A Secure Encrypted Protocol for Clients' Handshaking in the Same Network

https://doi.org/10.3991/ijim.v13i05.9845

Ibrahim M. Obeidat (✉), Ala Mughaid
Hashemite University, Az-Zarqa, Jordan
imsobeidat@hu.edu.jo

Shadi Alzoubi
Computer Science Zaytoonah University Amman, Jordan

Abstract—Users in the same network can trace the data being transmitted amongst users and other users to the internet using many available online tools such as packet sniffers and many packets capturing tools, the need to make the data resistible to be read comes obvious. The proposed solution is to encrypt the data using inscription algorithm. In this paper, we propose a solution to protect Network Clients from other Clients in the same network.

Keywords—Introduction, Network Clients, Security, Cryptography

1 Introduction

In today's digital world, People are becoming increasingly adept at using convenient technology to make their work easier and to provide prompt advice and services to clients. Laptop computers, remote access to firm servers and wireless networking are just some of the expedient ways that lawyers can connect to the Internet and their own offices from around the world.

A computer network can be characterized as an arrangement of nodes that are connected and associated together for the purpose of sharing assets in an anticipated and controllable manner. These nodes are associated by using an arrangement of the sets of rules known as protocols. There are many types of network systems that empower the sharing of assets, for example (Hirviniemi 1998):

Local Area Network (LAN): A group of nodes that are connected through a wireless link or a communication line to share resources. Typically, the nodes are connected to the server within a distinct geographical area such as a library. Wide Area Network (WAN): Group of nodes that are extended over a large geographical area. Organizations and governments use WANs to relay data to others and to carry out their daily function irrespective of location. Internet: A network of networks that provides information and communication facilities globally.

Computer networks make it easier for firms to distribute their business globally at a low cost. The Internet particularly increases trading operations where firms are

targeting billions of customers. The open nature of the Internet makes it easy for people to access services from all over the world by using their own devices. Companies have developed and implemented easy access applications to provide their services over the Internet.

However, how secure is confidential client information when people are not actually in their offices using a desktop computer, or they are using a laptop computer on a secured wireless network set up by network administrator? When peoples take advantage of networking, to connect to the Internet or an office server to access e-mail or client documents, they may unwittingly risk the loss and disclosure of sensitive data and confidential client information (Bishop 2003).

As if it were not disconcerting enough that the loss and disclosure of sensitive data such as online banking passwords and personal information can lead to fraud and identity theft, People who are required by the "confidentiality rule" to protect confidential client information risk running afoul of the ethical rules and facing attorney disciplinary sanctions.

Study of methods of analysis of security requirements and needs of such Systems, and consequent design, implementation, and deployment is the primary scope of the discipline named as Network Security. Although named as network security, the principles and mechanisms involved herein do apply to internetworks as well. Security is often viewed as the need to protect one or more aspects of the network's operation and permitted use (access, behaviour, performance, privacy, and confidentiality included)(Pawar and Anuradha 2015).

Security requirements may be Local or Global in their scope, depending upon the networks or internetwork's purpose of design and deployment (Ahmad, Verma et al. 2011). Criteria for evaluating security solutions include the ability to meet the specified needs requirements, the effectiveness of approach across networks, computing resources needed rise the value of the protection offered, quality and scalability, availability of monitoring mechanisms, adaptability, flexibility, practicability from sociological or political perspective economic considerations and sustainability.

2 Literature Review

Network systems have provided many advantages to organisations, enabling access to facilities and computer resources anytime from anywhere, and might be considered a technological revolution. However, organisations need to give more attention and consideration to their system security and need to guarantee that unauthorised individuals cannot access their information.

One of the most unwanted situations to occur in networks is unauthorised access. This type of access may be accomplished by an outside or inside company intruder, or both. Such access may cause considerable damage to the company’s reputation by stealing its important data, which reflects negatively on the company’s commercial dealings and reduces its customer’s trust in it.

The definition of threat can be expressed as any possible action which causes damage to a network, data, users or security goals, either in a hostile manner or

accidentally. This unwanted damage, change or security bypass in the hostile/accidental manner is known as an attack on the network.

A number of risks and threats exist in the operational environment of computers and networks, particularly where they can become exposed to security breaches. There could be various reasons for the vulnerability, including incorrect installation of systems, incorrect usage or malicious software.

In general, information sharing among two or more computers over a network may be exposed to the risk of intrusion. There are four ways of intrusion that can negatively affect the system [Pfleeger, C,Shari. 2017]:

- **Interception:** An unwanted entity between the transmitter and the receiver steals the information.
- **Interruption:** Any unwanted entity between the conversations of two nodes stops the message and prevents it from being passed to the destination.
- **Modification:** An unwanted entity at the middle of conversation of two nodes changes the sender's messages, modifying their information before forwarding them to the receiver.
- **Fabrication:** A type of lie; here, one party is fabricated, and the other participants on the network are unaware that the messages are not from a valid participant.

Security Attacks compromises the information-system security. Active attacks involve active attempts on security leading to modification, redirection, blockage or destruction of data, devices or links (Hamid, Gianluigi et al. 2010). Passive attacks involve simply getting access to link or device and consequently data. Security Threats are those having a potential for the security violation. Security Mechanism is a mechanism that detects / locates / identifies / prevents / recovers from "security attacks"(Mendez, Papapanagiotou et al. 2017).

Security Service is a service that enhances security, makes use of security mechanisms.

Importance of identification of sources cannot be underestimated. Strategic importance applies to plan, preventing and/or countering whereas another variety of importance is with respect to Sensitivity-analysis and Economic-impact-analysis and pro-active protection.

Cryptography is the method of writing and converting data into a format that is unreadable for unauthorized users, where only the intended recipient can reverse it into a readable format to obtain the original message. It is a tool used to hide data in both the transmission process and when stored. It is a technique that can provide virtually unbreakable protection to sensitive information.

Cryptography requires the following two main components (Kahate 2013):

- A cipher, which means that the encryption process used to hide data during transition or/and storage; and
- Keys required to perform the encryption/decryption processes. They are the core part of cryptography operations used to transform the text into cipher.

Symmetric encryption is one of the most familiar cryptography techniques used to protect data. It applies a secret key to the original text of a message to change the content in a way that cannot be read by any others except those who have the key to encrypt/decrypt it (Curtmola, Garay et al. 2011). Encryption is the process of changing data into the ciphertext form that cannot be understood by anyone except the authorized parties. Decryption is the process of decoding the encrypted text and converting it back to the original text. The key could be a number, a word or a string of random letters. That key is shared between two or more parties and can be used to encrypt private information. Sharing the key is a drawback for this encryption mechanism because anybody who knows the key can read and create messages.

Advanced encryption standard (AES) [NIST. 2017] is an example of a symmetric encryption algorithm. AES is a symmetric block cipher chosen by the US government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data. In present-day cryptography, AES is widely adopted and supported in both hardware and software. To date, no practical cryptanalytic attacks against AES have been discovered. Additionally, AES has a built-in flexibility of key length, which allows a degree of 'future-proofing' against progress in the ability to perform exhaustive key searches.

Asymmetric encryption applies two keys to encrypt the information. A public key is published to all the users of the system, and the private key is made available only for a specific receiver customer who will receive the information. The public key can be represented in a short sequence of bytes that simplifies it during the cryptography mechanism. The short sequence is called a fingerprint and can be certified to represent the public key. A message that has been encrypted using the public key can only be decrypted by applying the matching private key to the encryption algorithm. Any message that is encrypted using the private key can only be decrypted by using the matching public key (Gupta and Silakari 2011).

RSA may be considered one of the most secure methods of data transmission and is named after its designers: Rivest, Shamir, and Adleman (Rivest, Shamir et al. 1978). RSA utilizes public and private keys that are based on a pair of large random prime numbers. Its security depends on the difficulty of factorizing large numbers. Public keys can be stored in any location without compromising the security of the system, although there is an issue in determining that a public key does, in fact, belong to a particular person.

A hash function is one of the secure mechanisms used to produce a fixed-size alphanumeric string as an output without changing the original message content (Sobti and Geetha 2012). The string is called a hash value or message digest, as it contains a string of digits generated by a one-way function that verifies whether the input matches the hash value. It is nearly impossible to retrieve the original data from only the hash value, and unfeasible to fabricate a data block that matches a given hash value. A hash function was used in this research to ensure that the information sent from the sender is identical to the information received by the recipient.

3 Methodology

The main focus of this research is to develop a protocol that controls the number of allowed or granted clients to communicate with each other also to secure their established connection.

The developed protocol was built for securing users from each other involves securing the data being transmuted in different manners as discussed below:

Preventing unauthorized clients from reading the data is being transmitted in the local network. Users in the same network can trace the data being transmitted between the users and the users to the internet using many available online tools such as packet sniffers and many packets capturing tools, the need to make the data resistible to be read comes obvious. The proposed solution is to encrypt the data using inscription algorithm.

To be sure from the send data is the same were received. Experienced hackers in the local network can sabotage the data being transmitted in the links by adding or removing or even change all the messages being transmitted over the lines. The proposed solution is to inject in the message being sent redundant data that represents a one-way encryption (Hash function).

Make sure of the sender identity. Hackers also can impersonate other identities to send faked messages, which lead to misunderstanding and dealing with wrong information, which may expose many problems. The proposed solution is to inject the message being sent redundant data that represent the digital signature of the sender person.

The protocol main function is to control the number of users that allowed accessing each client. This will be achieved by not allowing any clients to be communicated until the server allows to. Then encrypt the data being transmitted and add a Hash function to each message to confirm that the data has arrived the same it was sent. Finally, to add a digital stamp to the sender message to be sure from the sender's identity.

3.1 The protocol design

- Each client connected to the network establishes a connection with the server.
- Send the number of allowed connection concurrently.
- The server collects the data from the clients and establishes a database for decision-making purpose.
- For any client to communicate with any other client send the request to the server and wait.
- The server checks for an available connection to the client and if so, it sends a message to both clients for establishing a special secure tunnel between them.
- The two clients start the connection.
- Generate the public and the private keys and send them on the network.
- When closing the connection the two clients send a close message to the server to free their reserved connections.

4 Implementation

To prove the idea of this research by using a combination of security and control protection techniques a demo has been implemented. The demo consists of three tools/ applications:

4.1 The socket connection

In computer networking, an Internet socket or network socket is an endpoint of a bi-directional inter-process communication flow across an Internet Protocol-based computer network, such as the Internet (Cooper 2016).

The term Internet sockets are also used as a name for an application programming interface (API) for the TCP/IP protocol stack, usually provided by the operating system. Internet sockets constitute a mechanism for delivering incoming data packets to the appropriate application process or thread, based on a combination of local and remote IP addresses and port numbers. Each socket is mapped by the operating system to a communicating application process or thread.

A socket address is the combination of an IP address (the location of the computer) and a port (which is mapped to the application program process) into a single identity. In our simulation, we choose the TCP connection as it guarantees the connection reliability. To communicate with the TCP protocol we need a special API called Socket, which discussed above.

4.2 Combination of symmetric encryption and asymmetric encryption

If we want the benefits of both types of encryption algorithms mentioned in the previous sections, the general idea is to create a random symmetric key to encrypt the data, and then encrypt that key asymmetrically. Once the key is asymmetrically encrypted, we add it to the encrypted message. The receiver gets the key, decrypts it with their private key, and uses it to decrypt the message. This phase of the research is to protect the data during transmission from being available to anonymous persons also to make sure the data was not alternated and to be sure, of the sender identity which will be achieved by using the encryption combination explained.

In this research, we chose to use the Asymmetric Encryption (RSA algorithm) because it serves the research objectives especially for data transmission and can be used for multi-sessions communication

4.3 Client / server application

The client-server model distinguishes between applications as well as devices. Network clients make requests to a server by sending messages, and servers respond to their clients by acting on each request and returning results. One server generally supports numerous clients, and multiple servers can be networked together in a pool to handle the increased processing load as the number of clients grows.

Using the mechanism of the socket connection and the concepts of client-server applications our developed protocol will be generated to prevent the network from being congested and preventing the data from not being delivered.

The server application: Our topology requires a server that controls the network transactions and this can be done using server application which opens a port and starts listening to incoming requests to be granted or delayed.

The server application consists of a thread that keeps listing for incoming data and an SQL database for recording the status and connection information of each client also to store the generated public keys for later use.

We choose the SQL client because it can generate reports for administration purposes as a future work for enhancing the tool. The SQL data table consists of clients IP and the maximum number of connections allowed concurrently and the public keys(Mictosoft).

The server application algorithm:

- Generate the database.
- Open the specific port and start listening.
- The server receives the maximum number of connections for each client and stores them with the IP of the client.
- If a request arrives the server chick the requested client status and decide to grant or not on the connection.
- If the connection denied the server queue the request until the client is free to tack another connection.
- If connection granted, the server adds the connection to both connected clients and sends the approval.
- Then each client generates the keys and sends them to the server to be stored.

The client application: The client application enables the user for connecting to the server and configures the maximum number of allowed connections. It also represents the application for exchanging data between clients in the network. It generates the needed keys and distributes them using a secure connection and analysis the command messages for handshaking with the server.

The client application algorithm:

- Connect to the server and sends the needed data.
- If a client tries to connect to any other client the application implicitly, establish a sequence of messages and calculation for establishing the secure tunnel.
- Send a message to the server with the IP of the requested client.
- Waiting for response from the server (the server supervising the clients' connection establishment).
- If the server granted the requested, the application generates the keys and sends them to the server, then retrieves the public key of the requested client from the server.
- As soon as key exchanging done the two clients establish the tunnel and start the secure session.

- When the tunnel is closed the application sends a termination message to the server to free the reserved connections.

5 Server Application Some Code Examples

```
If Listening = False Then
    Dim T As New Thread(AddressOf Listen)
    T.IsBackground = True
    T.Start()
    Me.Text = "Listening"
    btnStart.Text = "Stop Server"

    connectionIP_ = txtsendip.Text
    sendPort_ = txtsendport.Text
    listenPort_ = txtPort.Text

Else
    Listening = False
    Me.Text = "Not Listening"
    btnStart.Text = "Start Server"

End If

sb = CType(ar.AsyncState, SocketAndBuffer)
  Dim numbytes As Int32 = sb.Socket.EndReceive(ar)
  If numbytes > 0 Then
            '-- Convert the buffer to a string
  Dim Receive As String = ASCII.GetString(sb.Buffer, 0, numbytes)

  _count += 1
  If _count = 1 Then
  Thread.Sleep(100)
  MsgBox(1)
  Else

End If


If Receive.StartsWith("QUIT") Then
      '-- Close the socket
      sb.Socket.Shutdown(SocketShutdown.Both)
      sb.Socket.Close()

Else

      '-- Show the data
```

```
    Dim dlg As New ShowReceiveDataDelegate(AddressOf
ShowReceiveData)
    Dim args() As Object = {Receive}
    Me.Invoke(dlg, args)
    '-- Echo the data

sb.Socket.Send(sb.Buffer) '-- Clear the buffer
Array.Clear(sb.Buffer, 0, sb.Buffer.Length) '-- Receive again

sb.Socket.BeginReceive(sb.Buffer, 0, sb.Buffer.Length, SocketFlags.None,
AddressOf
ReceiveCallBack, sb)

End If
```

6 Client Application Some Code Examples

```
Dim clientSocket As New System.Net.Sockets.TcpClient()
clientSocket.Connect(connectionIP, Convert.ToInt32(sendPort))
Dim serverStream As NetworkStream = clientSocket.GetStream()
Dim outStream As Byte () =
System.Text.Encoding.ASCII.GetBytes(txtmsg.Text)
serverStream.Write(outStream, 0, outStream.Length)
serverStream.Flush()
clientSocket.Close ()
ShowReceiveData ("me: " + txtmsg.Text)
----------------------------------------------------------------------
listenPort = 8881
Dim con As New
SqlConnection(ConfigurationManager.ConnectionStrings("Conn").Connectio
nString)
Dim com As New SqlCommand()
com.Connection = con
com.CommandText = "select * from UsersStatus where status='True' "
con.Open()

Dim dr As SqlDataReader = com.ExecuteReader()

While dr.Read()

ListBox1.Items.Add(dr("UserNmae").ToString)

End While

con.Close()
```

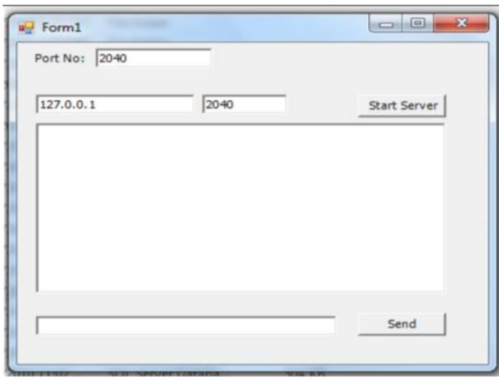

Fig. 1. Shows a sample run of the protocol environment simulation.

7 Conclusion

The primary focus of this work was the development of a secure connections scheme for users when communicating throughout the same network. The study developed an encryption model that to combine the modules/users securely. A simulator that realized the research objectives was designed and implemented in this work. This research showed that it is possible to achieve a secure connection environment by introducing a better designed encrypted connection for users' communication. The communication model represented as users that get successfully communicated only from whoever has been granted by the server which in contrast, secures the clients from being flooded by unwanted messages to make the network more efficient. The keys are kept encrypted in transit and at rest, with robust encryption mechanism with no method to decrypt the keys without providing the encryption keys.

8 References

[1] Ahmad, K., S. Verma, N. Kumar and J. Shekhar (2011). Classification of Internet Security Attacks. Proceeding of the 5th National Conference INDIACom-2011Bharti Vidyapeeth's Institute of Computer Applications and Management, New Delhi ISSN.

[2] Bishop, M. (2003). "What is computer security?" IEEE Security & Privacy 99(1): 67-69.

[3] Cooper, P. (2016). Networking and Sockets. Beginning Ruby, Springer: 363-378. https://doi.org/10.1007/978-1-4842-1278-3_15

[4] Curtmola, R., J. Garay, S. Kamara and R. Ostrovsky (2011). "Searchable symmetric encryption: improved definitions and efficient constructions." Journal of Computer Security 19(5): 895-934. https://doi.org/10.3233/jcs-2011-0426

[5] Gupta, K. and S. Silakari (2011). "Ecc over rsa for asymmetric encryption: A review." International Journal of Computer Science Issues (IJCSI) 8(3): 370.

[6] Hamid, J., M. Gianluigi and W. D. Lilburn (2010). Handbook of electronic security and digital forensics, World Scientific.

[7] Hirviniemi, S. (1998). Wide area network (wan) interface for a transmission control protocol/internet protocol (tcp/ip) in a local area network (lan), Google Patents.
[8] Kahate, A. (2013). Cryptography and network security, Tata McGraw-Hill Education.
[9] Mendez, D. M., I. Papapanagiotou and B. Yang (2017). "Internet of things: Survey on security and privacy." arXiv preprint arXiv:1707.01879.
[10] Mictosoft https://www.microsoft.com/en-us/download/details.aspx?id=50402.
[11] Pawar, M. V. and J. Anuradha (2015). "Network security and types of attacks in network." Procedia Computer Science 48: 503-506. https://doi.org/10.1016/j.procs.2015.04.126
[12] Rivest, R. L., A. Shamir and L. Adleman (1978). "A method for obtaining digital signatures and public-key cryptosystems." Communications of the ACM 21(2): 120-126. https://doi.org/10.1145/359340.359342
[13] Sobti, R. and G. Geetha (2012). "Cryptographic hash functions: a review." International Journal of Computer Science Issues (IJCSI) 9(2): 461.
[14] Pfleeger, C,Shari.L, Is There a Security Problem in Computing? , informIT, [Online]. Available: http://www.informit.com/articles/article.aspx?p=680830&seqNum=2. 2017.
[15] National Institute of Standards and Technology, Advanced Encryption Standard, [Online]. Available: https://csrc.nist.gov/publications/detail/fips/197/final. Last accessed 9/5/2017.

9 Authors

Ibrahim M. Obeidat is an associate Professor, working in Prince Al-Hussein Bin Abdullah II Faculty of

Information Technology Hashemite University, Jordan since 2008, his interest is in networking and cyber security

Ala Ala Mughaid is an assistance professor working in the Hashemite University, Jordan His interest is in cyber security and Networking

Shadi Alzoubi is an assistance professor working in Zaytoonah University Amman, Jordan, His interest is in cyber security and Networking smalzubi@zuj.edu.jo

Article submitted 2018-11-10. Resubmitted 2019-05-06. Final acceptance 2019-05-14. Final version published as submitted by the authors.