Journal of Babylon University/Pure and Applied Sciences/ No.(4)/ Vol.(21): 2013

Formulate A Sheltered Communication Channel For Realization Of Encryption, Legalization And Authentication Of Massage Transferred.

Hawraa Adil Nori
University of Babylon - Computer Center

Abstract
When two entities are communicating with each other, and they do not want a third party to listen to their communication, so secure communication includes means by which they can share information and without being known to a third party. Accordingly, some may think that a secure channel of communication means its ability to transfer encrypted data, but in fact the encryption is one of the specifications of this channel For security purposes, we try to formulate a sheltered channel in a model satisfying its required real attributes (encryption, legalization and authentication) . The formulated model utilized TCP/IP as the interior transport layer which is liable to guarantee that packets of data are propelled to the intended recipient in the right arrange.in this paper we describe the structure of a Very Simple Secured Protocol (VSSP) that exists above the TCP/IP layer and has a major effect managing connection through a protected communication channel.

خلاصة
عندما يتواصل كيانين او طرفي اتصال مع بعضهما البعض ، فأنهم لا يريدون طرف ثالث الاستماع إلى اتصالاتهم، فالاتصال الآمن يتضمن الوسائل التي تمكنهم من تبادل المعلومات دون أن يعرفها طرف ثالث غير مخول. وبناء عليه ، قد يعتبر البعض ان قناة اتصال آمنة يعني قدرتها على نقل البيانات المشفرة، ولكن في الواقع يعد التشفير احد مواصفات هذه القناة .لأغراض أمنية، نحن نحاول صياغة قناة اتصال آمنة في نموذج يلبي الخصائص الحقيقية المطلوبة للقناة (التشفير ، والتصديق والتوثيق). حيث يستخدم هذا النموذج هيكل TCP/IP كطبقة النقل الداخلية الذي من شأنه أن يضمن إيصال حزم البيانات إلى المستلم المقصود وحسب الترتيب.في هذه الورقة وصفنا بنية البروتوكول (VSSP) الموجود فوق طبقة TCP/IP حيث لها تأثير كبير إدارة التواصل عبر قناة الاتصال الآمنة.

1. Introduction
In order to provide useful services or to allow people to perform tasks more conveniently, computer systems are attached to networks and get interconnected and form the Internet that composed of thousands of hosts spread all over the world. When two hosts are communicating, the whole traffic between them passes through several other hosts from its source to its destination and are administrated by third parties which can view and/or alter the transferred packets. This is a serious problem and its significance increases when there is the need of transmitting confidential and important data. (Christopher,2005)
In order to solve it, a secure data channel can be used. A secure data channel can be seen as if it were a tunnel. The information is placed on one end of the tunnel and they can be read again only at the other end. It is needed to provide the connectivity and help to exchange information and services electronically and this will need to include access, authentication, authorization and confidentiality (Communication Security Crop.,2003).
In the reality, a special treatment is given to the data that will be transmitted so that they can neither be altered during their way (authentication), nor viewed (encryption). The combination of the two techniques produces invisible and unalterable data for any host met on the way of the packets, from the source to the destination. The suggested

algorithm makes use of TCP/IP as the fundamental transport layer which has a significant effect on connection. TCP/IP is in charge for ensuring sending data packets to the endpoint and assembled in the correct order when they arrive. This assumption removes a lot of overhead from our recommended sheltered channel. (Stephen, 2011)

2. Background and theory

2.1 What is a sheltered channel (applications and assets)

The safe channel is being established to provide the connectivity and underlying support services necessary to deliver information and services electronically, so it is used in the following applications (Kenny Paterson,2010):

1- Branch office connectivity.
2- Connecting to business partners at remote site.
3- Remote access for employees.
4- Remote administration of network devices and servers.
5- E-commerce: protecting credit card numbers in transactions.
6- Secure file transfers and others.

There is a common believe that the safe communication channel is meant by transferring encrypted data through it, but encryption in fact is an important property of this channel and the sheltered channel should have the following three assets:(Hideki I., SeongHan S., and Kazukuni K., 2009; Christopher D. and Gavin L.,2005)

1. Encryption (data shouldn't viewed by unauthorized parties)
2. Message validation (checksum for data going though channel)
3. Message authentication (data shouldn't altered and get by intended receiver)

2.2 Encryption

Cryptography is the study of "mathematical" systems involving two kinds of security problems: privacy and authentication. A privacy system prevents the extraction information by unauthorized parties from messages transmitted over a public channel, thus assuring the sender of a message that it is being read only by the intended recipient. An authentication system prevents the unauthorized injection of messages into a public channel,assuring the receiver of a message of the legitimacy of its sender (Roger M.,2003; Whitfield and Martin,1980).

In our paper we use asymmetric encryption (public key algorithm-RSA). It can be used both for encryption and for digital signatures. It's security is generally measured equivalent to factoring. (Chris,2009; Tom Davis, 2003)

2.2.1 Parameter generation

R1. Select two prime numbers p and q.

R2. Find n=p*q, Where n is the modulus that is made public. The length of n is considered as the RSA key length.

R3. Choose a random number 'e' as a public key in the range $0 < e < [(p-1)(q-1)]$ such that $\gcd(e,(p-1)(q-1))=1$.

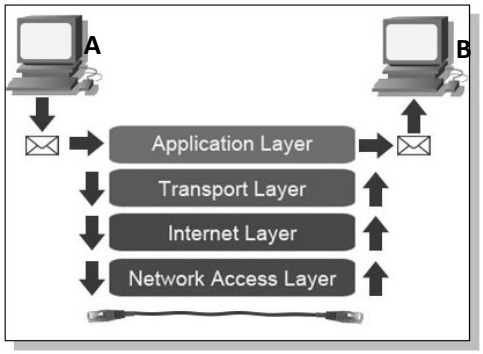
R4. Find private key d such that $ed \equiv 1 \pmod{(p-1)(q-1)}$.

2.2.2 Encryption

Consider A that needs to send a message to B securely.
R5. Let (e) be B's public key. Since e is public, A has access to e.
R6. To encrypt the message M, represent the message as an integer in the range 0<M<n.
R7. Cipher text C = Me mod n, where n is the modulus.

2.3 TCP/IP

Today, the Internet and World Wide Web (WWW) are familiar terms to millions of people all over the world. Many people depend on applications enabled by the Internet, such as electronic mail and Web access. In addition, the increase in popularity of business applications places additional emphasis on the Internet. The Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite is the engine for the Internet and networks worldwide. Its simplicity and power has led to its becoming the single network protocol of choice in the world today and the security architectures often make use of secure transport protocols to protect network messages: the transport protocols provide secure channels between two hosts A & B as in figure (1). (Christopher and Gavin,2005; Learn Network,2008)



Figure(1) TCP/IP Encapsulation

As with all other communications protocol, TCP/IP is composed of layers (Howard G., 1995**):**

- **IP** - is responsible for moving packet of data from node to node. IP forwards each packet based on a four byte destination address (the IP number). The Internet authorities assign ranges of numbers to different organizations. The organizations assign groups of their numbers to departments. IP operates on gateway machines that move data from department to organization to region and then around the world.
- **TCP** - is responsible for verifying the correct delivery of data from client to server. Data can be lost in the intermediate network. TCP adds support to detect errors or lost data and to trigger retransmission until the data is correctly and completely received.
- **Sockets -** is a name given to the package of subroutines that provide access to TCP/IP on most systems.

3. Method and Algorithm

The communication between two hosts takes place every time we log on to the Internet. Essentially, it's the process of sharing data from one location to many. The logical

connection between a client and a server can be able by three procedures as in figure (2): (Michael C. , Charles E, Matthew J. and Rob Rosenthal ,2005):

- **Handshake** - Where the client and the server agree on cryptographic algorithms that will be used, and authenticate each other.
- **Data transfer** - Where the real data is transferred, i.e., files, text, etc.
- **Closure** - Ending the connection in a secured manner

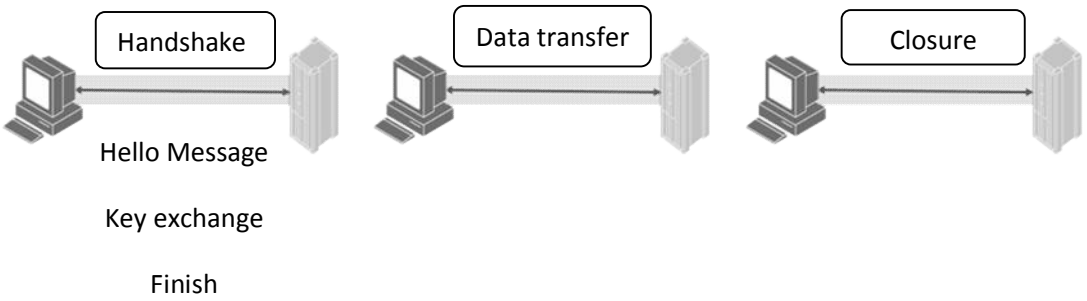


Figure (2) Phases of communication between Clint and Server

1. Algorithm1

1- **Assumptions**:

- as_k stands for asymmetric public key
- as_pk stand for asymmetric private key

2- A Initiate connection to B over TCP/IP

```
3- as_k = gets from B
4- k = create a random key
5- encrypted_key = as_encrypt (as_k, k)
6- send to B (encrypted_key)
7- e = encrypt (k, t)
8- d = digest (k, e)
9- m = e + d
10-   send to B (m)
```

11- B Initiate connection to A over TCP/IP

```
12- send to A (as_k)
13- encrypted_key = gets from A
14- k = as_decrypt(encrypted_key, as_pk)
15- (e, d) = m
16- if (digest (k,e)==d) then  t=decrypt(k,e)  else  error
```

In the above algorithms, the hypothesis is that encrypt, as_encrypt, decrypt, and as_decrypt are identified to both ends and they need to agree on a set of algorithms that will be used during the entire connection. We have to ensure that both the client and the server talk in the same language. The handshake phase assures that and the authentication occurs during the handshake.

3-1 Handshake:

1- **Hello**: the Hello Client message initiates the connection. It contains two parameters. The first is a random value (nonce) that is used as a seed to the Key Derivation Function (KDF). The second is a list of supported suite of cryptographic algorithms that will be used during a session that composed of four algorithms: asymmetric key algorithm, symmetric algorithm, digest algorithm, and a compression algorithm. When the server receives the Hello Client message and it accepts the connection, it replies with its own Hello Server message that contains three parameters. The first one is a random value (nonce) that has the same role as the random value that the client sends. The second is the chosen suite. The third parameter is a certificate. The certificate contains the public key that will be used during the key exchange, but it also allows the client to validate the server.

2- **Key exchange**: in this phase, the client encrypts a shared secret using the public key and sends it to the server.

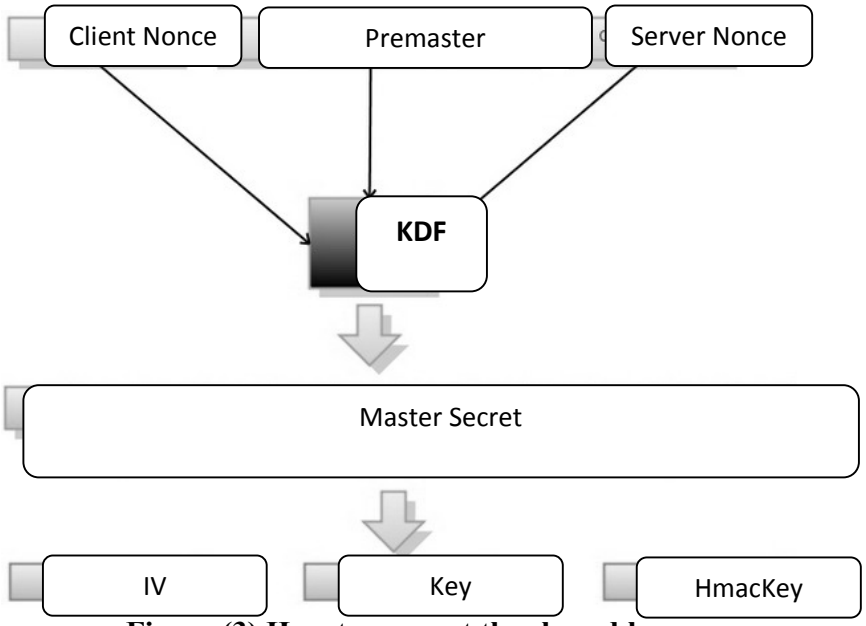


Figure (3) How to encrypt the shared key

2. <u>Algorithm2</u>

1- Create preMaster
2- keysalt = random server bits + random client bits
3- **masterKey** = prf(preMaster, salt)
4- send masterKey to server
5- **iv** = empty array
6- **key** = empty array
7- **hmackKey** = empty array
8- KDF (masterKey, iv, key, hmacKey)

The above algorithm describes steps to create the ultimate keys used to initialize the algorithms that were defined in the chosen suite.

preMaster is a long randomly generated array of bits

salt is a concatenation of the random values generated by the server and the client in phase 1.
prf (Pseudo Random Function) expands the preMaster into a new random value called the masterKey, and from it
The IV is the initialization vector used for symmetric encryption algorithms
hmacKey is the key used for HMAC digest algorithms
kdf (Key Derivation Function) takes the master key, and creates from it the various keys.

In VSSP, The server side does exactly the same except for the fact that it does not create the premaster key but receives it from the client.

3- **Closure**: in this phase the cryptographic algorithms are initialized. The messages were sent so it is quite useless to encrypt then, but it is perfectly reasonable to validate their integrity. In order to do so, we need to check if any of them where changed by an attacker. Both the client and the server save all the messages that they received and sent. They can run a digest algorithm (created in the last phase) on the sent messages and send it to the other side. The other side compares the digest that it received to the digest that it just calculated on the received messages. If the two digests are equal, then the entire process is valid, otherwise something interfered and there is a need to break the connection. After the handshake is done, the real data can now be sent.

3-2 Data transfer

Data is segmented into packets each has a header, payload, and a digest. The header consists of the following values:
VSSP magic number.
VSSP version – the version of the current protocol.
Message type - has several values that indicate what the content of the message is.
Data size – the size of the payload and the digest.
To transfer data, we use the following algorithms:

3. Algorithm 3

Send (t)

1. header = create_header (t)
2. comp = compress (t)
3. e = encrypt (comp, k)
4. d = digest (k, header + e + sent_counter)
5. m = header + e + d
6. sent_counter++
7. tcpSend (m)

Receive (m)

1. header = extract_header (m)
2. if header is valid goto (3) else goto (8)
3. receive_counter++
4. (k, d) = m
5. if (digest (k, header + e + receive_counter) == d) goto (6) else error
6. comp = decrypt (k, e)
7. t = decompress (comp) goto (9)
8. Error
9. End

We compress the data in order to reduce the total size of the packet transferred and individually the client and the server must keep follow of send and receive counters. So, at any time a message is received/sent, the receive/send counter is increased by 1.

1.3 Closure

This message is sent by either client or server to indicate the finalization of the session.

4. Conclusion

The primary aspire of our paper is to underline several challenges in the design, implementation and of secure channel protocols. We have examined a secure channel specifications and illustrated them

But we have not proven that the implementations are correct and there are other properties (e.g. recentness, non-repudiation). We often want to guarantee the confidentiality and integrity of data travelling over un trusted networks. The encryption used by VSSP provides confidentiality and integrity of data over an insecure network, such as the Internet.

References

Chris L., 2009, "Secure Channel Communication", http://www.lomont.org .

Christopher K., 2005, "Internet Security", Automation Systems Group, Technical University Vienna.

Christopher D. and Gavin L., 2005, " On the Specification of Secure Channel ", Oxford University Computing Laboratory, UK.

Communications Security Corp.,2003," SSH Secure Shell for Workstations Windows Client version 3.2.9 User Manual, SSH Communications Security Inc, USA.

Hideki I., SeongHan S., and Kazukuni K., 2009, "New Security Layer for OverLay Networks", Journal of Communications and Networks, vol. 11, No. 3.

Howard Gilbert, 1995, "Introduction to TCP/IP"

Kenny Paterson,2010," Cryptography for Secure Channels", Information Security Group Royal Holloway, University of London.

Learn Networking, 2008, " How Encapsulation Works Within the TCP/IP Model".

Michael C., Charles E., Matthew J. and Rob Rosenthal, 2005, "Computer Security", US Department of Commerce.

Roger M. Needham, 2003, "Cryptography and Secure Channels", Huygens Systems Research Laboratory

Stephen B. Cooper, 2011, “How SSL Provides Security to TCP/IP",

Tom Davis, 2000, " RSA Encryption", http://www.geometer.org/mathcircles.

Whitfield D. and Martin E. Hellman, 1980,"New Directions in Cryptography".