International Journal of Internet, Broadcasting and Communication Vol.4 No.1 3-7 (2012)
http://dx.doi.org/10.7236/IJIBC.2012.4.1.3

IJIBC 12-1-2

Securing Internet-based SCADA Wireless Component Communication

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

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

Abstract

Traditionally SCADA is connected only in a limited private network. With new technology and facilities, there are also demands of connecting SCADA though the internet. The internet SCADA facility has brought a lot of advantages in terms of control, data viewing and generation. Aside from connecting SCADA to the internet, there are also operators who want to connect their system wirelessly. This can save budget for communication lines. Along with the advantages it brings, are security issues regarding wireless internet SCADA. In this paper, 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 internet SCADA is proposed.

Keywords: *SCADA, Symmetric-Key, Encryption, Internet*

1. Introduction

SCADA like other Control Systems have been so important since it control most of our commodities. Traditional SCADA communications has been Point-to-Multipoint serial communications over lease line or private radio systems. With the advent of Internet Protocol (IP), IP Technology has seen increasing use in SCADA communications. The connectivity of the Internet can give SCADA more scale which enables it to provide access to real-time data display, alarming, trending, and reporting from remote equipment. Wireless communication is the transfer of information over a distance without the use of electrical conductors or wires. [1]

Wireless technology can also be applied to SCADA especially when it is connected through the internet. It can save a lot of budget for communication lines. On the Next parts of this paper, SCADA is discussed, the conventional setup, Internet SCADA and the wireless SCADA. Advantages which can be attained using wireless technology for Internet SCADA are also covered. Security issues are being pointed out.

We proposed a Symmetric-key encryption for Wireless Internet SCADA security.

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. 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.

Manuscript Received: Dec. 01, 2011 / Revised: Jan. 18, 2012 / Accepted: Feb. 13, 2012
Corresponding Author: taihoonn@hnu.kr
Tel:+82-42-629-8373, Fax: +82-42-629-8373
GVSA and UTAS, Australia

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. [2] 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.

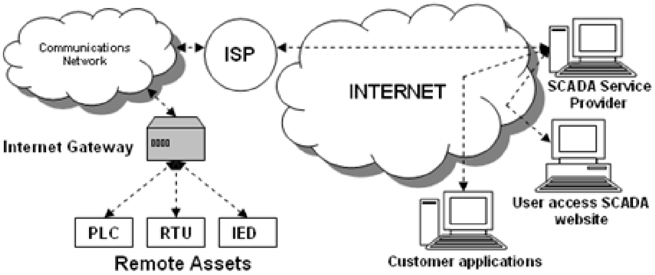


Figure 2-1. Internet SCADA Architecture [48]

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, [3] Internet connection reliability, and latency.

3. Application

As stated in the previous sections, SCADA was connected only in a limited private network when it was introduced. With new technology and facilities, there are also demands of connecting SCADA though the internet. The internet SCADA facility has brought a lot of advantages in terms of control, data viewing and generation. Aside from connecting SCADA to the internet, there are also operators who want to connect their system wirelessly. This can save budget for communication lines. [4]

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. [4]

3.1 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. [5]

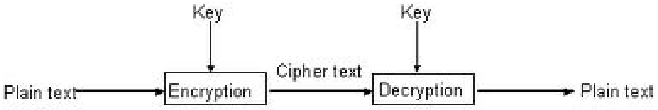


Figure 3-1. Symmetric Key utilizing same key to encrypt and decrypt the data

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

3.2 RC4 Cipher

RC4 is a stream cipher designed by Rivest for RSA Data Security (now RSA Security). It is a variable key-size stream cipher with byte-oriented operations. [3] It is the most widely-used software stream cipher and is used in popular protocols such as Secure Sockets Layer (SSL) (to protect Internet traffic) and WEP (to secure wireless networks).[5] While remarkable for its simplicity and speed in software, RC4 has weaknesses that argue against its use in new systems.[5] It is especially vulnerable when the beginning of the output keystream is not discarded, nonrandom or related keys are used, or a single keystream is used twice; some ways of using RC4 can lead to very insecure cryptosystems such as WEP. The algorithm is based on the use of a random permutation. Analysis shows that the period of the cipher is overwhelmingly likely to be greater than 10100. Eight to sixteen machine operations are required per output byte, and the cipher can be expected to run very quickly in software. Independent analysts have scrutinized the algorithm and it is considered secure. [5] Many stream ciphers are based on linear feedback shift registers (LFSRs), which while efficient in hardware are less so in software. The design of RC4 avoids the use of LFSRs, and is ideal for software implementation, as it requires only byte manipulations. It uses 256 bytes of memory for the state array, S[0] through S[255], c bytes of memory for the key, key[0] through key[c-1], and integer variables, a, b, and c. Performing a modulus 256 can be done with a bitwise AND with 255.

4. Analysis

Symmetric cryptography uses the same key for both encryption and decryption. Using symmetric cryptography, it is safe to send encrypted messages without fear of interception. This means only the SCADA master and the remote assets can communicate with each other because of the said key.

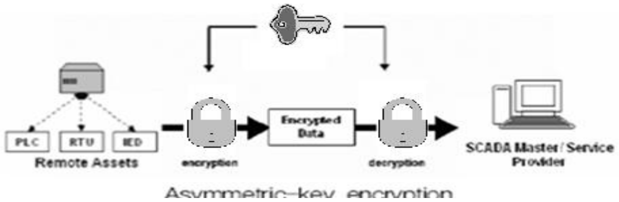


Figure 4-3. Symmetric cryptography between SCADA Master Station and Remote Components

WEP was included as the privacy of the original IEEE 802.11 standard. WEP uses the stream cipher RC4 for confidentiality, and the CRC-32 checksum for integrity. It can be implemented to wireless SCADA as it is implemented to other wireless systems. Messages between remote RTU's can be converted to ciphertext by utilizing this mechanism. The next Figure shows how this is done. [4]

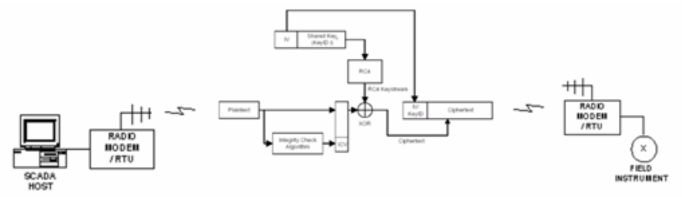
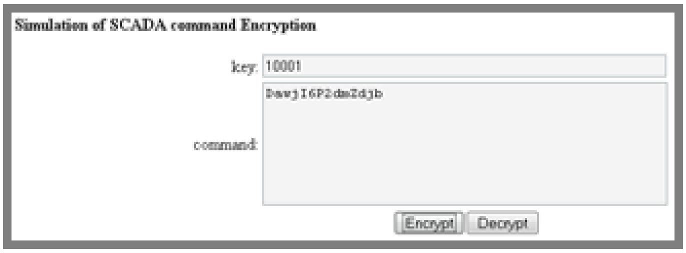


Figure 4-4. Standard WEP Encryption in Wireless SCADA environment

The use of symmetric key encryption specifically the RC4 cipher was also is applicable in a wireless Web-SCADA. It can provide security to the data that is transmitted from the SCADA master and the remote assets and also communication between remote RTU's. Once a system is connected to the internet specially wirelessly, it is not impossible for other internet users to have access to the system that is why encryption should be implemented. Data and report generation is also in demand so the internet SCADA is designed to have a web based report generation system through http. And to cut off the budget for communication lines, SCADA operators utilize the wireless based SCADA. [4]

To test the usability of this scheme, it was tested using the web base Symmetric-key Encryption simulator. Since there are many kinds of Symmetric-key Encryption, in this simulator, RC4 is used.



Simulation of SCADA command Encryption

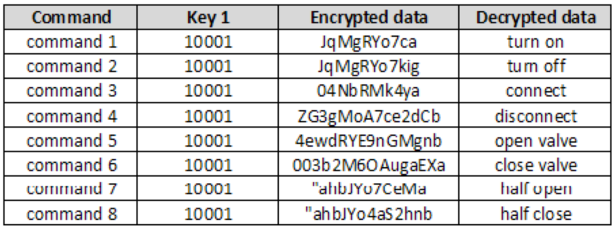
key: 10001

command: DawjI6P2dmZdjb

Figure 4-5. Browser based RC4 Simulator

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

5. Conclusion

Wireless Internet based SCADA systems can provide access to real-time data display, alarming, trending, and reporting from remote equipment. However, it also presents some vulnerabilities and security issues. In this paper, we discuss how to set up SCADA through a wireless medium to the internet. We also discuss the advantages it brings and also some security issues surrounding it.

The use of symmetric key encryption specifically the RC4 cipher was also proposed. It can provide security to the data that is transmitted from the SCADA master and the remote assets and also communication between remote RTU's. 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 should be implemented. Data and report generation is also in demand so the internet SCADA is designed to have a web based report generation system through http. And to cut off the budget, we suggest in this paper to set it up in a wireless environment.

References

[1] Wikipedia, Wireless, http://en.wikipedia.org/wiki/Wireless

[2] 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

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

[4] Rosslin John Robles and Min-Kyu Choi, "Symmetric-Key Encryption for Wireless Internet SCADA", Communications in Computer and Information Science, Volume 58, Security Technology, Pages 289-297, ISSN: 1865-0929

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