Applied cryptography for Secure Communication

P.A Daham Thameera
(IT20077624)
Sri Lanka Institute of Information Technology
Department of Computer Systems Engineering
Malabe, Sri Lanka
it20077624@my.sliit.lk

Wijesingha W.M.P.M
(IT20023614)
Sri Lanka Institute of Information Technology
Department of Computer Systems Engineering
Malabe, Sri Lanka
it20023614@my.sliit.lk

K.N Dilshan
(IT20021870)
Sri Lanka Institute of Information Technology
Department of Computer Systems Engineering
Malabe, Sri Lanka
it20021870@my.sliit.lk

Abeywickrama O.D
(IT20153540)
Sri Lanka Institute of Information Technology
Department of Computer Systems Engineering
Malabe, Sri Lanka
it20153540@my.sliit.lk

***Abstract* — Using cryptography to encrypt and decode data as it travels across a network is an important step in keeping sensitive data safe. Keys, hash functions, and secret and public keys are all used in cryptography's implementation in a secure network environment to guarantee the four aforementioned properties of data: secrecy, integrity, authentication, and irrefutability. However, securing communications to avoid eavesdropping, interruption, alteration, or fabrication on network systems has proven difficult to implement. Network systems are being breached using a wide variety of methods and techniques, including the use of digital signatures, virtual private networks, and others. As a result, it is now crucial to think about using cryptography-based approaches to ensure safe and reliable data transmission and processing. This study delves into the use of cryptographic principles in information and network systems security for the purposes of thwarting cyberattacks and bolstering the privacy of online communication. Cryptography has many applications, ranging from protecting online accounts and passwords to protecting sensitive military communications.**

Keywords — Cryptography, Encryption, SSL/TLS, Communication, Hashing, Integrity, Authentication

I. Introduction

The field of study known as cryptography focuses on the development of secure communication methods that restrict access to a message's contents to its intended sender and receiver. It is strongly linked to encryption, the transformation of plaintext into ciphertext and its subsequent decipherment. In addition, cryptography encompasses picture obfuscation using methods like microdots or merging. Email and other forms of plain-text communication are the most prevalent targets of cryptographic manipulation during electronic data transmission. Symmetric systems, sometimes called "secret key" systems, are the simplest kind of encryption [1].

In this case, data is encrypted with a secret key, and then both the encoded message and the key are given to the receiver. What's wrong? A third party that intercepts the message will have all the tools at their disposal to decode it and read its contents. The asymmetric or "public key" scheme was developed by cryptologists as a solution to this problem. Each user in this system has both a public and private key. Messages are encrypted using the recipient's public key that is requested by the sender [2]. As the communication will be unreadable without the private key, stealing is useless.

To prevent information from being intercepted or modified without authorization, mathematic functions are used in applied cryptography. Cryptographic technologies are used by nearly every computing and communications equipment to ensure the security and privacy of all data transmitted and stored. However, cryptographic security is only as reliable as its weakest component [3]. Data secrecy, data integrity, authentication, and non-repudiation are some of the goals of applied cryptography, which makes use of a secret key, public key, and hash functions.

The ideas take into account encrypting and decrypting plaintext as well as ciphertext. You may use digital signatures using the RSA security protocol, which includes PGP for email security, SSL/TSL for web application security, IPSec/IKE for IP data security, SILC for conferencing services security, and SSH for terminal connection security .

II. SSL / TLS Encryption

A. What is SSL/TLS Encryption?

SSL/TLS encrypts communications between a client and server, primarily web browsers and web sites/applications. Data delivered over the internet, or a computer network may be encrypted using either SSL (Secure Sockets Layer) or TLS (Transport Layer Security). By doing so, sensitive information sent between two endpoints (such a user's browser and a web/app server) is protected from prying eyes and alteration by ISPs and other malicious parties. To safeguard the transmission of sensitive data like passwords, payment information, and other personal information deemed private, most website owners and administrators are required to adopt SSL/TLS.

To encrypt and decode data exchanged between a server and a client—typically a website and a browser or a mail server and a mail client like Microsoft Outlook—SSL Cryptography employs public key cryptography, which needs asymmetric keys [4]. In short, SSL is a fantastic protocol. It's

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE

useful if you know how to use it, but it's also simple to use, like many tools. Although they are easily avoidable with preparation, many people make common mistakes when adopting SSL.

B. History of TLS/SSL

The Secure Socket Layer (SSL) protocol's most recent version is Transport Layer Security (TLS). Both methods are critical for protecting data privacy and authenticity when transmitting data over the internet. These commonly used protocols enable end-to-end security for web-based communication by utilizing encryption. TLS and SSL have many commonalities, but they also have important differences as well.

Due to security vulnerabilities, SSL 1.0 was never deployed, and SSL 2.0 was the first public release by Netscape in 1995. However, due to security flaws and limitations, it was superseded in November 1996 by another SSL version 3.0. The most recent SSL version is likewise no longer in use due to its vulnerability to the POODLE exploit in October 2014, and it was formally deprecated in June 2015 [1].

TLS was introduced in 1999 as an application-independent protocol, as an improvement to SSL 3.0 by the Internet Engineering Task Force (IETF). The plan was to use TLS over TCP to encrypt programs that used the FTP, IMAP, SMTP, and HTTP protocols [1]. Basically, the idea was to implement TLS to secure data transformation by preventing content modifications and eavesdropping. TLS contains major four versions v1.0, v1.1, v1.2 and v1.3 is the latest and stable version.

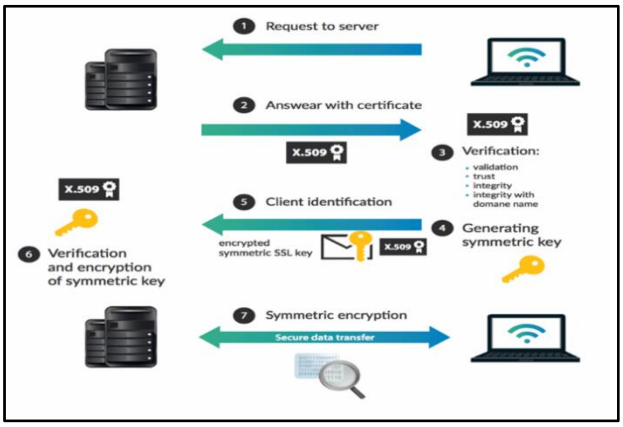
C. How do asymmetric and symmetric encryption work together in TLS/SSL?

Create, administer, distribute, use, store, and revoke digital certificates with the help of a PKI, which consists of the necessary hardware, software, personnel, rules, and processes. In addition, PKI is responsible for associating user keys with their respective identities through a Certificate Authority (CA). In order to get the advantages of both forms of encryption, PKI employs a hybrid crypto system [5]. As an example, an asymmetric public/private key pair is included in the TLS certificate used by the server in TLS/SSL connections. A symmetric session key is generated by the server and the browser during the SSL Handshake.

Using cryptographic algorithms securely and reliably is tough. Cryptographic protocols are notoriously tough to get correctly, and algorithms are only building blocks. Cryptographers and developers struggle to create protocols that withstand all known assaults. Developers aim to safeguard network connections by encrypting and decrypting data before transferring it. This method seldom ensures data integrity. Attackers may occasionally retrieve tampered data. Implementation problems occur even with well-designed protocols [6]. Most cryptographic protocols are constrained, like online voting. Protocols for communicating safely across an unsafe medium are universal. SSL and TLS give standard security services to arbitrary (TCP-based) network connections with no cryptographic understanding.

D. TLS/SSL Handshake

When you visit a website, an invisible procedure known as the "TLS/SSL handshake" establishes a secure connection between your web server and web browser very instantly. TLS/SSL-secured websites will display HTTPS and the little padlock icon in the browser address bar. TLS/SSL certificates are used to safeguard end users' information during transmission as well as to validate the website's organization identification to guarantee users are dealing with legitimate website owners [2].



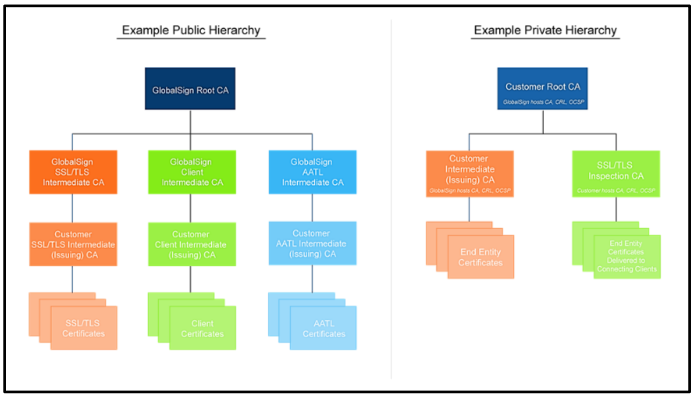
1 Request to server
2 Answear with certificate
X.509
X.509
3 Verification:
- validation
- trust
- integrity
- integrity with domane name
X.509
5 Client identification
4 Generating symmetric key
encrypted symmetric SSL key
X.509
6 Verification and encryption of symmetric key
7 Symmetric encryption
Secure data transfer

Figure 1 : TLS/SSL Handshake

III. TLS/SSL CERTIFICATES

TLS certificates, often known as SSL or digital certificates, are essential to ensuring a secure online experience. When you visit a website, the information sent between your browser and the server of that site is encrypted using a Transport Layer Security (TLS) or Secure Sockets Layer (SSL) certificate. They guarantee that data is sent discreetly and without alterations, loss or theft [7].

All major web browsers employ TLS/SSL certificates to protect users online. Internet consumers trust TLS/SSL-secured websites more because they encrypt and safeguard private data. They certify your website's brand. TLS/SSL certificates safeguard online brands' identities and secure online data transmissions.



Example Public Hierarchy
GlobalSign Root CA
GlobalSign SSL/TLS Intermediate CA
GlobalSign Client Intermediate CA
GlobalSign AATL Intermediate CA
Customer SSL/TLS Intermediate (Issuing) CA
Customer Client Intermediate (Issuing) CA
Customer AATL Intermediate (Issuing) CA
SSL/TLS Certificates
Client Certificates
AATL Certificates
Example Private Hierarchy
Customer Root CA
GlobalSign hosts CA, CRL, OCSP
Customer Intermediate (Issuing) CA
GlobalSign hosts CA, CRL, OCSP
SSL/TLS Inspection CA
Customer hosts CA, CRL, OCSP
End Entity Certificates
End Entity Certificates Delivered to Connecting Clients

Figure 2 : TLS/SSL Certificate Hierarchy

IV. USAGE OF SSL/TLS

Whether you need to use TLS/SSL depends on your organization's operations. For organizations involved in health services or payment processing, using a security protocol such as TLS/SSL to encrypt network communications may be a federal or commercial requirement. If the organization keeps personal user information but does not transmit health or financial information, you should still utilize security measures such as TLS/SSL. Encryption might help human rights and justice organizations protect the information, and possibly the identity, of the individuals they serve. Though these precautions would not be mandated by the federal government or a commercial company, they might help to guarantee that security breaches do not jeopardize an organization's objective [3].

- **Secure online Transactions and Card Details**

Implementing TLS/SSL may be a requirement of the Payment Card Industry Data Security Standard for firms that store or handle payment information, such as donor credit card numbers (PCI DSS). The PCI Security Standards Council, a collaboration of many major payment card manufacturers, developed this standard to secure cardholder data. Organizations may be obliged by their acquiring bank or payment processor to comply with the PCI DSS.

- **Protect Electronic health records**

Using security precautions such as TLS/SSL in health services may be a federal mandate. The Health Insurance Portability and Accountability Act (HIPAA) applies to any entity that transmits electronic billing information to any health insurance provider, Medicare, or Medicaid and must fulfill specified security criteria [4]. Furthermore, even if a company is not legally a covered entity, it may be required to comply with the HIPAA Security Standard if it maintains or transmits user login or patient information. It is critical to understand that while security methods like TLS/SSL can assist a company in becoming HIPAA compliant, they do not offer compliance on their own.

- **Securing a Directory Servers, Web Servers, Mail Servers or Database Servers**

Securing the web servers is the most prevalent application of TLS/SSL. That may encrypt online transactions and private data transferred between a user's web browser and a website when used in conjunction with a web server. A secure web server is distinguished by a padlock icon at the bottom of the browser window or in the address bar, as well as a URL that begins with "https" rather than "http."

TLS/SSL can be used to encrypt email messages on mail servers. When an email is sent with TLS/SSL encryption, the recipient's email client may display a ribbon or other symbol. TLS/SSL may also be used to encrypt server queries on database and directory servers.

- **Securing a Virtual Private Network (VPN)**

Secure Sockets Layer (SSL) VPN is a new technology that gives remote-access VPN functionality by utilizing the SSL function incorporated into most recent web browsers. SSL VPN enables users to start a web browser from any Internet-enabled location to establish remote-access VPN connections, offering increased productivity and availability as well as significant IT cost savings for VPN client software and maintenance [5].

V. CONCLUSION

ACKNOWLEDGMENT

Thank you, especially, to our Cryptography Lecture In Charge, Mr. Kavinga Yapa Abeywardena, for his invaluable mentorship and technical assistance, which inspired us to finish our task. Furthermore, we'd want to take this opportunity to thank our cybersecurity classmates for their invaluable criticism and assistance during this mini research project.

REFERENCES

[1] "Real Life Applications of CRYPTOGRAPHY | by Prashanth_Reddy | Medium." https://medium.com/@prashanthreddyt1234/real-life-applications-of-cryptography-162ddf2e917d (accessed Oct. 11, 2022).

[2] "Applied Cryptography | NCCoE." https://www.nccoe.nist.gov/applied-cryptography (accessed Oct. 11, 2022).

[3] A. Yeboah-Ofori, C. K. Agbodza, F. A. Opoku-Boateng, I. Darvishi, and F. Sbai, "Applied Cryptography in Network Systems Security for Cyberattack Prevention," *Proc. - 2021 Int. Conf. Cyber Secur. Internet Things, ICSIoT 2021*, pp. 43–48, 2021, doi: 10.1109/ICSIOT55070.2021.00017.

[4] "What is SSL Cryptography? | DigiCert FAQ." https://www.digicert.com/support/resources/faq/cryptography/what-is-ssl-cryptography (accessed Oct. 11, 2022).

[5] H. Krawczyk, "The Order of Encryption and Authentication for Protecting Communications (or: How Secure Is SSL?)."

[6] "SSL | SSL/TLS Protocol | SSL Certificates | TLS Certificates." https://www.appviewx.com/education-center/what-is-tls-ssl-protocol/ (accessed Oct. 11, 2022).

[7] "What is SSL, TLS and HTTPS? | DigiCert." https://www.websecurity.digicert.com/security-topics/what-is-ssl-tls-https (accessed Oct. 11, 2022).