International Journal of Internet, Broadcasting and Communication Vol.4 No.2 17-21 (2012)
http://dx.doi.org/10.7236/IJIBC.2012.4.2.17

IJIBC 12-2-4

Applying Asymmetric Key Encryption to Secure Internet based SCADA

Rosslin John Robles[1], Tai-hoon Kim[1*]

[1,1]GVSA and UTAS, Australia*
rosslin_john@yahoo.com, taihoonn@hnu.kr

Abstract

As an acronym for Supervisory Control and Data Acquisition, SCADA is a concept that is used to refer to the management and procurement of data that can be used in developing process management criteria. The use of the term SCADA varies, depending on location. Conventionally, SCADA is connected only in a limited private network. In current times, there are also demands of connecting SCADA through the internet. 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, we discuss web SCADA and its connectivity along with the issues regarding security and suggests a web SCADA security solution using asymmetric-key encryption.

Keywords: *SCADA system, Security Issues, Asymmetric Encryption, Internet-based*

1. Introduction

SCADA refers to a system that performs the same basic functions, but operates in a number of different environments as well as a multiplicity of scales. It is so important since it control most of our commodities. SCADA communications has been Point-to-Multipoint serial communications over lease line or private radio systems. With the increasing popularity of Internet Protocol (IP), IP Technology has seen increasing use in SCADA communications.

The Internet can give SCADA more scale which can make it provide access to real-time data display, alarming, trending, and reporting from remote equipment. On the next section, SCADA is discussed, the conventional and the Internet SCADA. Advantages which can be attained using the Internet for SCADA are also covered. Security issues are being pointed out. The integration of asymmetric key encryption to internet SCADA is also suggested to provide security in SCADA communication.

2. Internet-based SCADA

Conventional SCADA only have 4 components: the master station, plc/rtu, fieldbus and sensors. Internet SCADA replaces or extends the fieldbus to the internet. This means that the Master Station can be on a different network or location.

Manuscript Received: May. 03, 2012 / Revised: Jul. 29, 2012 / Accepted: Aug. 10, 2012
Corresponding Author: taihoonn@hnu.kr
Tel:+82-42-629-8373, Fax: +82-42-629-8373
GVSA and UTAS, Australia

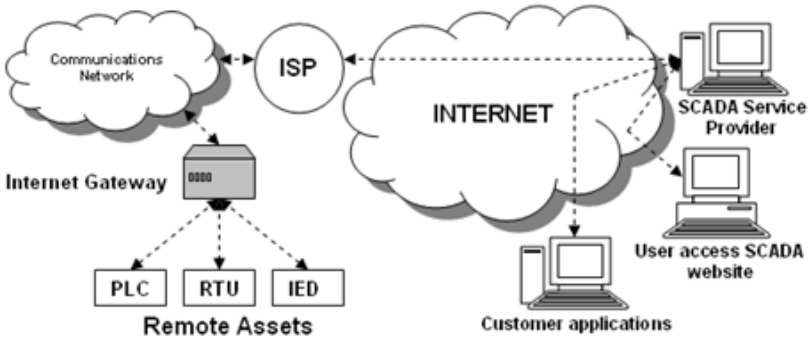

Figure 2-1. Internet SCADA Architecture [48]

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. [1]

AS the system evolves, SCADA systems are coming in line with standard networking technologies. Ethernet and TCP/IP based protocols are replacing the older proprietary standards. Although certain characteristics of frame-based network communication technology (determinism, synchronization, protocol selection, environment suitability) have restricted the adoption of Ethernet in a few specialized applications, the vast majority of markets have accepted Ethernet networks for HMI/SCADA.

A few vendors have begun offering application specific SCADA systems hosted on remote platforms over the Internet. This removes the need to install and commission systems at the end-user's facility and takes advantage of security features already available in Internet technology, VPNs and SSL. Some concerns include security, [2] Internet connection reliability, and latency.

3. Application

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 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 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. [2]

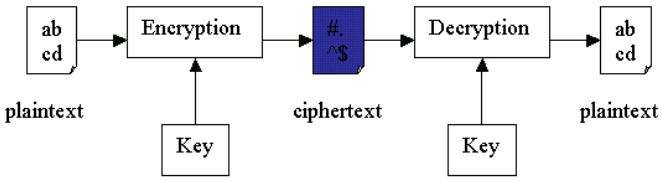

Figure 3-1. Asymmetric key encryption uses different keys for decryption and encryption

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. [2]

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. [3] 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. [2]

4. Analysis

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 [2]. SCADA web server must always be secure since the data in it are very critical. Web server security software can also be added.

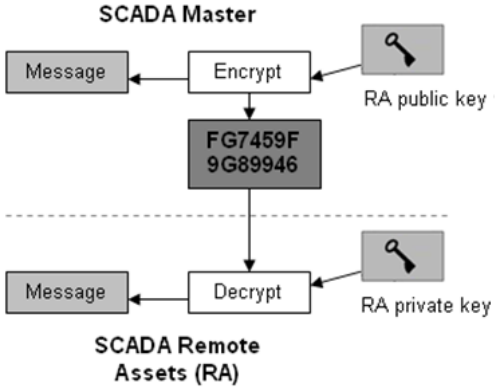

Figure 4-1. Asymmetric-key encryption applied to internet SCADA

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. [3] 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.

Figure 4-2. Browser based RSA Cipher Simulator

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 4-3. 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. [3]

5. Conclusion

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 paper; we pointed out the security issues in internet SCADA. 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.

References

[1] 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
[2] D. Wallace, (2003), "Control Engineering. How to put SCADA on the Internet",
[3] 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