Comparison of Encryption Schemes as used in Communication between SCADA Components

Rosslin John Robles[#1], Maricel Balitanas[#2], Ronnie Caytiles[#3],
Yvette Gelogo[#4], Tai-hoon Kim[#5]

[#]*Department of Multimedia Engineering, Hannam University*
Daejeon, Korea

[1]rosslin_john@yahoo.com
[5]taihoonn@hnu.kr

Abstract— **In Symmetric encryption, a secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. While is Asymmetric Encryption, two keys are used. A public key is made freely available to anyone who might want to send you a message. A second, private key is kept secret, so that only you know it. These Schemes can be integrated to SCADA communication. SCADA (Supervisory Control and Data Acquisition) communication can take place in a number of ways. Early SCADA communication took place over radio, modem, or dedicated serial lines. The internet SCADA facility has brought a lot of advantages in terms of control, data generation and viewing. With these advantages, come the security issues regarding web SCADA. In this paper, comparison between Encryption Schemes as used in Communication between SCADA Components is discussed.**

Keywords— **SCADA, Encryption, Internet, Communication, Control System**

I. INTRODUCTION

SCADA or Supervisory Control and Data Acquisition systems provide automated control and remote human monitoring of real world processes. SCADA systems can be used to improve quality and efficiencies in processes such as beer brewing and snow making for ski resorts, but are traditionally used by utilities and industries in the areas of oil and natural gas, electric power, rail transportation, water and wastewater. SCADA systems provide near real time monitoring and control with time delays ranging between fractions of seconds to minutes. Depending on the size and sophistication, SCADA systems can cost from tens of thousands of dollars to tens of millions of dollars. [1]

Supervisory Control and Data Acquisition systems or SCADA is just one implementation of process control systems (PCS). Another common method is Distributed Control Systems (DCS). SCADA systems are typically spread over miles of distance and sometimes have their programmed control functions in the central host computer. [1]

Because of the complexity of SCADA systems, vulnerabilities and threats often occur. SCADA control systems and protocols were often designed decades ago, when security was of little concern because of the closed nature of the communications networks and the general model of trusting the data on them. As these systems have been modernized, they have become interconnected and have started running more modern services such as Web interfaces and interactive consoles and have implemented remote configuration protocols. Sadly, security has been lagging during the increased modernization of these systems. [2]

Encryption in communication between SCADA components is very important. There are two widely used techniques for encrypting information: symmetric encryption which is also called secret key encryption and asymmetric encryption which is also called public key encryption. In the next sections, comparison between Encryption Schemes as used in Communication between SCADA Components is discussed.

II. RELATED LITERATURE

In this section, Related Technologies are discussed, Technologies such as Supervisory Control and Data Acquisition systems or SCADA, Web SCADA, Symmetric Encryption and Asymmetric Encryption.

A. SCADA

Supervisory Control and Data Acquisition (SCADA) existed long time ago when control systems were introduced. SCADA systems that time use data acquisition by using strip chart recorders, panels of meters, and lights. Not similar to modern SCADA systems, there is an operator which manually operates various control knobs exercised supervisory control. These devices are still used to do supervisory control and data acquisition on power generating facilities, plants and factories. [3][4]

Telemetry is automatic transmission and measurement of data from remote sources by wire or radio or other means. It is also used to send commands, programs and receives monitoring information from these remote locations. SCADA is the combination of telemetry and data acquisition.

978-0-7695-4435-9/11 $26.00 © 2011 IEEE
DOI 10.1109/UCMA.2011.33

Supervisory Control and Data Acquisition system is compose of collecting of the information, transferring it to the central site, carrying out any necessary analysis and control and then displaying that information on the operator screens. The required control actions are then passed back to the process. [5].

The measurement and control system of SCADA has one master terminal unit (MTU) which could be called the brain of the system and one or more remote terminal units (RTU). The RTUs gather the data locally and send them to the MTU which then issues suitable commands to be executed on site. A system of either standard or customized software is used to collate, interpret and manage the data. Supervisory Control and Data Acquisition (SCADA) is conventionally set upped in a private network not connected to the internet. This is done for the purpose of isolating the confidential information as well as the control to the system itself. [4]

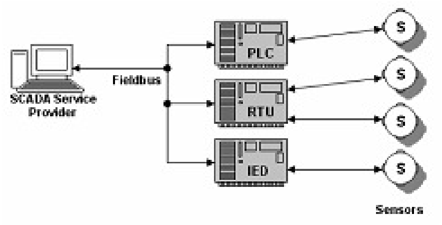


Figure 1. Conventional SCADA Architecture

B. *Web SCADA*

In the next Figure, you can see the architecture of SCADA which is connected through the internet. Like a normal SCADA, it has RTUs/PLCs/IEDs, The SCADA Service Provider or the Master Station. This also includes the user-access to SCADA website. This is for the smaller SCADA operators that can avail the services provided by the SCADA service provider. It can either be a company that uses SCADA exclusively. Another component of the internet SCADA is the Customer Application which allows report generation or billing. Along with the fieldbus, the internet is an extension. This is setup like a private network so that only the master station can have access to the remote assets. The master also has an extension that acts as a web server so that the SCADA users and customers can access the data through the SCADA provider website. [7]

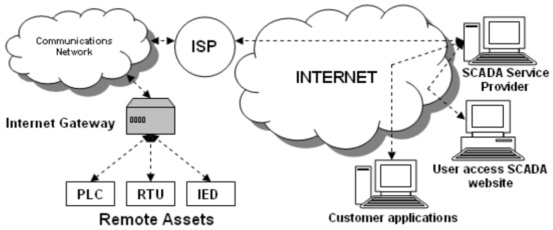


Figure 2. Internet SCADA Architecture [8]

C. *Symmetric Encryption*

Along with the advantages it brings, are security issues regarding wireless internet SCADA. In this section, we discuss internet SCADA, its connection through wireless communication and the security issues surrounding it. To answer the security issues, a symmetric-key encryption for wireless internet SCADA was proposed. [54]

3.2.1 Utilization of Symmetric Key Encryption

Symmetric-key algorithms are a class of algorithms for cryptography that use trivially related, often identical, cryptographic keys for both decryption and encryption. The encryption key is trivially related to the decryption key, in that they may be identical or there is a simple transform to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. [9]

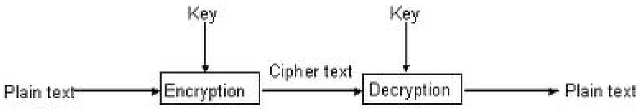


Figure 3. Symmetric Key utilizing same key to encrypt and decrypt the data

Symmetric-key algorithms can be divided into stream ciphers and block ciphers. Stream ciphers encrypt the bytes of the message one at a time, and block ciphers take a number of bytes and encrypt them as a single unit. Blocks of 64 bits have been commonly used; the Advanced Encryption Standard algorithm approved by NIST in December 2001 uses 128-bit blocks. [9]

D. *Asymmetric Encryption*

The internet SCADA facility has brought a lot of advantages in terms of control, data generation and viewing. With these advantages, comes the security issues regarding web SCADA. In this section, web SCADA and its connectivity along with the issues regarding security will be discussed. A web SCADA security solution using asymmetric-key encryption will be explained.

3.1.1 Asymmetric-key Encryption

Asymmetric key encryption uses different keys for decryption/encryption. These two keys are mathematically related and they form a key pair. One key is kept private, and is called private-key, and the other can be made public, called public-key. Hence this is also called Public Key Encryption. Public key can be sent by mail. A private key is typically used for encrypting the message-digest; in such an application private-key algorithm is called message-digest encryption algorithm. A public key is typically used for encrypting the secret-key; in such a application private-key algorithm is called key encryption algorithm. [12]

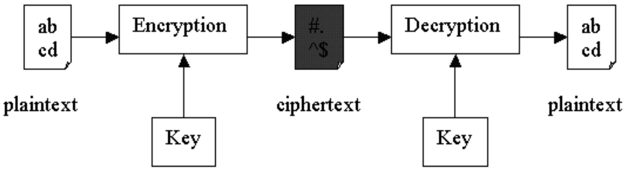


Figure 4. Asymmetric key encryption uses different keys for decryption and encryption

Popular private-key algorithms are RSA and DSA (Digital Signature Algorithm). While for an ordinary use of RSA, a key size of 768 can be used, but for corporate use a key size of 1024 and for extremely valuable information a key size of 2048 should be used. Asymmetric key encryption is much slower than symmetric key encryption and hence they are only used for key exchanges and digital signatures. RSA is an algorithm for public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key cryptography. [12]

RSA is widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations. One of the most common digital signature mechanisms, the Digital Signature Algorithm (DSA) is the basis of the Digital Signature Standard (DSS), a U.S. Government document. As with other digital signature algorithms, DSA lets one person with a secret key "sign" a document, so that others with a matching public key can verify it must have been signed only by the holder of the secret key. Digital signatures depend on hash functions, which are one-way computations done on a message. [12] They are called "one-way" because there is no known way (without infeasible amounts of computation) to find a message with a given hash value. In other words, a hash value can be determined for a given message, but it is not known to be possible to construct any message with a given hash value.

Hash functions are similar to the scrambling operations used in symmetric key encryption, except that there is no decryption key: the operation is irreversible. The result has a fixed length, which is 160 bits in the case of the Secure Hash Algorithm (SHA) used by DSA. [12]

III. Implementation and discussion

The following sub-sections discuss the implementation of the proposed solution. It contain the implementation of solutions like the Integration of Asymmetric-key Encryption to Internet SCADA; and Symmetric Key Encryption in SCADA Environment.

A. Integration of Asymmetric-key Encryption to Web SCADA

Authentication will be required to access the data and reports so that only users who have enough permission can access the information. Quality system administration techniques can make all the difference in security prevention [13]. SCADA web server must always be secure since the data in it are very critical. Web server security software can also be added.

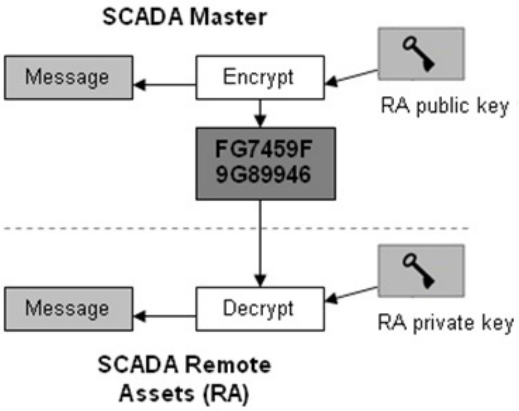


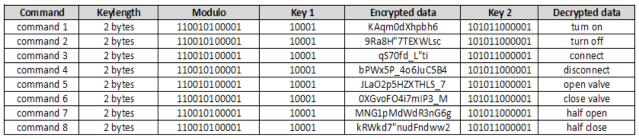
Figure 5. Asymmetric-key encryption applied to internet SCADA

Communication from the customer or client will start with an http request to the master server. The client will be authenticated before the request will be completed. The SCADA master will then send back the requested information to the client. The information will also be encrypted using the same encryption that is proposed to be used between the SCADA master and the remote assets. [12]

To test the usability of this scheme, it was tested using the web base Asymmetric-key Encryption simulator. Since there are many kinds of Asymmetric-key Encryption, in this simulator, RSA Cipher is used.

The following table shows the results of encrypted commands. The first column shows the command; the second column shows the key length; the third column shows the Modulo, the fourth column shows the key which is used for encrypting the command, the fifth column shows the encrypted data; the sixth column shows the key which is used to decrypt the data and the last column shows the actual command.

TABLE 4-1. ASYMMETRIC-KEY ENCRYPTION OF SCADA COMMANDS



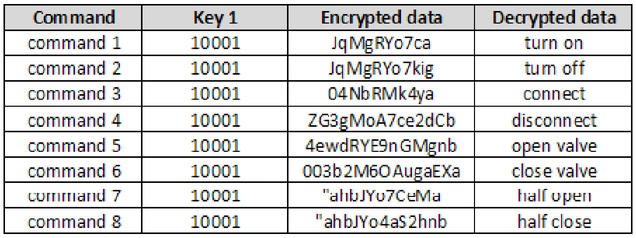
Command	Keylength	Modulo	Key 1	Encrypted data	Key 2	Decrypted data
command 1	2 bytes	110010100001	10001	KAqm0dXhpbh6	101011000001	turn on
command 2	2 bytes	110010100001	10001	9Ra8H"7TEXWLsc	101011000001	turn off
command 3	2 bytes	110010100001	10001	qS70fd_L"ti	101011000001	connect
command 4	2 bytes	110010100001	10001	bPWx5P_4o6JuC5B4	101011000001	disconnect
command 5	2 bytes	110010100001	10001	JLaO2p5HZXTHLS_7	101011000001	open valve
command 6	2 bytes	110010100001	10001	0XGvoFO4i7mIP3_M	101011000001	close valve
command 7	2 bytes	110010100001	10001	MNG1pMdWdR3nG6g	101011000001	half open
command 8	2 bytes	110010100001	10001	kRWkd7"nudFndww2	101011000001	half close

SCADA systems connected through the internet can provide access to real-time data display, alarming, trending, and reporting from remote equipment. But it also presents some vulnerabilities and security issues. In this section, the security issues in internet SCADA were pointed out. The utilization of asymmetric key encryption is suggested. It can provide security to the data that is transmitted from the SCADA master and the remote assets. Once a system is connected to the internet, it is not impossible for other internet users to have access to the system that is why encryption is very important. [12]

B. Symmetric Key Encryption in Web SCADA

The following table shows the results of encrypted commands. The first column shows the command; the second column shows the key which is used for encryption; the third column shows the encrypted data and the last column shows the actual command.

TABLE 4-2. SYMMETRIC-KEY ENCRYPTION OF SCADA COMMANDS



Command	Key 1	Encrypted data	Decrypted data
command 1	10001	JqMgRYo7ca	turn on
command 2	10001	JqMgRYo7kig	tum off
command 3	10001	04NbRMk4ya	connect
command 4	10001	ZG3gMoA7ce2dCb	disconnect
command 5	10001	4ewdRYE9nGMgnb	open valve
command 6	10001	003b2M6OAugaEXa	close valve
command 7	10001	"ahbJYo7CeMa	half open
command 8	10001	"ahbJYo4aS2hnb	half close

IV. CONCLUSIONS

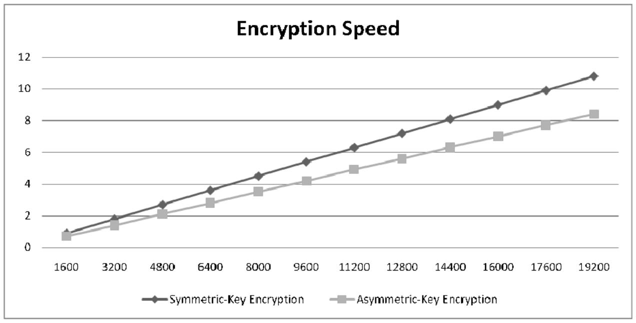


Figure 6. Encryption Speed Comparison

The process of communication over a SCADA system involves several different SCADA system components. These include the sensors and control relays, Remote Terminal Units (RTUs), SCADA master units, and the overall communication network. Each of these parts is necessary for effective SCADA communication. A system can effectively monitor alarms and status updates within the network only when all of these system components function properly. A lot of communication issues emerged as of late. In this paper, we compare different encryption schemes for SCADA communication.

An important thing to be considered is the Encryption Speed. Compared to Asymmetric Key Encryption, Symmetric Key Encryption appears to be slower. It's important to note right from the beginning that beyond some ridiculous point, it's not worth sacrificing speed for security. However, the measurements will still help us make certain decisions. It is also important to remember that SCADA Communication is a core component of a SCADA Monitoring System therefore it may not function properly without proper communication.

References

[1] Andrew Hildick-Smith (2005), "Security for Critical Infrastructure SCADA Systems", SANS Institute InfoSec Reading Room

[2] Tim Yardley (2008), "SCADA: issues, vulnerabilities, and future directions", http://www.usenix.org/publications/login/2008-12/pdfs/yardley.pdf Accessed: March 2011

[3] Rosslin John Robles, Min-kyu Choi, Maricel Balitanas, Feruza Sattarova, Farkhod Alisherov, Nayoun Kim, Tai-hoon Kim, "Vulnerabilities in Control Systems, Critical Infrastructure Systems and SCADA", Proceedings of the 8th KIIT IT based Convergence Service workshop & Summer Conference, Mokpo Maritime University (Mokpo, Korea), pp. 89, ISSN 2005-7334

[4] Tai-hoon Kim, (2010), "Weather Condition Double Checking in Internet SCADA Environment", WSEAS TRANSACTIONS on SYSTEMS and CONTROL, Issue 8, Volume 5, August 2010, ISSN: 1991-8763, pp. 623

[5] D. Bailey and E. Wright (2003) Practical SCADA for Industry

[6] Andrew Hildick-Smith (2005) Security for Critical Infrastructure SCADA Systems

[7] Rosslin John Robles, Kum-Taek Seo, Tai-hoon Kim, "Communication Security solution for internet SCADA", Korean Institute of Information Technology 2010 IT Convergence Technology - Summer workshops and Conference Proceedings, 2010.5, pp. 461 ~ 463

[8] D. Wallace, (2003), "Control Engineering. How to put SCADA on the Internet", http://www.controleng.com/article/CA321065.html Accessed: January 2010

[9] RSA LAboratories "What is RC4?", http://www.rsa.com/rsalabs/node.asp?id=2250 Accessed: June 2009

[10] P. Prasithsangaree and P. Krishnamurthy, (2003), "Analysis of Energy Consumption of RC4 and AES Algorithms in Wireless LANs"

[11] "RC4", http://www.wisdom.weizmann.ac.il/~itsik/RC4/rc4.html Accessed: June 2009

[12] Minkyu Choi, Rosslin John Robles, Taihoon Kim, “Application Possibility of Asymmetric-key Encryption to SCADA Security”, The Journal of Korean Institute of Information Technology, Vol.7 No.4, August 2009, pp. 208-217, ISSN: 1958-8619

[13] NACS, "Client/Server Security Assessment and Awareness" Accessed: April 2009