CS2107 Live Class Lec5: Network Security

$_{/}|/|U_{C}h@NgRu!$

May 11, 2021

Purpose

1. The Confidentiality is guaranteed by cryptography
2. The authentication is guaranteed by PKC
3. The availability?
4. Controlling and monitoring the traffic flow.

1 Network Layer

The network is built with 5 layers, each layer divided data pkt into smaller data unit, which is called PDU(protocol data unit) Network layers are covered in great detail in CS2105
Original design of Internet does not take into account of intentional attack, as a consequence, attacker at any layer can modify the data, including the header. For example, an man-in , the middle attacker can spoof source IP address.

1.1 Multiple hops

Data would go through different layers during transportation, and it will go through multiple hops. Intermediate nodes could be owned by different semi-trusted third parties, such as internet service provider(ISP), company's firewall. Intermediate nodes might change header information, translate the address etc, typically up to layer 3. Nonetheless, some intermediate nodes might change data in layer4 and even application layer data

1.2 The hardness of Network security

Nodes are own by many different semi-trusted parties
Intermediate node has access to both the header and the payload, and can modify(authenticity),read(confidentiality), drop(availability). An attacker at certain layer can access all info in and below the layer

1.3 Security requirement

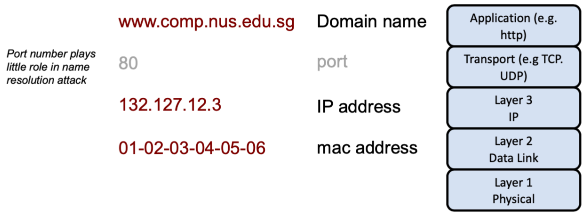
Many different security requirements.

1. availability can't be handled by crypto alone.
2. anomymity
3. accountability
4. routing integrity

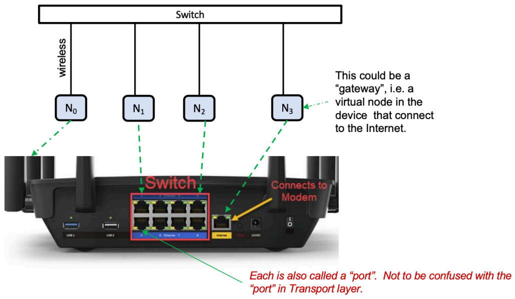
1.4 Transportation Layer protocol

1. UDP: not reliable not secure
2. TCP: reliable, not secure(cannot detect if there is a man in the middle whether listening or modifying)

2 Name resolution and attacks



1. Resolution of demain name into IP address relies on DNS.
   (ps: resolver is the client who initiates the query)
   IMPORTANT: The DNS protocol does not protect confidentiality and authenticity of the query and answer
   (a) The query contains a 16-bit number, known as QID(query ID)
   (b) The response from the server must also contains a QID
   (c) If the QID in the response does not match the QID in the query, the client reject the answer. The design consideration of having QID probably is to match the query result to multiple queries sent out by the client, which can be treated as a light-weight authentication
2. Resolution of IP address into MAC address relies on ARP.

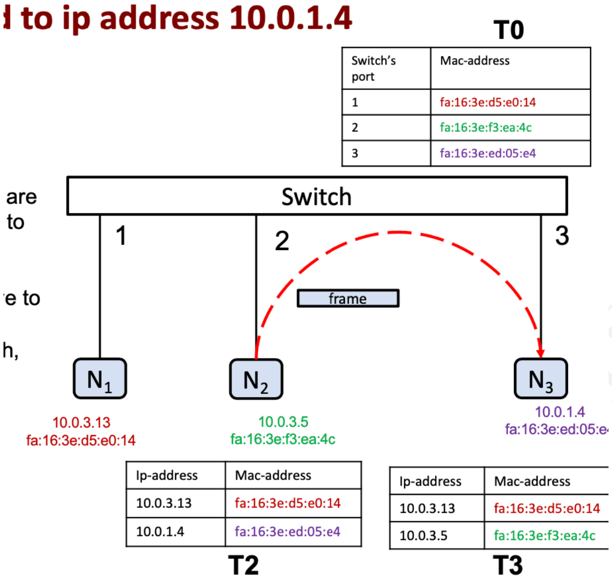


This could be a "gateway", i.e. a virtual node in the device that connect to the Internet.

Each is also called a "port". Not to be confused with the "port" in Transport layer.

The port pointed by the yellow is the port connects to the internet

In our home wifi ”router”, it usually contains function of both router and switch



T0

Switch’s port	Mac-address
1	fa:16:3e:d5:e0:14
2	fa:16:3e:f3:ea:4c
3	fa:16:3e:ed:05:e4

Ip-address	Mac-address
10.0.3.13	fa:16:3e:d5:e0:14
10.0.1.4	fa:16:3e:ed:05:e4

T2

Ip-address	Mac-address
10.0.3.13	fa:16:3e:d5:e0:14
10.0.3.5	fa:16:3e:f3:ea:4c

T3

How the switch works when N_2 tries to send a pkt to 10.0.1.4

(a) N_2 looks up the tabl T2. Resolve to fa:3e:ed:05:e4

(b) N_2 sends the frame to the switch specifying destination fa:16:3e:ed:05:e4

(c) Switch looks up the table T0, redirect the fram to port3

There are attacks to these protocols. which targets the authenticity of the association

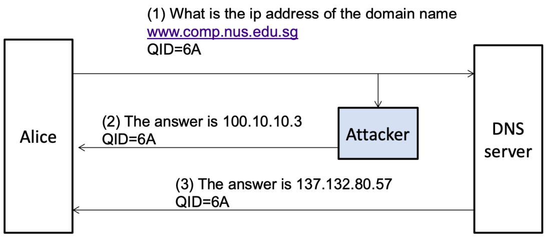
1. ARP attack targets at the association of ip-address with mac addr
2. DNS attack targets at the association of domain name with ip address

Two basic attack is DNS attack and ARP poisoning

3 DNS spoofing Attack

DNS is covered in CS2105. Regarding security, there is a lightweight authentication for DNS queries

The DNS attack:


(1) What is the ip address of the domain name
www.comp.nus.edu.sg
QID=6A
Alice
(2) The answer is 100.10.10.3
QID=6A
Attacker
DNS
server
(3) The answer is 137.132.80.57
QID=6A

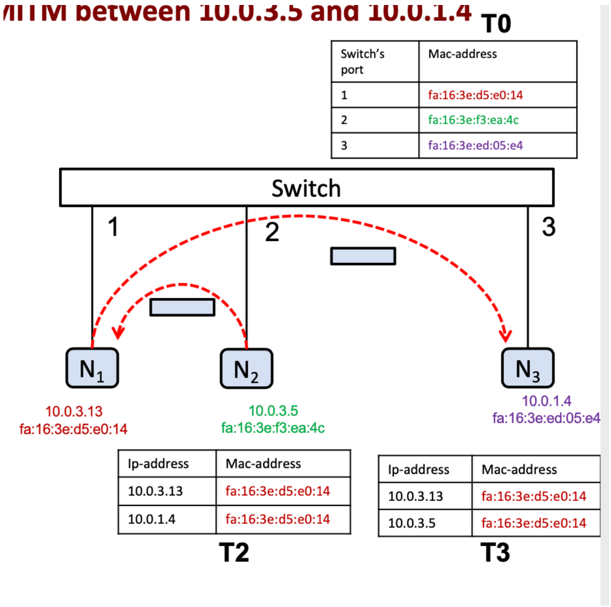
1. Alice send DNS query to the DNS server for the address of the website (nus.edu.sg here)
2. Eve sniffs and knows about the DNS query, which includes the domain name of website (nus.edu.sg) and QID
3. Eve spoofs a reply with the same QID but with an IP address to website Y (Y may be in control of Eve) Since DNS is a application layer protocol, the detail of spoofing is not important
4. DNS server also sends a reply. However, eve's reply will most likely reach Alice first(Because the Eve tends to be in a nearer location)
5. Alice takes the first reply, which is from Eve, as the answer and connect to website Y.

However, this attack will not work for DNS queries to domain protected with https, as authenticated key exchange will ensure authenticity of both parties; The attacker's answer will be dropped by Alice if the attacker cannot response with Alice's challenge with private key

3.1 DNS poinsoning

Poinsoning is a attack where the attacker poinsoning a table

4 ARP poisoning



T0

Switch's port	Mac-address
1	fa:16:3e:d5:e0:14
2	fa:16:3e:f3:ea:4c
3	fa:16:3e:ed:05:e4

T2

Ip-address	Mac-address
10.0.3.13	fa:16:3e:d5:e0:14
10.0.1.4	fa:16:3e:d5:e0:14

T3

Ip-address	Mac-address
10.0.3.13	fa:16:3e:d5:e0:14
10.0.3.5	fa:16:3e:d5:e0:14

Note: T0 stores in switch, T2 stores in N_2,T3 stores in N_3
The ARP attack where N_1 wants to be MITM between 10.0.3.5 and 10.0.1.4

1. N_1 inform N_2 that mac address of 10.0.1.4 is fa:16:3e:d5:e0:14
2. N_1 inform N_3 that mac address of 10.0.3.5 is fa:16:3e:d5:e0:14
3. After the tables are poisoned, all frame will be sent to N_1
4. N_1 can relay the frames, or modify the frames before relaying
5. Hence N_1 become the MITM in layer2

The protocol is designed like this, any one can change the table

5 Denail of Service(DOS) Attack

Denial of service attack is an attack on availability, the property of being accessible and usable upon demand by an authorised entity

5.1 Denial of service

Denial of service is the prevention of authorised access to resources or the delaying of time-critical response

The idea of DOS attack is to flood the victim with overwhelming requests/data
Distributed Denial of Service attack is DOS carried out by a large number of attackers
Example:

1. Flood a web-server with http requests
2. Sending large number of DNS requests to the DNS server

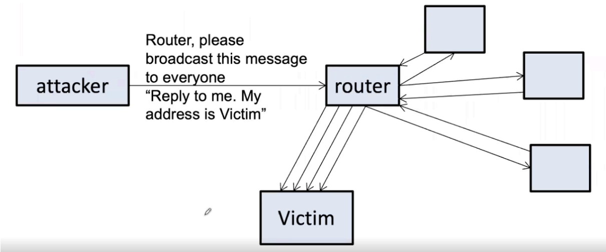
5.1.1 DDOS

When DOS is carried out by a large number of attackers, this is called DDOS: Distributed Denial of Service

6 Reflection/Amplification attack

Reflection attack is a type of DOS in which the attackers send requests to intermediate nodes, which in turn send overwhelming traffic to the victim
For some protocols, the reflected traffic is amplified, in a sense a single request could trigger multiple responses from the intermediate nodes. These are known as amplification attack.

6.1 Reflecting attack using ICMP/Smurf flood


attacker
Router, please broadcast this message to everyone "Reply to me. My address is Victim"
router
Victim

1. Attackers forges a ”ICMP Ping” request by spoofing the source IP address as the victim’s IP address
2. Attack sends the request ”ICMP Ping” to a router, instructing the router to broadcast the request, in which ask every one to reply to the victim
3. The router broadcasts
4. Each enity which received the requst will reply to the victim by sending an ”echo reply” response
5. The victim is overwhelmed by the ”echo reply”

The attacker only sends out one request but the victim receive four requests here
This attacker is no longer applicable, because the reply feature is removed To prevent this attack, we can simply disable the broadcast function of the router. Similar reflection attack can be conducted with DNS

6.2 DNS reflection attacker

During DNS amplification attack, the perpetrator sends out a DNS query with a forged IP address(the victim's) to an open DNS resolver. prompting it to reply back to that address with a DNS response. With numerous fake queries begin sent out, and with serveral DNS resolvers replying back simultaneously, the victim's network can easily be overwhelmed by the the sheer number of DNS response

6.2.1 The largest DDOS attack

Targeted at Github using Memcache on 5 March 2018. Generated data at a rate of 1.7 Terabits per second

7 Bot, Botnet

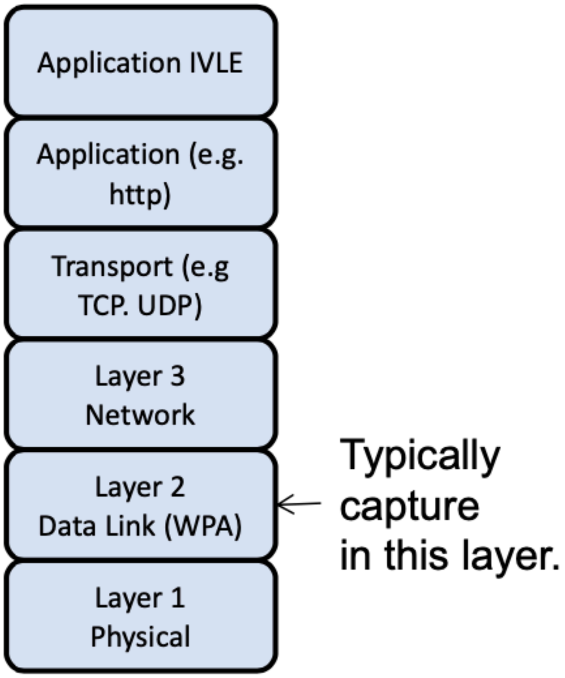
A bot, aka zombie, is a compromised machine. A botnet, aka zombie army, is a collection of connected bots, communicating via covert channels.
A botnet has a command and control mechanism and thus can be controlled by an individual to carry out DDOS, or sending spam. botnet can be bought from dark net

7.1 Way to minimize the DOS

1. Apply cloud services, which can expand its server when numerous requests come
2. Note that the DOS cannot be prevent because the server just serves the bots as normal client, there is no absolute way to differentiate, but some strategy can be made to differentiate

8 Useful tools for network securiy

8.1 Wireshark

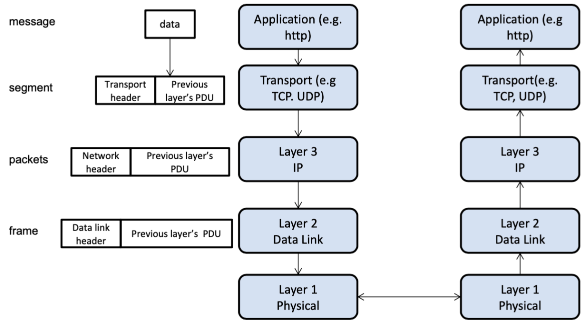


Wireshark: packet analyser
Wireshark listens to interactions betweenm OS and the network card driver(It's a MITM between OS and network card); Hence header added by the network card or modified by network card or lower layer attackers may not be captured by Wireshark, which is OS and hardware dependednt

8.2 nmap

Nmap: port scanner
nmap -v -p 1-65535 -sV -sS -T4 https://cs2107-ctfd-i.comp.nus.edu.sg

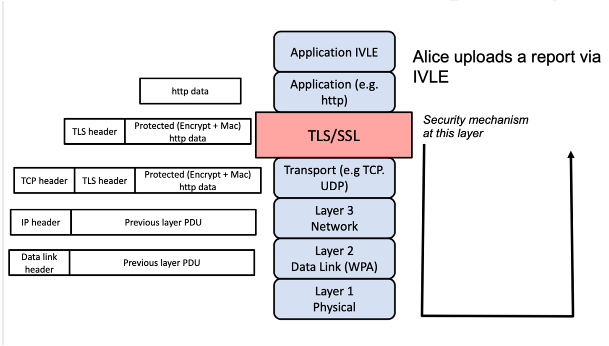
9 Protection: Securing the communication channel using cryptography



TLS/SSL, WPA, IPSec are several well known security protocol on top of Transport Layer. A security protocol that protects layer k, would protect information in **layer k and above**
The key idea is that as the PDU arrive lower layer, it will be encrypted layer by layer

9.1 SSL/TLS

SSL/TLS protects confidentiality and integrity of application layer's data via enryption and mac and passes to the transport layer



Therefore, for SSL/TLS, the protection will not cover below transport layer(inclusive), because it is on top of the transport layer. It will also not protect from malicious scripts injected to the application layer
MITM

1. if MITM in physical layer, just see every information
2. Link layer thesame

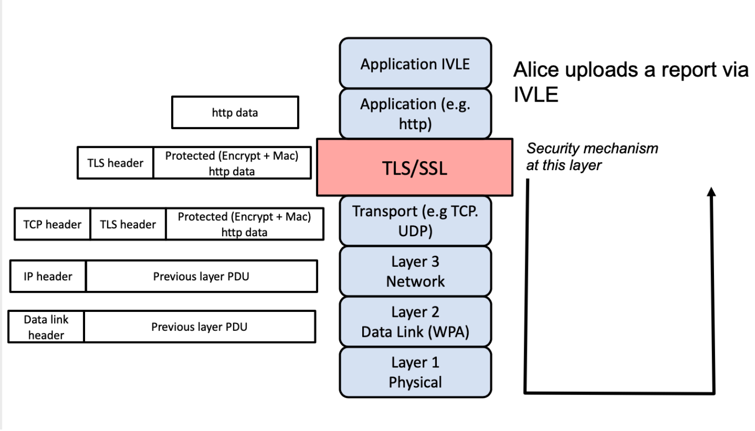
3. Network layer: can also see: e.g. Suppose attacker conducts DNS attacks, all traffics will be routed to the spoof person, but he cannot understand it because the upper layer is protected by cryptography
4. Application layer: if the malware is in application layer, the SSL/TLS cannot protect the information

9.1.1 A Scenario

Suppose that there is an attacker in the physical layer who can sniff and spoof message at that layer (i.e. MITM in the physical layer). For example, Alice uploading her report in a cafe using free wifi (without WPA protection). Hence anyone in the café has access to the physical layer and thus can sniff and spoof messages in that layer.

1. The attacker can get Alice's link layer pkt, but cannot get the report, which is encrypted on top of Transportation layer(TLS or SSL)
2. The attacker can know Alice is visiting IVLE website

9.2 WPA2



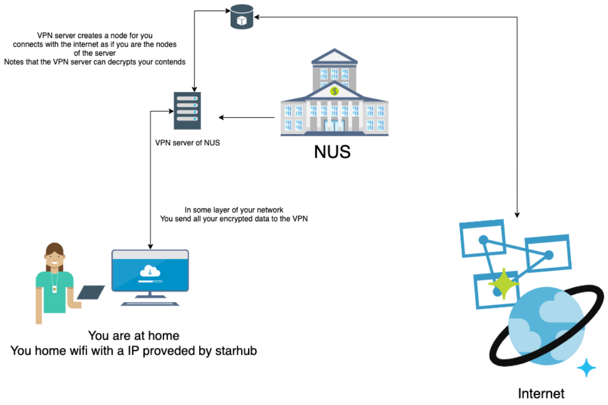
Wifi Protected Access II(WPA2) is a security protocol employed in home Wifi access point. WPA2 protects at link and physical layer. However, not all information at link layer is protected For example, it is not clear whether WPA2 protects the confidentiality of the mac address

9.3 IPSec

IPSec is a mechainism whose goal is to protect the IP layer. IPSec protects the integrity and authenticity of the IP address but not the confidentiality

The attackers are unable to sppof the source ip-source, but can learn the source and destination ip-address of the sniffed packets
However, it turns out that the IPSec is hard to implemented, because it needs to modify the OS in reality, while TLS/SSL needs only add a layer above TCP

10 VPN


VPN server creates a node for you
connects with the internet as if you are the nodes
of the server
Notes that the VPN server can decrypts your contends
VPN server of NUS
NUS
In some layer of your network
You send all your encrypted data to the VPN
You are at home
You home wifi with a IP proveded by starhub
Internet

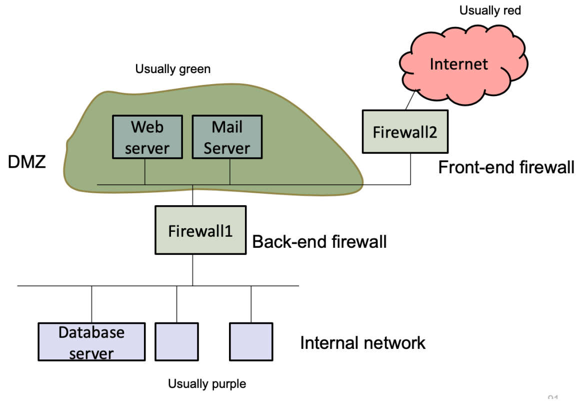
11 Firewall

Having the security protocol above is not sufficient to protect the network. For example, they cnanot prevent DOS attack, or ther are services not established on those protocol, such as DNS query

11.1 Firewall

A firewall controls what traffic is allowed to enter the network(ingress filtering), or leave the network(egress filter) to impose differing security postures

11.2 2-firewall setting



11.3 Demilitarised Zone(DMZ)

Demilitarised zone in this context is a sub-network that exposes the organization service to untrusted Internet
Usually the back-end firewall will be more strigent compared to the front-end firewall. The rules of firewall are usually recorded in a table format, where the first entry matching the packet will be applied on the packet
(Usually, attacker would not choose to attack DMZ)

11.3.1 3 types of firewall

1. Packet filters:Packet filters inspects of every packet. typically only on the IP packet's header information.
2. Stateful Inspection:if the payload is inspected, we call it deep packet inspection(DPI)
3. Proxy:modify the packet (for more advanced device)(proxy)

11.4 Packet filtering

occur in router, gateway/bridge and host etc
Action takien after inspection could be

- Allow the packet to pass
- just drip the packet
- reject the packet(i.e. drop and i9nform the sender)
- Log info

- Notify system admin
- modify the packet (for more advanced device)(proxy)

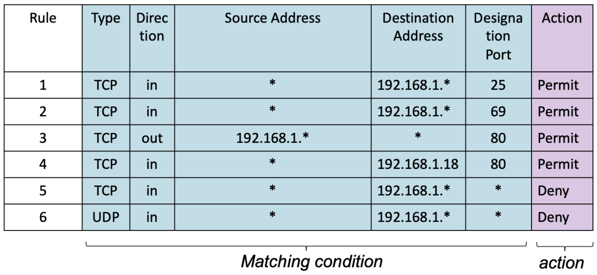
11.4.1 Whitelist and Blacklist

1. Whitelist: drop all packets except those specified in the white-list
2. Blacklist: accept all packets except those specified in the blacklist

The firewall set a set of rules regarding the network communication.
E.g.

- Rules for firewall1
  - Block: HTTP
  - Allow internal to mail server: SMTP, POP3
- Rules for firewall2
  - Allow from anywhere to mailserver: SMTP only

The rules' setting styles differ among systems



Rule	Type	Direction	Source Address	Destination Address	Designation Port	Action
1	TCP	in	*	192.168.1.*	25	Permit
2	TCP	in	*	192.168.1.*	69	Permit
3	TCP	out	192.168.1.*	*	80	Permit
4	TCP	in	*	192.168.1.18	80	Permit
5	TCP	in	*	192.168.1.*	*	Deny
6	UDP	in	*	192.168.1.*	*	Deny

Matching condition
action

CS2107 fix the above way

12 Intrusion Detection System(IDS)

An Intrusion detection system consists of a set of "sensor" who gather data. Sensors could be in the host, or network router. The data are analyzed for intrusion.
Three types of IDS:

1. Attack signature detection: The attack has specific, well-defined signature. For e.g. using certain port number, certain source IP address

2. Anomaly detection: The IDS attempt to detect abnormal pattern. For e.g. a sudden surge of packets with certain port number
3. Behavior-based IDS: Can be viewed as a type of anomaly detection that focuses on human behavior. For e.g. the system might keep the profile of each other. It then tries to detect any user who deviates from the profile(e.g. start to download large file)

A popular open-source IDS: snort:https://www.snort.org/

13 Security operation center(SOC)

A centralized unit in an organization that monitors the IT systems and deals with security issues

14 Security information annd event management(SIEM)

pronounced as ”SIM”. Approaches and tools for SOC
A popular system Splunk (https://www.splunk.com/)