academicJournals

Vol. 7(24), pp. 2342-2351, 28 June, 2013
DOI: 10.5897/AJBM12.300
ISSN 1993-8233 © 2013 Academic Journals
http://www.academicjournals.org/AJBM

African Journal of Business Management

*Full Length Research Paper*

# Applying encryption schemed to supervisory control and data acquisition systems for security management

**Tai-hoon Kim**

GVSA and University of Tasmania, Australia.

Accepted 27 May, 2013

**Supervisory Control and Data Acquisition (SCADA) is the combination of telemetry and data acquisition. 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. Encryption Schemes are needed to secure communication in SCADA Systems. In the case of Symmetric key 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 in the case of 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 for managing security level. In this paper, author compares Encryption Schemes as used in Communication between SCADA components to show the escalation of security level.**

**Key words:** Supervisory Control and Data Acquisition, encryption, internet, communication, control system.

## INTRODUCTION

Supervisory Control and Data Acquisition (SCADA) is an 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 (Yardley, 2008; Hildick-Smith, 2005). SCADA 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 (Hildick-Smith, 2005).

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 inter-connected 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 (Yardley, 2008; Zhu et al., 2011; Abawajy and Robles, 2010).

E-mail: taihoonn@paran.com.

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.

## RELATED LITERATURE

### Supervisory control and data acquisition (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 (Robles et al., 2009; Kim, 2010).

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. 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 (Bailey and Wright, 2003).

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 (Figure 1). This is done for the purpose of isolating the confidential information as well as the control to the system itself (Kim, 2010).

### Hardware

A SCADA system consists of a number of remote terminal units (RTUs) collecting field data and sending that data back to a master station, via a communication system (Hildick-Smith, 2005). The master station displays the acquired data and allows the operator to perform remote control tasks. The accurate and timely data allows for optimization of the plant operation and process. Other benefits include more efficient, reliable and most importantly, safer operations. These results in a lower cost of operation compared to earlier non-automated systems (Kim, 2010).

Supervisory Control and Data Acquisition Systems usually have Distributed Control System components. PLCs or RTUs are also commonly used; they are capable of autonomously executing simple logic processes without a master computer controlling it. A functional block programming language, IEC 61131-3, is frequently used to create programs which run on these PLCs and RTUs. This allows SCADA system engineers to perform both the design and implementation of a program to be executed on an RTU or PLC. From 1998, major PLC manufacturers have offered integrated HMI /SCADA systems, many use open and non-proprietary communications protocols. Many third-party HMI/SCADA packages, offering built-in compatibility with most major PLCs, have also entered the market, allowing mechanical engineers, electrical engineers and technicians to configure HMIs themselves. Much other hardware are also basing its functionality to those of PLC's (NACS 2009).

The communications system provides the pathway for communication between the master station and the remote sites. This communication system can be wire, fiber optic, radio, telephone line, microwave and possibly even satellite. Specific protocols and error detection philosophies are used for efficient and optimum transfer of data. The master station (or sub-masters) gather data from the various RTUs and generally provide an operator interface for display of information and control of the remote sites. In large telemetry systems, sub-master sites gather information from remote sites and act as a relay back to the control master station (Kim, 2010).

### Software

Supervisory Control and Data Acquisition software can be divided into proprietary type or open type. Proprietary software are developed and designed for the specific hardware and are usually sold together. The main problem with these systems is the overwhelming reliance on the supplier of the system. Open software systems are designed to communicate and control different types of hardware. It is popular because of the interoperability they bring to the system (Bailey and Wright, 2003). WonderWare and Citect are just two of the open software packages available in the market for SCADA systems. Some packages are now including asset management integrated within the SCADA system (Kim, 2010).

### Human machine interface (HMI)

In SCADA and in the industrial design field of human-

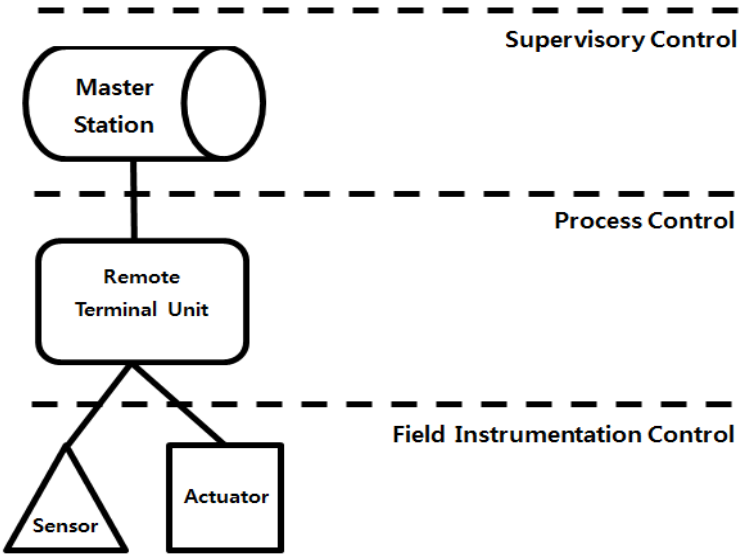


**Figure 1.** Conventional SCADA architecture.

machine interaction, the user interface is (a place) where interaction between humans and machines occurs. The goal of interaction between a human and a machine at the user interface is effective operation and control of the machine, and feedback from the machine which aids the operator in making operational decisions. Examples of this broad concept of user interfaces include the interactive aspects of computer operating systems, hand tools, heavy machinery operator controls and process controls (Kim, 2010).

The goal of human-machine interaction engineering is to produce a user interface which makes it easy, efficient, and enjoyable to operate a machine in the way which produces the desired result. This generally means that the operator needs to provide minimal input to achieve the desired output, and also that the machine minimizes undesired outputs to the human (Kim, 2010). Ever since the increased use of personal computers and the relative decline in societal awareness of heavy machinery, the term user interface has taken on overtones of the (graphical) user interface, while industrial control panel and machinery control design discussions more commonly refer to human-machine interfaces (Robles et al., 2009).

The design of a user interface affects the amount of effort the user must expend to provide input for the system and to interpret the output of the system, and how much effort it takes to learn how to do this. Usability is the degree to which the design of a particular user interface takes into account the human psychology and physiology of the users, and makes the process of using the system effective, efficient and satisfying. Usability is mainly a characteristic of the user interface, but is also associated with the functionalities of the product and the process to design it. It describes how well a product can be used for its intended purpose by its target users with efficiency, effectiveness, and satisfaction (Kim, 2010).

SCADA system includes a user interface which is usually called Human Machine Interface (HMI). The HMI of a SCADA system is where data is processed and presented to be viewed and monitored by a human operator. This interface usually includes controls where the individual can interface with the SCADA system. HMI's are an easy way to standardize the facilitation of monitoring multiple RTU's or PLC's (programmable logic controllers). Usually RTU's or PLC's will run a pre programmed process, but monitoring each of them individually can be difficult, usually because they are spread out over the system. Because RTU's and PLC's historically had no standardized method to display or present data to an operator, the SCADA system communicates with PLC's throughout the system network and processes information that is easily disseminated by the HMI. HMI's can also be linked to a database, which can use data gathered from PLC's or RTU's to provide graphs on trends, logistic info, schematics for a specific sensor or machine or even make troubleshooting guides accessible. In the last decade, practically all SCADA systems include an integrated HMI and PLC device making it extremely easy to run and monitor a SCADA system (Kim, 2010).

The HMI package for the SCADA system typically includes a drawing program that the operators or system maintenance personnel use to change the way these points are represented in the interface. These representations can be as simple as an on-screen traffic light, which represents the state of an actual traffic light in the field, or as complex as a multi-projector display representing the position of all of the elevators in a skyscraper or all of the trains on a railway (Kim, 2010).

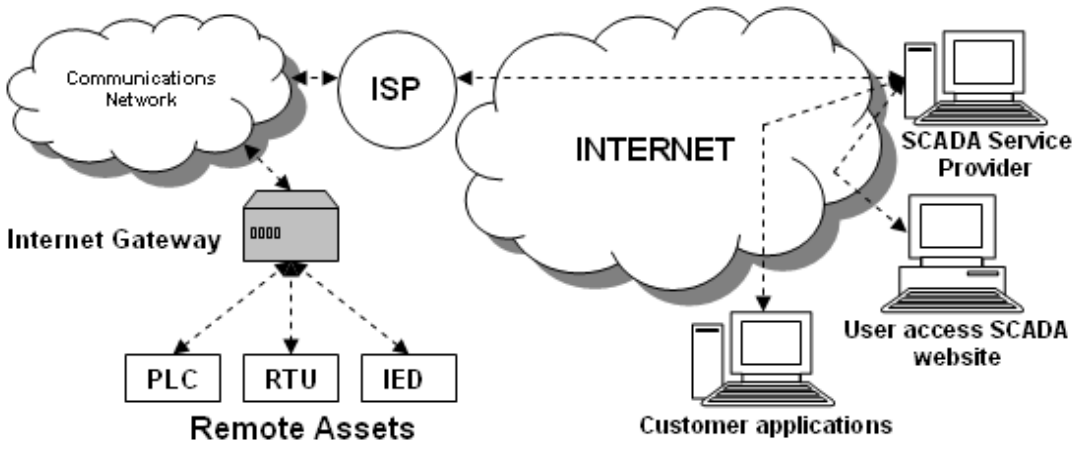


**Figure 2.** Internet SCADA architecture [Wallace, 2003].

Alarm handling is an important part of most SCADA implementations. The system monitors whether certain alarm conditions are satisfied, to determine when an alarm event has occurred. Once an alarm event has been detected, one or more actions are taken (such as the activation of one or more alarm indicators, and perhaps the generation of email or text messages so that management or remote SCADA operators are informed).

## Internet SCADA or web SCADA

Conventional SCADA only have 4 components: The master station, plc/rtu, fieldbus and sensors (Figure 1). Internet SCADA replaces or extends the fieldbus to the internet. This means that the Master Station can be on a different network or location.

Figure 2 shows 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 (Robles et al 2010).

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, (NACS, 2009) Internet connection reliability, and latency.

## 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 (Prasithsangaree and Krishnamurthy, 2003).

## 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 (Figure 3). 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 (RSA Laboratories).

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

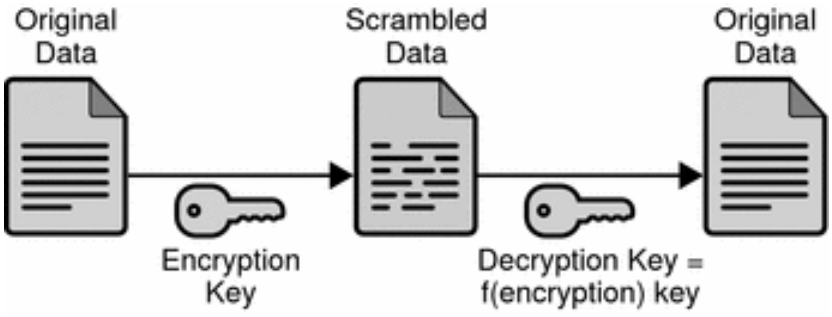


**Figure 3.** Symmetric key utilizing same key to encrypt and decrypt the data.

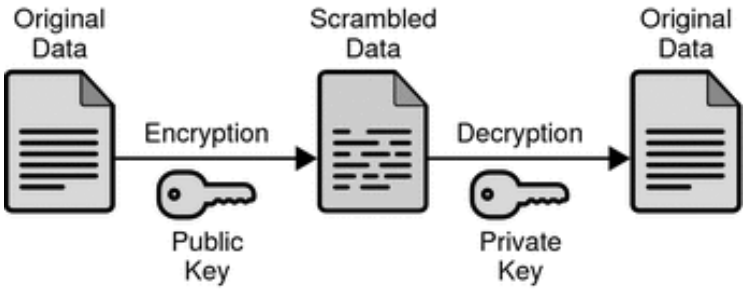


**Figure 4.** Asymmetric key encryption uses different keys for decryption and encryption.

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 (RSA Laboratories).

## Asymmetric encryption

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.

## Asymmetric-key encryption

Asymmetric key encryption uses different keys for decryption/encryption (Figure 4). 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 (Choi et al., 2009).

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 (Choi et al., 2009).

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 (Choi et al., 2009). They are called "one-way" because there is no known way (without infeasible amounts of computation) to find a

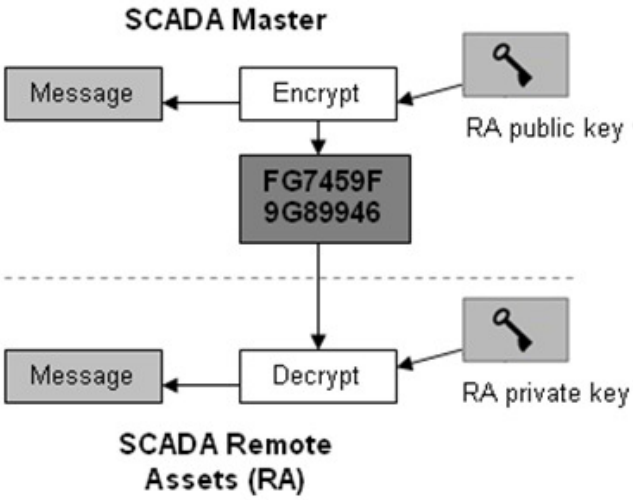


**Figure 5.** Asymmetric-key encryption applied to internet SCADA.

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 (Choi et al., 2009; Robles and Kim, 2011).

## IMPLEMENTATION AND DISCUSSION

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

### 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 (NACS, 2009). SCADA web server must always be secure since the data in it are very critical. Web server security software can also be added.

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 (Choi et al., 2009; Robles and Kim, 2011).

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 6).

Table 1 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.

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 (Figure 5). 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 (Choi et al., 2009; Stoica and Robles, 2010).

### Symmetric key encryption in web SCADA

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

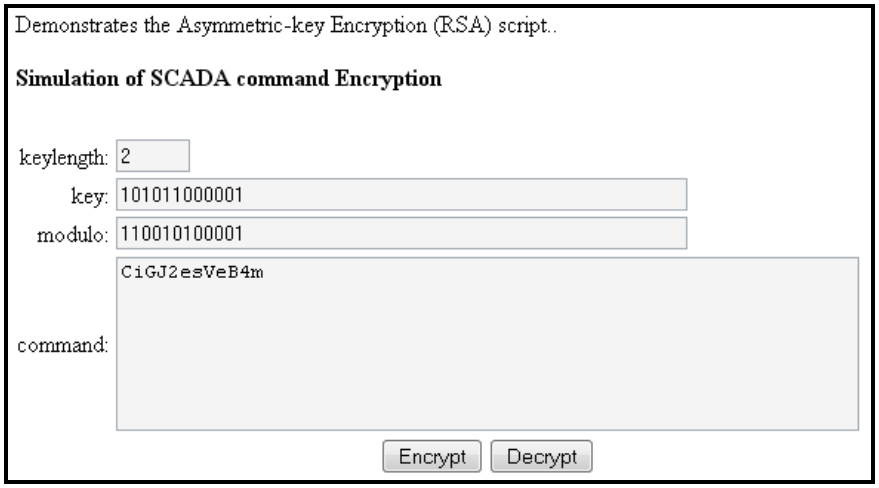


**Figure 6.** Browser based RSA Cipher simulator.

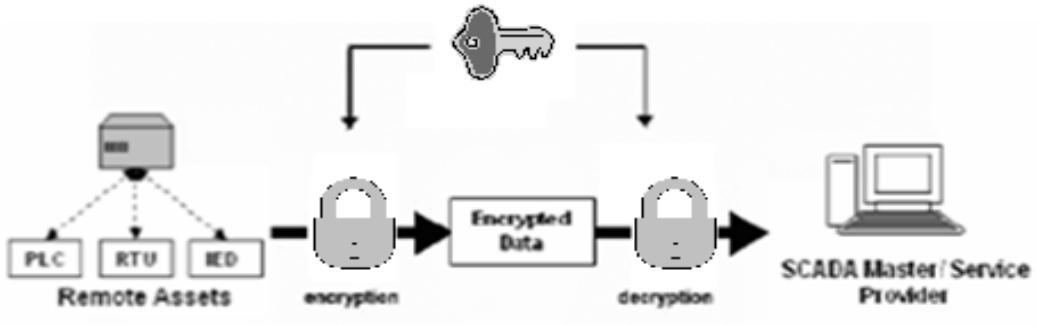


**Figure 7.** Symmetric cryptography between SCADA master station and remote components.

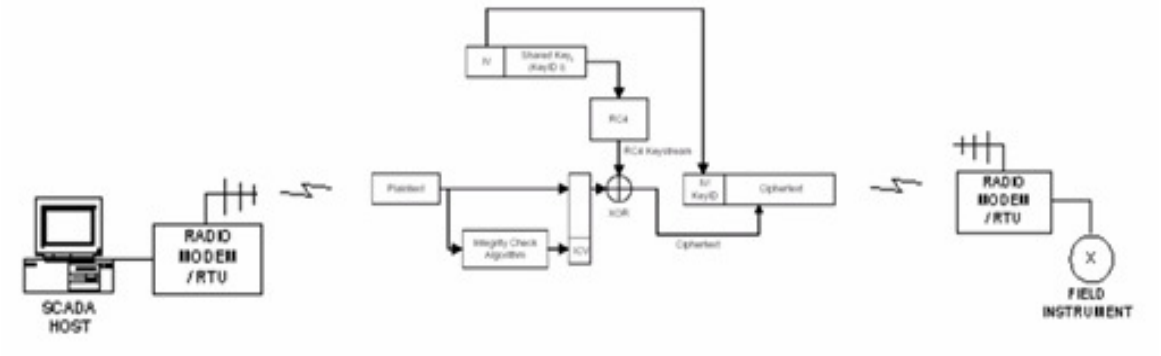


**Figure 8.** Standard WEP encryption in wireless SCADA environment.

and the remote assets can communicate with each other because of the said key (Figure 7).

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. Figure 8 shows how this is done.

The use of symmetric key encryption specifically the RC4 cipher is also 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


**Figure 9.** Browser based RC4 simulator.

**Table 1.** Asymmetric-key Encryption of SCADA commands.

| Command | Key length | 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 | class valve |
| Command 7 | 2 bytes | 110010100001 | 10001 | MNG1pMdWdR3nG6g | 101011000001 | half open |
| Command 8 | 2 bytes | 110010100001 | 10001 | kRWKd7”nudFndww2 | 101011000001 | half close |

**Table 2.** Symmetric-key encryption of SCADA commands.

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

is connected to the internet especially 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 (NACS, 2009).

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 (Figure 9). The simulator uses the following javascript function to encrypt the command:

```
function rc4encrypt() {
document.rc4.text.value=textToBase64(rc4(document.rc
4.key.value,document.rc4.text.value))
}
```

And the following javascript function is used to decrypt the command:

```
function rc4decrypt() {
document.rc4.text.value=(rc4(document.rc4.key.value,ba
se64ToText(document.rc4.text.value)))
}
```

Table 2 shows the results of encrypted commands. The

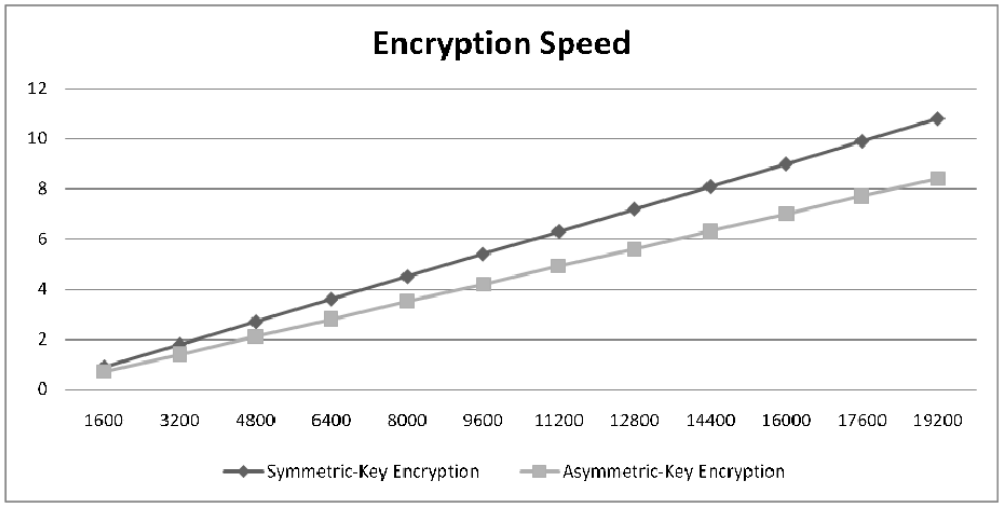


**Figure 10.** Encryption speed comparison.

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.

## CONCLUSION

SCADA refers to the control system of the industry which is a computer system which controls and monitors a process. SCADA Communication is a core component of a SCADA Monitoring System. Common misconception regarding SCADA security was SCADA networks were isolated from all other networks and so attackers could not access the system. As the industry grows, the demand for more connectivity also increased. From a small range network, SCADA systems are sometimes connected to other networks like the internet. The open standards also make it very easy for attackers to gain in-depth knowledge about the working of these SCADA networks. Because of so many vulnerabilities encryption Schemes are applied to secure the communication between the components. This work compares different Encryption Schemes for Securing Internet SCADA Component Communication. And this work shows new method can manage the higher level in security.

An important thing to be considered is the Encryption Speed (Figure 10). 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.

## ACKNOWLEDGEMENTS

Author wishes to express special thanks to Dr. Rosslin John Robles and Dr. Maricel O. Balitanas who helped simulation. This work was done based on their endless passion.

### REFERENCES

Abawajy J, Robles RJ (2010). “Secured Communication Scheme for SCADA in Smart Grid Environment”. J. Sec. Eng. 7(6): 575:584

Bailey D, Wright E (2003). Practical SCADA for Industry, IDC Technologies, ISBN: 07506 58053.

Choi M, Robles RJ, Kim T (2009). “Application Possibility of Asymmetric-key Encryption to SCADA Security”. J. Korean Inst. Info. Technol. 7(4): 208-217, ISSN: 1958-8619.

Hildick-Smith A (2005). "Security for Critical Infrastructure SCADA Systems", SANS Institute InfoSec Reading Room, http://www.sans.org/reading_room/whitepapers/warfare/security-critical-infrastructure-scada-systems_1644.

Kim T-h (2010). "Weather Condition Double Checking in Internet SCADA Environment", WSEAS TRANSACTIONS on SYSTEMS and CONTROL. 5(8): 623-634, ISSN: 1991-8763.

NACS (2009). "Client/Server Security Assessment and Awareness" Accessed: April 2009.

Prasithsangaree P, Krishnamurthy K (2003). "Analysis of Energy Consumption of RC4 and AES Algorithms in Wireless LANs", GLOBECOM 2003. pp. 1445-1449, 0-7803-7974-8.

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

Robles RJ, Choi M, Balitanas M, Sattarova F, Alisherov F, Kim N, Kim T (2009). "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), p.89, ISSN 2005-7334.

Robles RJ, Seo K, Kim T (2010). "Communication Security solution for internet SCADA", Korean Institute of Information Technology 2010 IT Convergence Technology - Summer workshops and Conference Proceedings 5:461-463.

Robles RJ, Kim T (2011). “Scheme to Secure Communication of SCADA Master Station and Remote HMI’s through Smart Phones”. J Sec. Eng. 8(3): 349-358.

RSA LAboratories "What is RC4?" http://www.rsa.com/rsalabs/node.asp?id=2250 Accessed: June 2009.
Stoica A, Robles RJ (2010). “Encryption Scheme for Control Systems through Web”. J. Sec. Eng. 7(5): 511-520.
Wallace D (2003). "Control Engineering. How to put SCADA on the Internet", http://www.controleng.com/article/CA321065.html Accessed: January 2010.
Yardley T (2008). "SCADA: issues, vulnerabilities, and future directions", Systems and Internet Infrastructure Security Laboratory, http://www.usenix.org/publications/login/2008-12/pdfs/yardley.pdf. Accessed: March 2011.
Zhu B, Joseph A, Sastry S (2011). “A Taxonomy of Cyber Attacks on SCADA Systems”, Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing. DOI: 10.1109/iThings/CPSCom.2011.34: 380-388.