African Journal of Business Management Vol.6 (44), pp. 10974-10982, 7 November 2012
Available online at http://www.academicjournals.org/AJBM
DOI: 10.5897/AJBM12.229
ISSN 1993-8233 ©2012 Academic Journals

Full Length Research Paper

Hiding solution for internet-based supervisory control and data acquisition (SCADA) system threats management

Tai-hoon Kim

GVSA and University of Tasmania, Australia. E-mail: taihoonn@paran.com.

Accepted 27 March, 2012

Supervisory control and data acquisition (SCADA) systems are real-time process control systems that monitor and control local or geographically remote devices. They are in wide use throughout a variety of critical infrastructure sectors, and are a critical component of operations. The SCADA system also provides a management way for important plant performance information to be obtained for use by managers and engineers at a corporate level. SCADA historically is responsible for monitoring and controlling critical infrastructures and manufacturing processes in an isolated environment. But with the requirement of a timely access of information for making decisions, large and modern companies being in a geographically diverse location take advantage of the internet as an important communication channel to allow the exchange of data. However, with SCADA being in the internet raise the issue of security. As more components of control systems become interconnected with the outside world using IP-based standards, the probability and impact of a cyber attack heighten. Since, the reliable function of SCADA systems in our modern infrastructure may be crucial to public health and safety management. Attacks on these systems may directly or indirectly threaten public health and safety since SCADA control the sources of our daily necessities such as oil and gas, air traffic and railways, power generation and transmission, water and manufacturing. With the posted threats and listed vulnerabilities in this study, a retrofit for these threats through the crossed cipher scheme is presented. To get the best of both types of cipher symmetric using advanced encryption standard (AES) and the asymmetric elliptic curve cryptography (ECC) to address the confidentiality, authentication, integrity and non-repudiation issues in SCADA system management.

Key words: Supervisory control and data acquisition (SCADA), security, threats, vulnerability, management.

INTRODUCTION

Supervisory control and data acquisition (SCADA) systems affects our daily lives, it operates in a large, geographically distribution. In a typical SCADA system, data acquisition and control are performed by remote terminal units (RTU) and field devices that include functions for communications and signaling. SCADA systems normally use a poll-response model for communications with clear text messages. Poll messages are typically small (less than 16 bytes) and responses might range from a short “I am here” to a dump of an entire day’s data. Some SCADA systems may also allow for unsolicited reporting from remote units.

Major concern about cyber attack initiated from the notion that the SCADA network is no longer an isolated network which prevents outsiders from entering the network, nor is the specialized network based on private platforms and protocols, allowing only technical staffs with special knowledge to access to the resources.

The reasons of claiming that the SCADA network is not a protected closed network it is twofold. First, the communication architecture is more relying on the open standard communication protocols. The use of the open communication protocols depicts the system more vulnerable to cyber attacks in many applications.

Second, the SCADA network is gearing toward being connected to corporate networks for convenience and other business reasons. Thus the SCADA network may open its doors to outsiders who can enter the corporate networks maliciously (Balitanas et al., 2009; Robles and Choi, 2009).

Historically, the industrial control and SCADA systems that are responsible for monitoring and controlling our critical infrastructures and manufacturing processes have operated in isolated environments. These control systems and devices communicated with each other almost exclusively, and rarely shared information with systems outside their environment. As more components of control systems become interconnected with the outside world using IP-based standards, the probability and impact of a cyber attack will heighten. In fact, there is increasing concern among both government officials and control systems experts about potential cyber threats to the control systems that govern critical infrastructures. Even the flaws in SCADA specific technologies have become general knowledge

For the past several years, few researches have been done on the SCADA security issues. Along with the works in the research community, the international standard bodies also have worked to derive the standard documents for the SCADA security. The purpose of this study is not only to define the challenges for a known isolated SCADA system, but also to organize the results that these isolated case is no longer isolated but is now vulnerable to cyber attack threats. The current results on these challenges will be summarized from the efforts of the international organization as well as research communities. And as a contribution this study presents a crossed cipher for an internet-based SCADA System.

RELATED STUDIES

Encryption fundamentally consists of scrambling a message so that its contents are not readily accessible while decryption is the reversing of that process (Galbraith 2005). These processes depend on particular algorithms, known as ciphers. Suitably scrambled text is known as cipher text while the original is, not surprisingly, plain text.

Readability is neither a necessary nor sufficient condition for something to be plain text. The original might well not make any obvious sense when read, as would be the case, for example, if something already encrypted were being further encrypted.

It is also quite possible to construct a mechanism whose output is readable text but which actually bears no relationship to the unencrypted original. A key is used in conjunction with a cipher to encrypt or decrypt text. The key might appear meaningful, as would be the case with a character string used as a password, but this transformation is irrelevant, the functionality of a key lies in its being a string of bits determining the mapping of the plain text to the cipher text.

It is desired to communicate data with high security. At present, various types of cryptographic algorithms provide high security to information on controlled networks. These algorithms are required to provide data security and users authenticity. This security protocol has been designed for security using a combination of both symmetric and asymmetric cryptographic techniques (Robles and Kim, 2011; Abawajy and Robles, 2010; Stoica and Robles, 2010).

In Figure 1, the symmetric key cryptographic techniques such as elliptic curve cryptography and message digest 5 (MD5) are used to achieve both the confidentiality and integrity. The asymmetric key cryptography technique, dual RSA used for authentication.

PROBLEM

In the past, the SCADA, and industrial control systems in general, that have been responsible for monitoring and controlling critical infrastructures and manufacturing processes operated in isolated environments. These control systems and devices communicated with each other within an isolated network, and rarely shared information with systems outside their environment. However, over time as more components of control systems have become interconnected with the outside world using Internet-based standards, and as control networks have become integrated into larger corporate networks in order to share valuable data, the probability and impact of a cyber attack has increased (Drahansky and Balitanas, 2010). This report examines the possibility and implications of a cyber attack on a SCADA system.

A cyber attack (Owens et al., 2009) is defined as the deliberate actions (perhaps over an extended period of time) to alter, disrupt, deceive, degrade and destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks. A cyber attack consists of vulnerability, an access path to the vulnerability and a payload to be executed. A vulnerability is an aspect (or defect) of a system that can be used by an adversary to compromise one or more of its attributes. An access path is the means by which a target can be reached. An access path to a target may be remote or close (Zhu et al., 2011).

A remote-access cyber attack is launched at some geographical distance from the adversary computer or network. A close-access cyber attack occurs in close proximity to the computer or network; in this type of attack the adversary has physical control over the device or network, just as an insider would. Close access is a possibility anywhere in the supply chain of a system that will be deployed. Payload is a term used to describe the action that will be performed once the vulnerability has been exploited. For example, a payload which functions as a virus will have a function of reproducing and retransmitting itself.

Documented Attacks

There are three broad categories of documented attacks on SCADA

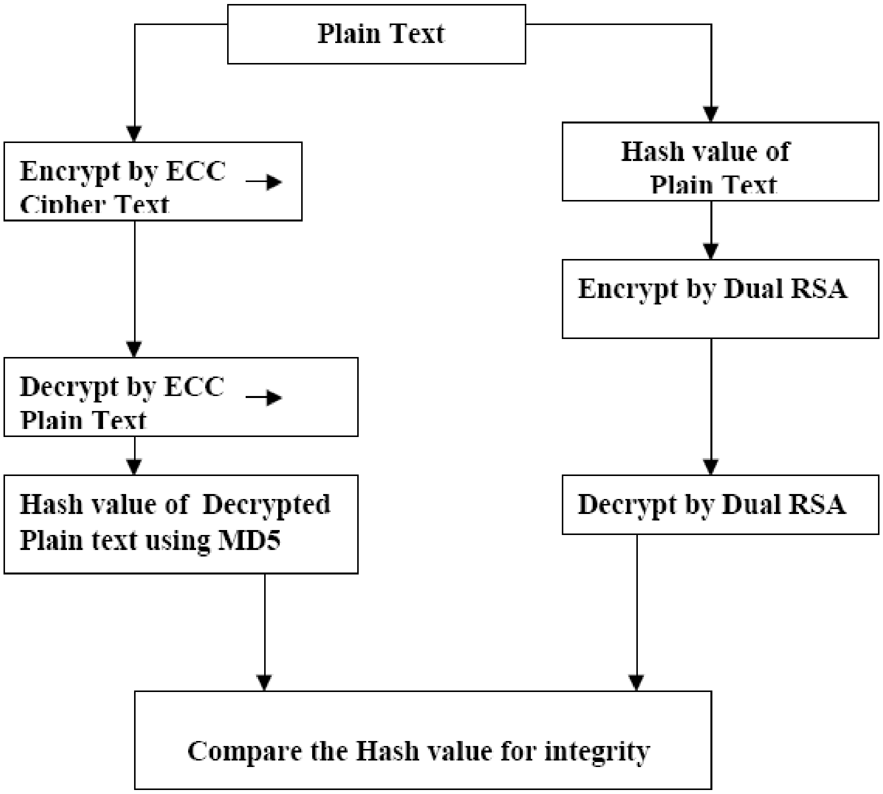

Plain Text
Encrypt by ECC → Cipher Text
Hash value of Plain Text
Encrypt by Dual RSA
Decrypt by ECC → Plain Text
Hash value of Decrypted Plain text using MD5
Decrypt by Dual RSA
Compare the Hash value for integrity

Figure 1. Hybrid protocol architecture (Subasree and Sakthivel, 2010).

systems, other industrial control systems or critical infrastructures.

1. Intentional targeted attacks such as gaining un-authorized access to computers within the network infrastructure, performing a denial of service (DoS) attack, or spoofing.
2. Unintentional consequences or collateral damage from worms, viruses or control system failures.
3. Unintentional consequences caused by internal personnel or mechanisms. This may include the testing of inappropriate software on operational systems or unauthorized system configuration changes.

The first category of attacks, the intentional targeted attacks, have the most potential for damage, however are the least frequently occurring. An intentional targeted attack requires detailed knowledge of the system and supporting infrastructure and is almost always caused by an insider with personal grievances.

Supervisory control and data acquisition (SCADA) cyber Attacks

The complexity of modern SCADA systems leaves many vulnerabilities as well as vectors for attack. Attacks can come from many places, including indirectly through the corporate network, virtual private networks (VPN), wireless networks, and dial-up modems. Possible attack vectors on an SCADA system include:

1. Backdoors and holes in network perimeter.
2. Vulnerabilities in common protocols.
3. Database attacks.
4. Communications hijacking and 'man-in-the-middle' attacks (Kim et al., 2010).

All but the most naive adversary would seek to conceal their identity (that is, the machine which would launch the attack), before initiating any steps to an attack or even a preliminary set-up or probe for an attack. The method for concealing the identity of the adversary's machine is to set up an intermediary machine(s) which would directly probe or attack the target network. This would entail doing one of the following:

1. Set up an anonymous proxy, which is a tool that makes any activity performed difficult to trace,
2. Set up a "botnet" of intermediary machines, or
3. Enlist the services of a bot-network operator from the underground market that is, "rent" a bot-net. Two major deterrents to adversaries include system hardening and intrusion detection systems.

However, it is important to note that consistent system hardening is dependent upon a disciplined security staff who will monitor the uses of every computer/device and disable all components which are not necessary for its correct execution. Intrusion detection systems also require dedicated administration and correct configuration from the security staff.

Intentional attacks

So far there has been remarkably few documented intentional cyber attack on critical infrastructure networks. This section describes those few known cases.

January 2000, Maroochy Shire sewage spill [5]: The most well-known attack upon a SCADA system was the attack on the Maroochy Shire Council's sewage control system in Queensland, Australia. On January 2000, almost immediately after the control system for the sewage plant was installed by a contractor company, the plant experienced a series of problems. Pumps failed to start or stop when specified. Alarms failed to be reported. There were intermittent loss of communications between the control center and the pumping stations.

At the beginning, the sewage system operators thought there was a leak in the pipes. Then they observed that valves were opening without being months of logging that they discovered that spoofed controllers were activating the valves. It took several more months to find the culprit: a disgruntled ex-employee of the contractor company that had installed the control system originally. The ex-employee was trying to convince the water treatment company to hire him to solve the problems he was creating.

The effect of the attacks was the flooding of the grounds of a nearby hotel, park, and river with appro-ximately 264,000 gallons of raw sewage. In analyzing this attack, one of the insights was that cyber attacks may be unusually hard to detect (compared to physical attacks). The response to this attack was very slow; the attacker managed to launch 46 documented attacks before he was caught.

March 1997, Worcester Air Traffic Communications Attack (CNN Interactive 1988): In March 1997, a teenager in Worcester, Massachusetts broke into the Bell Atlantic computer system and disabled part of the public switched telephone network using a dial-up modem connected to the system. This attack disabled phone service at the control tower, airport security, the airport fire department, the weather service, and carriers that use the airport. The tower's main radio transmitter and another transmitter that activates runway lights were shut down, as well as a printer that controllers use to monitor flight progress. The attack also knocked out phone service to 600 homes and businesses in the nearby town of Rutland.

2000 and 1982, Gas Pipelines in Russia (and the former Soviet Union): In 2000, the Interior Ministry of Russia reported that hackers seized temporary control of the system regulating gas flows in natural gas pipelines, although it is not publicly known if there was physical damage (Quinn-Judge, 2002). The former Soviet Union was victim of an attack to their gas pipeline infrastructure in 1982 when a logic bomb caused an explosion in Siberia (Reed, 2004).

June 2010, security author and analyst Brian Krebs broke a story about a new flaw in windows that is being used to spread Malware. Since then, the Malware itself has sparked concern in certain SCADA circles and Microsoft has confirmed the Zero-Day attack. Microsoft has confirmed the existence of a new vulnerability that is targeting Windows Shell, due to the fact that the Windows operating system incorrectly parses shortcuts. The Malware itself, dubbed Stuxnet, has been flagged by several security vendors including Symantec, Sophos, ESET, Panda, Kaspersky, F-Secure, and Microsoft. It is concluded to target SCADA systems (Ragan, 2010).

PROPOSED RETROFIT

Cryptography is the science of writing in secret code and is an ancient art; the first documented use of crypto-graphy in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet.

Purpose of cryptography

A cryptosystem consists of three algorithms: one for key generation, one for encryption, and one for decryption. Their application to industrial control systems may present design and operational challenges. This primer provides assistance to control systems security pro-fessionals to identify appropriate encryption techniques and determine whether to deploy a cryptosystem solution as a security feature in their specific control systems environment. This primer also presents examples of cryptosystem deployment solutions to assist users in identifying appropriate application for their specific system.

Cryptosystems have four intended goals:

1. Confidentiality
2. Authentication
3. Integrity
4. Non-repudiation

Integration of symmetric and asymmetric

Symmetric and asymmetric ciphers each have their own advantages and disadvantages. Symmetric ciphers are significantly faster than asymmetric ciphers, but require all parties to somehow share a secret (the key). The asymmetric algorithms allow public key infrastructures and key exchange systems, but at the cost of speed. So, in this study a combination of the best features of both symmetric and asymmetric encryption techniques is presented in the form of a crossed-cipher for SCADA system as shown in Figure 2.

This crossed-cipher is capable of providing implicit authentication for the sender's identity. From the two major types of encryptions, asymmetric encryption provides more functionality than symmetric encryption, at the expense of speed and hardware cost. On the other hand, symmetric encryption provides cost-effective and efficient methods of securing data without compromising security and should be considered as the correct and most appropriate security solution for many applications.

In some instances, the best possible solution may be the complementary use of both symmetric and asymmetric encryption. The algorithm presented here combines the best features of both the symmetric and asymmetric encryption techniques. The plain text data is to be transmitted in encrypted using the AES algorithm. Where in it will generate a random secret key for a symmetric cipher (AES), and then encrypt this key via an asymmetric cipher (ECC) using the recipient's public key. The message itself is then encrypted using the symmetric cipher and the secret key. Both the encrypted secret key and the encrypted message are then sent to the recipient.

Symmetric

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key (Diffie and Hellman, 1976). With secret key cryptography, a single key is used for both encryption and decryption. As shown in Figure 3, the sender uses the key (or some set of rules) to encrypt the plaintext and sends the ciphertext to the receiver. The receiver applies the same key (or ruleset) to decrypt the message and retrieve the plaintext because a single key is used for both functions (Bauer, 2002; Spillman, 2005).

With this form of cryptography, it is obvious that the key must be

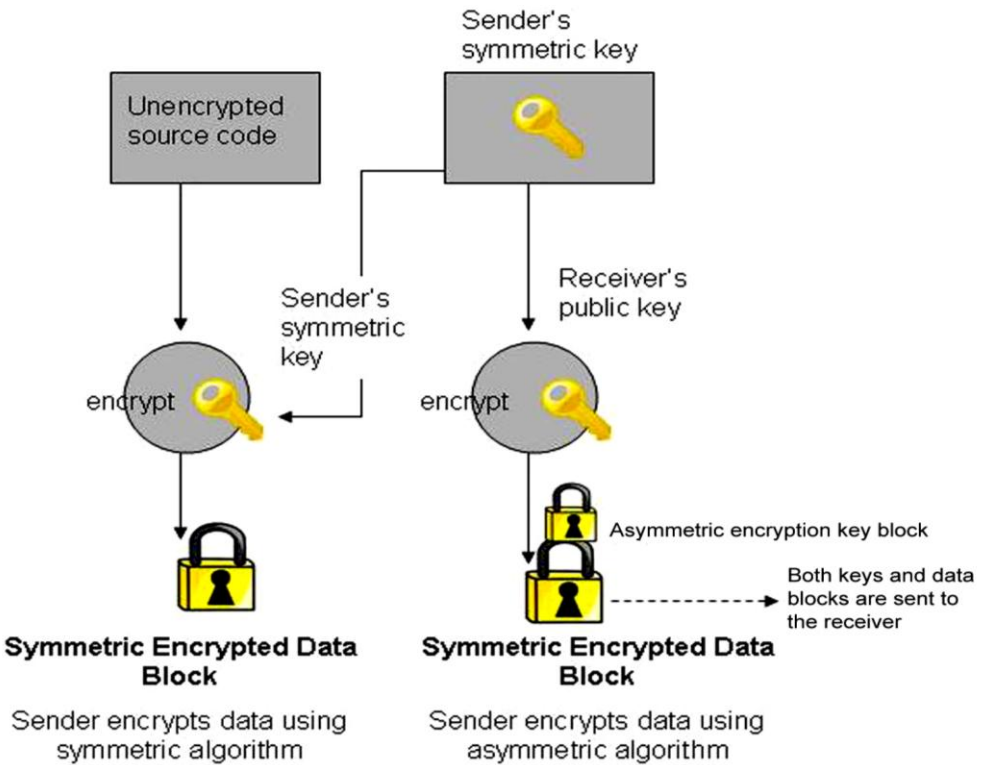

Sender's symmetric key
Unencrypted source code
Sender's symmetric key
Receiver's public key
encrypt
encrypt
Asymmetric encryption key block
Both keys and data blocks are sent to the receiver
Symmetric Encrypted Data Block
Sender encrypts data using symmetric algorithm
Symmetric Encrypted Data Block
Sender encrypts data using asymmetric algorithm

Figure 2. The scheme.

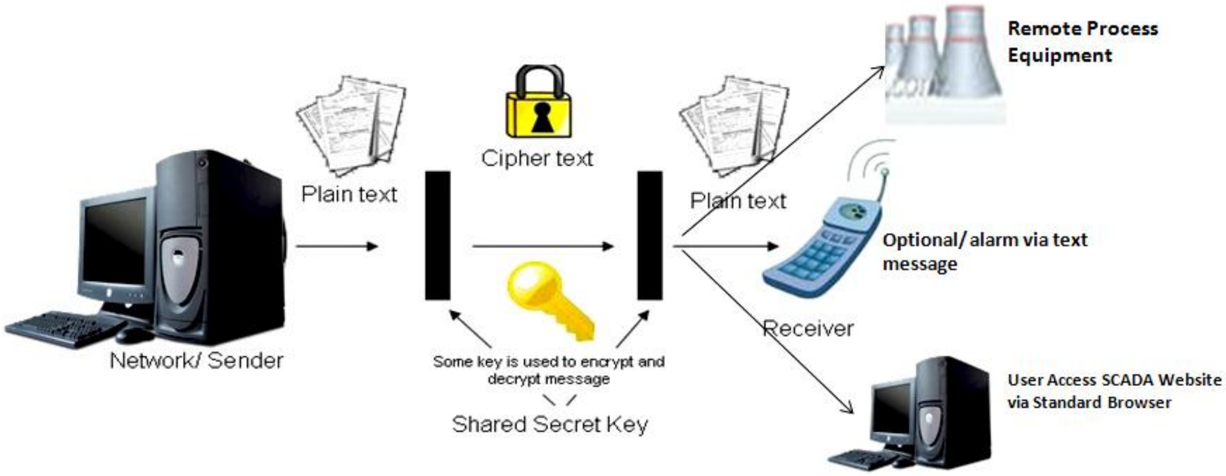

Remote Process Equipment
Plain text
Cipher text
Plain text
Optional/ alarm via text message
Receiver
Network/ Sender
Some key is used to encrypt and decrypt message
Shared Secret Key
User Access SCADA Website via Standard Browser

Figure 3. Symmetric encryption.

known to both the sender and the receiver; that, in fact, is the secret. The biggest drawback with this approach is the distribution of the key.

Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism so that the key is constantly changing. A block cipher is so-called because the scheme encrypts one block of data at a time using the same key on each block.

In general, the same plaintext block will always encrypt to the same ciphertext when using the same key in a block cipher whereas the same plaintext will encrypt to different ciphertext in a stream cipher.

Asymmetric

Asymmetric cryptography is also known public-key cryptography (PKC) which have been said to be the most significant new

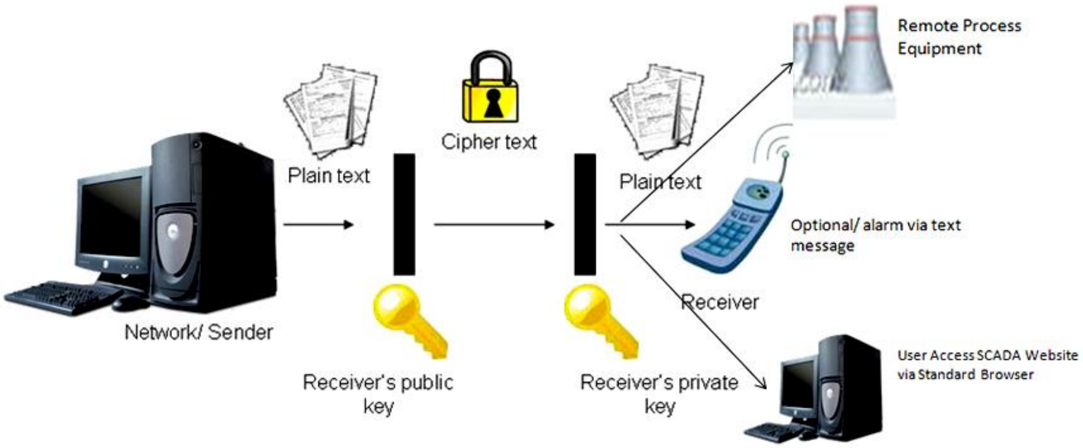


Figure 4. Asymmetric encryption.

development in cryptography in the last 300 to 400 years. Modern PKC was first described publicly by Stanford University professor Martin Hellman and graduate student Whitfield Diffie in 1976. Their paper described a two-key crypto system in which two parties could engage in a secure communication over a non-secure communications channel without having to share a secret key.

In asymmetric cryptography, one of the keys is designated the public key and may be advertised as widely as the owner wants as shown in Figure 4. The other key designated the private key and is never revealed to another party. This method could be also used to prove who sent a message and can address the Non-repudiation vulnerability of a system (Diffie and Hellman, 1976).

IMPLEMENTATION

The implementation was done using out in Java 2, Standard Edition (J2SE) v 1.4.0. J2SE has the built-in classes for AES, and MD5 hashing. The code uses these packages and the header files have the following header.

Using Java, a method has been developed for elliptic curve generation, base point generation, keys (both public and private) generation and encryption and decryption. The class of BigInteger in Java has been used to handle large integers and the method of Is ProbablePrime to determine whether the large integer is prime or not.

Figure 5 depicts the chain of operation in the proposed cipher scheme. The AES key which is used to encrypt the data is encrypted using ECC. The cipher text of the message and the cipher text of the key are then sent to the receiver.

To ensure integrity of the data that is transmitted, the data is subjected to MD5 hash algorithm. The message digest obtained by this process is also encrypted using ECC technique. Thus the sender sends (1) Cipher text of the message, (2) Ciphertext of the AES key, and (3) Ciphertext of the message digest. The receiver upon receiving the Cipher text of the message, Ciphertext of the AES key, and Ciphertext of the message digest, first decrypts the Ciphertext of the AES key to yield the AES key. This is then used to decrypt the cipher text of the message to yield the plain text. The plaintext is again subjected to MD5 hash algorithm. This process yields a message digest.

The ciphertext of the message digest is decrypted using ECC technique to obtain the message digest sent by the sender. This value is compared with the computed message digest. If both of them are equal, the message is accepted else rejected. Figure 6 shows the simple application developed based on the chain of operation.

RESULTS

Communication over the internet has impact the field of SCADA systems. It is desired to communicate data with high security. Security attacks compromises the security and hence various symmetric and asymmetric cryptographic algorithms have been proposed to achieve the security services such as authentication, confidentiality, integrity and non-repudiation.

At present, various types of cryptographic algorithms provide high security to information on controlled networks. These algorithms are required to provide data security and users authenticity. To improve the strength of these security algorithms, a new security protocol for on line transaction was designed using combination of both symmetric and asymmetric cryptographic techniques in the study, design of a new security protocol using hybrid cryptography algorithms (Subasree and Sakthivel, 2010). This protocol provides three cryptographic primitives such as integrity, confidentiality and authentication. It uses elliptic curve cryptography for encryption, Dual-RSA algorithm for authentication and MD-5 for integrity. This hybrid cryptography has been compared with the crossed cipher in this study

The expected technological advances indicate the tremendous potential of auto planner technology. Several emerging technologies, promise further performance improvements. However, a number of challenging tasks which the authors will consider in future studies should be further addressed in an effort to make this technology affordable, robust, secure, and easy to use.

Table 1 shows the comparison of the Crossed-Cipher as the proposed retrofit for SCADA systems CAIN threats

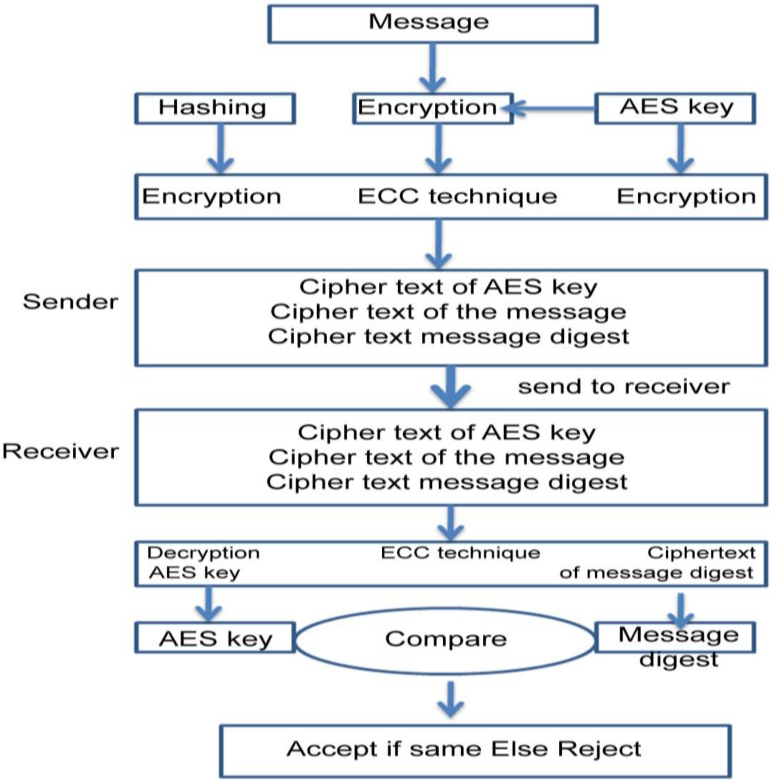
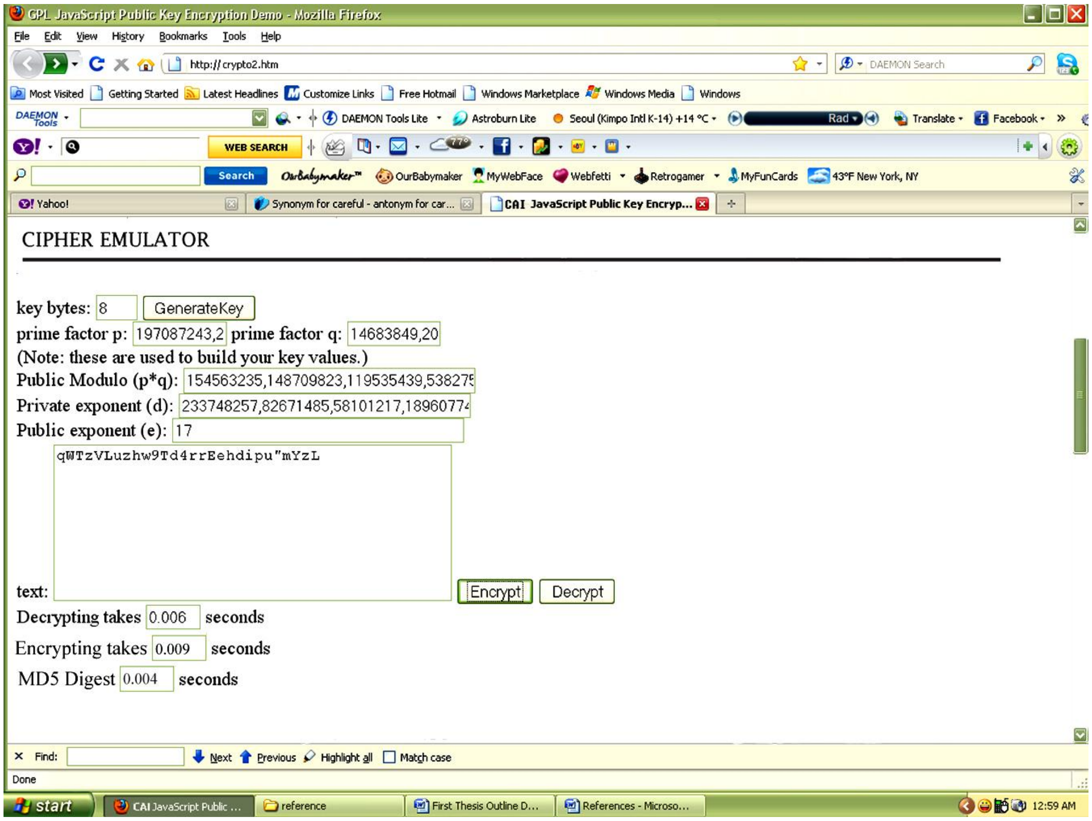


Figure 5. Crossed cipher chain of operation.


GPL JavaScript Public Key Encryption Demo - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://crypto2.htm
Yahoo!
Synonym for careful - antonym for car...
CAI JavaScript Public Key Encryp...

CIPHER EMULATOR

key bytes: 8 GenerateKey

prime factor p: 197087243,2 prime factor q: 14683849,20

(Note: these are used to build your key values.)

Public Modulo (p*q): 154563235,148709823,119535439,538275

Private exponent (d): 233748257,82671485,58101217,18960774

Public exponent (e): 17

text: qWTzVLuzhw9Td4rrEehdipu"mYzL

Decrypting takes 0.006 seconds

Encrypting takes 0.009 seconds

MD5 Digest 0.004 seconds

Figure 6. Cipher emulator.

Table 1. Comparison of crossed-cipher and hybrid cryptography algorithm (Subasree and Sakthivel, 2010).

Block size	Crossed-cipher		Hybrid-Crypto algorithm (Subasree and Sakthivel, 2010)	
	Encryption (s)	Decryption (s)	Encryption (s)	Decryption (s)
10	0.951	0.948	1.079	1.079
50	1.126	1.221	2.040	2.159
100	2.38	2.217	4.020	4.138

and the hybrid cryptography algorithm (Subasree and Sakthivel, 2010). In the hybrid cryptography algorithm, it was done with ECC and key is encrypted by using Dual RSA. In this case the intruder may derive different key for decryption, which is equivalent to the original key. Even though the intruder got the key, he will not be able to get the original message because of Dual RSA.

Dual RSA got two advantages one is the message cannot be decrypted and time required performing the encryption and decryption operation less compare to RSA because Dual RSA perform encryption and decryption by two block at a time.

However, comparing the two Cryptographies it is notable that in terms of computation costs and memory storage requirements the crossed-cipher has advantage over the hybrid cryptography algorithm (Subasree and Sakthivel, 2010).

The significant smaller parameter used in ECC in crossed-cipher is an advantage that can be gained from smaller parameters included in speed and smaller keys or certificates. Thus, ECC is especially well suited for constrained environments over Dual-RSA.

CONCLUSION

The move of SCADA system from proprietary technologies to more standardized and open solutions together with the increased number of connections between systems and office networks and the Internet has made system more vulnerable to attacks.

The reliable function of SCADA systems in our modern infrastructure may be crucial to people. Attacks on these systems may directly or indirectly threaten public health and safety since SCADA control the sources of our daily necessities such as oil and gas, air traffic and railways, power generation and transmission, water and manufacturing.

Devising a crossed-cipher scheme as presented in this study is one way to retrofit on to the system and be able to address the confidentiality, authentication, integrity and non-repudiation issues in SCADA.

The design and implementation of the crossed-cipher scheme was done in Java combining the best of both symmetric (AES) and asymmetric (ECC) cryptography and to ensure integrity of the data, the MD5 hash algorithm was adopted. A test for the scheme for various sizes of files was done.

By combining AES, the algorithm which can use a variable block length and allowed any combination of keys lengths of 128, 192, or 256 bits and blocks of length 128, 192, or 256 bits proven to be effected against known attacks. The design and strength of all key lengths of the AES algorithm (that is, 128, 192 and 256) are sufficient to protect classified information up to the Secret level. Top secret information will require use of either the 192 or 256 key lengths.

This symmetric cryptography AES was used along with ECC asymmetric cryptography. ECC are mathematical objects that have been subject to much scrutiny by top mathematicians over the past 150 years. They have many important, elegant, and delightful properties and many research papers have been written solely exploring the various characteristics of these objects. An important feature of these curves is that their points can be interpreted as part of a mathematical group and the challenging and somewhat complicated nature of elliptic curve groups makes it harder to crack the ECC discrete logarithm problem. With less bits required by ECC to give the same security compared to other existing asymmetric cryptography, ECC is indeed a reliable cryptographic scheme that will be important in the near future.

ACKNOWLEDGEMENTS

Author wishes to express special thanks to Drs. Rosslin John Robles and 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. Security Eng. 7(6):575-584.

Balitanas M, Robles RJ, Kim Nayoun, Kim T (2009). Crossed Crypto-scheme in WPA PSK Mode, BLISS 2009, Edinburgh, GB, IEEE CS, ISBN 978-0-7695-3754-5.

Bauer FL (2002). Decrypted Secrets: Methods and Maxims of Cryptology. 2nd ed. New York: Springer Verlag.

CNN Interactive (1988). Teen Hacker Faces Federal Charges, March 18, 1988, http://www.cnn.com/ TECH/computing/9803/18/ juvenile.hacker/index.html.

Diffie W, Hellman M (1976). New Directions in Cryptography. IEEE Transac. Inform. Theor. IT-22:644-654.

Drahansky M, Balitanas M (2010). Incentive Approach to the Active Network Privacy Threats and Vulnerabilities. J. Security Eng. 7(6):585-598.

Galbraith SD, Heneghan C, McKee JF (2005). Tunable balancing of RSA, Updated version of ACISP 2005.

Kim UH, Kim KS, Lim KH, Im EG (2010). Study on Possibility of Man-in-the-Middle Attacks in RS-232C Serial Communication of the SCADA Systems for Power Systems. J. Security Eng. 7(4):295-310.

Owens WA, Dam KW, Lin HS (2009). “Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyber attack Capabilities. National Research Council of the National Academies. 2009. 978-0-309-13850-5.

Quinn-Judge P (2002), Cracks in the system. Time Magazine (9th Jan 2002).

Ragan S (2010). Windows Shell vulnerability confirmed as concern grows”, Jul 19 2010, 12:20 http://www.thetechherald.com/articles/Windows-Shell-vulnerability-confirmed-as-concern-grows/10786/.

Reed T (2004). At the Abyss: An Insider’s History of the Cold War. Presidio Press, ISBN-13: 978-0891418214.

Robles RJ, Choi M (2009). Assessment of the Vulnerabilities of SCADA, Control Systems and Critical Infrastructure Systems. Int. J. Grid Distrib. Comput. 2(2):27-34.

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

Spillman RJ (2005). Classical and Contemporary Cryptology. Upper Saddle River, NJ: Pearson Prentice-Hall.

Stoica A, Robles RJ (2010). Encryption Scheme for Control Systems through Web. J. Security Eng. 7(5):511-520.

Subasree S, Sakthivel NK (2010). Design of a new Security Protocol using Hybrid Cryptography Algorithms. IJRRAS 2(2):95-103.

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.