Internet is communication infrastructure for exchanging info

A WAN that is a collection of smaller networks

Based on TCP/IP protocols (set of rules that define communication across network)

Each device uniquely recognised via IP addresses

Internet technologies refers to the architecture., protocols and services behind the internet

Network is collection of devices that can communicate with each other

Some mediums used for network communications: wi-fi, optical, copper wires, infra-red etc

Network architecture is set of layers and protocols

Protocol refers to both specification and implementation

Network communication very complex, so layering used

Reduces design complexity and testing, maintenance simplified

Easy to replace layers with different versions as well

Application layer: service location – support multimedia – wired and wireless access to www

Presentation layer: conversion of data structures from abstract to concrete, e.g., a banking record

Session layer: dialogue control

Transport layer: accept data from the above layer, split in smaller units and pass to the network layer, establish an end-to-end connection – quality of service – flow and congestion control

Network layer: control the operation in a subnet, routing packets – addressing - handover between networks.

Data link layer: transform a raw transmission in a line free of undetected transmission errors, Accessing the medium – multiplexing (break the data in data frames) - error correction – synchronization

Physical layer: conversion of stream of bits into signals

Stands for Hypertext transfer Protocol

It delivers mostly all files and resources on WWW

Uses client-server model (stateless)

URIs are like postal addresses, uniquely identify websites and other resources

URLs have a protocol first then object address, consists of domain name and document path

HTTP servers uses port 80, handles the requests and sends back responses

HTTPS (secure version) uses port 443 and is end-to-end encrypted

Get uses file path and version of HTTP being used, versions range from 1.0 to 3.0 atm

Responses lines have HTTP version, status code and then description of status code

Header lines contain fields (name and value) not case sensitive, and full header ends in CRLF

Body can contain more info about request/response and header describes this

HTTP uses MIME types (multimedia), contains a type, subtype and optional parameters

HTTP statelessness, forgets states, cookies store them, client-side

FTP stands for file transfer protocol, transfers files between different users

Downloads can be performed over web browsers or specialized FTP clients

Can transfer data, either as ascii (plaintext) or binary (raw data), client and server ensure that data is preserved during transfer

Information security – general practice of protecting info from unauthorized users

Computer security just one aspect, other info assurance, data not lost

Confidentiality – principle of maintain privacy for data, certain info must be kept secret, can result in loss of revenue, rep, customers, embarrassment or legal breaches, encryption and access control usually used to ensure this.

Integrity – principle of ensuring data accurate and correct, ensure info and systems not altered in unauthorised ways, also includes being prepared for disasters and recovery, breaches can be malfunctions, people changes or malware changes, regular backups, checksums and data correcting codes usually used to ensure integrity.

Availability – principle of making info available to authorized users, info/systems accessible and modifiable to those with permissions, lack of availability referred to as Denial of Service

Internal actors are the people who work for the organization. Although they account for a small percentage of the attacks, they are especially dangerous due to their internal knowledge of the systems

External actors are the people outside of the organization. It turns out that more than three quarters of external actors are linked with organized crime or nation states

Partner actors are linked with an organization that you partner or work with. Quite often partners are granted some access to each other’s systems (to place orders, for example)

A loss of availability prevents users from accessing some or all of the systems, this might marked as a denial of service attack, or a SQL injection attack, where the payload removes the entire user database, preventing logins from registered users

A loss of confidentiality includes the expose of confidential information to a (often malicious) third party, this could marked as a cross-site script attack where data is stolen right off your screen or a full-fledged database theft where credit cards and passwords are taken

A loss of integrity changes your data or prevents you from having correct data, this might marked as an attacker hijacking a user session, perhaps placing fake orders or changing a user’s home address

A threat refers to a particular path that a hacker could use to exploit a vulnerability and gain unauthorized access to your system. A flood destroying your data centre is a threat just as much as malicious SQL injections, buffer overflows, denial of service, and cross-site scripting attacks.

Spoofing – The attacker uses someone else’s information to access the System.

Tampering – The attacker modifies some data in non authorized ways.

Repudiation – The attacker removes all trace of their attack, so that they cannot be held accountable for other damages done.

Information disclosure – The attacker accesses data they should not be able to.

Denial of service – The attacker prevents real users from accessing the systems.

Elevation of privilege – The attacker increases their privileges on the system thereby getting access to things they are not authorized to do.

Once vulnerabilities are identified, they can be assessed for risk. Some vulnerabilities are not fixed because they are unlikely to be exploited, while others are low risk because the consequences of an exploit are not critical. The top five classes of web vulnerability are:

1. Injection

2. Broken authentication and session management

3. Cross-site scripting

4. Insecure direct object references

5. Security misconfiguration