Network security

Nicolò Fornari

March 9, 2016

Chapter 1

Network protocols

1.1 Introduction

Data link layer
It is the lowest logical level, the data link interconnects physical interfaces. Each interface is identified by a MAC address (Media Access Control).
The MAC address is 48 bit long, it is usually represented in Hex notation and it is used to route packets in local networks.
It uniquely identifies a network interface. It is assigned by the producer according to the standard IEEE 802.

Network Layer
IP operates at this level. IP addresses are dynamically assigned by an authority (eg. ISP's DHCP server).

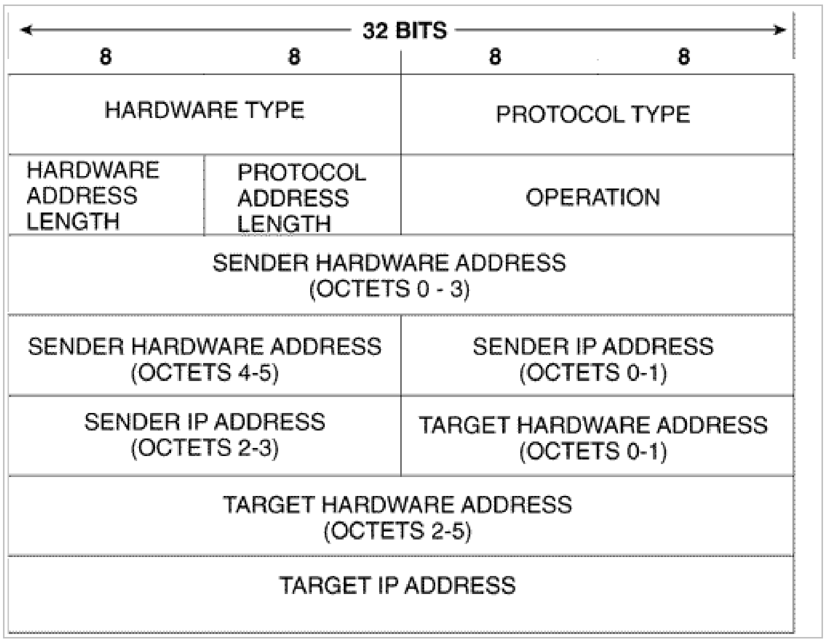
Stateful: communication starts, develops,ends. eg. TCP
Stateless: IP

1.2 ARP

ARP (address resolution protocol) allows systems to associate an ip address to a MAC address. All addresses in the ARP table are added by one of these mechanisms:

- ARP request-reply:
  who is 192.168.0.16 tell 192.168.0.1
  192.168.0.16 is at 00-10-BC-2c-11-56
- Gratuitous ARP
  192.168.0.16 is at 00-10-BC-2c-11-56

ARP frame header



<table>
<tr><th colspan="4">32 BITS</th></tr>
<tr><th>8</th><th>8</th><th>8</th><th>8</th></tr>
<tr><td colspan="2">HARDWARE TYPE</td><td colspan="2">PROTOCOL TYPE</td></tr>
<tr><td>HARDWARE ADDRESS LENGTH</td><td>PROTOCOL ADDRESS LENGTH</td><td colspan="2">OPERATION</td></tr>
<tr><td colspan="4">SENDER HARDWARE ADDRESS (OCTETS 0 - 3)</td></tr>
<tr><td colspan="2">SENDER HARDWARE ADDRESS (OCTETS 4-5)</td><td colspan="2">SENDER IP ADDRESS (OCTETS 0-1)</td></tr>
<tr><td colspan="2">SENDER IP ADDRESS (OCTETS 2-3)</td><td colspan="2">TARGET HARDWARE ADDRESS (OCTETS 0-1)</td></tr>
<tr><td colspan="4">TARGET HARDWARE ADDRESS (OCTETS 2-5)</td></tr>
<tr><td colspan="4">TARGET IP ADDRESS</td></tr>
</table>

ARP poisoning
The ARP protocol is declarative, it does not need an answer.
Nodes are not authenticated.
Limitations: it works only on LAN

Subnets and CIDR

Subnets are logical divisions of IP addresses. IP bits are partitioned as network,subnet,host.
A subnet mask indicates sections of IP addresses meant for network and subnet.
Eg. 255.255.255.0 means 24 bits for network and subnet and 8 bits for hosts.

CIDR

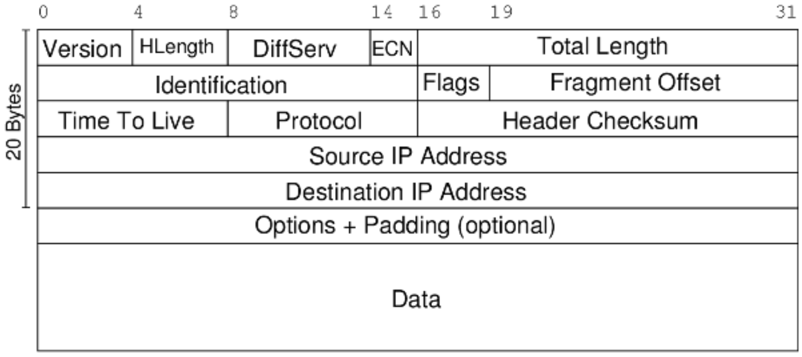
Classless Inter Domain Routing, it is a synthetic way to represent subnet masks.
Example:

- Network mask: 255.255.0.0.
- CIDR representation: 132.132.1.10/16
- Hosts = 2^{16}

Formulas: (everything as binary)

- Network = Ip AND Subnet
- Host = Ip AND Not(Subnet)

1.3 IP



Some IPs are reserved for private networks:

- 10.0.0.0 → 10.255.255.255
- 192.168.1.1 → 192.168.255.255
- 172.16.0.0 → 172.16.255.255

Def A *datagram* is a basic transfer unit associated with a packet-switched network. The delivery, arrival time, and order of arrival need not be guaranteed by the network.

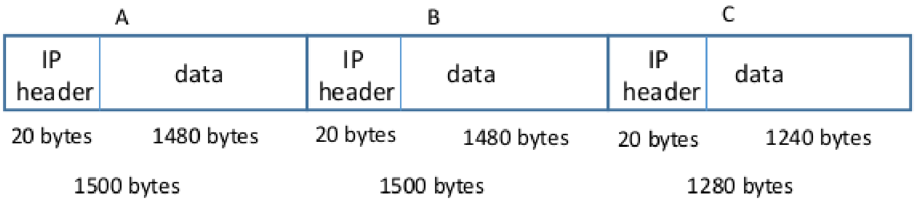
Def MTU maximum transmission unit

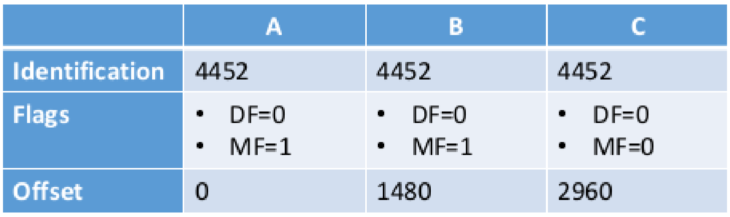
IP fragmentation *Identification:* 16 bit, is the unique identifier of the fragmented datagram. Note that all fragments have the same identification number.
Flags: 3 bits

- 0 Reserved, must be zero
- DF Don't fragment
  If set to 0 → there may be fragments
  If set to 1 → drop datagram if it has to be fragmented
- MF More fragments
  0 → last fragment
  1 → there are more fragments

Offset 13 bits, offset of this datagram wrt the first fragment with that ID

Fragmentation example



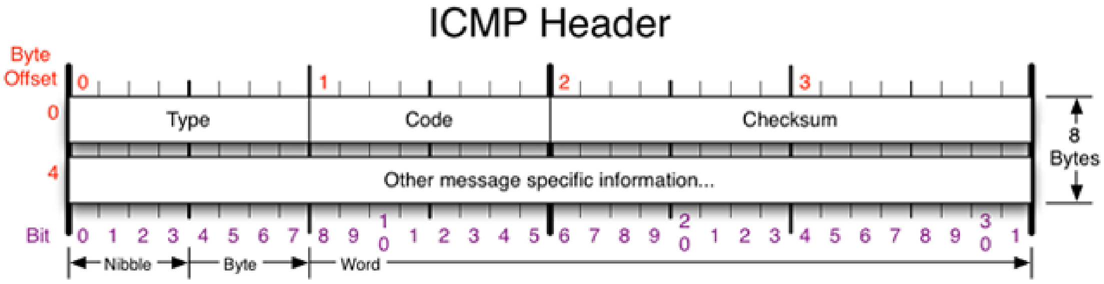


	A	B	C
Identification	4452	4452	4452
Flags	• DF=0 • MF=1	• DF=0 • MF=1	• DF=0 • MF=0
Offset	0	1480	2960

Remark 1. ***DOS with IP fragments*** *You keep sending fragments without sending the first fragment, the router keeps waiting for it until it exhausts its memory.*

1.4 ICMP

Internet control message protocol. It relies on IP and is and integral part of it.



Some message types

- 0 Echo Reply

- 3 Destination Unreachable
  Code 0 → Net unreachable
  Code 1 → Host unreachable
  Code 2 → Protocol unreachable
  Code 3 → Port unreachable
  Code 4 → Fragmentation needed and DF set
  Code 5 → Source route failed

- 4 Source Quench

- 5 Redirect

- 8 Echo

- 11 Time Exceeded
  Code 0 → Net unreachable
  Code 1 → Host unreachable

- 12 Parameter Problem

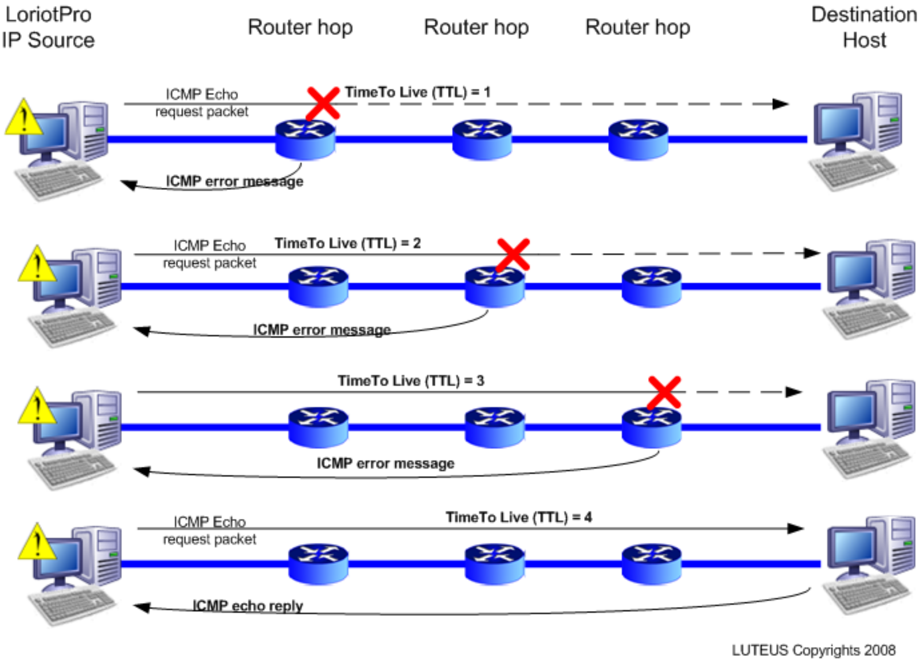
- 13 Timestamp

- 14 Timestamp Reply

- 15 Information Request

- 16 Information Reply

1.5 Traceroute



1.6 Denial of service

Def a Denial of Service is a type of attack that aims at congesting or overpowering a system's capacity by generating requests the system will have to answer.

Examples

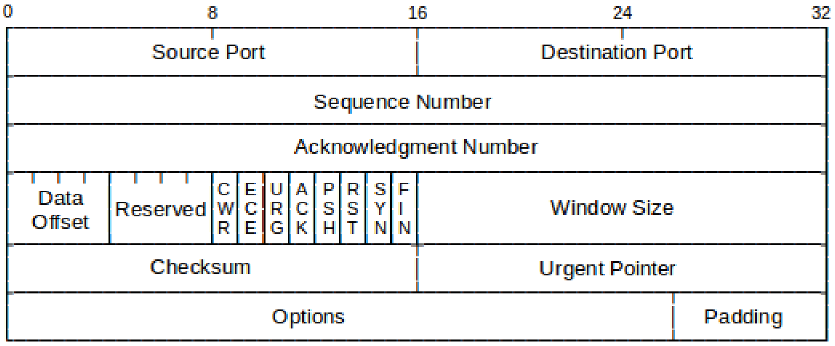
- Dos with IP fragmentation
- Ping Flooding (the attacker exploit his wider bandwidth)
- Ping of death

Chapter 2

Osi Transport Layer

2.1 TCP

The Transmission Control Protocol builds on top of IP the notion of state. Infact IP just delivers data while TCP manages the data segments by mean of checksums and re-delivery of unreceived/corrupted packets.

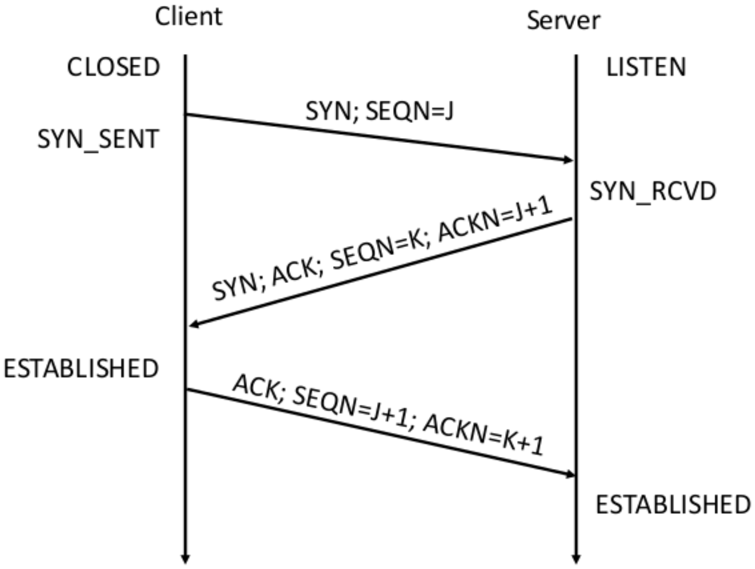


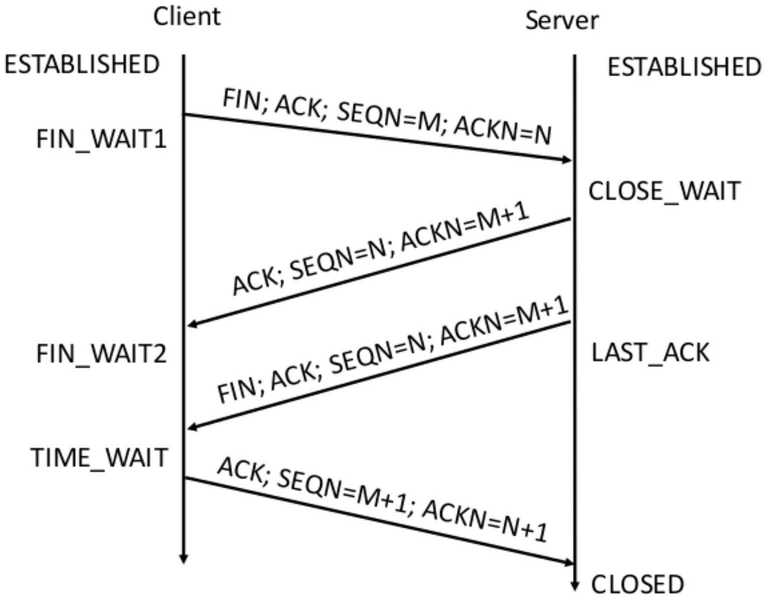
A server and a client that partecipate in a TCP connection open a *socket* which is a tuple (source-ip:source-port,destination-ip:destionation-port).
Note that a client generates a source port randomly.
TCP details - some flags:

- **SYN:** initializes the TCP session, it should be set to 1 only for the first datagram
- **ACK:** ackwnoledge the reception of the segment
- **FIN:** it signals the intention of closing the connection
- **RST:** drop the connection (reset)

Sequence number: it is a 32 bit generated by each end (note that the sequence number of the client is independent from the server's one).
Acknoledgement number: 32 bits

2.2 Handshakes





2.3 Some TCP specifics

Both client and server set up a TCB (Transmission control block) to keep track of connection. The TCB structure is freed from memory when connection reaches status CLOSED.

A packet with RST flag up does not receive an answer.
If the state is CLOSED any packet with no RST receives a RST.
If the state is LISTEN

- SYN flag up + no ACK opens a TCP session. Answer is SYN+ACK
- Only ACK receives a RST
- Drop with no answer otherwise

2.4 SYN DoS

When the server receives SYN J it answers back with SYN K, ACK J+1.
The server opens a new session in a separate threat/ allocates resources. Then the server waits for the ACK K+1 from the client, it waits for the MSL (maximum segment lifetime set by default to 2 minutes). The same mechanism is on the sender side but of course the attacker controls it and can bypass it.

The attacker drops all SYN ACKs with a firewall to avoid exhausting its own resources. Note that a server typically has more bandwidth than a single client.

Remark 2. *The attack currently works in $\mathcal{O}(2n)$ because for each SYN a SYN ACK is received $\rightarrow$ less bandwidth.*

However the attack can be improved by spoofing the source ip address, now the attacker is operating in $\mathcal{O}(n)$.
In theory the attack should not work because the server should receive a RST by each zombie, consequently free the TCB making the attack fail.
Still the attacker can choose a set of IPs which do not reply.

2.5 Dos mitigations

- Load balancing: distribute traffic loads evenly
- Rate limiter: deny traffic above a certain rate of SYN/sec
- Proof of work: require the source to solve a cryptopuzzle before allocating resources for the connection (note that this requires a protocol support).

2.6 TCP scans

It is possible to exploit specifications of a network protocol (TCP,UDP,..) to learn something about a system or a network.

SYN Scan: the attacker forges TCP packets with SYN=1. It is useful to see whether the remote system accepts incoming connections on a certain port.
Note that a polite way of scanning is performed in the following way: after the server's SYN ACK reply, the attacker sends a RST so that the 3-way handshake is never finished.

Host fingerprinting: different operating systems have their own independent implementation of the TCP stack.

Examples:

- FIN = 1
- all flags set to 0
- Xmas: FIN,URG,PSH = 1

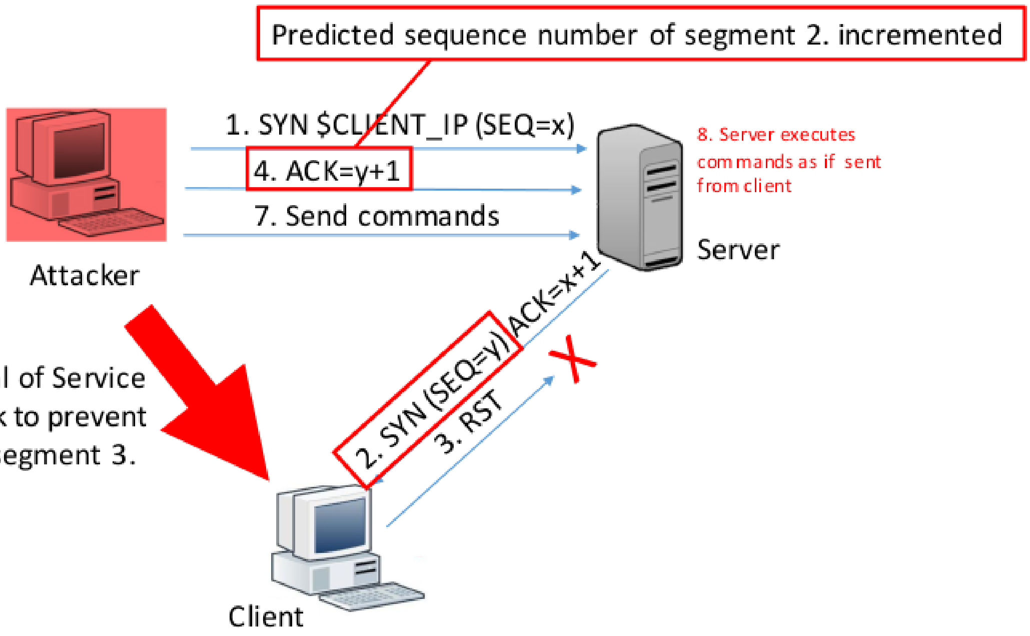
2.7 TCP Session hijacking - Mitnick attack

The attacker wants to send commands to a server they have no access to (eg. simple IP address authentication). The server has to think the attacker is the client, however the attacker does not sit in between client and server.

A TCP segment is identified and validated by:

- client ip → known
- destination ip → known
- port → known (if not standard, scan)
- client SEQ number → known(the attacker generates it)
- server SEQ number → *unknown*

Back in the old days algorithms for generating the SEQ number were really simple.


Predicted sequence number of segment 2. incremented
1. SYN $CLIENT_IP (SEQ=x)
4. ACK=y+1
7. Send commands
Attacker
8. Server executes commands as if sent from client
Server
2. SYN (SEQ=y) ACK=x+1
3. RST
Denial of Service Attack to prevent TCP segment 3.
Client

2.8 UDP

The User Datagram protocol is a stateless. It is designed for fast delivery of data

- Data integrity can be controlloed at application level
- It relies on the reliability of the underlying network link
- It does not guarantee delivery (there is no ACK mechanism)

Usage

- DNS servers
- NFS (network file systems)
- SNMP (simple network management protocol)
- DHCP (dinamic host configuration protocol)
- Most real time applications

2.9 UDP scans

It can be used to discover open ports on the network:

- CLOSE → ICMP port unreachable
- OPEN → no answer

However it is possible to configure a stealth system that does not reply to UDP requests to CLOSED ports by dropping ICMP packets with a firewall or router.

Chapter 3

Osi Session - Presentation - Application Layer

3.1 DNS

DNS (Domain Name Service) is a hierarchical system for domain name resolving. It translates human readable addresses to IP addresses the domain is reachable at. It uses UDP for fast answer (port 53).
Motivation: it is possible to assign multiple names to the same ip or viceversa. This flexibility is useful for:

- Server substitution
- Virtual hosting (a single server hosting multiple websites)
- A name is assigned to multiple IPs (so that the workload is distributed).

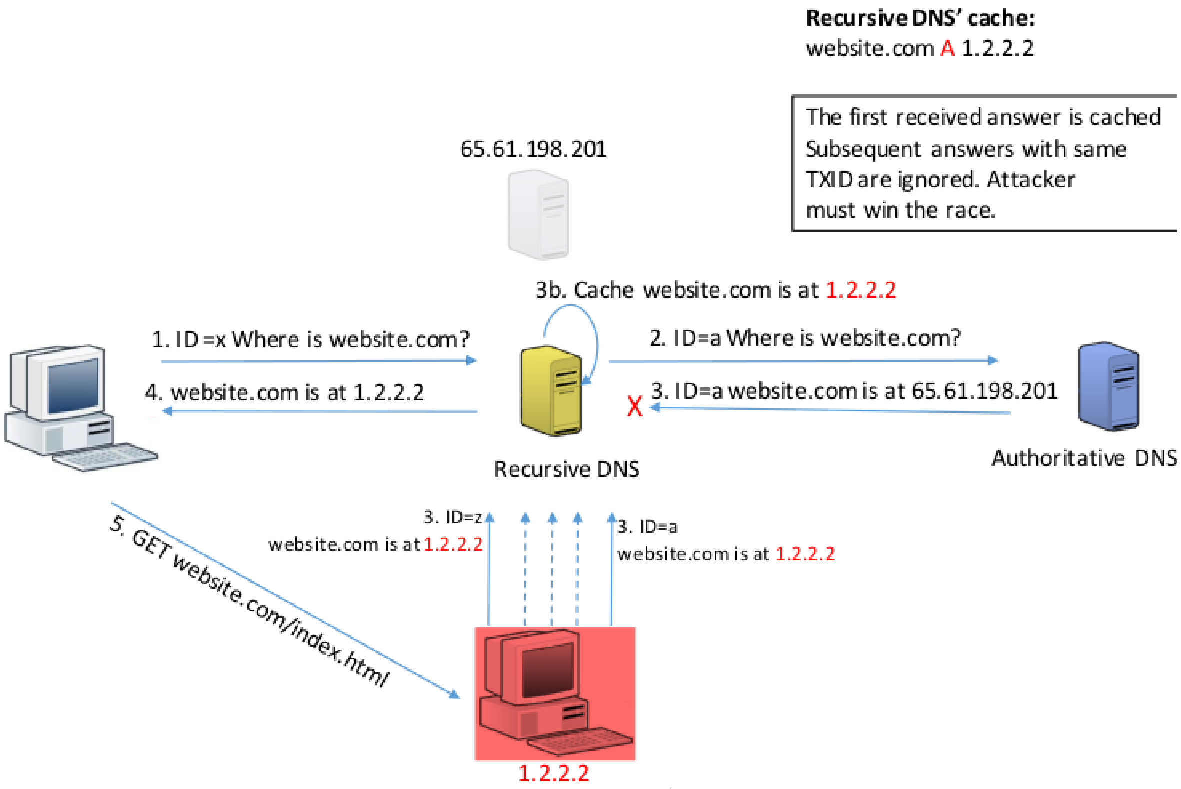
There exists different kind of DNS records, here we lista few:

- **A** correspondence name - IP(s)
- **AAAA** Same as A but works for ipv6
- **NS** ip of the DNS server to ask

DNS hierarchy

- Root DNSs → they are responsible for top level domain queries
- Authoritative DNS → A DNS that ”knows the answer” (ie. it does not ask to other DNSs)
- Recursive DNS → It forwards queries to authoritative DNSs

3.1.1 DNS Cache poisoning



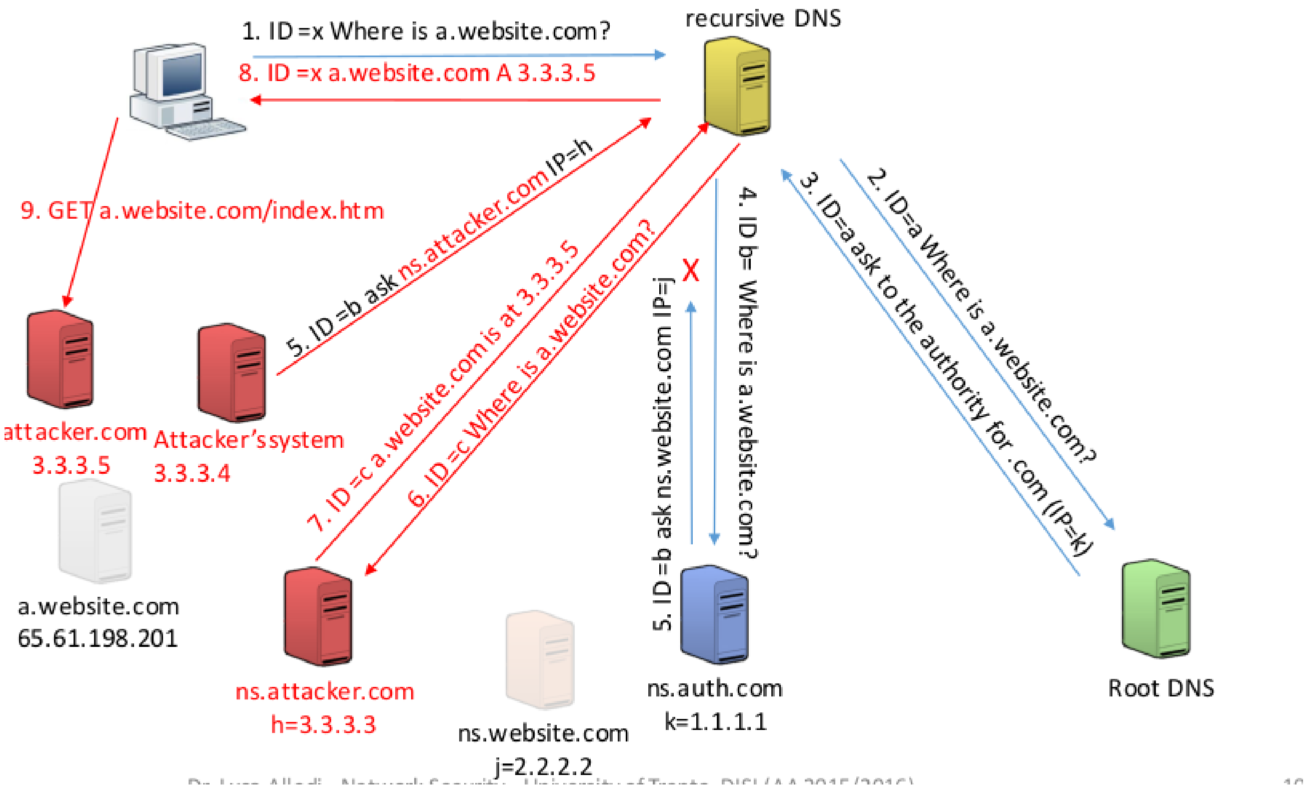
Recursive DNS' cache:
website.com A 1.2.2.2

The first received answer is cached Subsequent answers with same TXID are ignored. Attacker must win the race.

65.61.198.201
3b. Cache website.com is at 1.2.2.2
1. ID =x Where is website.com?
4. website.com is at 1.2.2.2
2. ID=a Where is website.com?
X
3. ID=a website.com is at 65.61.198.201
Recursive DNS
Authoritative DNS
3. ID=z
website.com is at 1.2.2.2
3. ID=a
website.com is at 1.2.2.2
5. GET website.com/index.html
1.2.2.2

3.1.2 Kaminsky attack

The attacker rather than replacing an A record replaces an NS record, in this way he can get control over any (sub)domain.


1. ID =x Where is a.website.com?
8. ID =x a.website.com A 3.3.3.5
recursive DNS
9. GET a.website.com/index.htm
5. ID =b ask ns.attacker.com IP=h
7. ID =c a.website.com is at 3.3.3.5
6. ID =c Where is a.website.com?
5. ID =b ask ns.website.com IP=j
X
4. ID b= Where is a.website.com?
3. ID=a ask to the authority for .com (IP=k)
2. ID=a Where is a.website.com?
attacker.com
3.3.3.5
Attacker's system
3.3.3.4
a.website.com
65.61.198.201
ns.attacker.com
h=3.3.3.3
ns.website.com
j=2.2.2.2
ns.auth.com
k=1.1.1.1
Root DNS

Mitigation: the source of attack is low entropy with a 16 bit ID. Randomness is not enough and it is not feasible to change the protocol to 32 bits.
The solution is to randomize the source port to increase the entropy: any answer that does not match both source port and transaction ID will be dropped.

3.1.3 DNS amplification attack

It is DoS attack that exploits certain types of DNS answers that are much bigger in size than the requests.
Recall that the DNS works over UDP so the source IP is easy to spoof.

3.1.4 DNS zone transfer

A sone is a domain for which a server is authoritative. "Slave" servers can ask "authoritative" servers to copy their zone database (over TCP).
An attacker pretends to be a slave server and dump the zone DB. In this way he acquires knowledge of zone's infrastructure and it is eased in performing further attacks.

3.1.5 DNS Sec

It is a secure implementation of the DNS protocol: it implements DNS auth on top of normal DNS. Note that it protects just integrity and not confidentiality.

3.2 HTTP

HTTP is the main protocol on which the www works. It is based on the notion that a client can either reuest or submit data to a server. There are two methods: GET and POST.
HTTP is stateless, HTTP cookies enable statefulness.

3.2.1 Cookies

- Domain (who can read)
- Expires (if NULL valid only for a session)
- Secure (only over SSL)

HTTP session hijacking the attacker can read the session ID cookie and spoof the victim's identity (eg. facebook until 2011).
Secure cookies provide confidentiality but no integrity.

3.3 Telnet

It is a protocol used in remote control services. It operates over TCP port 23. Typically there is no authentication and no encryption.

3.4 Common issues

- Lack of authentication
- Communication channel is in the clear

Chapter 4

Vulnerabilities

Software bug a bug is a problem in the execution of the software that leads to unexpected behaviour (eg. crashes,infinite loops, wrong entries of db displayed)
Charachteristics of a bug

- Replicability
- Logic/configuration/design/implementation
- Fix priority
- If it is documented it is a feature

4.1 Types of vulnerabilities

- Configuration v.
  eg. Ssh accepts root connections from any ip
- Insfrastructural v.
  eg. sensitive db in a network's DMZ
- Software v.
  eg. authorization mechanism can be bypassed

4.2 Vulnerability discovery

Vulnerabilities are different in nature

- Often implementation dependent
- May require deep understanding of sw module interaction
- Necessary in-depth knowledge of system design (kernel structure, memory allocation)

Discovery techniques

- Code lookups (searches for known patterns)
  either you are a developer or the software is open source

- Fuzzing (semi-automatic random input generation)
- Google hacking (outdated)
  you look for software that you already know it is vulnerable

Vulnerabilites can be found either internally or externally to a company.

4.3 Vulnerability handling

The ISO 30111 is a standard to handle vulnerabilities.
The initial investigation

- The reported problem is a security vulnerability
- The vulnerability affects a supported version of the software the vendors maintains, not third parties modules (else: exit).
- The vulnerability is eploitable with know techniwues (else: exit)
- Root cause analysis
- Prioritisation (evaluate potential threat)

Resolution decision
Vendor must decide how to resolve the vulnerability.

- Configuration v. → advisory may be enough
- Code v. → patch
- Critical v. → release a mitigation before full patch

Remediation development
Every solution must be tested before being delivered. This is very expensive both for customer and vendor

Release and Post-Release

4.4 Different issues

Vulnerability advisories are typically published after pathcing.
Security researchers expect economic return and or credit.
Issue: communication between security researcher and the vendor: tradeoff between saying little and being verbose.
Often involves development of Proof of concept exploit to show the vulnerability is exploitable.

4.5 Social Engineering

The biggest threat to the security of a company is not a computer virus, an unpatched hole in a key program or a badly installed firewall. In fact, the biggest threat could be you. What I found personally to be true was that it's easier to manipulate people rather than technology. Most of the time organisations overlook that human element
Kevin Mitnick

Social engineering identifies a set of techniques that attack weaknesses in human psychology.
Situational theory of publics: why people take action, or feel part of a collective

- Problem recognition → subject thinks the problem is relevant to them
- Active involvement → subject thinks he will suffer the consequences of the threat
- Constraint recognition → subject thinks his actions are limited by factors outside of their control

4.5.1 ELM - Elaboration Likelihood Model

ELM describes the ways humans change their attitudes or decide to perform actions they would not perform without external "stimuli".
Two routes to persuasions:

- Central route
  Stimuli are weighted by the subject and the final decision is carefully elaborated. Persuasions happens through careful elaboration of information
- Peripheral route
  Subject is convinced by under analyzing apparently relevant clues that are in reality unrelated to the subject matter. Examples of adjunct elements of the communication: likeability of subject,attractiveness,trust,etc.

Remark 3. *Social engineering differs from marketing in that attackers typically do not try to sell products. Rather social engineers must persuade victims to disclose sensitive or private network.*

4.5.2 Hacking a human

- **Reciprocation**
  Normative Commitment: subject will perform an action because it is customary or mandated by law or contract. It is based on the notion of reciprocation of benefits. When subject receives something he values he feels *cognitive dissonance* (eg. sun cream free tester example). People tend to comply because they feel gratitude for the unsolicited proposal.
- **Consistency**
  Continuance commitment: subject keeps doing a determined actio even if it is clearly bad (eg. lottery, keep spending money, eventually it will work).
  Upfront costs are low wrt promised benefit.
- **Social proof**
  Affective commitment: people are influenced by the opinion of those they esteem or like. Example: pretend you are on a vacation with a friend of the victim and ask money to solve an emergency

- **Likeability**
  If you like somebody you will trust him and viceversa
  Example: actors in advertisment

- **Authority**
  Subjects fear punishment and will comply
  Example: Milgram's experiment with electric shocks

- **Scarcity**
  Subject think freedom of choice is a function of time: similarly to fear scarcity leads people to take quick potentially uninformed decisions in fear of losing an opprtunity that will disappear in time or scarce in quantity.

Chapter 5

CVSS

Why to grade vulnerability?
Vulnerability counting can not be a measure of severity. Vulnerabilities are not the same (eg. XSS vs BoF).
Clients and user should be informed too: security researcher → vendor → user. A standard is needed.

5.1 Common vunerability system

CVSS is an open framework for communication the characteristics and severity of sw vulnerability.
The goal is different users score the same vulnerability in the same way → severity assessment and different people read the same vulnerability in the same way → severity communication.

Remark 4. *CVSS v2 and v3 are different*

CVSS v3 has three metrics:

- **Base metric**
  Exploitability metrics: attack vector, attack complexity, privilegs required, user interaction
  Scope metric (where is the vulnerability and wrt whom is affected)
  Impact metrics (CIA)
- **Temporal metric**
  Exploitability, remediation level,report confidence
- **Environmental metric**
  CIA requirements,mitigated base metrics

Example: think of ssh open to the wild or available just in the LAN, the environmental metrics measures this difference.

5.2 Attack vector

The more remote an attacker can be from the target the greater the vunlerability score. Possible values

- Network
- Adjacent network: same subnet
- Local: the attack needs to be locally on the system (log-in locally or rely user interaction, eg. virus by email)
- Physical

5.3 Attack complexity

This metrics describes the conditions beyond the attacker's control that must exist in order to exploit the vulnerability. Possible values:

- High: there is a grade of stochasticity meaning that the attack will not work with probability 1 eg. hash collision
- Low: specialized access conditions do not exist

Examples:

- Target specific reconnaisance (configuration settings, sequence numbers, shared secrets etc.) eg. ssh listening on default port 22
- Target environment: repeat exploitation to win a race condition
- the attacker injects himself into logical network path
  eg. the routing of packets is not in control of the attacker

5.4 Privileges required

Possible values:

- High → admin privileges
- Low → guest, any account is going to work
- None

5.5 Scope

Scope refers to the collection of privileges defined by a computer authority (eg. an application,an operating system, a sandbox environment etc.)

5.6 Summary

Field	**Value**			
Access Vector	Network	Adjacent network	Local	Physical
Access complexity	High	Low		
Privileges required	High	Low	None	-
User interaction	Required	None	-	-
Scope	Unchanged	Changed	-	-
Impact	High	Low	None	-