VOL. 11, NO. 5, MARCH 2016 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

IMPLEMENTATION OF CRYPTOGRAPHY ALGORITHMS IN SCADAKRATOS APPLICATION

N. Salleh[1], S. M. Daud[2], S. F. Sabri[1], S. M. Sam[2] and M. Z. Adam[2]
[1]Space System Operational and Development Division, National Space Agency of Malaysia, Selangor, Malaysia
[2]Advanced Informatics School, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia
E-Mail: asni_salleh@yahoo.com

ABSTRACT

This paper studies cryptography algorithms to be implemented into the SCADAKratos application of thermal vacuum chamber (TVC) system. SCADAKratos application is used to control and monitor the operations of the TVC which is a satellite test equipment that is located at the Malaysia Space Centre, Banting, Malaysia. The security features had been put aside during the development as it was claimed that there is no threat to the system since the system is operated internally. However, during service and troubleshooting by the manufacturer, the system will be accessed through public network. Besides that, the system also can be accessed remotely during operation for control and monitoring purpose. In addition, the testing data results also need to be transferred to the customer through the internet as it is easier and faster. The remote access through public network will cause the TVC system to face a risk to any threat and attack. Therefore, the implementation of cryptography algorithm into TVC system is needed in order to secure and protect the system from unauthorized access. This paper explains the architecture of SCADAKratos application of TVC system and how the cryptography algorithms could be implemented through this application. Secure Hash Algorithm (SHA-1) and AES algorithm (AES) are chosen as the encryption technique which will be applied in the TVC system. Simulation result shows that this technique is feasible for the mentioned implementation.

Keywords: cryptography algorithm, thermal vacuum chamber, SHA-1, AES.

INTRODUCTION

The thermal vacuum chamber (TVC) system is a satellite test equipment used to simulate the space environment that will be experienced by the satellite in the orbit. It is used to simulate the harsh cycle of extreme temperature (hot and cold) in vacuum condition as experienced by the satellite in space [1]. The TVC system is an embedded system developed to be operated internally without involving public network communication. Therefore, it is designed without any security features added into the system. The security features had been put aside as the manufacturer claimed there is no threat to the system as the system will be operating using Ethernet line.

However, the remote access is still available in the TVC system in order to allow the manufacturer to service or troubleshoot the system. Besides that, the TVC system can also be accessed remotely during operation for control and monitoring. This is due to the shortage of staffing and the system is operated non-stop for at least 2 weeks. In addition, the testing data results also need to be transferred to the customer through the internet as it is easier and faster. Due to that, the TVC system will still operate remotely not as been claimed by the manufacturer. This operation through public network will put the TVC system at risk of any threat and attack. Therefore, security features need to be implemented in the TVC system in order to protect the system from unauthorized access. Moreover, with the attack from the stuxnet worm, that infected Siemens industrial equipment and software that was running on a Windows system reinforces why the security must be implemented [2]. This is because the TVC system also uses Siemens controller and it is implemented in Windows platform. In this study, Secure Hash Algorithm (SHA-1) and AES algorithm (AES) are chosen as the encryption technique which will be applied in the TVC system through SCADAKratos application in order to improve the security of the system.

This paper is organized as follows. In section 2, the SCADAKratos architecture of TVC system is explained. The cryptography algorithms are elaborated in Section 3 whereas the testing and findings are explained in Section 4. Section 5 presents and discusses the results. Finally, section 6 will draw the conclusion of the proposed security in the SCADAKratos application of TVC system.

Architecture of SCADAKratos application

The SCADAKratos application is an application used to interface the control of TVC system. It communicates via the communications drivers with the Programmable Logic Controller (PLC) in charge of the operations through an Ethernet connection. The SCADAKratos application consists of five (5) main modules as shown in Figure-1.

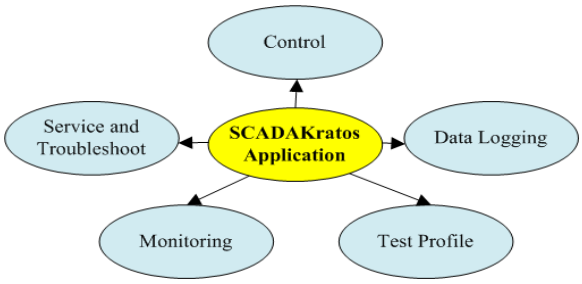

Figure-1. SCADAKratos application modules.

All the component modules are interconnected through the Ethernet and Profibus. These modules can be accessed remotely through public network. The control module is used to give commands to activate and deactivate a whole system or sub-system such as running the pumping system, thermal system and so on. The monitoring module is used to monitor the system and is performed by the visualization of several synoptic panels which are updated in real-time. All the measures acquired such as pressure and temperature are stored in the MS-SQL databases in the data logging module. The service and troubleshoot module is used by the manufacturer to service and troubleshoot the TVC system. Lastly, the test profile module is used to set the testing profile of tests that need to be conducted by TVC system. Figure-2 shows the graphical user interface (GUI) of the SCADAKratos application.

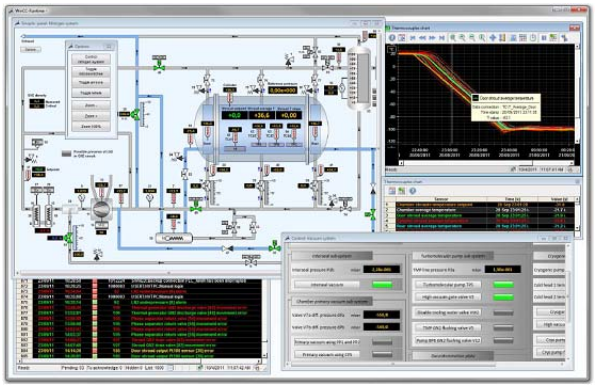

Figure-2. Graphical user interface (GUI) of SCADAKratos application.

Meanwhile, Figure-3 shows the overall control system architecture of the TVC system.

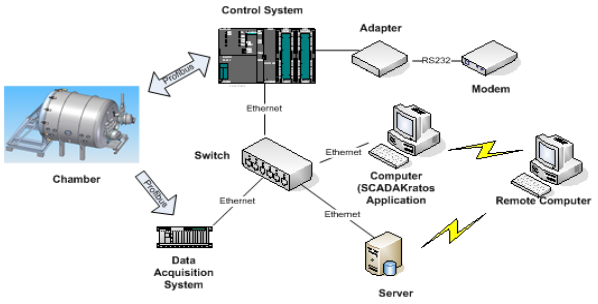

Figure-3. Control system architecture for Thermal Vacuum Chamber (TVC) system.

Cryptography algorithms

Supervisory control and data acquisition (SCADA) system has been widely used to monitor and control in industrial application [3]. That is why it has also been used in TVC system. However, its security is very vulnerable [3]. A review of the security for SCADA system has been conducted by the researcher to identify the most appropriate method to be used especially for communication in the SCADA system application. Among them are the key management and distribution protocol, security pattern, cryptography and so on [4]. The study results showed that in the future, cryptography algorithm will be the solution to be used for SCADA system communication [4]. In addition, other researchers also found that it is also suitable for remote communication [5-7].

Therefore, the cryptography algorithm is the most appropriate technique to be implemented in the SCADAKratos application. The ability of this technique in handling various attacks has been proven and investigation studies have also been conducted by researchers to identify the appropriate algorithm to be implemented for specific applications such as authentication, industry, images, communication and more. For SCADAKratos application, the algorithm needs to be applied as necessary to meet the necessary requirements in terms of authentication, network and so on. From a survey conducted by researchers [8], they had claimed that AES is the most secure algorithm for network security compared to other algorithms such as Rivest -Shamir-Adlemen (RSA), Triple – Data Encryption Standard (3-DES) and many more. AES was also found to be very efficient in hiding data [8] and is in accordance with SCADAKratos application for file data transfer functions. Its performance is even better and this will speed up the process of sending files using this algorithm. It is also chosen because it is suitable to encrypt large data [9]. Meanwhile the SHA-1 algorithm is chosen because of its capability to perform authentication function and secure stored password data [10].

The following elaborates the cryptography algorithms that have been chosen to be implemented into the TVC system which are SHA-1 and AES algorithm.

Secure Hash Algorithm (SHA-1)

SHA was developed by the National Institute of Standards and Technology (NIST) and published as a federal information processing standard (FIPS 180) in 1993 [11]. SHA-1 is a revised version that was issued as FIPS 180-1 in 1995. SHA-1 is widely used in applications and protocols compared to other SHA function. The hash size of SHA-1 is 160 bits. The concept of SHA-1 is once the input data is encrypted, there is no way to decrypt it again and get the source data. Figure-4 shows the concept of SHA-1 and how it will be implemented into the SCADAKratos application.

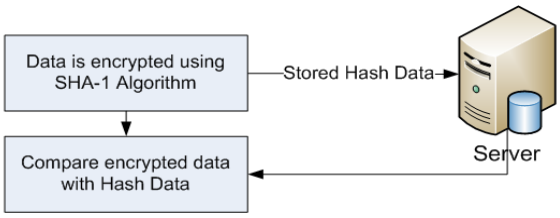

Figure-4. SHA-1 algorithm concept.

The server will store the encrypted password. In order to login to the TVC system the key in password will be encrypted using the same algorithm and then it will be compared with hashed data that had been stored in the server.

Advanced Encryption Standard (AES)

The AES was published by the NIST in 2001. The AES is a symmetric block cipher with a block length of 128 bits that is purposely created to replace DES as the approved standard for a wide range of applications. The structure of AES is quite complex and it can support any combination of data (128 bits) and key length of 128, 192, and 256 bits. The algorithm is referred as AES-128, AES-192, or AES-256 [12].

The AES allows a 128 bit data length that can be divided into four basic operational blocks. These blocks are treated as an array of bytes and organized as a matrix in the order of 4×4 that is called the state array.

For both encryption and decryption, the cipher begins with an Add Round Key stage. However, before reaching the final round, this output goes through nine main rounds, during each of those rounds four transformations are performed; 1) Sub-bytes, 2) Shift-rows, 3) Mix-columns, 4) Add round Key. In the final (10th) round, there is no Mix-column transformation. Decryption is the reverse process of encryption and using inverse functions: Inverse Substitute Bytes, Inverse Shift Rows and Inverse Mix Columns [13].

The AES algorithm is used to encrypt the test data results that need to be transferred to the customer. In order to maintain the integrity of data transferred, data will be encrypted using public key and decrypted using private key.

Testing and findings

For simulation purpose, a client-server application was developed using Visual Studio .Net 2012. A client will act as remote computer, while the server which will act as interfacing between SCADAKratos application of TVC system. The login authentication from the remote computer will use SHA-1 algorithm. Meanwhile, the file transfer between the remote computer and SCADAKratos application through the public network will use AES algorithm. These requirements can be described as follows:

- Security implementation for communication between remote computer and SCADAKratos application of TVC system.
- Security implementation for communication between SCADAKratos application of TVC system and remote computer access by the customer during file data transfer.

There will be two (2) main modules in this security application system which is login authentication and file data transfer. Figure-5 and Figure-6 show the flow chart of server and client.

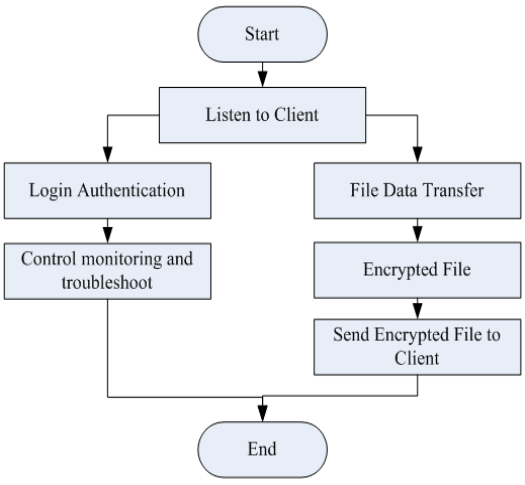

Figure-5. Server flow chart.

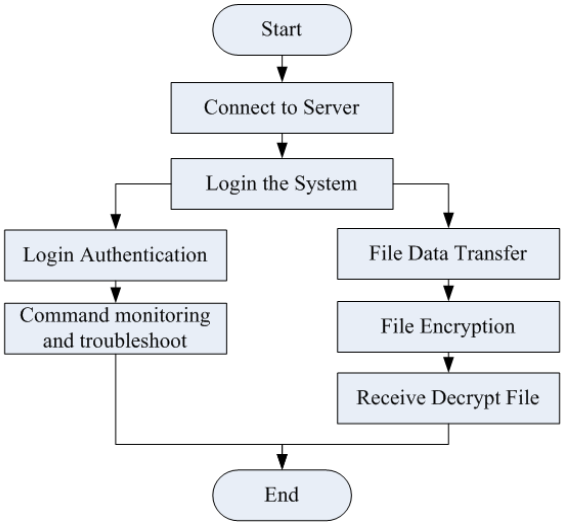

Figure-6. Client flow chart.

The testing is done using the following steps: Firstly, the user needs to login at the client side using a password that has been encrypted using SHA-1 algorithm. Once successful, the command, monitoring and troubleshoot can be done. Secondly, for file data transfer, the sample testing data will be encrypted before it is sent to the customer. The file is encrypted using AES algorithm and the customer key is generated. Once the customer receives the encrypted file, the customer can decrypt the file using the customer key.

The testing is done to ensure that the security application system is fully tested and secure to be integrated with the real system. The testing is done by using the sample data from the TVC system. Figure-7 is the sample testing data result of the TVC system.

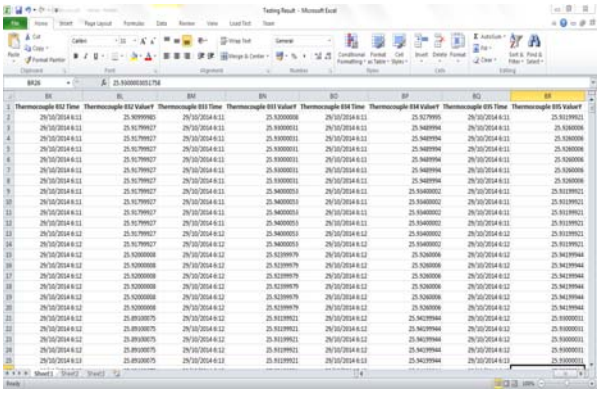

Figure-7. Sample testing data result.

RESULTS AND DISCUSSION

The following shows the test results for the cryptography algorithms added to the TVC system when it is tested by module.

Login authentication module

The SHA-1 Algorithm is used in the login authentication module. The following is the data value that had been tested.

- Sample Password: password
- Sample Hash Data for "password": 91170972282011856363613037111082485127126230143216

The Hash Data will be stored at the server in SCADAKratos and it cannot be decrypted.

File data transfer module

The AES algorithm is used to encrypt the sample testing data result and Figure-8 shows the sample of encrypted data.

Figure-8. Encrypted sample testing data result.

By using the key, the encrypted file can be decrypted and it is similar to the file before it is encrypted.

The SHA-1 algorithm is generated using Microsoft Visual Studio C#. The following code is used to generate the hash data.

```
private string GenerateSHA1HashData(string data)
{
SHA1  sha1 = SHA1.Create();
byte[] hashData =
sha1.ComputeHash(Encoding.Default.GetBytes(data));
StringBuilder returnValue = new StringBuilder();
for (int i = 0; i < hashData.Length; i++)
            { returnValue.Append(hashData[i].ToString());}
            return returnValue.ToString();
}
```

After the data has been encrypted, it will be stored in the server. The server will use the hash data to compare with input from the user during login authentication module. The following code shows how the comparison is done by the system.

```
Private bool CompareSHA1HashData(string inputData,
string storedHashData)
{
string getHashInputData =
GenerateSHA1HashData(inputData);
if (string.Compare(getHashInputData, storedHashData) ==
0){
MessageBox.Show("Login Successful!", "Information");
panel1.Visible = false;
return true; }
else {
 MessageBox.Show("Wrong Password!", "Attention");
 return false; } }
```

AES Algorithm Code is used in the file data transfer module. The following code shows how the file is encrypted.

```
private static void EncryptFile(string plainFilePath,
string encryptedFilePath, byte[] key, byte[] iv)
{ using (AesCryptoServiceProvider aes = new
AesCryptoServiceProvider())
{
aes.KeySize = 128;
aes.Key = key;
aes.IV = iv;
ICryptoTransform encryptor =
aes.CreateEncryptor(aes.Key, aes.IV);
using (FileStream plain = File.Open(plainFilePath,
FileMode.Open, FileAccess.Read, FileShare.Read))
{ using (FileStream encrypted =
File.Open(encryptedFilePath, FileMode.Create,
FileAccess.Write, FileShare.None))
            { using (CryptoStream cs = new
CryptoStream(encrypted, encryptor,
CryptoStreamMode.Write))
                  {  plain.CopyTo(cs);  }  }  }  }
}
```

Then, the remote computer or client is able to decrypt the file by using the private key. The following code shows how the decryption is done by the system.

```
public static void DecryptFile(string plainFilePath, string
encryptedFilePath, byte[] key, byte[] iv)
{ using (AesCryptoServiceProvider aes = new
AesCryptoServiceProvider())
{
aes.KeySize = 128;
aes.Key = key;
aes.IV = iv;
ICryptoTransform decryptor =
aes.CreateDecryptor(aes.Key, aes.IV);
 using (FileStream plain = File.Open(plainFilePath,
FileMode.Create, FileAccess.Write, FileShare.None))
{using (FileStream encrypted =
File.Open(encryptedFilePath, FileMode.Open,
FileAccess.Read, FileShare.Read))
{using (CryptoStream cs = new CryptoStream(plain,
decryptor, CryptoStreamMode.Write))
 { encrypted.CopyTo(cs); } } }
}
```

From the simulation done, the results obtained showed that the proposed system can handle the above situation well. Figure-9 and Figure-10 show the simulation application using Client Server Application.

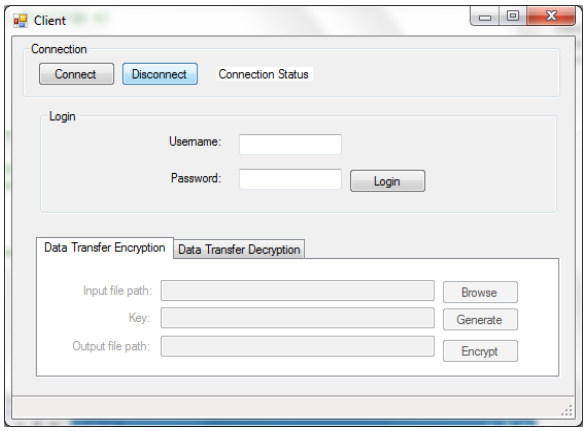

Figure-9. Client application.

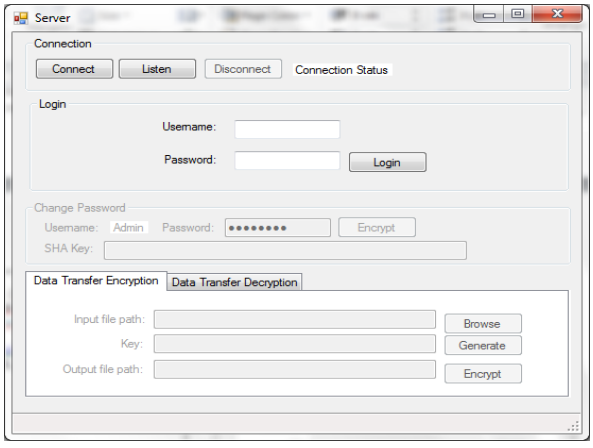

Figure-10. Server application.

CONCLUSIONS

As a conclusion, this project shows how cryptography algorithm can be implemented in TVC system to secure the remote access and data transferred to the customer. The command data and File Data Transfer through the public network cannot be read by the third party easily without knowing the key. Communication between the TVC system and remote computer can be controlled and monitored compared to before security is added into the system. Although antivirus and firewall are installed in Ethernet line, it is still exposed to threat and attack. Currently, the security has not been applied but in the future this security is important in order to protect the government properties, customer confidential and this will be tied to the standards and policies that can be implemented into the system.

ACKNOWLEDGEMENTS

We would like to express our gratitude to Ministry of Education for providing financial support (research grant 4F357) in conducting our study. Our special thanks to National Space Agency of Malaysia (ANGKASA) for execution of this study. Last but not least, we would also like to express our appreciation to Universiti Teknologi Malaysia (UTM) and specifically Advanced Informatics School (AIS) for realizing and supporting this research work.

REFERENCES

[1] Ng S. W. 2010. Towards Thermal Balance Testing Using Thermal Vacuum Chamber HVT-50. AIAA SPACE 2010 Conference & Exposition. Anaheim, California. AIAA 2010-8914.

[2] Thomas M. C. 2010. Stuxnet, the Real Start of Cyber Warfare? IEEE Network. 24(6). DOI: 10.1109/ MNET. 2010. 5634434.

[3] J. Gao, J. Liu, B., Rajan, R., Nori, B. Fu, Y. Xiao, W. Liang, and C. L., Philip Chen. 2014. SCADA Communication and security issues. Security Communication Network. 7(1): 175-194.

[4] Shahzad, A.S. Musa, A. Aborujilah and M. Irfan. 2014. The Security Survey and Analysis on Supervisory Control and Data Acquisition Communication. Journal of Computer Science. 2014 Science Publications. DOI: 10.3844 /jcssp. 2014. 2006. 2019.

[5] Amir S. and Shahrulniza M. 2012. Cryptography and Authentication Placement to Provide Secure Channel for SCADA Communication. Malaysia International Journal of Security (IJS). 6(3).

[6] Hoon K. 2012. Application of Asymmetric-key Encryption Method for Internet-based SCADA Security. Journal of Security Engineering.

[7] Reza K., Abdalhossein R. and Ehsan A. 2014. An Efficient Method to Improve WBAN Security.

Advanced Science and Technology Letters. vol. 64: 43-46.

[8] Swati K. and Er. Neeraj M. 2015. A Review on: Network Security and Cryptographic Algorithm. International Journal of Advanced Research in Computer Science and Software Engineering. 5(4), April.

[9] Ritu P. and Vikas K. 2013. Efficient Implementation of AES. International Journal of Advanced Research in Computer Science and Software Engineering. 3(7), July.

[10] Yagiz S., Husrev T. S. and Nasir M. 2005. A Secure Biometric Authentication Scheme Based On Robust Hashing. Proceeding MM & Sec '05 Proceedings of the 7th Workshop On Multimedia and Security Pages.

[11] Lamiaa M. E. B., Neveen I. G., Aboul E. H. and Tai H. K. 2011. A Fast and Secure One Way Hash Function. International Conference, SecTech. Jeju Island, Korea.

[12] William S. 2011. Cryptography and Network Security Principles and Practice Fifth Edition. Prentice Hall.

[13] Gurpreet S. and Supriya. 2013. A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security. International Journal of Computer Applications. 67(19).