Application of Asymmetric-key Encryption Method for Internet-based SCADA Security

Hoon Ko[1]

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, comes the security issues regarding web SCADA. 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, Security Issues, Asymmetric Encryption

1. Introduction

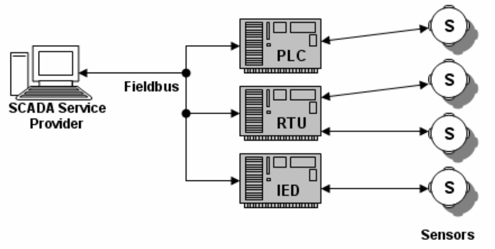
SCADA refers to a system that performs the same basic functions, but operates in a number of different environments as well as a multiplicity of scales. It is so important since it control most of our commodities. SCADA communications has been Point-to-Multipoint serial communications over lease line 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. SCADA System

Received(July 31, 2008), Review request(August 01, 2008), Review Result(1st:August 21, 2008, 2nd:September 10, 2008)
Accepted(December 31, 2008)

[1] Doctor Researcher GECAD ,ISEP, IPP, Rua Dr. Antonio Bernardino de Almeida, 431,4200-072, Porto, Portugal
email: hko@isep.ipp.pt

Supervisory Control And Data Acquisition is a large scale control system for automated industrial processes. SCADA also has applications in large scale experimental facilities like those used in nuclear fusion. 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[1]. Typically SCADA systems includes the SCADA master station, fieldbus, and remote assets like RTUs, PLCs or IEDs[2].



[Fig. 1] Common SCADA Installation

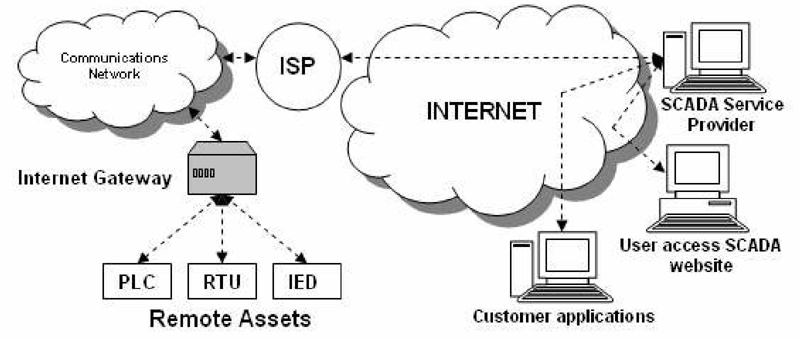
2.1 SCADA Hardware, Software and Human Machine Interface

A full fledged SCADA system is made up of signal hardware for input/ output, networks, control equipment, user interface (sometimes called the Human-Machine Interface or HMI), communication equipment and the software to go with it all. And here we are talking about the central command system of SCADA. The central system is often miles away from where the operations take place. Thus the system also needs on-site sensors to collect and monitor data.

SCADA 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[1]. 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. 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[3].

3. Internet SCADA Architecture

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 figure 2, you can see the architecture of SCADA which is connected through the internet. Like a normal SCADA, it has RTUs/PLCs/IEDs.Along with the fieldbus, the internet is an extension.



[Fig. 2] Architecture of Internet SCADA[4]

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.

3.1 Benefits of Internet SCADA

One may ask why we need to connect SCADA on the Internet even though there are a lot of issues surrounding it. The answer is because of many advantages it presents[4-5].

- Wide area connectivity and pervasive
- Routable
- Parallel Polling
- Redundancy and Hot Standby
- Large addressing range
- Integration of IT to Automation and Monitoring Networks
- Standardization

4. Security Issues in Internet SCADA

Internet has made them more vulnerable to attacks. Consequently, the security of SCADA-based systems has come into question as they are increasingly seen as extremely vulnerable to cyberwarfare/cyberterrorism attacks[6-7]. Here are the common security issues in SCADA:

- The lack of concern about security and authentication in the design, deployment and operation of existing SCADA networks.
- The belief that SCADA systems have the benefit of security through obscurity through the use of specialized protocols and proprietary interfaces.
- The belief that SCADA networks are secure because they are purportedly physically secured.
- The belief that SCADA networks are secure because they are supposedly disconnected from the Internet.
- IP Performance Overhead of SCADA connected to the Internet.

4.1 Many to many SCADA issues

Over the past year a SCADA solotion company[6] canvassed our customers and have technical feasibility of an Many to Many SCADA solution and they came to the following list of issues involving Many to many SCADA.

Not Setting Appropriate Expectations. A common cause of many to many SCADA project failure is promising a system based on traditional SCADA technical parameters, that may be more than you can deliver or more than the end-user needs. It is important to understand how the timing and availability characteristics of the Internet differ from traditional SCADA systems, and to communicate those differences and their ramifications to all project stakeholders.

Building the many to many SCADA System Around Polling. Traditionally, SCADA systems have operated within a “master/slave” architecture, the “master” being a central computer programmed to gather data and transmit instructions to “slaves”. These “slaves” are remote terminal units (RTUs) programmed to provide local data gathering and control under the supervision of the “master”. This approach minimized bandwidth usage and ensured predictable operation over a shared communication medium such as leased telephone lines.

However, Internet protocols, services and techniques make this architecture ineffective and obsolete. Because Web servers are designed to accept and process requests from many Web clients simultaneously, many to many SCADA is best built on a "push" architecture where each remote field device is programmed to intelligently transmit its data to the master system. The transmission can take place at set intervals (such as every five seconds) or when certain conditions occur, such as a device reaching a certain temperature or the voltage in an electric line reaching a critical point.

Rolling Over the End Users. The move to many to many SCADA is a big change, especially for field managers who may have done their jobs in the same way for decades. Those who are used to hands-on troubleshooting at a remote site might feel less valuable when a dispatcher can give them detailed repair information before they even get into their truck. They may remember earlier, failed attempts at many to many SCADA and not realize that new software, hardware and methodologies make many to many SCADA much more feasible than before.

At one oil and gas company, the automation manager championed an many to many SCADA project from headquarters and began with a pilot project to prove the ROI of the system and attract the necessary support for a full deployment. The project died, however, when users who hadn't been consulted or educated about the new system refused to use it, while managers of existing SCADA implementations battled the new system fearing it might cost them their jobs.

SCADA "surety" means the combination of security and continuity, both of which are major issues for a company monitoring a critical asset such as a transmission line over the Web. The public Internet exposes SCADA systems to a host of security and reliability threats that can be expensive to deal with, if not handled correctly.

Internet-based applications are prime targets for viruses, worms and denial of service attacks. Furthermore, hackers can exploit any vulnerable data streams they can "sniff" online, and SCADA systems are particularly attractive prey. If a determined attacker manages to break into a SCADA data stream, they could change the data, trigger false alarms, suppress actual alarms or send false controls to the remote devices. Each of these security breaches can be potentially devastating to your SCADA system and the operations it serves.

Your many to many SCADA effort could backfire if you don't have the infrastructure to continuously monitor the system, lock down every node, encrypt the information, and back-up the data that has been gathered. If you have any doubts that your own data center can provide these capabilities, consider a reliable, proven outsourcer with experience hosting many to many SCADA systems.

The many to many SCADA-wares of many vendors are simply tools that provide a limited Web interface into existing proprietary applications. For example, one major utility decided on an many to many SCADA system to monitor aging transformers to maximize their throughput and reliability. Rather than utilize an open, extensible framework for many to many SCADA, they used Web "snap-ons" to legacy SCADA applications and remote monitoring units. As a result, they were unable to later extend or integrate what were, in effect, standalone Web applications.

You're better off choosing a vendor who treats many to many SCADA as a central, open, accessible monitoring framework for the enterprise. Products and services built on such a philosophy give you full access to the real benefit of open interoperability across IP-based networks, so you can change your monitoring, alarming, analysis and control functions as your business changes.

5. 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 kei 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.

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. 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.

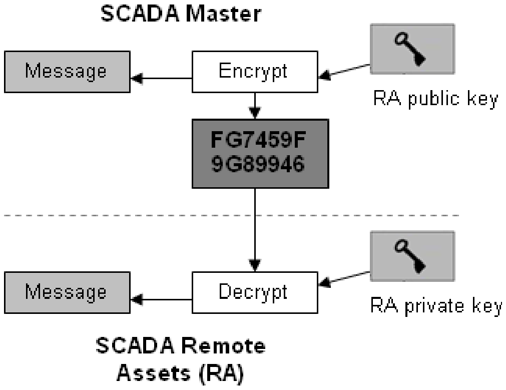
One of the most common digital signature mechanisms, the Digital Signature Algorithm (DSA) is the basis of the Digital Signature Standard (DSS), a U.S. Government document. As with other digital signature algorithms, DSA lets one person with a secret key "sign" a document, so that others with a matching 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. 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.

6. Integration of Asymmetric-key Encryption to Internet 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[7-9]. SCADA web server must always be secure since the data in it are very critical. Web server security software can also be added.



[Fig. 3] 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.

7. 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] D. Bailey and E. Wright, Practical SCADA for Industry, 2003.

[2] Andrew Hildick-Smith, Security for Critical Infrastructure SCADA Systems, 2005.

[3] Wikipedia-SCADA, http://en.wikipedia.org/wiki/SCADA, Accessed: January 2009

[4] D. Wallace, Control Engineering. How to put SCADA on the Internet,

http://www.controleng.com/article/CA321065.html Accessed: January 2009

[5] Internet and Web-based SCADA, http://www.scadalink.com/technotesIP.htm, Accessed: January 2009

[6] Top Ten M2M SCADA Mistakes, http://www.extraordinaryplaces.net/images/topten.htm, Accessed: April 2009

[7] D. Maynor and R. Graham, SCADA Security and Terrorism: We're Not Crying Wolf, http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf, Accessed: January 2009

[8] Robert Lemos, SCADA system makers pushed toward security, http://www.securityfocus.com/news/11402, Accessed: January 2009

[9] I. Curry, An Introduction to Cryptography and Digital Signatures, http://www.entrust.com/resources/pdf/cryptointro.pdf, Accessed: April 2009

Authors

Hoon Ko

Ph.D. School of Computing, Soongsil University, S Korea, August 2004.

MS. School of Computing, Soongsil University, S Korea, February 2000nBS. Department of Computer Science, Howon University, Gunsan, S Korea, February 1998.

Doctor Researcher GECAD , ISEP, IPP .

Rua Dr. Antonio Bernardino de Almeida, 431,4200-072, Porto, Portugal