 60870-5 were developed at the same time and the DNP3 designers intended to make DNP3 compliant with IEC 60870-5. Some differences appear inevitably during development of two protocols, but are very similar.

DNP3 is accepted as IEEE Standard 1815-2010 (Institute of Electrical and Electronics Engineers). Recent updates allow DNP3 to work with TCP/IP. DNP3 is basically bi-directional protocol in SCADA networks, supporting master-to-slave or slave-to-master communications via various network media. The designers of DNP3 have used open and proven technologies to ensure reliability. Low bandwidth and processing power usage of the protocol have brought the success of DNP3 in United States.

To achieve reliability and efficiency, DNP3 has adopted network layer model, Enhanced Performance Architecture (EPA) rather than Open Systems Interconnection Reference Model (OSI) for efficiency. EPA consists of only three layers: Application, Data Link, and Physical. Also, DNP3 has a transport function inside its Application layer for assembling and disassembling Application layer message fragments. DNP3 is very reliable and efficient protocol for SCADA networks, but DNP3 does not provide cyber-security protection from malicious threats. The designers of DNP3 are well aware of the security weaknesses in DNP3, and suggest the security-enhanced protocol called as DNP3 Secure Authentication.

III. Previous researches on security of SCADA

3.1 DNPSec[5]

DNPSec is a proposed security framework for DNP3 protocol, and provides encryption, authentication, and integrity. DNPSec changes original frame structure of DNP3 to include authentication data and new frame header. DNPSec modifies Data Link layer of DNP3 to achieve this.

Original DNP3 is encrypted using session key and encapsulated by new header, new frame sequence number used to update session key, and authentication data like tunnel mode in VPN. The session key is updated when time is expired or the new frame sequence number reaches its limit. DNPSec specifies 3-DES (Triple Data Encryption Standard) as an example

of encryption algorithm used. 3-DES uses a DES block three times to increase the security from known vulnerabilities of single DES encryption algorithm. For authentication, DNPSec uses HMAC (Hash-based Message Authentication Code) mechanism, where encryption/ decryption session key is used for the hash algorithm. DNPSec does not restrict the choice of encryption and hash algorithms. SHA-1 (Secure Hash Algorithm) is specified as an example used in the DNPSec. However, 3-DES is slower than AES[13], and SHA-1 becomes to be insecure[14] and outdated algorithm.

DNPSec specifies a simple key management scheme. Only session key between two nodes is discussed, and the master is responsible for new session key when session key is expired. The key revocation mechanism is not specified.

3.2 DNP3 Secure Authentication[4]

DNP3 SA (DNP3 Secure Authentication) is official security add-on to application layer of DNP3 protocol, and is a part of DNP3 specification. With DNP3 SA, DNP3 is compliant with IEC 62351-5. DNP3 SA provides data integrity, user and device authentication, and availability, but does not provide confidentiality.

DNP3 SA uses challenge-response mechanism with HMAC to provide security. HMAC in DNP3 SA supports all SHA algorithms. SHA-2 used in HMAC of DNP3 SA is becoming vulnerable[15][16]. DNP3 SA supports pre-shared key, asymmetric, and symmetric cryptography for key management, but DNP3 SA does not specify detailed key management mechanisms. DNP3 SA is backward compatible that secure devices can communicate with non-secure devices. Algorithms used in the protocol are based on open standard, and they are easily upgradeable. DNP3 SA ensures perfect forward secrecy and allows multiple users. This protocol protects SCADA networks from spoofing, modification, and replay attacks. However, DNP3 SA does not provide encryption for confidentiality, because IEC and DNP Users Group believe that encryption of SCADA data is unnecessary if impersonation and modification are prevented[17]. For efficiency, the authentication is usually done at critical functions defined by DNP3.

3.3 SKE[18]

SKE (Key Management for SCADA) is a key-management algorithm for SCADA networks proposed by Sandia National Laboratories in 2001. The key managed in this algorithm can be used for encryption and authentication. SKE approach involves both symmetric and asymmetric key cryptography to manage keys.

SKE divides communications in SCADA networks into controller-to-subordinate (C-S) communication and peer-to-peer (P2P) communication. C-S communication is the communication between master and slave devices, and P2P communication is the communication between master or sub-master devices. Slave devices have relatively low processing power, so C-S communication uses symmetric key cryptography to manage keys.

3.4 SKMA[19]

SKMA (Key-Management Architecture for SCADA system) is a key management system for SCADA networks using symmetric key cryptography to manage

keys proposed by Dawson *et al.*[19] in 2006. SKMA uses three levels of different keys, which are not frequently updated.

This algorithm is more efficient and simpler than SKE. SKMA adopts symmetric key cryptography which is simpler and more efficient than asymmetric key cryptography in managing keys. SKMA stores less number of keys in each devices and requires less bandwidth and processing power for key management process.

3.5 Bump-In-The-Wire[20]

This paper focuses on providing confidentiality and authenticity (integrity) to already operational SCADA systems using DNP3. Most SCADA systems using DNP3 do not adopt DNP3 SA which is relatively recent upgrade. Also, DNP3 SA provides authentication at application layer, and this will cause additional overhead for processors to calculate MAC. Thus, the real-time upgrading of DNP3 into DNP3 SA is difficult in operating or legacy SCADA systems.

To provide confidentiality and authenticity, this paper proposes a new bump-in-the-wire method which requires specialized hardware to encrypt, authenticate, and manage keys at data-link layer. The hardware is designed to be cost-efficient than the existing hardwares, and the key management system is designed to be fully automatic and invisible to human managers to eliminate possible key leakage by human.

3.6 Analysis

DNPSec does not specify how to provide encryption, authentication, or key management in detail. The authentication and encryption may be processed independently or may be processed in sequence. Key management system is not specified. Also, DNPSec modifies original data-link layer of DNP3, so the protocol replacement and the upgrading cost are required.

DNP3 SA does not provide confidentiality. DNP3 SA does not consider malicious master / slave devices or man-in-the-middle attack. SCADA systems may have many remote stations, so the attack can be possible at all points. The critical but unencrypted data can be exploited by an unauthenticated adversary for future attacks.

SKE is a complex and relatively inefficient key management scheme. Many number of different keys must be stored in each station: (2 + 2 × number of slaves) keys in C-S communication and (4 + 2 × number of peers) keys for P2P communications. SKMA can solve the efficiency problem in SKE. However, SKMA requires key distribution center (KDC) to be directly or indirectly communicated with every nodes in the system. Considering low resources and legacy serial-wire communication of low-level RTU, SKMA can be expensive.

Bump-In-The-Wire is a hardware-based solution, which can be easily applied to operating or legacy SCADA systems. However, encryption and authentication algorithms are hard-wired to the chip, which makes it impossible to upgrade the outdated algorithms without replacing hardware or at low cost. The key management is so simple that the revocation for the compromised key is not specified. Automated key management without any human intervention may be dangerous, because key management system itself can be compromised by

attackers. Human should be able to fix the system manually if everything fails.

IV. Proposed security improvement

To provide confidentiality and authenticity (integrity), this paper proposes modification to DNP3 SA using authenticated encryption with detailed key management scheme. Authenticated encryption is an encryption mechanism that provides both confidentiality and integrity at the same time. Improving and altering DNP3 SA to adopt authenticated encryption will add confidentiality to DNP3 SA with efficiency and backward compatibility by not changing original DNP3. Among three composition methods (Encrypt-and-MAC, MAC- then-Encrypt, and Encrypt-then-MAC) of authenticated encryption, Encrypt-then-MAC is the most secure composition method against attacks on confidentiality and integrity[21].

4.1 Authenticated encryption

Authenticated encryption may be more expensive than encryption or authentication alone, because both encryption and authentication algorithms must be used together. Powerful master devices in SCADA systems have enough processing power and memory space to adopt authenticated encryption. AES and HMAC using SHA-3 finalist (Keccak)[22] are the most up-to-date secure encryption and authentication algorithms. However, most master devices and all slave devices do not have sufficient resources to use those algorithms through Encrypt-then-MAC composition method with small overhead to satisfy real-time constraints. Electricity utility companies in Korea do not want more than 20% of resources of master stations to be spent on encryption or authentication[20]. Thus, lightweight but secure encryption and authentication algorithms as well as fast authenticated encryption modes are required for SCADA systems.

4.1.1 Encryption algorithms

PRINCE[23] encryption scheme is designed to reduce execution time upto one clock cycle without warm-up phase to execute encryption when implemented in hardware. The decryption can be done using same circuit with encryption using permuted key. PRINCE was designed to be resistant against classical attacks like linear and differential attacks. PRINCE requires considerably less hardware chip space than AES. Also, PRINCE has very low power consumption.

With PRINCE, slave devices of SCADA systems can encrypt their valuable data economically. A cost-efficient and lightweight algorithm like PRINCE provides a definite option for designers of bump-in-the-wire security hardware. Legacy slave devices have minimum processing power and memory to fulfil their functions at real-time, so bump-in-the-wire method should be considered to secure slave devices.

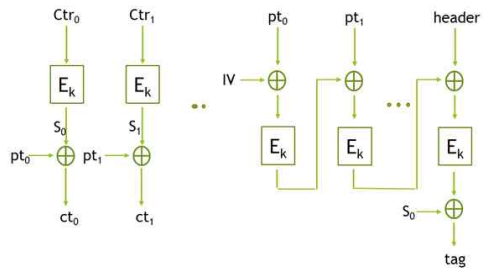
However, master devices can have sufficient resources to implement authenticated encryption by software. An issue in bump-in-the-wire approach is that upgrading is impossible without replacing the hardware making the SCADA system vulnerable to the sophisticated attacks aimed by the current technology or algorithms. For software-based approach, AES can be a common option for block cipher of authenticated encryption. For some master devices that cannot afford to

additional latency caused by AES, software-based encryption algorithms faster than AES should be considered. Most alternativea can be stream ciphers. Because GCM and CCM are designed for block ciphers, block cipher that is faster than AES with reasonable security is required. Or, new authenticated encryption mode that minimizes the overhead should be developed.

4.1.2 Authenticated encryption modes

4.1.2.1 CCM[24]

CCM (Counter with Cipher Block Chaining Message Authentication Code) is an Encrypt-then-MAC algorithm that uses a block cipher to provide encryption and authentication the same time. [Figure 2] illustrates the structure of CCM.

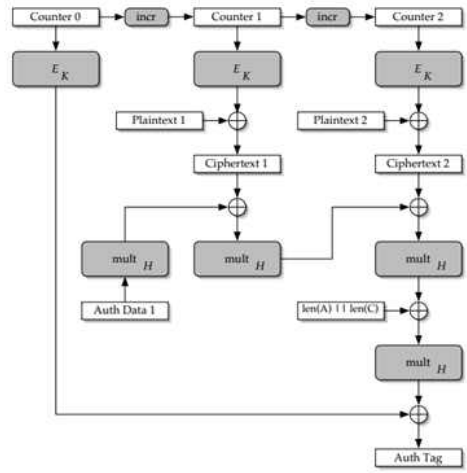


[Figure 2] CCM structure

While many authenticated encryption algorithms are patented around the world, CCM is patent-free and suitable for the packeted data. CCM uses counter method to encrypt and CBC-MAC method to produce MAC. CCM is serially connected algorithm that heavily depend on security and performance of underlying encryption algorithm. An advantage of CCM is that only one underlying algorithm is required, reducing cost of adoption.

4.1.2.2 GCM[25]

GCM (Galois / Counter Mode) is another Encrypt-the-MAC algorithm that utilizes a block cipher using counter mode to provide encryption and Galois hashing to provide MAC at the same time. [Figure 3][24] illustrates the structure of GCM.



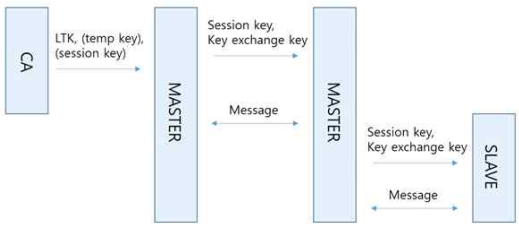
[Figure 3] GCM structure[25]

GCM is also patent-free, but is faster than CCM with little memory support. When implemented in hardware, GCM can take advantage of parallelization and pipelining to make its performance more faster. When a set of plaintexts is not given, GCM can generate MAC only. GCM can provide both authenticated encryption and authentication only. Thus, GCM can be direct alternative or upgrade to HMAC used in DNP3 SA. This paper implements PRINCE algorithm in software for CCM and GCM to test authenticated encryption for DNP3.

4.2 Key management scheme

In this key management scheme,

Cryptographic Authority (CA) is a device that is directly connected to some top-level master devices and is capable of generating high-quality random numbers. CA is responsible for generating all long term keys (LTK) for master devices. Master devices should be capable of generating pseudo-random number without heavy overhead. Slave devices are devices that have no enough resources to generate random or pseudo-random number without heavy overhead. Slave devices have very limited memory space. 〔Figure 4〕 illustrates the overall structure of the key management scheme.



〔Figure 4〕 Key management scheme

The whole scheme can be divided into three categories.

First, CA generates LTKs for all or some master devices in the network. A LTK of each mater is used to protect communication between CA and master. A session key based on LTK for the communication must be used. Also, CA may generate temporal keys for initialization of master devices. The temporal keys will be quickly deleted after master device receives its LTK.

Second, master devices generate a seed key using their LTK and ID. The seed key, slave/peer ID, and nonce are used to generate session keys and key exchange key (for update) for their slaves or peer master devices. All master devices are peer to each other. When communicating with peer, a master that has available free resources generate session key and key exchange key. When starting-up, they communicate with temporal key given by CA before initializing keys.

Third, master devices generates session key and key exchange key for each slave devices directly connected. If session key is compromised, key exchange key is used to distribute new session key. If key exchange key is compromised, session key is used to distribute new key exchange key. If both keys are compromised, key revocation is implementation-specific; human can set new temporal keys or the selected algorithm can be used to generate new temporal keys.

The number of keys stored for each devices is few. CA stores all LTKs generated for each master devices. A master device stores a LTK, Seed key, and session key / key exchange key pair for each device connected to the master device. A slave device only store a session key and a key exchange key. Lifetime of keys is as follows. (LTK 〉 Seed key ≥ key exchange key 〉 session key)

V. Experiment results

PRINCE takes 128 bit key and 64 bit plaintext to produce 64 bit ciphertext. In this simple experiment, 2 blocks of plaintext, 64 bit counter value, 64 bit initialization vector, and 64 bit associated data are given as input to authenticated encryption(CCM). There is no initialization vector in GCM. Xeon E3-1230 CPU and 8GB DDR3 RAM are used as development machine. Microsoft Windows 7 64bit OS, Microsoft Visual Studio 2012, C language, and GNU Scientific Library v1.13〔25〕 are used to implement CCM and GCM using PRINCE.

In test 1, key is 0x0, counter value is 0x0, associated data (e.g. header) is 0x0, and initialization vector is 0x12345678 90ABCDEF. In test 2, key is 0x13457B DE092FEA929CDA08EBF910A0CD, counter value is 0xDB4982DC00000000, associated data (*e.g.* header) is 0x0A13B49FF56C BA3E, and initialization vector is 0x29CDC1AF091ECB82. Tables [2] and [3] are experiment results from CCM method, and Tables [4] and [5] are our experimental results from GCM method.

[Table 2] CCM test 1

	Value
Plaintext1	0x0000000000000000 FFFFFFFFFFFFFFFF
Ciphertext1	0xEE327211A414B8B7 11CD8DEE5BEB4749
Tag(MAC)1	0xEDCBA9876F543210
Plaintext2	0x0123456789ABCDEF FDECBA9876543210
Ciphertext2	0xEF1137762DBF7668 13DEC889D2408AA6
Tag(MAC)2	0xEEFBA9876F543120

[Table 3] CCM test 2

	Value
Plaintext1	0x0000000000000000 FFFFFFFFFFFFFFFF
Ciphertext1	0x00B47CAFBF648701 FF4b8350409B78FF
Tag(MAC)1	0x07680813038D8E43
Plaintext2	0x0123456789ABCDEF FDECBA9876543210
Ciphertext2	0x019739C836CF49DE FD58C637C930B510
Tag(MAC)2	0x04580813038D8D73

[Table 4] GCM test 1

	Value
Plaintext1	0x0000000000000000 FFFFFFFFFFFFFFFF
Ciphertext1	0xEE327211A414B8B6 11CD8DEE5BEB474A
Tag(MAC)1	0xDB364E1CF33F4E3F
Plaintext2	0x0123456789ABCDEF FDECBA9876543210
Ciphertext2	0xEF1137762DBF7669 13DEC889D2408AA5
Tag(MAC)2	0x3542222C5EF0BE5B

[Table 5] GCM test 2

	Value
Plaintext1	0x0000000000000000 FFFFFFFFFFFFFFFF
Ciphertext1	0x04642F37BF648700 FB9BD0C8409B78FC
Tag(MAC)1	0xDD6A6A4C4A975B01
Plaintext2	0x0123456789ABCDEF FDECBA9876543210
Ciphertext2	0x05476A5036CF49DF F98895AFC930B513
Tag(MAC)2	0x6146A5E1C2D4C94D

VI. Analysis

6.1 Experiment analysis

Let CPU cycle of PRINCE be ρ ($\rho = 1$, if hardware). Let byte length of plaintext be $\rho\tau$. Total CPU cycle for CCM is

$(\rho\tau \div 8) \times 2 \times \rho$.

Let CPU cycle for Galois field multiplication (hashing) is ς. If GCM is fully parallelized, then total CPU cycle for GCM is

$((\rho\tau \div 8) + 2) \times \varsigma + \rho$.

GCM is faster than CCM, if

$\varsigma < (\rho \times (\rho\tau \times 2 - 8)) \div (\rho\tau + 16)$.

If everything is implemented in hardware, ρ is 1 and ς is 1. Thus, CCM CPU cycle is $(\rho\tau \div 4)$

and GCM CPU cycle is $(\rho\tau \div 8) + 3$.

If $\rho\tau$ is greater than 24 byte, then GCM

is faster than CCM. DNP3 packets are usually longer than 24 byte, thus GCM is faster. Also, GCM is generally faster than CCM with little memory support when both are implemented in software. Also, GCM does not need decryption algorithm. Therefore, GCM is more suitable candidate for authenticated encryption of SCADA systems where resources are constrained.

6.2 Comparison

When a faster authenticated encryption scheme is developed, even software implementation of authenticated encryption can be achieved at minimum overhead. It is not much slower than DNP3 SA where HMAC (SHA-3) is used only to authenticate. The same symmetric key can be used for encryption and authentication in GCM or CCM, so overhead caused by key management is minimal. The key management scheme is based on symmetric key cryptography to ensure efficiency, and the scheme covers from key initialization to key revocation with minimum number of key stored. 〔Table 6〕 represents comparison of our approach and previous ones.

〔Table 6〕 Comparison of each approaches

	DNP Sec	DNP 3 SA	Bump-in-the-wire	Ours
Confidentiality	O	X	O	O
Integrity	O	O	O	O
Authenticity	O	O	O	O
S/W	O	O	X	O
H/W	X	X	O	O
Key mgmt	X	X	O	O
Overhead	High	Mid	Low	Mid

DNPSec and DNP3 SA are software-based approach without a complete key management scheme. DNPSec induces a high overhead. DNP3 SA does not provide confidentiality. Bump-In-The-Wire approach is a hardware-based approach with low overhead. Our approach adds confidentiality and key management scheme to DNP3 SA, and also supports hardware-based security to the SCADA system.

VII. Conclusion

Some recent striking events, which have also caused echoes in the various media, have shown that cyber threats to critical infrastructures can no longer be considered as unlikely possibilities,but, unfortunately,they are real happenings〔2〕.

Although cyber-security techniques have evolved to protect general-purpose IT systems from cyber-threats, they cannot be applicable to protect SCADA systems because of their basic differences with general systems. Thus, many approaches to mold current cyber-security techniques are executed to fit the security requirements of SCADA systems.

DNP3 is a reliable and efficient SCADA network protocol with dominant popularity in United States and increasing popularity in the world. DNPSec and DNP3 SA both have attempted to provide cyber-security to DNP3, but don't satisfy both efficiency and security requirements of SCADA systems. Authenticated encryption adopted in DNP3 SA will satisfy both efficiency and security requirement.

As open problems, where and how authenticated encryption scheme proposed in this paper can be adopted into DNP3 SA should be specified in detail. Furthermore, the security and robustness of proposed scheme should be tested in a simple testbed where model SCADA

system using DNP3 is under development to experiment various attacks like man-in-the-middle attack.

참 고 문 헌

[1] Rosslin John Robles, Min-kyu Choi, and Tai-hoon Kim, "Importance of Supervisory Control and Data Acquisition Security in Critical Infrastructure" 한국정보기술학회 논문지 제7권 제4호, Aug. 2008, 198-207pg

[2] Manuel Cheminod, Luca Durante, and Adriano Valenzano, "Review of Security Issues in Industrial Networks" Industrial Informatics, IEEE Transactions on, Feb. 2013

[3] Modbus-IDA, Modbus Application Protocol Specification. "V. 1.1 b." Hopkinton, Massachusetts (www. modbus. org/docs/Modbus Application Proto col V1 1b. pdf), 2006

[4] IEEE 1815-2010 Standard for Electric Power Systems Communications - Distributed Network Protocol (DNP3), IEEE, July 2010

[5] Munir Majdalawiehr, Francesco Parisi-Presicce, and Duminda Wijesekera. "DNPSec: Distributed network protocol version 3 (DNP3) security framework." Advances in Computer, Information, and Systems Sciences, and Engineering. Springer Netherlands, 2006. 227-234.

[6] Stuxnet - Wikipedia, http://en.wikipedia.org/wiki/Stuxnet, Accessed : June 2013

[7] SCADA - Wikipedia, http://en.wikipedia.org/wiki/SCADA, Accessed : June 2013

[8] Specification, P. R. O. F. I. B. U. S. "Normative Parts of PROFIBUS-FMS,-DP,-PA according to the European Standard EN 50 170.", 1998

[9] PROFINET - Wikipedia, http://en.wikipedia.org/wiki/PROFINET, Accessed : June 2013

[10] AS-Interface - Wikipedia, http://en.wikipedia.org/wiki/AS-Interface, Accessed : June 2013

[11] Modbus - Wikipedia, http://en.wikipedia.org/wiki/Modbus, Accessed : June 2013

[12] IEC 60870-5 - Wikipedia, http://en.wikipedia.org/wiki/IEC_60870-5, Accessed : June 2013

[13] Tomoiaga Radu, and Stratulat Mircea. "Evaluation of DES, 3 DES and AES on Windows and Unix platforms." Computational Cybernetics and Technical Informatics (ICCC-CONTI), 2010 International Joint Conference on. IEEE, 2010

[14] Stéphane Manuel. "Classification and generation of disturbance vectors for collision attacks against SHA-1." Designs, Codes and Cryptography 59.1-3 (2011): 247-263

[15] Jian Guo, San Ling, Christian Rechberger, Huaxiong Wang. "Advanced meet-in-the-middle preimage attacks: First results on full Tiger, and improved results on MD4 and SHA-2." Advances in Cryptology-ASIACRYPT 2010. Springer Berlin Heidelberg, 2010. 56-75.

[16] Sanadhya, Somitra Kumar, and Palash Sarkar. "New collision attacks against up to 24-step SHA-2." Progress in Cryptology-INDOCRYPT 2008. Springer Berlin Heidelberg, 2008. 91-103

[17] "DNP Secure Authentication - Essential to Smart Grid Progress", Smart Grid News, Nov 18, 2008, http://www.smartgridnews.com/artma

n/publish/industry/DNP_Secure_Authentication_Essential_to_Smart_Grid_Progress.html, Accessed : May 2013

〔18〕 Cheryl Beaver, Donald Gallup, William Neumann, Mark Torgerson. "Key management for SCADA." Cryptog. Information Sys. Security Dept., Sandia Nat. Labs, Tech. Rep. SAND2001-3252, 2002

〔19〕 Robert Dawson, Colin Boyd, Ed Dawson, and Juan Manuel González Nieto, "SKMA - a key management architecture for SCADA systems" in Proc. 4th Australasian Information Security Workshop, 2006, vol. 54, pp. 138 - 192

〔20〕 최문석, 김충효, 임유석, 주성호, 임용훈, 전경석. "저지연 Legacy SCADA 보안 통신장치 개발." 정보보호학회논문지 23.2 (2013): 339-346.

〔21〕 Mihir Bellare, Chanathip Namprempre. "Authenticated encryption: Relations among notions and analysis of the generic composition paradigm." Advances in Cryptology—ASIACRYPT 2000. Springer Berlin Heidelberg, 2000. 531-545.

〔22〕 "NIST Selects Winner of Secure Hash Algorithm (SHA-3) Competition", NIST Tech Beat, Oct 2, 2012, http://www.nist.gov/itl/csd/sha-100212.cfm, Accessed : Aug 2013

〔23〕 Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knezevic, Lars R. Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, Peter Rombouts, Søren S. Thomsen, Tolga Yalçın. "PRINCE - A Low-latency Block Cipher for Pervasive Computing Applications." Advances in Cryptology - ASIACRYPT 2012. Springer Berlin Heidelberg, 2012. 208-225.

〔24〕 Morris J. Dworkin. "SP 800-38C. Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality." (2004).

〔25〕 David McGrew, John Viega. "The Galois/Counter mode of operation (GCM)." Submission to NIST. http://csrc.nist.gov/CryptoToolkit/modes/proposedmodes/gcm/gcm-spec.pdf (2004).

〔26〕 GNU Scienfitic Library, http://www.gnu.org/software/gsl/, Accessed : June 2013