ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

Security Deployment in TR-069 CPE WAN Management Protocol

Sarvotham B M[1], Ranjani G[2]

PG Student [Digital Comm.], Dept. of TCE, R.V. College of Engineering, Bengaluru, Karnataka, India[1]

Assistant Professor, Dept. of TCE, R.V. College of Engineering, Bengaluru, Karnataka, India[2]

ABSTRACT: TR-069 describes the Customer Premises Equipment (CPE) WAN Management Protocol (CWMP), intended for communication between a CPE and Auto-Configuration Server (ACS). The Secure Socket Layer (SSL) in the TR-069 CWMP gives solution for the security issue. This paper gives overview about SSL layer. The SSL handshake protocol authenticates the client and server. Once the handshake is completed, the record protocol processes the data and sends to the recipient. The use of SSL layer provides security.

KEYWORDS: Customer premises equipment, CPE WAN Management Protocol, Auto-Configuration Server, secure socket layer.

I.INTRODUCTION

TR-069 describes the Customer premises equipment (CPE) WAN Management Protocol, intended for communication between a CPE and Auto-Configuration Server (ACS). The CPE WAN Management Protocol defines a mechanism that encompasses secure auto-configuration of a CPE, and also incorporates other CPE management functions into a common framework [1]. The TR-069 CPE WAN Management Protocol provides communication between CPE like set-top box, gateways, routers etc and Auto-Configuration Server (ACS). The CPE WAN Management Protocol has five functional components, they are

- Auto-Configuration and dynamic service provisioning of CPE.
- Software/firmware image management of CPE.
- Software module management of CPE.
- Diagnostics.
- Status and performance monitoring.

Auto-Configuration and dynamic service provisioning of CPE: Based on a variety of criteria the CPE WAN Management protocol allows an ACS to provision a CPE or a collection of CPE. The provisioning mechanism has specific provisioning parameters and a general mechanism is used for adding vendor-specific provisioning capabilities as needed. At the time of initial connection to the broadband access network, the provisioning mechanism allows CPE provisioning and at any subsequent time, the provisioning mechanism got the ability to re-provision the CPE. The identification mechanism included in the protocol allow CPE provision based either on the requirements of the each specific CPE or on a collective criteria such as CPE vendor, model, software, version or other parameters.

Software/firmware image management of CPE: The CPE WAN Management protocol provides tools to manage downloading a CPE software/firmware image files. The version identification, file download initiation and notification of the ACS of the success or failure of a file download are the mechanisms provided by the protocol.

Software module management of CPE: The CPE WAN Management protocol enables an ACS to manage modular software and execution environments on a CPE. The ability to install, update and to uninstall software modules as well as notification to the ACS of success or failure of each action is provided by the CPE WAN Management Protocol. This protocol also supports to start and stop applications on the CPE, to enable and disable execution environments and to inventory the software modules available on the device.

DOI: 10.15662/ijareeie.2015.0408014

Diagnostics: The CPE WAN Management protocol provides support for a CPE to make available information that the ACS may use to diagnose and resolve connectivity or service issues as well as the ability to execute defined diagnostic tests.

Status and performance monitoring: The CPE WAN Management protocol provides support for a CPE to make available information that the ACS may use to monitor the CPE's status and performance statistics. It also defines a set of mechanisms that allow the CPE to actively notify the ACS of changes to its state.

The Auto-Configuration Server in the network manages the devices in or at the subscriber premises. Digital Subscriber Line Broadband Networks (DSL B-NTs) and other types of CPE such as stand-alone routers and LAN-side client devices are managed by the CPE WAN Management protocol. The figure 1 shows the positioning in the end-to-end architecture.

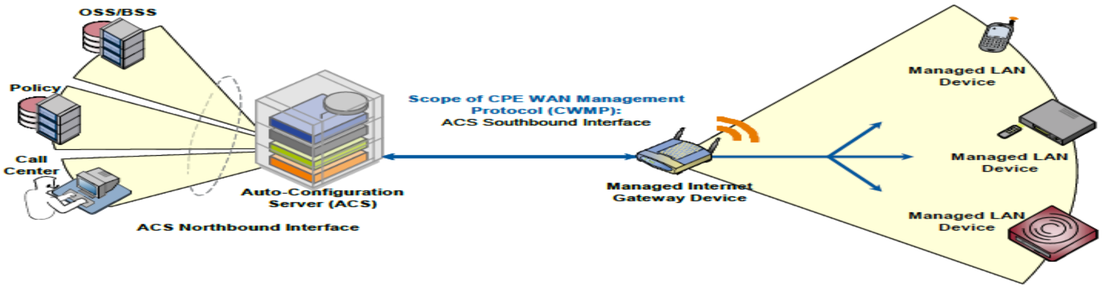

OSS/BSS
Policy
Call Center
Auto-Configuration Server (ACS)
ACS Northbound Interface
Scope of CPE WAN Management Protocol (CWMP): ACS Southbound Interface
Managed Internet Gateway Device
Managed LAN Device
Managed LAN Device
Managed LAN Device

Figure 1: Positioning in the end to end architecture

A high degree of security is provided by the CPE WAN Management protocol. The CPE WAN Management protocol also provides scalability. The CPE WAN Management protocol has some security goals and they are:

- The CPE WAN Management protocol prevent tampering with the management functions of a CPE or ACS, or the transactions that take place between a CPE or ACS.
- The confidentiality is provided for the transactions that take place between a CPE and ACS.
- CPE WAN Management protocol allows appropriate authentication for each type of transaction.

II. LITERATURE SURVEY

With the quick advancement of Internet innovation, network innovation has entered into all aspects of the financial society. Notwithstanding, because of the open Internet and secrecy of the natural attributes, prompting security has turned into a noteworthy obstruction of web application. Step by step instructions to ensure the transmission of touchy data adequately turns into the center of client. For this situation, Secure Sockets Layer (SSL) rises as the times require. So we concentrate on the execution process of SSL Handshake Protocol in view of examines the Secure Sockets Layer (SSL) protocol actualize component [3]. The Secure Socket Layer (SSL) gives the essential components of secure communications and they are integrity, privacy and authentication [4].

III.SECURE SOCKET LAYER PROTOCOL

SSL is the most popular application of public key cryptography in the world. SSL can be used to provide strong authentication of both parties in a communication session, strong encryption of data in transit between them, and verification of the integrity of the data in transit. TLS/SSL can be used to secure a broad range of critical business functions such as web browsing, server-to-server communications, e-mail, client-to-server communications, software updating, database access, virtual private networking and others. The main role of SSL is to provide security for web traffic. Security includes confidentiality, message integrity and authentication. SSL achieves these elements of security through the use of cryptography, digital signatures and certificates.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

Cryptography: SSL protects confidential information through the use of cryptography. Sensitive data is encrypted across public networks to achieve a level of confidentiality. There are two types of data encryption and they are symmetric and asymmetric cryptography. Symmetric cryptography uses the same key for encryption and decryption. Key distribution is the inherent weakness in symmetric cryptography. Asymmetric algorithms use one key for encryption of data, and then a separate key for decryption. Asymmetric algorithms are more favorable than symmetric algorithms because even if the encryption key is learned in one direction, the third party still needs to know the other key in order to decrypt the message in the other direction. With asymmetric encryption, both sides can spontaneously spawn a transaction without ever having met. This is achieved by the use of a public and private key pair. The public key of the entity is public knowledge and is used for encryption, whereas the private key of the entity remains secret and is used for decryption.

Digital signature: To ensure message integrity, each message exchanged in SSL has a digital signature attached to it. A digital signature is a hashed message digest with public key information. The message digest is based on the checksum of the message. The message digest is difficult to reverse. Both parties compute the message digest separately and compare the hashed results. Matching results means that the checksum was unaltered during transit, minimizing the chance of a compromised message. The digital signature is shown in figure 2

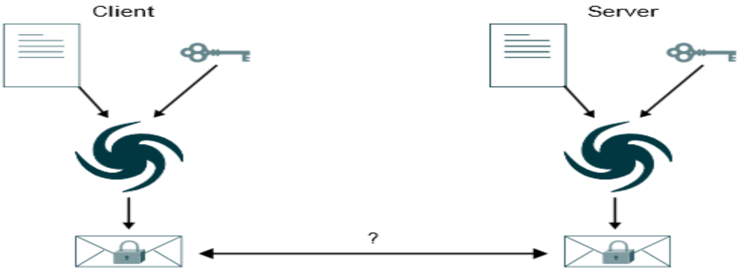


Figure 2: Digital signature

Certificates: SSL uses digital certificates to authenticate servers. SSL also includes an optional authentication for clients. Certificates are digital documents that will attest to the binding of a public key to an individual or other entity. They allow verification of the claim that a specific public key does, in fact, belong to the specified entity. Certificates help prevent someone from impersonating the server with a false key. SSL uses X.509 certificates to validate identities. X.509 certificates contain information about the entity, including public key and name. A certificate authority then validates the certificate.

IV.SSL ARCHITECTURE

SSL has two distinct entities, server and client. The client is the entity that initiates the transaction, whereas the server is the entity that responds to the client and negotiates which cipher suites are used for encryption. In SSL, the web browser is the client and the web-site server is the server. The SSL protocol contains four protocols, the Handshake protocol, the Record protocol, the Alert protocol and the Change Cipher Specification protocol. The client authenticates the server during the handshake protocol. When the session is initiated and the handshake is complete, the data transfer is encrypted during the record protocol phase. If there are any alarms at any point during the session, the alert is attached to the questionable packet and handled according to the alert protocol. The SSL architecture is shown in figure 3.

DOI: 10.15662/ijareeie.2015.0408014

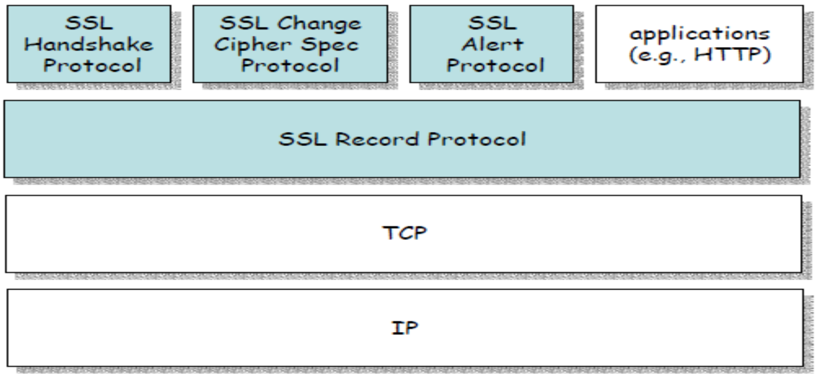


Figure 3: SSL architecture

SSL handshake protocol: The SSL Handshake protocol is layered on top of the SSL Record protocol. It allows a client and server to authenticate each other and to negotiate items like cipher suites and compression methods. The client always authenticates the server, and the server has the option of also authenticating the client. The SSL handshake protocol is shown in figure 4. During the handshake protocol, the following important steps takes place and they are:

- The session capabilities are negotiated.
- The encryption algorithms are negotiated.
- The server is authenticated to the client.

The steps of the Handshake protocol are:

1. Client sends **ClientHello** message.
2. Server acknowledges with **ServerHello** message.
3. Server sends its certificate.
4. Optional: server requests client’s certificate.
5. Optional: client sends its certificate.
6. Client sends **ClientKeyExchange** message.
7. Client sends **Certificate Verify** message.
8. Both send **ChangeCipherSpec** messages.
9. Both send **Finished** messages.

SSL Change cipher spec protocol: This consists of a single message which consists of single byte with the value 1. This is used to cause the pending state to be copied into the current state which updates the cipher suite to be used on this connection.

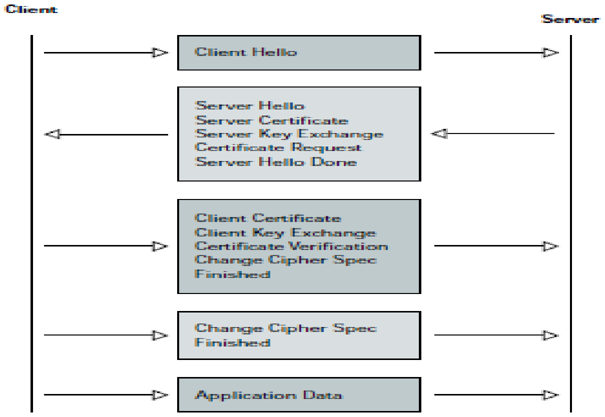


Figure 4: Handshake protocol

SSL Alert protocol: SSL Alert protocol is used to convey SSL related alerts to the peer entity. It consists of two bytes, the first of which takes the value 1(warning) or 2(fatal). If the level is fatal, SSL immediately terminates the connection. The second byte contains a code that indicates the specific alert.

SSL record protocol: The SSL Record protocol is used for the encapsulation of higher layer protocol data and therefore it fragments the data into manageable pieces (called fragments) and processes each fragment individually. Each fragment is optionally compressed and cryptographically protected according to the compression method and cipher spec of the SSL session state and the cryptographic parameters of the SSL connection state. The encryption for all messaging in SSL is handled in the record protocol. SSL record consists of the encapsulated data, digital signatures, message type, version and length. SSL records are 8 byte long. The SSL record protocol is shown in figure 5.

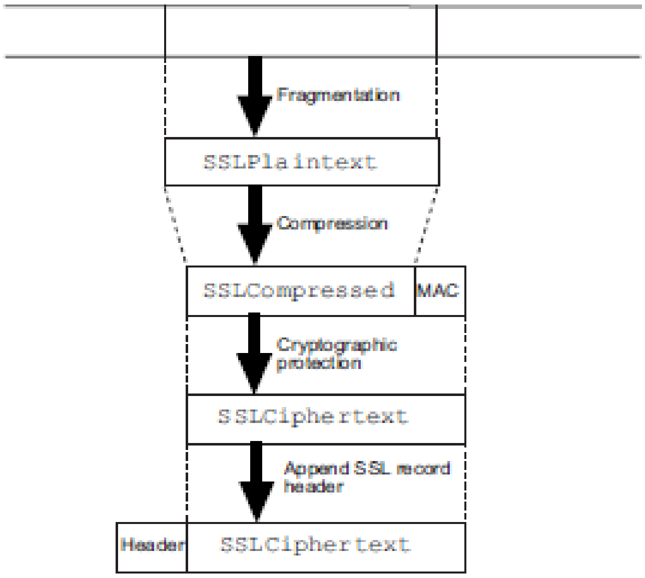
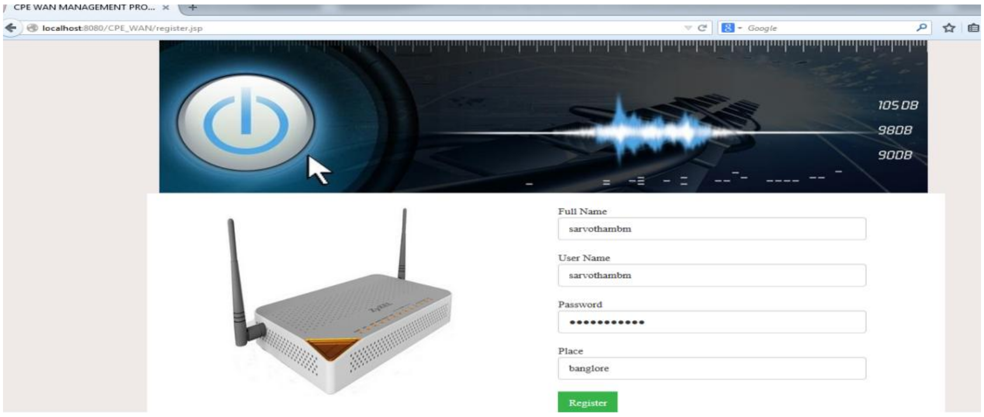


Figure 5: SSL Record protocol

V.RESULT AND DISCUSSION

Firstly, the client gets register with the server. The client gets register to the server by providing his full details. The client registration is shown in figure 6.


CPE WAN MANAGEMENT PRO...
localhost:8080/CPE_WAN/register.jsp
Google
105 DB
980B
900B

Full Name
sarvothambm

User Name
sarvothambm

Password
●●●●●●●●●●●●

Place
banglore

Register

Figure 6: Client registration

DOI: 10.15662/ijareeie.2015.0408014

During handshake, the server sends the public key to the client, the same public key appears on the client side. The public key exchange is shown in figure 7.

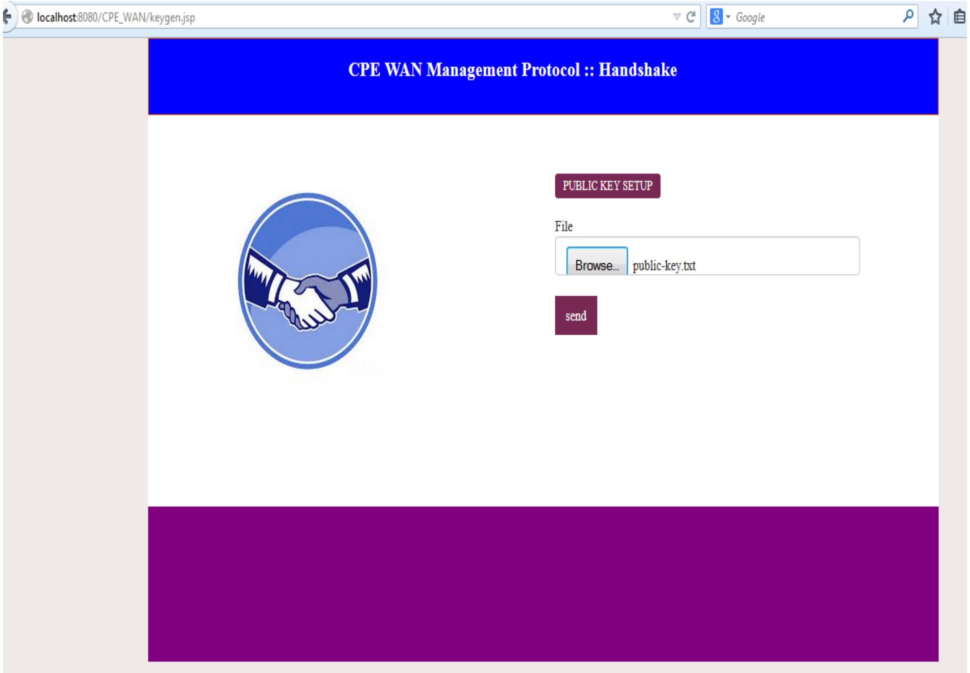
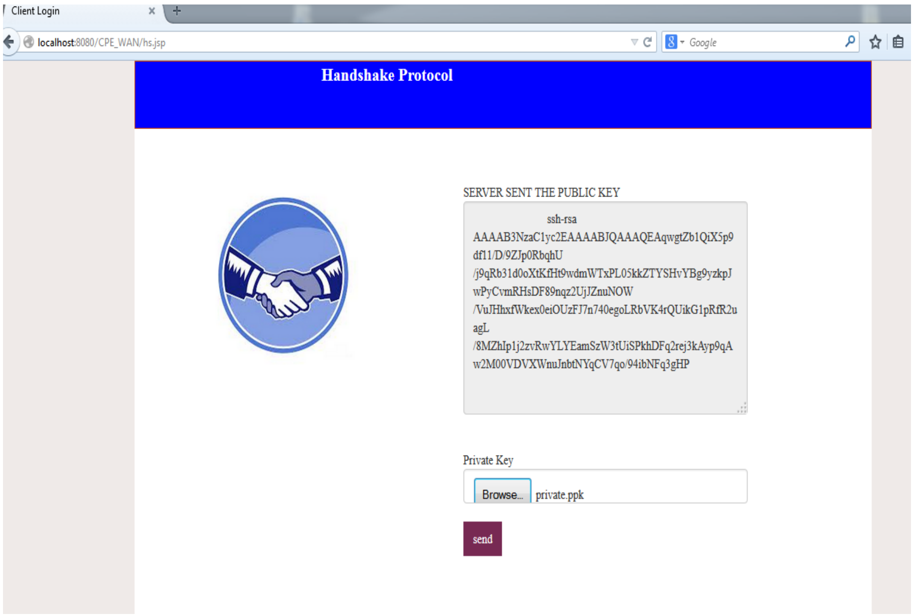

localhost:8080/CPE_WAN/keygen.jsp
Google
CPE WAN Management Protocol :: Handshake
PUBLIC KEY SETUP
File
Browse...
public-key.txt
send

Figure 7: Public key exchange

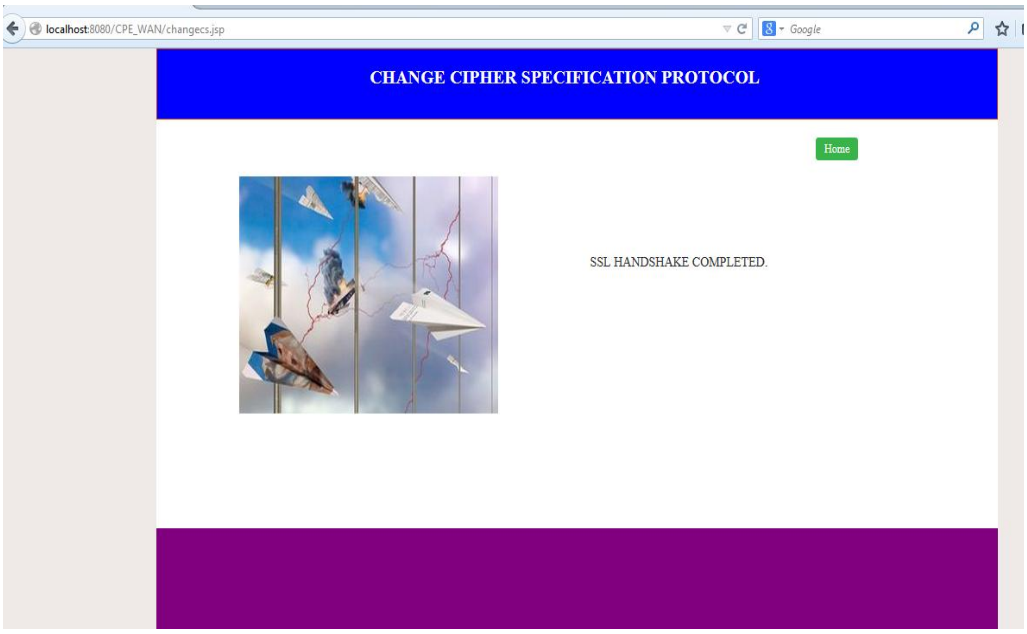
The client also sends the private key to the server during handshake process. The private key exchange is shown in figure 8.



```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQEAqwgtZb1QiX5p9
df11/D/9ZJp0RbqhU
/j9qRb31d0oXtKfHt9wdmWTxPL05kkZTYSHvYBg9yzkpJ
wPyCvmRHsDF89nqz2UjJZnuNOW
/VuJHhxfWkex0eiOUzFJ7n740egoLRbVK4rQUikG1pRfR2u
agL
/8MZhIp1j2zvRwYLYEamSzW3tUiSPkhDFq2rej3kAyp9qA
w2M00VDVXWnuJnbtNYqCV7qo/94ibNFq3gHP
```

Figure 8: Private key exchange

Once the key exchanges are finished, the change cipher spec protocol gets activate and sends the message that the handshake process is completed. The handshake completed message is shown in figure 9.

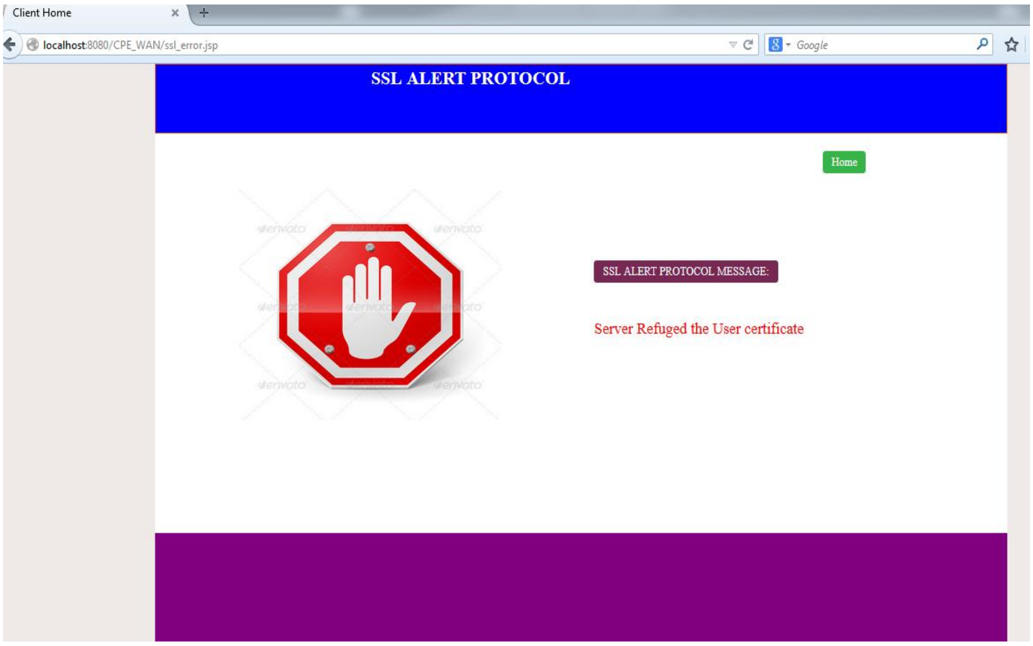


CHANGE CIPHER SPECIFICATION PROTOCOL

SSL HANDSHAKE COMPLETED.

Figure 9: Handshake completed message

During handshake process, if the server does not accept the user certificate then the alert protocol gets activated. The alert protocol is shown in figure 10.



SSL ALERT PROTOCOL

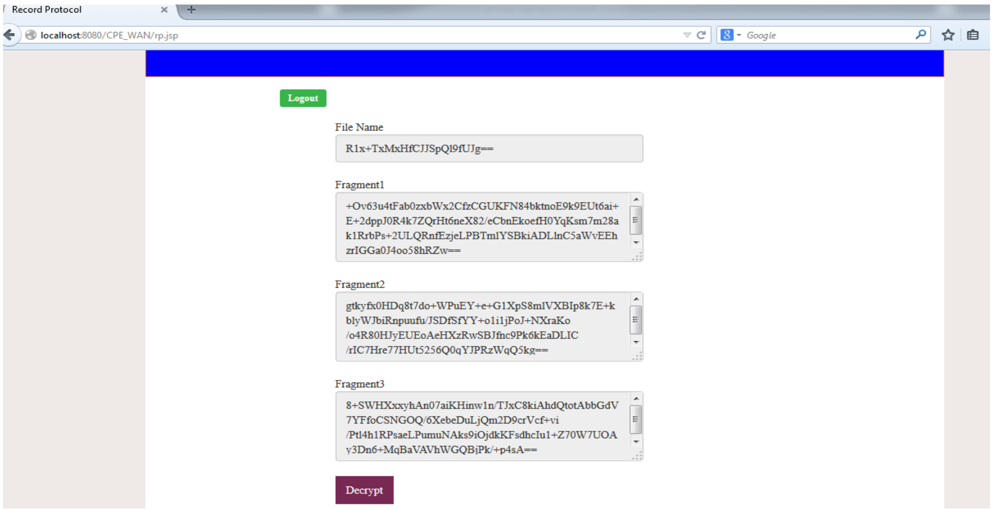
SSL ALERT PROTOCOL MESSAGE:

Server Refuged the User certificate

Figure 10: Alert protocol

DOI: 10.15662/ijareeie.2015.0408014

In record protocol, the data is fragmented, compressed and then the data is encrypted. The encrypted data is sent to the client. The encrypted message is shown in figure 11.



File Name

R1x+TxMxHfCJJSpQl9fUJg==

Fragment1

+Ov63u4tFab0zxbWx2CfzCGUKFN84bktnoE9k9EUt6ai+
E+2dppJ0R4k7ZQrHt6neX82/eCbnEkoefH0YqKsm7m28a
k1RrbPs+2ULQRnfEzjeLPBTm1YSBkiADLlnC5aWvEEh
zrIGGa0J4oo58hRZw==

Fragment2

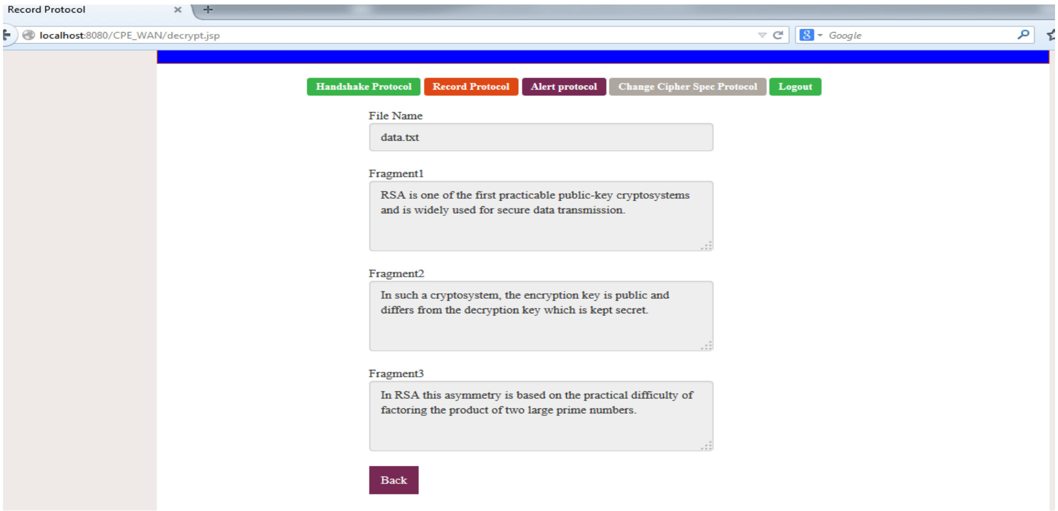
gtkyfx0HDq8t7do+WPuEY+e+G1XpS8mlVXBIp8k7E+k
b1yWJbiRnpuufu/JSDfSfYY+o1i1jPoJ+NXraKo
/o4R80HJyEUEoAeHXzRwSBJfnc9Pk6kEaDLIC
/rIC7Hre77HUt5256Q0qYJPRzWqQ5kg==

Fragment3

8+SWHXxxyhAn07aiKHinw1n/TJxC8kiAhdQtotAbbGdV
7YFfoCSNGOQ/6XebeDuLjQm2D9crVcf+vi
/Ptl4h1RPsaeLPumuNAks9iOjdkKFsdhcIu1+Z70W7UOA
y3Dn6+MqBaVAVhWGQBjPk/+p4sA==

Figure 11: Encrypted message

The encrypted data from the server is decrypted in the client side to get the original data. The decrypted original message is shown in figure 12.



File Name

data.txt

Fragment1

RSA is one of the first practicable public-key cryptosystems and is widely used for secure data transmission.

Fragment2

In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret.

Fragment3

In RSA this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers.

Figure 12: Decrypted original message

VI.CONCLUSION

SSL is vital to Web security. It provides a strong sense of confidentiality, message integrity, and server authentication to users. The secure socket layer provides security in TR-069 CPE WAN Management protocol. The TR-069 CPE WAN Management protocol also maintains the wide network.

DOI: 10.15662/ijareeie.2015.0408014

REFERENCES

[1] TR-069 Amendment 5, “CPE WAN Management Protocol”, Broadband Forum Technical Report, November 2013.

[2] LI Wei, XIANG Shuyue and CHEN Shuangbao, “Improvement Method of SSL Protocol Identity Authentication based on the Attribute Certificate”, International Conference on Computer Science and Service System, pp.1154-1157, 2012.

[3] Jiang Du, Xinghui Li and Hua Huang, “**A** Study of Man-in-the-Middle Attack Based on SSL Certificate Interaction”, International Conference on Instrumentation, Measurement, Computer, Communication and Control, pp.445-448, 2011.

[4] Ordean M, Giurgiu M, “Implementation of a security layer for the SSL/TLS protocol”, International Symposium on Electronics and Telecommunications, pp.209-212, 2010.

[5] Feiyan Mu, Jiafen Zhang, Jing Du and Jie Lin, “Application of the Secure Transport SSL Protocol in Network Communication”, International Symposium on Computational Intelligence and Design, pp.63-66, 2011.

[6] Wang Yanhua, Yang Kuihe and Zhang Yun, “Research and Realization of Security Proxy Based on SSL Protocol”, International Conference on Electronic Measurement and Instruments, pp.264-267, 2007.

[7] Yunyoung Lee, Soonhaeng Hur, Dongho Won and Seungjoo Kim, “Cipher Suite Setting Problem of SSL Protocol and It’s Solutions”, International Conference on Advanced Information Networking and Applications Workshops, pp.140-146, 2009.

[8] K R Jayaram, “Identifying and testing for insecure paths in cryptographic protocol implementations”, International Conference on Computer Software and Applications, Vol.2, pp.368-369, 2006.