Computer Network Security

Lesson 9

Network & Internet Security

Lecturer: Dr Msagha J Mbogholi, PhD

Flashback from Lesson 8

- Steganography is not cryptographic in nature *per se.* It is the science of hiding a message within another message.
- Data integrity algorithms purpose to preserve the integrity of data by ensuring mechanisms that confirm it has not been modified in any way whatsoever.
- Hash functions work on data by producing message digests which are then compared at the receiver's end to confirm the integrity of the data.
- Message authentication codes (MAC) combine authentication with data integrity by introducing a symmetric key in the mechanism.
- Digital signatures enforce authentication and non-repudiation by using the sender's private key at the sender's end and his/her public key at the recipient's end.

Content

- Transport Level Security
- Wireless Security
- E-mail Security
- Internet Protocol Security

Part 1

Transport Level Security

Introduction

- Recall from your networking knowledge the OSI and TCP/IP model?
- While a detailed review is not within the scope of this course just a few points to remind you of some of the working is important in order to understand how it relates to this part.
- The OSI model has 7 layers: Application, Presentation, Session, Transport, Network, Datalink, and Physical.
- The classical TCP/IP model has 4 layers: Application, Transport, Internet and Network Interface. In other literature the Network Interface layer is split into 2 resulting in a 5 layer TCP/IP model.

Introduction (cont'd)

- Each layer uses the services of the layer beneath it. Our interest is more in the TCP/IP model which shows where different protocols are placed and what role they play.
- In this model layer 4 uses the services of layer 3, while layer 3 uses the services of layer 2, and layer 2 uses the services of layer 1.
- Over the Internet transport level security is about how different security services protect the transmission of data between a browser and web server.
- Most of these services will center around TCP/IP which is the universal protocol of the Internet. This protocol enables different hardware and applications to communicate over the Internet, hence its importance.
- TCP is found in the transport layer while IP is found in the Internet layer of the TCP/IP model. However, the TCP/IP protocol suite consists of many protocols that enable communication over the Internet.

1. Secure Sockets Layer (SSL)

- SSL was first developed by Netscape. There are 3 versions that were developed, 1.0, 2.0 and 3.0
- SSL works between the Application and Transport layers of the TCP/IP model. Figure 1 shows its place in the model. Since every layers uses the services of the layer below it, the application layer passes data to SSL which then provides 2 key security functions: confidentiality and authenticity. The figure also shows that SSL provides by a 'tunnel' between two communicating devices on the Internet.
- As the Internet mostly runs on a client-server architecture most of SSL's operations occur between a web server and a web client browser.

SSL & TCP/IP Model

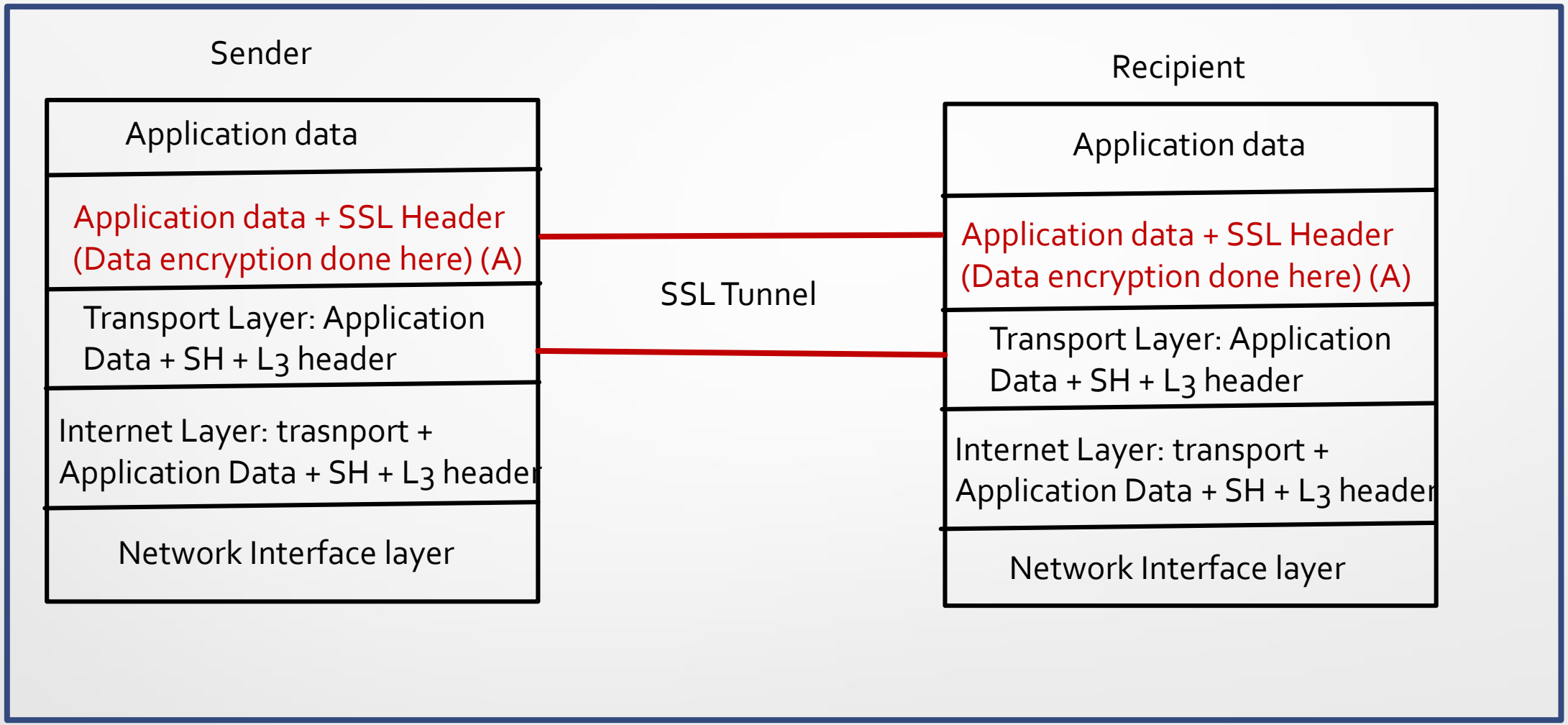


Fig 1. SSL and TCP/IP model relationship

Working of SSL

- SSL has within it 3 sub-protocols which constitute its overall working.
- Figure 2 shows how these protocols are related. An explanation of their workings follows

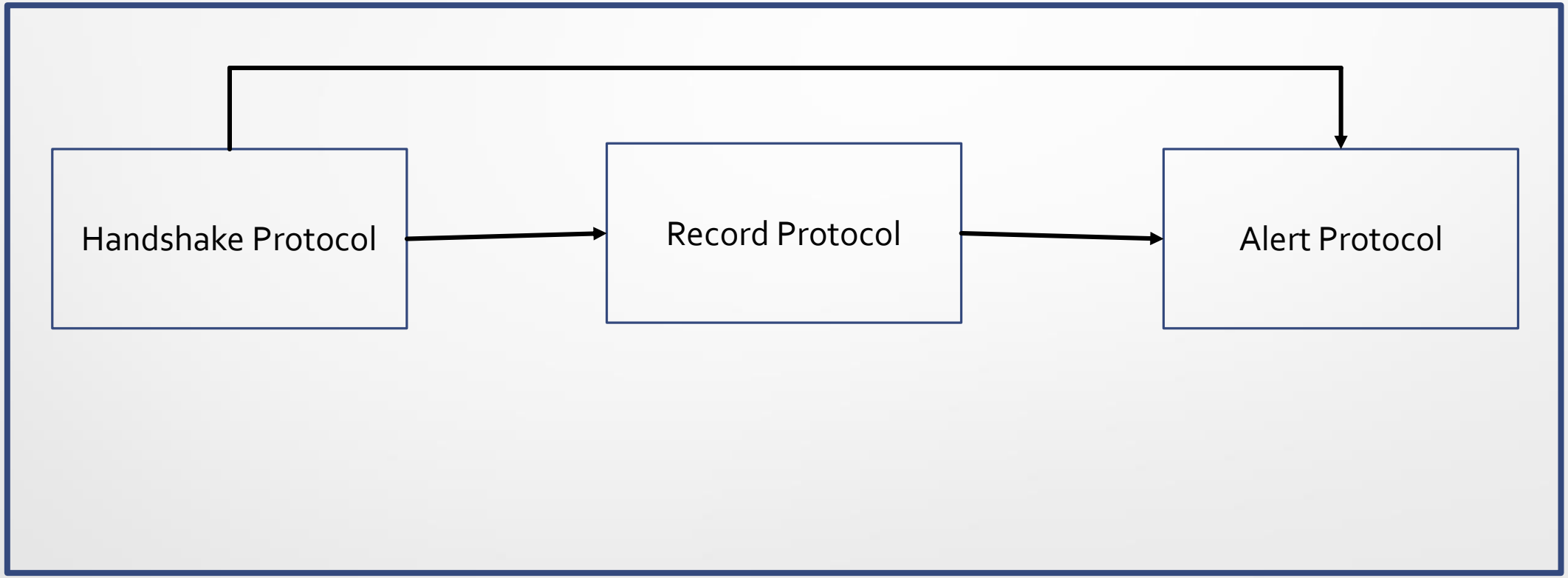


Fig 2. SSL Sub-protocols

Handshake Protocol

- When you meet someone you would normally start by offering a handshake (well probably not in these Covid 19 times, but this is the norm) followed by a polite hello. Do you know that when meeting a person for the first time it is the first 10 seconds that make you subconsciously decide whether you like the person or not? (Story for another day!)
- In the same manner the handshake sub protocol is the one that is used to initiate conversation between client and server. It is the computers' way of handshaking and saying hello to each other.
- It consists of a series of messages between the client and the server.

Handshake Protocol (cont'd)

- The handshake message has 3 fields and each field serves a special purpose:
- First field – type of message; second field – length of the message; third field – message parameters (dependent on message type)
- The handshake itself constitutes four steps:
- Step 1: Security capabilities – this is an exchange between client and server establishing the security parameters either is capable of using; this includes the compression algorithm to be used in the communication.
- Step 2: Server key exchange – the server sends its digital certificate (or public key) (so client can authenticate it). Optionally it may also ask for the client's digital certificate.

Handshake Protocol (cont'd)

- Step 3: Client key exchange – the steps here are similar only that are performed by the client. To note is that the client will create its key (called premaster secret) which it encrypts with the server's public key and sends this back to the server. If the server had asked for the client's digital certificate then the latter will do so by digitally signing random numbers exchanged in step 2 and sending back to the server.
- Step 4: Finished – a change cipher spec message is initiated by the client and sent to the server; the server responds with the same message. This is an indication that the remaining communication will be encrypted. Lastly a finished message is sent by both server and client; this is the first encrypted message between them.
- A master secret is now created using the premaster and random numbers generated by both server and client. These 3 (premaster + server random + client random) then have their message digests computed, and this produces the master secret. It is used to generate the secret keys (also used in MAC calculations)
- The master secret together with server random and client random again have their message digests computed and this is what produces the symmetric key used for the session (session key)

Record Protocol

- This is the second sub-protocol. It comes into play after a successful handshake (in the handshake protocol)
- The working of the record protocol is focused on (A) in fig. 1.
- Since SSL uses both encryption and MAC then their properties are also provided; thus confidentiality and integrity are provided respectively.
- From the explanation in fig. 1 the application data is passed from application layer to SSL. The record protocol breaks down the data into blocks (fragments), compresses each block, encrypts it, adds its header (SSL header in fig. 1) and passes it to the layer below it (transport layer). At the recipient end the process is reversed.

Alert Protocol

- This protocol deals with errors detected by either party.
- It contains two fields: the first field indicates the severity of the error (warning or fatal) while the second field gives an explanation of the error.
- A list of these codes can be found at https://techcommunity.microsoft.com/t5/iis-support-blog/ssl-tls-alert-protocol-and-the-alert-codes/ba-p/377132

2. Transport Layer Security (TLS)

- TLS is an advanced version of SSL.
- It was developed to be the Internet standard of SSL. SSL's developers gave the standard to IETF to develop the standard.
- It is defined in RFC 5246. The current version is TLS 1.3 (defined in 2018)
- There are some differences, however, between TLS and SSL.
- These differences are summarized well in table 1 from Kahate (2013, pg. 282). However, his comparison is limited to TLS 1.0 only.
- Another comparison can also be found at https://alldifferences.net/difference-between-ssl-and-tls/

3. Secure Shell (SSH)

- Secure shell (SSH) protocol is defined in RFCs 4251 -3. It is a protocol that was designed to replaced remote login protocols like telnet and rlogin which were deemed to be insecure.
- SSH also replaces file transfer protocols as it is more secure than most of them.
- It provides authentication, confidentiality and integrity of data.
- Versions include SSH 1 and SSH2; SSH 1.99 was released in 2006 to provide backward compatibility between SSH1 and SSH2.
- There is also the open source version of SSH called openSSH (current version as the time of this writing is 8.8)
- SSH normally refers to both the protocol and utilities that use it.

Working of SSH

- Just like SSL, SSH (version 2) has three sub-protocols.
- These three sub-protocols establish the security of SSH (integrity, confidentiality and authenticity)
- The three sub-protocols are SSH-TRANS, SSH-AUTH, and SSH-CONN. Each plays a role in establishing and maintaining the connection.
- Let us examine how they work together to do this.

SSH - TRANS

- It is the transport layer protocol component of SSH.
- RFC 4251 defines it as "provides server authentication, confidentiality, and integrity. It may optionally also provide compression. The transport layer will typically be run over a TCP/IP connection, but might also be used on top of any other reliable data stream."
- This the component that sets up the communication channel by encrypting all sessions (in a manner very similar to SSL) and providing integrity using MACs. It also negotiates the encryption algorithm to be used.

SSH - AUTH

- It is the second sub-protocol.
- It runs over SSH-TRANS. It is the second phase of the process whereby user logs in and authenticates themselves.
- RFC 4251 defines it as being used for "authenticates the client-side user to the server"
- The user may authenticate himself to the server using either password, public key encryption or host based authentication. Host based authentication uses trust in that once a host has been placed in the list of trusted hosts the server will assume it is the same user using it. However, the client host must authenticate himself the first time they connect since it's only server authentication that's done by default by the transport layer protocol (SSH-TRANS).
- A popular SSH client in use nowadays is PuTTY.

SSH - CONN

- RFC 4251 defines this protocol as the one which “provides channels that can be used for a wide range of purposes. Standard methods are provided for setting up secure interactive shell sessions and for forwarding ("tunneling") arbitrary TCP/IP ports and X11 connections.”
- The idea is to enable TCP applications to use SSH to run these applications. They do so by dedicating ports that will run SSH and using the ports a secure channel is created; hence the term ‘port forwarding’.

Others

- Other transport level security protocols worth mentioning which the reader is encouraged to read on are:
- S-http
- Https

Part 2

Wireless Security

Introduction

- Wireless technology has evolved over the years to become a standard used by most Internet users today.
- The wireless family of standards 802.11x (a/b/g/n) was developed by IEEE to address wireless technology using WiFi. However, another technology, Bluetooth, is also widely used. IEEE have stopped issuing standards for Bluetooth.
- The types of attacks that wireless networks are exposed to were covered in a different lesson.
- In this lesson we are concerned with the different ways in which wireless networks can be protected.

WLAN Weaknesses

- MAC Address filtering: this is a functionality found in wireless access points (APs). The function allows the AP to permit or deny certain devices from accessing it. The weakness of this is that when a device joins the MAC address is sent visibly (unencrypted) to the AP, enabling an attacker to hijack it and substitute it with his own.
- SSID broadcast: the service set identifier (SSID) of the network is normally broadcast by the AP every few microseconds enabling users to join it (including attackers). The best way to protect the network is to hide the SSID so that only users who know the credentials can join it within its range.
- Wired Equivalent Privacy (WEP): this security protocol which is responsible for encryption between AP and user has also been known to be vulnerable to attacks from hackers.

Solutions

- As a result of the aforementioned weaknesses (in encryption via WEP and authentication via SSID broadcast) together with the weaknesses described in earlier lessons protective standards needed to be developed.
- The IEEE developed the 802.11i standard to address security concerns in wireless networks; the WiFi alliance in response to this developed two standards to implement better wireless security. These were:
  - WiFi Protected Access (WPA)
  - WiFi Protected Access 2 (WPA2)

WiFi Protected Access (WPA)

- Belongs to 802.11i and addresses the weaknesses of encryption and authentication described earlier.
- Encryption: uses Temporal Key Integrity Protocol (TKIP) which offers stronger encryption (128 bit key) and which generates a new key for each packet in the network. TKIP also uses message integrity check (MIC) which makes it harder for an attacker to modify the packets.
- Authentication: uses preshared key (PSK) authentication. The key is entered into the AP and devices before they connect, and when a device attempt to connect they are prompted for the key. If the keys don't match connection is denied.
- Weaknesses: improper management of PSKs, weak passphrases (used to generate the PSK like the password a user enters to join a network).

WiFi Protected Access 2 (WPA 2)

- Based on a later 802.11i standard.
- Encryption: based on Advanced Encryption Standard (AES).
- Authentication: supports both PSK and 802.1x standard. The latter authenticates clients via ports (authentication provided by the server) thereby providing port security.
- Authentication protocols are secured using Extensible Authentication Protocol (EAP), a framework for authentication defined in RFC 3748.

Others

- Other ways to protect the WLAN include the following:
- Place AP (antennae) where it's not easily physically accessible to protect it.
- Limit the range of the AP by adjusting the power levels (most APs have this functionality)
- The reader is also encouraged to some further reading on the following technologies (Stallings (2011) provide good details on these):
  - Wireless Transport Layer Security (WTLS)
  - WAP end-to-end security

Part 3

Email Security

Introduction

- E-mail is arguably the most used application on the Internet today; there are millions of emails exchanged between individuals and groups in any given day.
- E-mail is also arguably the most abused service on the Internet; attackers know that one of the easiest ways to reach you is through your email.
- An attacker will try and intercept your email, pretend to be who they're not and send you email (phishing), and many other forms of attack via your email.
- In order to protect email there are four main standards that are used:
  - Secure MIME (S/MIME)
  - Pretty Good Privacy (PGP)
  - Privacy Enhanced Mail (PEM)
  - Domain Keys Identified Mail (DKIM)

Secure MIME (S/MIME)

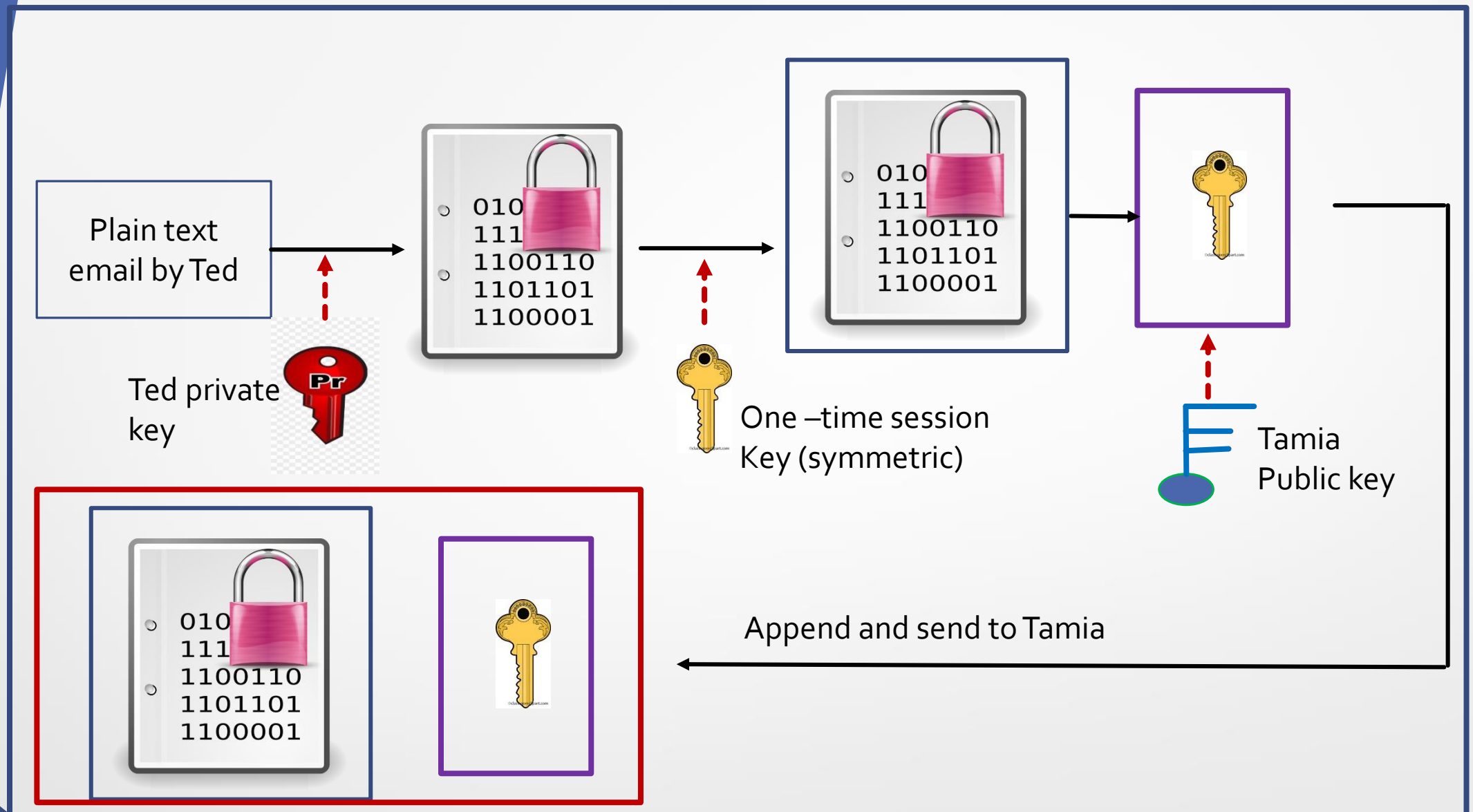
- Secure Multipurpose Internet Mail Extensions (S/MIME). As the name implies it permits for users to send more than just text in an email (the older systems only allowed for text).
- MIME is defined in RFC 2045-9. When MIME incorporates security features it is called Secure MIME (S/MIME).
- It provides the following functionalities on the data it supports:
- Enveloping – content encryption, with the encryption key being further encrypted (enveloped) with recipient's public key; this ensures that it's only the recipient who has access to the encryption key (double security)
- Signing – provision for the digital signature of the sender (see digital signatures in lesson 8); both the content and signature are encoded.
- Clear signing – here the content is not encoded.
- Signing and enveloping – combining signing and enveloping where enveloped data can be signed, or vice versa.

S/MIME Algorithms

- S/MIME provides authentication, integrity and non-repudiation; it uses the following cryptography algorithms:
  - Digital signature standard (DSS)
  - Diffie – Hellman (encryption of symmetric keys)
  - RSA – for digital signatures or enveloping
  - DES -3 – symmetric encryption

Pretty Good Privacy (PGP)

- This is a popular approach to providing security for email.
- The principles are strikingly similar to S/MIME.
- PGP provides authentication, integrity, confidentiality and non-repudiation.
- This happens by the use of digital signatures and asymmetric encryption.
- Let us demonstrate this using fig 3. Our good friend Ted wishes to send an email to Tamia. The figure demonstrates the steps involved in the transmission.



- Fig 3. Ted sending email to Tamia using PGP

Sending Email using PGP

- Let us describe the events in fig. 3
- In the first step Ted constructs his email; he then digitally signs it using his private key.
- Next the signed message is encrypted using a one time session key.
- The session key is then encrypted using Tamia's public key.
- The encrypted session key is then appended to the encrypted signed message; the whole package is now sent to Tamia.
- Based on this scenario it is now clear where the authentication, integrity, confidentiality and non-repudiation are applied.

Domain Keys Identified Mail (DKIM)

- This is a proposed standard whereby the domain from which an email comes from is used to verify it rather than an individual sender.
- When using PGP or S/MIME the sender is the one who undergoes the various security steps associated with the use of either.
- With DKIM the domain owner digitally signs the email with their private key before sending it out.
- The receiving domain then confirms the identity of the sending domain by applying the latter's public key to the email (much like what happens when an individual signs the email).
- By so doing the receiving domain can confirm that the email indeed comes from a trusted domain.

Privacy Enhanced Mail (PEM)

- This standard provides encryption, non-repudiation and integrity.
- It consists of 4 steps that are taken to protect the email.
- Step 1 – make email architecture independent
- Step 2 – sender signs the email with their digital signature
- Step 3 – Email and digital signature encrypted with symmetric key
- Step 4 – encode back into printable output (using ASCII base 64 encoding)

Part 4

Internet Protocol Security

Introduction

- Internet Protocol Security (IPSec) is more a framework for secure communication than a specific protocol or standard.
- It is optional in IPv4 but compulsory in IPv6.
- It provides authentication, confidentiality and integrity; also provides anti-replay.
- It is a collection of protocols.

Advantages

- Advantages of IPSec are as follows:
- It is flexible – users get to chose which algorithms and protocols they wish to use.
- Users choose which security features they wish to use, e.g. authentication, access control, integrity, and so on.
- It can protect singular TCP connections or all connections from the gateway.

Parts of IPSec

- There are three main parts of IPSec
- IPSec Authentication Header (AH) – provides authentication services and by extension access control. It also ensures integrity of the message and provides anti-replay functionality.
- Encapsulating Security Payload (ESP) – it encrypts the payload of the datagram and ensures confidentiality.
- IPSec Internet Key Exchange (IKE) - provides the capabilities for parties to exchange security association information

Summary

- SSL provides 2 key security functions: confidentiality and authenticity; it provides a 'tunnel' between two communicating devices on the Internet. TLS is and advanced version of SSL.
- Secure shell (SSH) protocol was designed to replace remote login protocols like telnet and rlogin which were deemed to be insecure.
- Wireless networks are protected using WPA or WPA2.
- In order to protect email there are four main standards that are used: Secure MIME (S/MIME), Pretty Good Privacy (PGP), Privacy Enhanced Mail (PEM) and Domain Keys Identified Mail (DKIM)
- Internet Protocol Security (IPSec) is more a framework for secure communication than a specific protocol or standard

References

- Ciampa, M. D. (2012). *Security+ guide to network security fundamentals* (4th ed.). Course Technology, Cengage Learning.
- James, J., & McCabe, J. D. (2008). *Network security: Know it all*. Morgan Kaufmann/Elsevier.
- Kahate, A. (2013). *Cryptography and network security*. McGraw Hill Education.
- Stallings, W. (2011). *Cryptography and network security: Principles and practice*. essay, Prentice Hall.