Chapter 5

Web security

SYLLABUS

- 5.1 Intruders, Intrusion detection systems (IDS): host based IDS, network based IDS, logical components of IDS, signature based IDS, anomaly based IDS, network IDS components, advantages and disadvantages of NIDS, host based IDS components, advantages and disadvantages of HIDS.
- 5.2 Web security threats, web traffic security approaches, Introduction to Secure Socket Layer (SSL) & Transport Layer Security(TLS), Concepts of secure electronic transaction

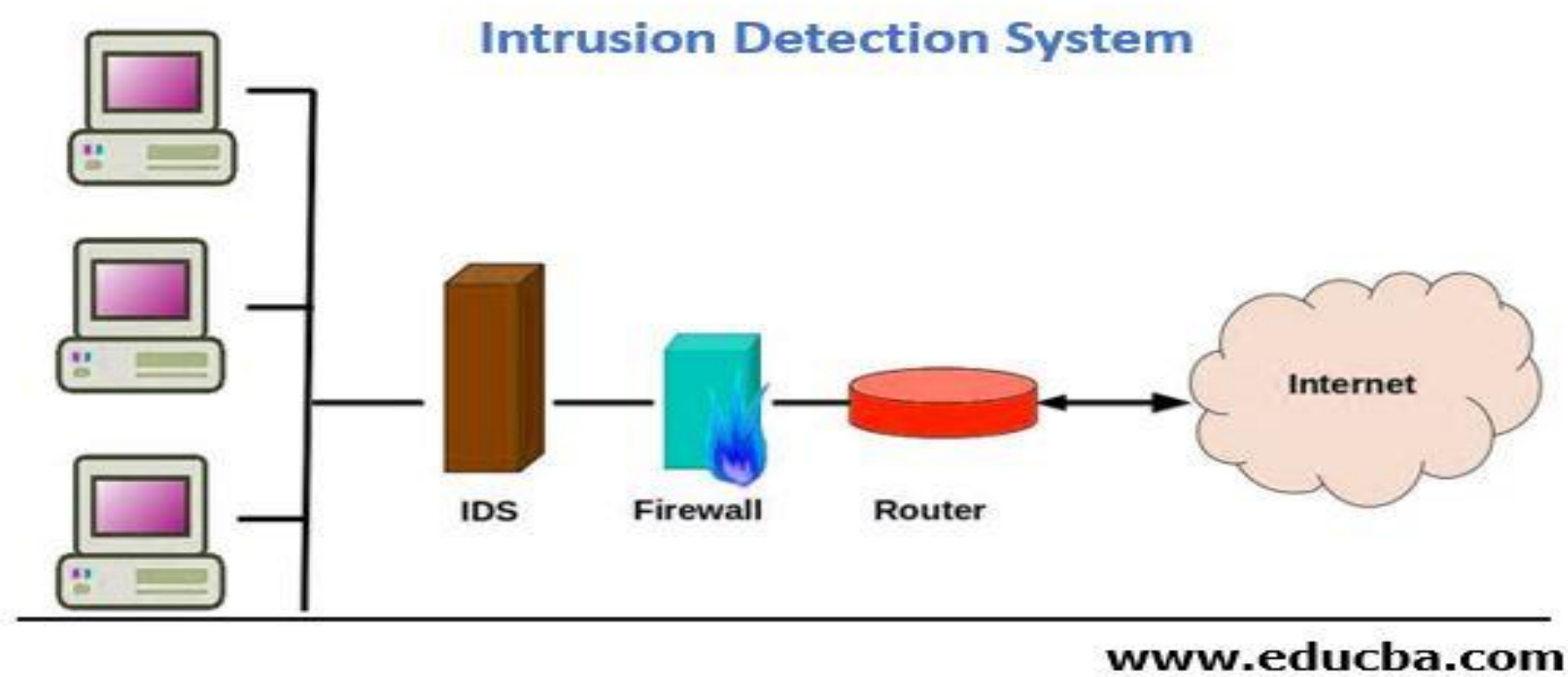
Intrusion detection systems (IDS):

- Intruders same as chapter 1 (refer chapter 1 ppt)
- **Intrusion detection system (IDS)**

- An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Any interruption movement or infringement is commonly detailed either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM framework consolidates yields from different sources and uses alert separating methods to recognize malicious movement from false alarms.

Contd…

- IDS types range in scope from single computers to large networks.
- The most common classifications are network intrusion detection systems (NIDS) and host-based intrusion detection systems (HIDS).
- Monitors important operating system files is an example of an HIDS, while a system that analyses incoming network traffic is an example of an NIDS.
- It’s possible to classify IDS by detection approach. The most well-known variants are signature-based detection and anomaly-based detection (identifying deviations from a model of "good" traffic, which frequently depends on AI).


Intrusion Detection System
IDS
Firewall
Router
Internet
www.educba.com

IDS

HOST BASED INTRUSION DETECTION SYSTEM (HIDS)

HOST BASED INTRUSION DETECTION SYSTEM (HIDS)

- Host intrusion detection systems (HIDS) run on individual hosts or devices on the network.
- A HIDS screens the inbound and outbound bundles from the gadget just and will caution the client or overseer if dubious movement is distinguished. It takes a depiction of existing framework records and matches it to the past preview.
- It takes a snapshot of existing system files and matches it to the previous snapshot. If the critical system files were modified or deleted, an alarm is sent to the admin.

ADVANTAGES :

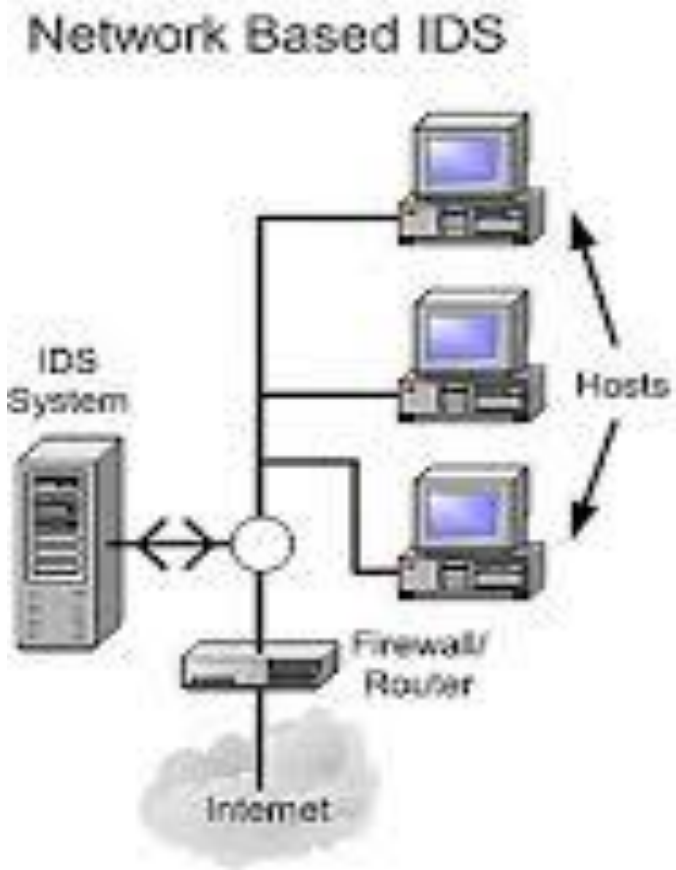
1. **Verifies success or failure of an attack**: Since a host based IDS uses system logs containing events that have actually occurred, they can determine whether an attack occurred or not.
2. **Monitors System Activities**: A host based IDS sensor monitors user and file access activity including file accesses, changes to file permissions, attempts to install new executables etc.
3. **Detects attacks that a network based IDS fail to detect**: Host based systems can detect attacks that network based IDS sensors fail to detect. For example, if an unauthorized user makes changes to system files from the system console, this kind of attack goes unnoticed by the network sensors.
4. **Near real time detection and response**: Although host based IDS does not offer true real-time response, it can come very close if implemented correctly.
5. **Lower entry cost**: Host based IDS sensors are far cheaper than the network based IDS sensors.

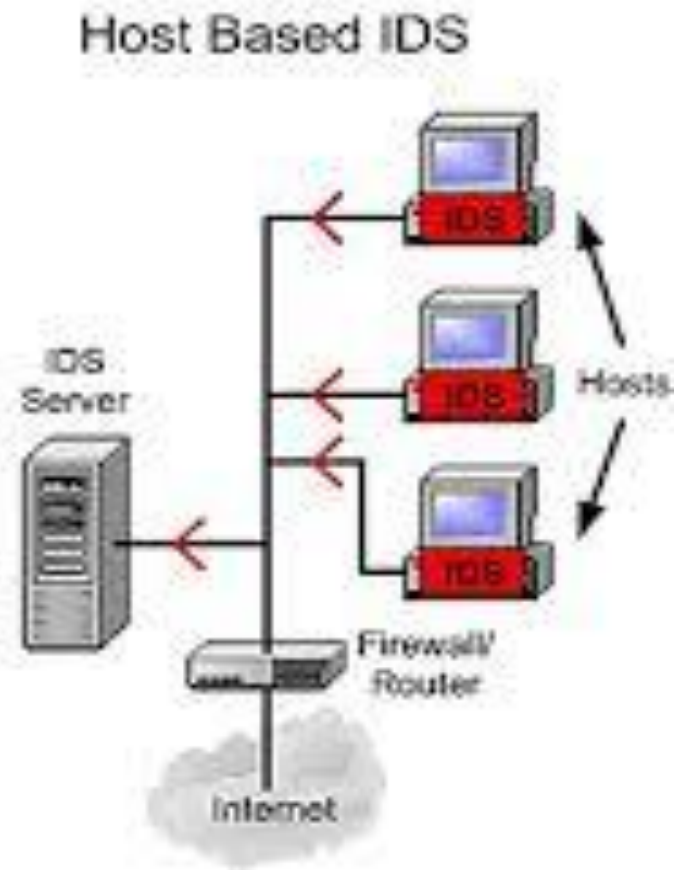
DISADVANTAGES :

1. Host based IDSs are harder to manage, as information must be configured and managed for every host.
2. The information sources for host based IDSs reside on the host targeted by attacks, the IDSs may be attacked and disabled as part of the attack.
3. Host based IDSs are not well suited for detecting network scans or other such surveillance that targets an entire network.
4. Host-based IDSs can be disabled by certain denial-of- service attacks.

NETWORK BASED INTRUSION DETECTION SYSTEM (NIDS):

- **NETWORK BASED INTRUSION DETECTION SYSTEM (NIDS):**
- Network intrusion detection system (NIDS) are put at a vital point or focuses inside the system to screen traffic to and from all gadgets on the system
- It performs an analysis of passing traffic on the entire subnet, and matches the traffic that is passed on the subnets to the library of known attacks.
- Once an attack is identified, or any abnormal or sensitive behaviour is matched, the alert can be sent to the admin. An example of an NIDS would be installing it on the subnet where firewalls are located in order to see if someone is trying to enter or break into the firewall.


Network Based IDS
IDS System
Hosts
Firewall/ Router
Internet


Host Based IDS
IDS
IDS
IDS
IDS Server
Hosts
Firewall/ Router
Internet

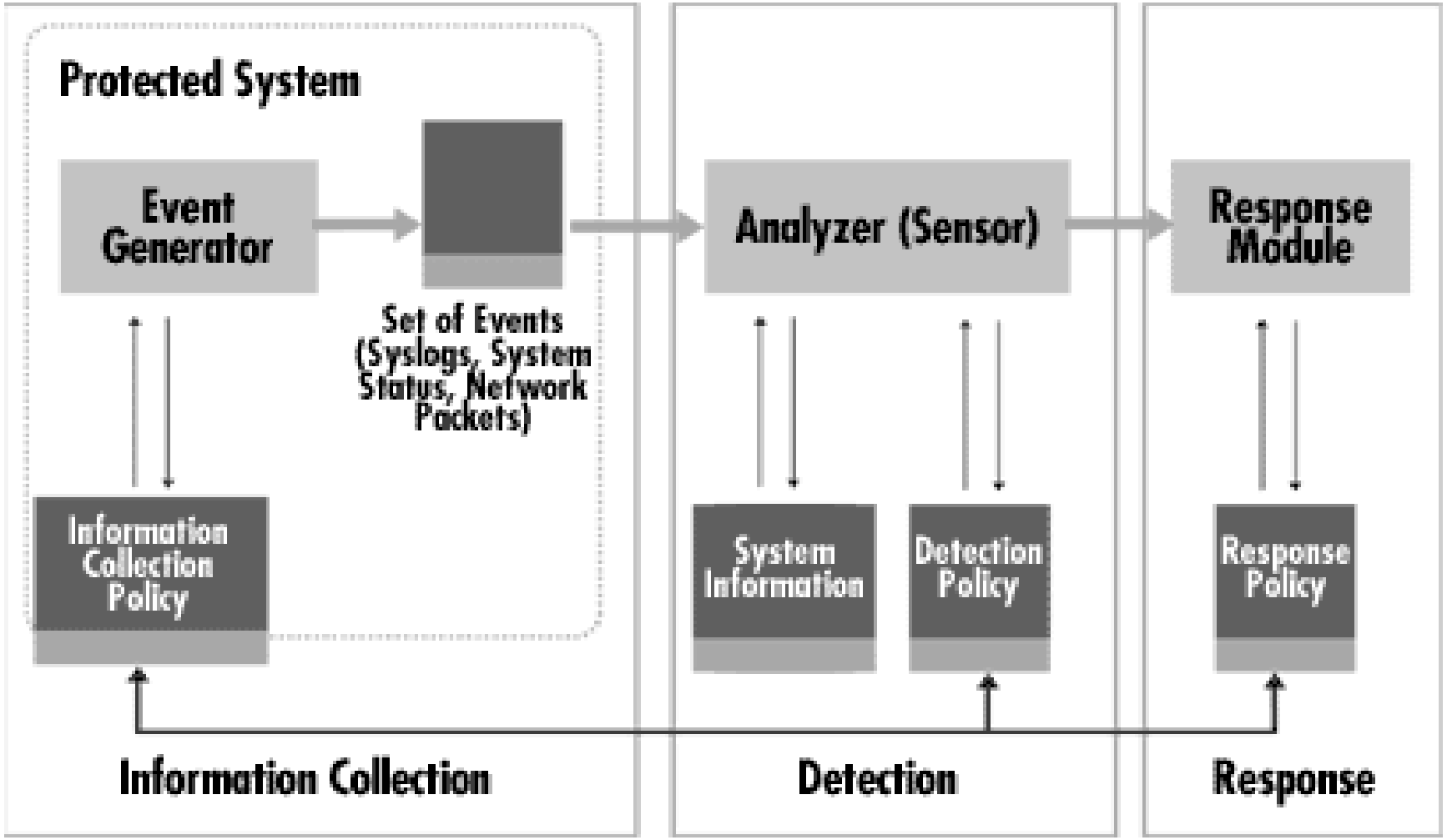
Advantages of NIDS

1. A few well-placed network-based IDS can monitor a large network.
2. The deploying of NIDSs has little impact upon an existing network. NIDSs are usually passive devices that listen on a network wire without interfering with the normal operation of a
3. NIDSs can be made very secure against attack and even made invisible to many attackers.

DISADVANTAGES :

1. NIDSs may have difficulty possessing all packets in a large or busy network and, therefore, may fail to recognize an attack launched during period of high traffic.
2. Many of advantages of NIDSs don’t apply to more modern switch-based networks.
3. NIDSs cannot analyze encrypted information. This problem is increasing as organizations and attackers use virtual private network.
4. Most NIDSs cannot tell whether or not an attack was successful; they can only find that an attack was initiated.

Logical components of IDS



CONTD...

- Logical Architecture of IDS is shown in above figure.
- It consist

1.Event Generator

2.Analyzer

3.Response Module

- The collection of Information policy is determined by the event generator policy that defines the filtering mode of event notification information.
- The event generator (operating system, network, application) produces a policy-set of events that may be a log (or audit) of system events, or network packets.

CONTD..

- This, set along with the policy information can be stored either in the protected system or outside.
- An intrusion detection system always has its core element – a sensor that is responsible for detecting intrusions. This sensor contains decision-making mechanisms regarding intrusions.
- Sensors receive raw data from three major information sources as shown in above figure: own IDS knowledge base, syslog and audit trails.
- This information creates the basis for a further decision-making process.
- Response Module will fire alarm if any threat or intrusion or violation of policy is detected by sensors.

Detection method

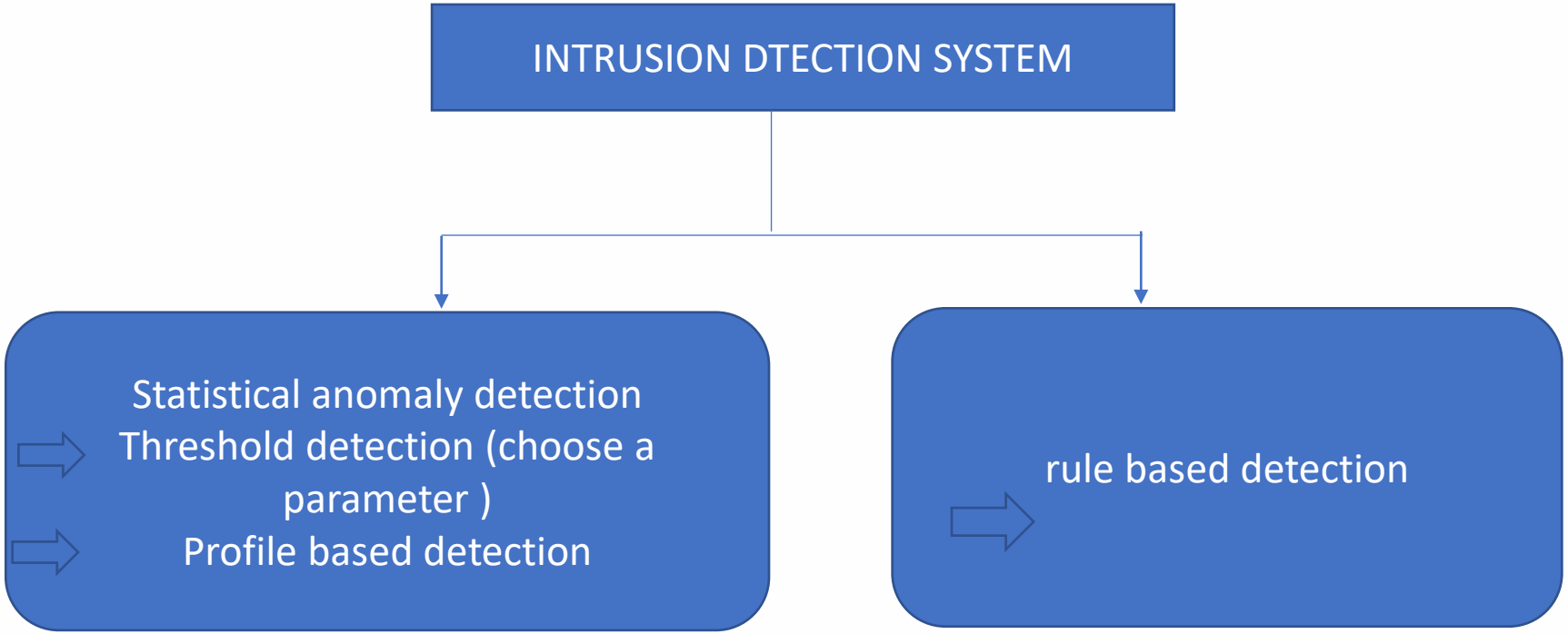
- signature based IDS AND anomaly based IDS,
- Signature-based IDS refers to the detection of any attacks by looking for patterns, such as byte sequences in network traffic, or known malicious instruction sequences used by malware.
- The issue is that there will be a lag between a new threat being discovered in the wild and the signature for detecting that threat being applied to the IDS.
- During that lag time the IDS would be unable to detect the new threat.

ANOMALY BASED IDS

- **ANOMALY BASED IDS**
- Anomaly-based intrusion detection systems were primarily introduced to detect unknown attacks, in part due to the rapid development of malware. The basic approach is to use machine learning to create a model of trustworthy activity, and then compare new behaviour against this model
- Since these models can be trained according to the applications and hardware configurations, machine learning based method has a better generalized property in comparison to traditional signature-based IDS.
- The issue is that it may raise a False Positive alarm for a legitimate use of bandwidth if the baselines are not intelligently configured.

OTHER DETECTION METHODS

IDS

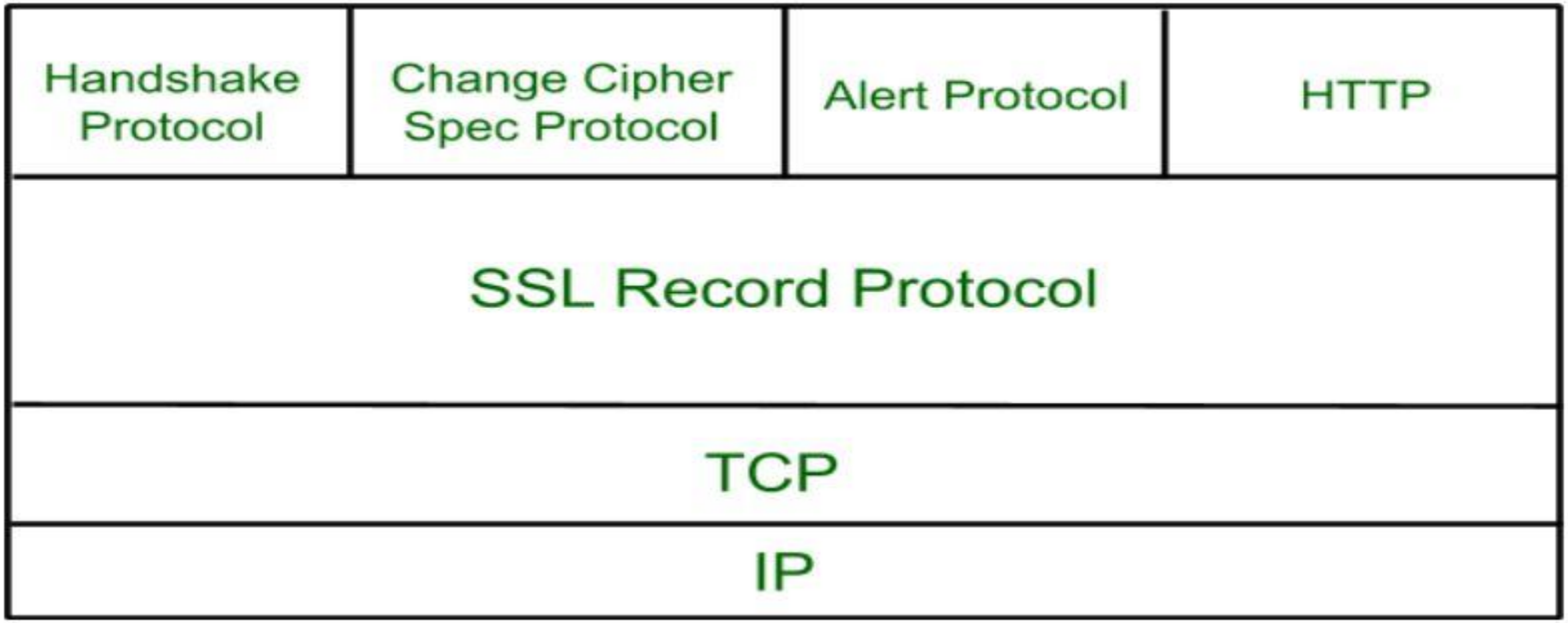


- Behaviour of user is analysed over a period of time and rules created to differentiate b/w legitimate and illegal user .

5.2 WEB SECURITY THREATS

- A web threat is a threat that uses the World Wide Web to open the door for cybercrime.
- Web threats use multiple types of malware and fraud, all of which utilize HTTP or HTTPS protocols, but may also employ other protocols and components, such as links in email or IM, or malware attachments or on servers that access the Web.
- It can divide into 2 primary category:
- Pull based threat
- Push based threat

secure socket layer (SSL)



CONTD…

- Secure Sockets Layer (SSL) is a protocol developed by Netscape for transmitting private documents via the Internet. SSL uses a cryptographic system that uses two keys to encrypt data − a public key known to everyone and a private or secret key known only to the recipient of the message

- SSL follows an asymmetric cryptographic mechanism, in which a Web browser creates a public key and a private (secret) key.

- The public key is placed in a data file known as a certificate signing request (CSR). The private key is issued to the recipient only.

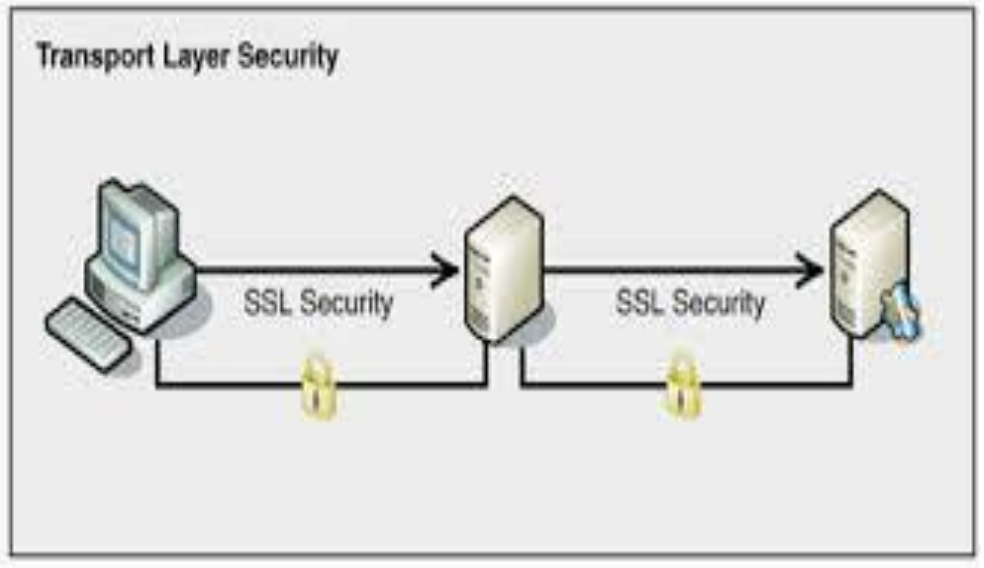
How does SSL work?

- In order to provide a high degree of **privacy**, SSL encrypts data that is transmitted across the web. This means that anyone who tries to intercept this data will only see a garbled mix of characters that's nearly impossible to decrypt.
- SSL initiates an **authentication** process called a handshake between two communicating devices to ensure that both devices are really who they claim to be.
- SSL also digitally signs data in order to provide **data integrity**, verifying that the data is not tampered with before reaching its intended recipient.

- **The objectives of SSL are**:
- Data integrity: Data is protected from tampering.
- Data privacy: Data privacy is ensured through a series of protocols, including the SSL Record Protocol, SSL Handshake Protocol, SSL Change CipherSpec Protocol and SSL Alert Protocol.
- Client-server authentication: The SSL protocol uses standard cryptographic techniques to authenticate the client and server.

TRANSPORT LAYER SECURITY(TLS)

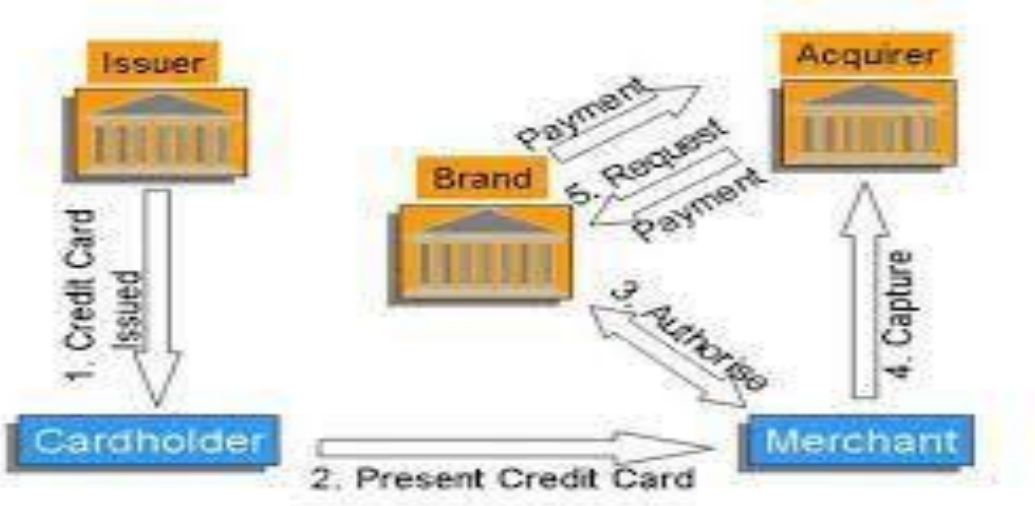
- A protocol that provides communications privacy and security between two applications communicating over a network.
- It composed of 2 layer
    1. TLS Record Protocol
    2. TLS Handshake



- **TLS Record Protocol**
- The TLS Record protocol secures application data using the keys created during the Handshake.
- The Record Protocol is responsible for securing application data and verifying its *integrity* and origin.
- **TLS Handshake Protocol**
- TLS Handshake Protocol is responsible for the authentication of the user and key exchange necessary to establish or resume secure sessions.
- When establishing a secure *session*, the Handshake Protocol manages the following:
- Cipher suite negotiation
- Authentication of the server and optionally, the client Session key information exchange.

SECURE ELECTRONIC TRANSACTION

1.Secure Electronic Transaction (SET) is a suit of protocol that has been developed and promoted by a consortium of Visa and MasterCard to ensure security Of online financial transactions.



CONTD..

- Issuer (could be consumer's High street bank) issues consumer with the credit card
- 2. Cardholder (consumer) presents the merchant with his credit card for payment along with the order
- 3. Merchant requests and receives authorisation of payment from the credit card brand (could be Visa, MasterCard, American Express, etc) before processing the order
- 4. Having received authorisation from the brand, merchant initiates the process of capture of monitory funds through the acquirer (could be Merchant's High street bank)

CONTD...

- 5.Acquirer forwards authorisation details to the brand and requests settlement from the brand
- 6. Having received payment from the brand, acquirer credits Merchant's account with the funds
- 7. Brand bills the consumer for the funds

LINKS :

1. https://www.youtube.com/watch?v=cGIgJOICpX0
2. https://www.youtube.com/watch?v=RbjYHZ3ZZFw
3. https://www.youtube.com/watch?v=hExRDVZHhig
4. https://www.geeksforgeeks.org/threats-to-information-security/
5. https://www.geeksforgeeks.org/secure-electronic-transaction-set-protocol/