ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 3, pp: (239-243), Month: July - September 2015, Available at: www.researchpublish.com

Strong Encryption for Public Key Management through SSL

CH.SUSHMA, D.NAVANEETHA

[1,2]Assistant Professor, Information Technology, Bhoj Reddy Engineering College For Women, Hyderabad, India

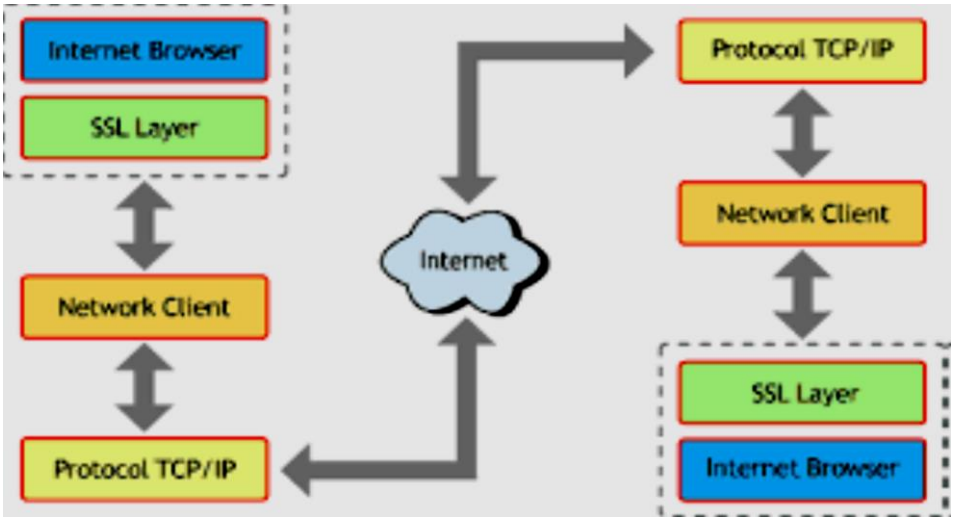
Abstract: **Public-key cryptography and related standards and techniques underlie the security features of many products such as signed and encrypted email, single sign-on, and Secure Sockets Layer (SSL) communications. This document introduces the basic concepts of public-key cryptography. SSL (Secure Sockets Layers) is a process that manages the security of transactions made on the Internet. It is based on a public-key encryption process to guarantee that data sent over the Internet remain secure. Its principle involves establishing a secure (encrypted) communication channel between two machines (a client and a server) after an authentication phase.**

Keywords: **public key, SSL, Secure Communication.**

I. INTRODUCTION

Public-key cryptography is used for protecting communications from eavesdropping, tampering, and impersonation attacks. Encryption and decryption allow two communicating parties to disguise information they send to each other.

The sender encrypts, or scrambles, information before sending it. The receiver decrypts, or unscrambles, the information after receiving it. While in transit, the encrypted information is unintelligible to an intruder. Tamper detection allows the recipient of information to verify that it has not been modified in transit. Any attempt to modify data or substitute a false message for a legitimate one will be detected. Authentication allows the recipient of information to determine its origin- that is, to confirm the sender's identity. Non-repudiation prevents the sender of information from claiming at a later date that the information was never sent. A certificate is an electronic document used to identify an individual, a server, a company, or some other entity and to associate that identity with a public key. Public-key cryptography uses certificates to address the problem of impersonation.



1. SSL Protocol diagram

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 3, pp: (239-243), Month: July - September 2015, Available at: www.researchpublish.com

Public-key refers to a cryptographic mechanism. It has been named public-key to differentiate it from the traditional and More intuitive cryptographic mechanism known as: symmetric-key, shared secret, secret-key and also called private-key. Symmetric-key cryptography is a mechanism by which the same key is used for both encrypting and decrypting; it is more intuitive because of its similarity with what you expect to use for locking and unlocking a door: the same key.

1. The characteristic requires:

Sophisticated mechanisms to securely distribute the secret-key to both parties Public-key on the other hand, introduce another concept involving key pairs: one for encrypting, the other for decrypting. This concept, as you will see below, is very clever and attractive, and provides a great deal of advantages over symmetric-key:

• Simplified key distribution

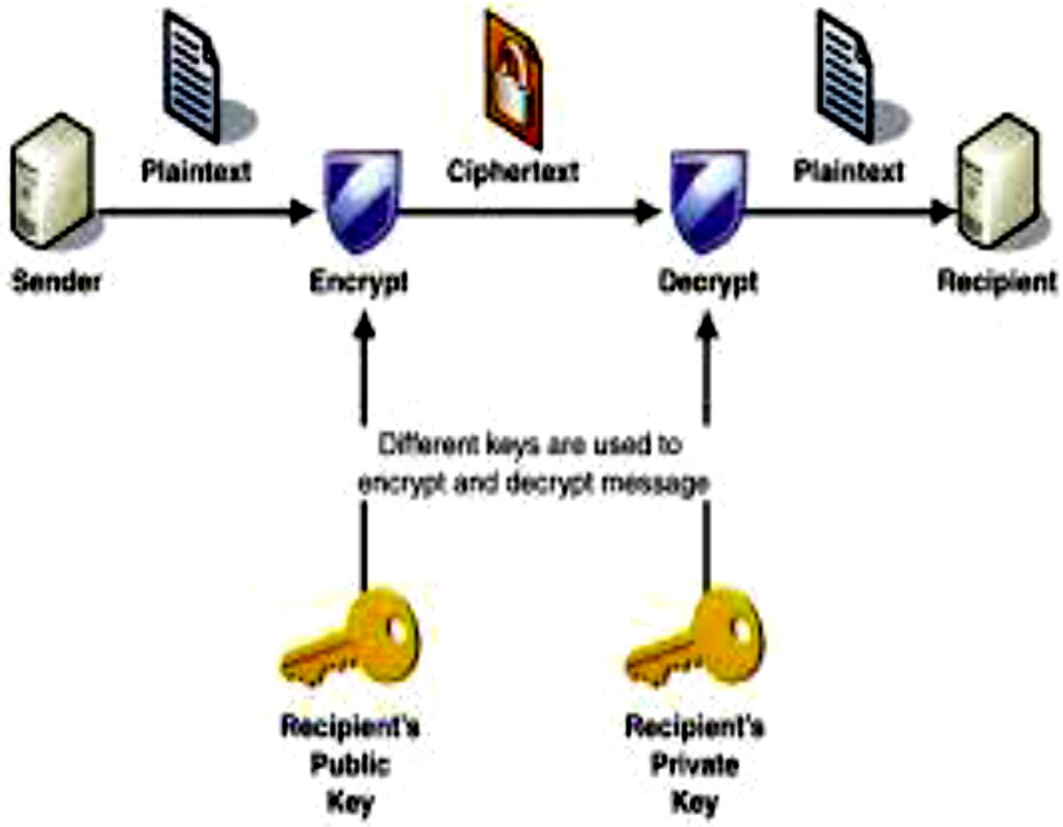
• Digital Signature

• Long-term encryption

However, it is important to note that symmetric-key still plays a major role in the implementation of a Public-key Infrastructure.

2. PKI (Public-key Infrastructure):

Public-key encryption uses that key pair for encryption and decryption. The public-key is made public and is distributed widely and freely. The private-key is never distributed and must be kept secret. Given a key pair, data encrypted with the public-key can only be decrypted with its private- key. Conversely, data encrypted with the private-key can only be decrypted with its public- key. This characteristic is used to implement encryption and digital signature Encryption is a mechanism by which a message is transformed so that only the sender and recipient can see. For instance, suppose that Alice wants to send a private message to Bob. To do so, she first needs Bob's public-key; since everybody can see his public-key, Bob can send it over the network in the clear without any concerns. Once Alice has Bob's public-key, she encrypts the message using Bob's public-key and sends it to Bob. Bob receives Alice' message and using his private key, decrypts it.



2. Figure encryption and decryption

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 3, pp: (239-243), Month: July - September 2015, Available at: www.researchpublish.com

II. HISTORY OF SSL

A. SSL PROTOCOL:

The Secure Sockets Layer (SSL) protocol is a set of rules governing server authentication, client authentication, and encrypted communication between servers and clients. SSL is widely used on the Internet, especially for interactions that involve exchanging confidential information such as credit card numbers. SSL requires a server SSL certificate, at a minimum. As part of the initial "handshake" process, the server presents its certificate to the client to authenticate the server's identity. The authentication process uses public-key encryption and digital signatures to confirm that the server is in fact the server it claims to be. Once the server has been authenticated, the client and server use techniques of symmetric-key encryption, which is very fast, to encrypt all the information they exchange for the remainder of the session and to detect any tampering that may have occurred.

Servers may optionally be configured to require client authentication as well as server authentication. In this case, after server authentication is successfully completed, the client must also present its certificate to the server to authenticate the client's identity before the encrypted SSL session can be established. SSL allows sensitive information such as credit card numbers, social security numbers, and login credentials to be transmitted securely. Normally, data sent between browsers and web servers is sent in plain text—leaving you vulnerable to eavesdropping. If an attacker is able to intercept all data being sent between a browser and a web server they can see and use that information.

B. TYPES OF CERTIFICATE:

1. Signed and Encrypted Email:

Some email programs support digitally signed and encrypted email using a widely accepted protocol known as Secure Multipurpose Internet Mail Extension (S/MIME). Using S/MIME to sign or encrypt email messages requires the sender of the message to have an S/MIME certificate. An email message that includes a digital signature provides some assurance that it was in fact sent by the person whose name appears in the message header, thus providing authentication of the sender. If the digital signature cannot be validated by the email software on the receiving end, the user will be alerted.

The digital signature is unique to the message it accompanies. If the message received differs in any way from the message that was sent-even by the addition or deletion of a comma-the digital signature cannot be validated. Therefore, signed email also provides some assurance that the email has not been tampered with. As discussed at the beginning of this document, this kind of assurance is known as non-repudiation. In other words, signed email makes it very difficult for the sender to deny having sent the message. This is important for many forms of business communication. (For information about the way digital signatures work, see "Digital Signatures".)S/MIME also makes it possible to encrypt email messages. This is also important for some business users. However, using encryption for email requires careful planning. If the recipient of encrypted email messages loses his or her private key and does not have access to a backup copy of the key, for example, the encrypted messages can never be decrypted.

2. Single Sign-On:

Network users are frequently required to remember multiple passwords for the various services they use. For example, a user might have to type a different password to log into the network, collect email, use directory services, use the corporate calendar program, and access various servers. Multiple passwords are an ongoing headache for both users and system administrators. Users have difficulty keeping track of different passwords, tend to choose poor ones, and tend to write them down in obvious places. Administrators must keep track of a separate password database on each server and deal with potential security problems related to the fact that passwords are sent over the network routinely and frequently. Solving this problem requires some way for a user to log in once, using a single password, and get authenticated access to all network resources that user is authorized to use-without sending any passwords over the network. This capability is known as single sign-on. Both client SSL certificates and S/MIME certificates can play a significant role in a comprehensive single sign-on solution. For example, one form of single sign-on relies on SSL client authentication (see "Certificate-Based Authentication"). A user can log in once, using a single password to the local client's private-key database, and get authenticated access to all SSL-enabled servers that user is authorized to use without sending any passwords over the network. This approach simplifies access for users, because they don't need to enter passwords for each new server. It also simplifies network management, since administrators can control access by controlling lists of certificate authorities (CAs) rather than much longer lists of users and passwords.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 3, pp: (239-243), Month: July - September 2015, Available at: www.researchpublish.com

In addition to using certificates, a complete single-sign on solution must address the need to interoperate with enterprise systems, such as the underlying operating system, that rely on passwords or other forms of authentication.

3. Object Signing:

Communicator supports a set of tools and technologies called object signing. Object signing uses standard techniques of public-key cryptography to let users get reliable information about code they download in much the same way they can get reliable information about shrink-wrapped software. Most importantly, object signing helps users and network administrators implement decisions about software distributed over intranets or the Internet-for example, whether to allow Java applets signed by a given entity to use specific computer capabilities on specific users' machines. The "objects" signed with object signing technology can be applets or other Java code, JavaScript scripts, plug-ins, or any kind of file. The "signature" is a digital signature. Signed objects and their signatures are typically stored in a special file called a JAR file. Software developers and others who wish to sign files using object-signing technology must first obtain an object-signing certificate.

III. FUTURE WORK

1. Client SSL certificates:

Used to identify clients to servers via SSL (client authentication). Typically, the identity of the client is assumed to be the same as the identity of a human being, such as an employee in an enterprise. See "Certificate-Based Authentication" for a description of the way client SSL certificates are used for client authentication. Client SSL certificates can also be used as part of a single sign-on solution.

2. Server SSL certificates:

Used to identify servers to clients via SSL (server authentication). Server authentication may be used with or without client authentication. Server authentication is a requirement for an encrypted SSL session.

3. S/MIME certificates:

Used for signed and encrypted email. As with client SSL certificates, the identity of the client is typically assumed to be the same as the identity of a human being, such as an employee in an enterprise. A single certificate may be used as both an S/MIME certificate and an SSL certificate (see "Signed and Encrypted Email"). S/MIME certificates can also be used as part of a single sign-on solution.

4. Object-signing certificates:

Used to identify signers of Java code, JavaScript scripts, or other signed files.

3. SSL Certificate diagram

IV. CONCLUSION

The contents of certificates are organized according to the X.509 v3 certificate specification, which has been recommended by the International Telecommunications Union (ITU).Certificate requests and certificates can be created, stored, and installed in multiple formats: binary and text. All of these formats conform to X.509 standards.

REFERENCES

[1] Adams, C., and Farrell, S. (1999). Internet X.509 Public Key Infrastructure Certificate Management Protocols. IETF RFC 2510. http://www.ietf.org/

[2] IEEE 1363-2000. Standards specification for public key cryptography. IEEE Press.

[3] L. Rivest, A. Shamir, and L. Adleman."Method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM 21 (1978), 120-126.

[4] T.Elgamal, "A public key cryptosystem and a signature protocol based on discrete logarithms", IEEE Trans.