CSE 127: Introduction to Security

Lecture 13: Network Attacks

Deian Stefan

UCSD

Fall 2020

Material from Nadia Heninger, Stefan Savage, David Wagner, and Nick Weaver

Threat modeling for network attacks

Basic security goals:

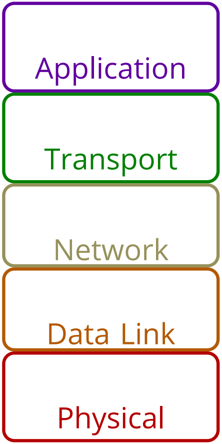
- **Confidentiality:** No one should be able to read our data/communications unless we want them to.
- **Integrity:** No one can manipulate our data/communications unless we want them to.
- **Availability:** We can access our data/communication capabilities when we want to.

Threat modeling for network attacks

Attacker capabilities:

- **Physical access:** Attacker has physical access to the network infrastructure.
- **In path/Man in the middle:** Attacker can see, add, and block packets.
- **On path/Man on the side:** Attacker can see and add packets, but cannot block packets.
- **Passive:** Attacker can see victim’s network traffic, but cannot add or modify packets.
- **Off path:** Attacker cannot see network traffic of the victim.

Different attacks at different layers



Application

Transport

Network

Data Link

Physical

- DNS, HTTP, HTTPS
- TCP, UDP
- IP, BGP
- Ethernet, WiFi, ARP
- Physical wires, photons, RF modulation

Physical/link layer threats

Eavesdropping: Violates confidentiality.

Who can see the packets you send?

- Network (routers, switches, access points) see all traffic passing by.

Physical/link layer threats

Eavesdropping: Violates confidentiality.

Who can see the packets you send?

- Network (routers, switches, access points) see all traffic passing by.
- Unprotected WiFi network:
- WPA2 Personal (PSK):
- Non-switched Ethernet:
- Switched Ethernet: maybe everyone on the same network

Network eavesdropping

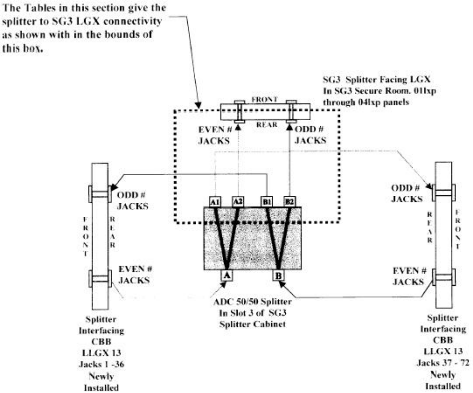
Tools like tcpdump and Wireshark let you capture local network traffic

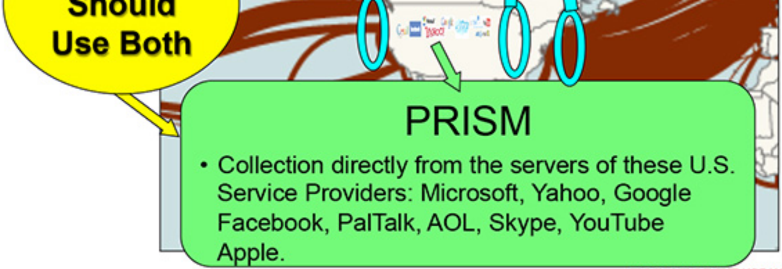
```
$ sudo tcpdump -v -n -i eno1
tcpdump: listening on eno1, link-type EN10MB (Ethernet), capture size 262144 bytes
17:29:41.757880 IP (tos 0x10, ttl 64, id 38565, offset 0, flags [DF], proto TCP (6), length 176)14)
    132.239.15.243.4258 > 66.10.100.54.62681: Flags [P.], cksum 0x3bc5 (incorrect -> 0x2e82), seq 16870791
17:29:41.770734 IP (tos 0x0, ttl 50, id 0, offset 0, flags [DF], proto TCP (6), length 52)
    66.10.100.54.62681 > 132.239.15.243.4258: Flags [.], cksum 0x8e71 (correct), ack 124, win 11736, optio
17:29:41.789239 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 132.239.15.119 tell 132.239.15.1, len
17:29:41.936864 IP (tos 0x0, ttl 1, id 20121, offset 0, flags [none], proto UDP (17), length 202)
    132.239.15.210.65021 > 239.255.255.250.1900: UDP, length 174
17:29:42.036268 IP6 (hlim 1, next-header UDP (17) payload length: 83) fe80::225:b3ff:fefa:a13d.546 > ff02:
17:29:42.390349 IP (tos 0x0, ttl 64, id 35459, offset 0, flags [DF], proto UDP (17), length 51)
    132.239.15.243.40288 > 172.217.4.138.443: UDP, length 23
17:29:42.419390 IP (tos 0x0, ttl 57, id 0, offset 0, flags [DF], proto UDP (17), length 48)
    172.217.4.138.443 > 132.239.15.243.40288: UDP, length 20
17:29:42.443102 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 132.239.15.34 tell 132.239.15.1, leng
17:29:42.541827 STP 802.1w, Rapid STP, Flags [Learn, Forward], bridge-id 81b0.00:a3:d1:25:06:00.801a, leng
        message-age 2.00s, max-age 20.00s, hello-time 2.00s, forwarding-delay 15.00s
        root-id 21b0.3c:08:f6:21:a8:40, root-pathcost 2001, port-role Designated
17:29:43.752250 IP (tos 0x0, ttl 64, id 61970, offset 0, flags [DF], proto TCP (6), length 109)
    132.239.15.243.55866 > 52.37.243.173.443: Flags [P.], cksum 0xbd14 (incorrect -> 0xcfbd), seq 3280138
17:29:43.788285 IP (tos 0x0, ttl 38, id 43082, offset 0, flags [DF], proto TCP (6), length 109)
    52.37.243.173.443 > 132.239.15.243.55866: Flags [P.], cksum 0x65eb (correct), seq 1:58, ack 57, win 8
17:29:43.788311 IP (tos 0x0, ttl 64, id 61971, offset 0, flags [DF], proto TCP (6), length 52)
    132.239.15.243.55866 > 52.37.243.173.443: Flags [.], cksum 0xbcdb (incorrect -> 0xab20), ack 58, win 5
17:29:43.905367 IP (tos 0x0, ttl 128, id 19913, offset 0, flags [none], proto UDP (17), length 414)
    132.239.15.14.17500 > 255.255.255.255.17500: UDP, length 386
17:29:43.907037 IP (tos 0x0, ttl 128, id 59034, offset 0, flags [none], proto UDP (17), length 414)
    132.239.15.14.17500 > 132.239.15.255.17500: UDP, length 386
17:29:43.907052 IP (tos 0x0, ttl 128, id 19914, offset 0, flags [none], proto UDP (17), length 414)
    132.239.15.14.17500 > 255.255.255.255.17500: UDP, length 386
17:29:43.907057 IP (tos 0x0, ttl 128, id 19915, offset 0, flags [none], proto UDP (17), length 414)
    132.239.15.14.17500 > 255.255.255.255.17500: UDP, length 386
17:29:43.907060 IP (tos 0x0, ttl 128, id 19916, offset 0, flags [none], proto UDP (17), length 414)
```

Advanced threats: Physical cables can be tapped

Mathew F. Casamassima, (732) 420-2033, mcasamassima@att.com

Splitter to SG3 LGX Connectivity


The Tables in this section give the splitter to SG3 LGX connectivity as shown with in the bounds of this box.
SG3 Splitter Facing LGX In SG3 Secure Room. 01lxp through 04lxp panels
FRONT
REAR
EVEN # JACKS
ODD # JACKS
A1
A2
B1
B2
A
B
ODD # JACKS
EVEN # JACKS
FRONT
REAR
ODD # JACKS
EVEN # JACKS
REAR
FRONT
ADC 50/50 Splitter In Slot 3 of SG3 Splitter Cabinet
Splitter Interfacing CBB LLGX 13 Jacks 1 -36 Newly Installed
Splitter Interfacing CBB LLGX 13 Jacks 37 - 72 Newly Installed



Should
Use Both

PRISM

- Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google Facebook, PalTalk, AOL, Skype, YouTube Apple.

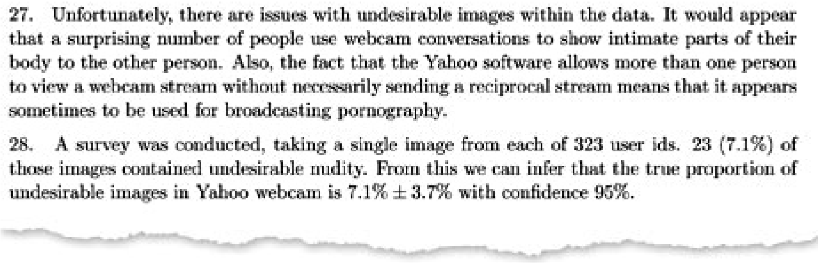
TOP SECRET//SI//ORCON//N

Optic Nerve

> "Optic Nerve was based on collecting information from GCHQ's huge network of internet cable taps, which was then processed and fed into systems provided by the NSA. Webcam information was fed into NSA's XKeyscore search tool, and NSA research was used to build the tool which identified Yahoo's webcam traffic."
>
> – The Guardian 2/27/14

Optic Nerve

> "Optic Nerve was based on collecting information from GCHQ's huge network of internet cable taps, which was then processed and fed into systems provided by the NSA. Webcam information was fed into NSA's XKeyscore search tool, and NSA research was used to build the tool which identified Yahoo's webcam traffic."
>
> – The Guardian 2/27/14



27. Unfortunately, there are issues with undesirable images within the data. It would appear that a surprising number of people use webcam conversations to show intimate parts of their body to the other person. Also, the fact that the Yahoo software allows more than one person to view a webcam stream without necessarily sending a reciprocal stream means that it appears sometimes to be used for broadcasting pornography.

28. A survey was conducted, taking a single image from each of 323 user ids. 23 (7.1%) of those images contained undesirable nudity. From this we can infer that the true proportion of undesirable images in Yahoo webcam is 7.1% ± 3.7% with confidence 95%.

Advanced threats: Physical cables can be tapped

Trevor Paglen, NSA-Tapped Undersea Cables, North Pacific Ocean, 2016

Physical/link layer threats

Injection: Violates integrity.

- Ethernet packets are unauthenticated: attacker who can inject traffic can create a frame with any addresses they like.

Packet injection: ARP spoofing

- Recall: ARP used to map IP addresses to MAC addresses on local network

```
$ sudo tcpdump -v -n -i eno1
tcpdump: listening on eno1, link-type EN10MB (Ethernet), capture size 262144 bytes
17:29:47.455929 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 172.16.15.1
    tell 172.16.15.151, length 46
```

- ARP requests broadcast to local subnetwork
- Anyone can send an ARP response
- Attacker on local network can impersonate any other host.

Physical/link layer threats

Jamming: Violates availability.

- Physical signals can be overwhelmed or disrupted.
- Radio transmission depends on power and distance.

Radio jamming: P25 law enforcement radios

Figure 1: Motorola XTS5000 Handheld P25 Radio

By careful synchronization, a jammer that attacks only the NID subfield of voice traffic can reduce its overall energy output so that it effectively has *more than 14dB of average power advantage* over the legitimate transmitter.

Radio jamming: P25 law enforcement radios

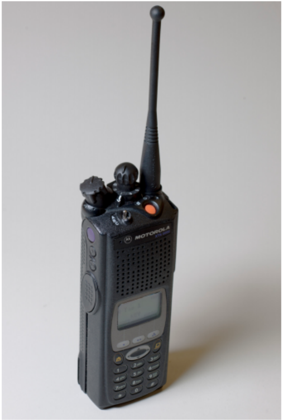


Figure 1: Motorola XTS5000 Handheld P25 Radio

By careful synchronization, a jammer that attacks only the NID subfield of voice traffic can reduce its overall energy output so that it effectively has *more than 14dB of average power advantage* over the legitimate transmitter.

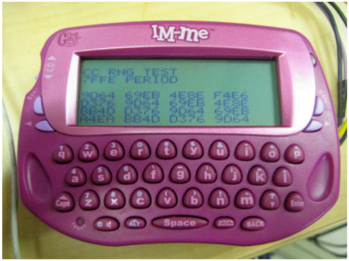


Figure 7: Girltech IMME, with modified firmware

While any CC1110 board for the correct frequency range is sufficient, we used the *GirlTech IMME,* a commercial toy intended for pre-teen children to text message one another without cellular service. Presently priced at $30 USD, the package includes a handheld unit and a USB adapter, either of which may be used with our P25 client (for an aggregate price of $15 per jammer).

Why (Special Agent) Johnny (Still) Can't Encrypt: A Security Analysis of the APCO Project 25 Two-Way Radio System Clark et al. 2011

Network layer threats

Spoofing: Set arbitrary source address.

- IP packets offer no authentication.
- Source address in IP set by sender.
- Off-path attacker who spoofs a source address may not be able to see response sent to that address. (Sometimtimes that’s okay.)

Example: DHCP response spoofing

- Recall: DHCP used to configure hosts on network.

Example: DHCP response spoofing

- Recall: DHCP used to configure hosts on network.
- DHCP requests broadcast to local network.
- Local attacker can race real server for response, set victim’s network gateway and DNS server to attacker-controlled values.
- Allows attacker to act as invisible man-in-the-middle and relay victim’s traffic.

Network layer threats

Set arbitrary destination address: No authentication of traffic sender at network layer

Applications:

- **Network scanning:**
  - Example tools: nmap, zmap, shodan
  - IPv4 has 2^{32} possible addresses, possible to enumerate all of them.
  - Send traffic to a port on some protocol, if you get a response then there is a live service.
- **Unwanted traffic:**
  - Denial of service attacks: overwhelm recipient with traffic

Network Layer Threats

Misdirection: BGP hijacking.

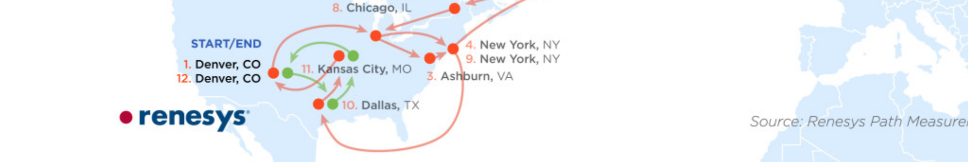
- Recall: BGP protocol manages IP routing information between networks on the internet.
- Each BGP node maintains connections to a set of trusted neighbors.
- Neighbors share routing information.
- Routes are not authenticated: malicious or malfunctioning nodes may provide incorrect routing information that redirects IP traffic.

Compliance report should reach this office through return fax or at email peshawar@pta.gov.pk today please.

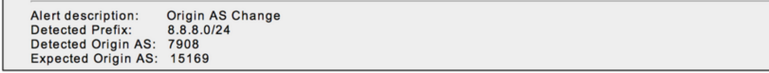
Deputy Director
(Enforcement)

To:

1. M/s Comsats, Peshawar.
2. M/s GOL Internet Services, Peshawar.
3. M/s Cyber Internet, Peshawar.
4. M/s Cybersoft Technologies, Islamabad.
5. M/s Paknet, Limited, Islamabad
6. M/s Dancom, Peshawar.
7. M/s Supernet, Peshawar.



Source: Renesys Path Measure



```
Alert description:     Origin AS Change
Detected Prefix:       8.8.8.0/24
Detected Origin AS:    7908
Expected Origin AS:    15169
```

TCP threats

Recall:

- TCP session identified by (source address, source port, destination address, destination port)
- TCP packets identified by sequence number that determines where in stream they are placed.

On-path injection

- Connection hijacking: If an on-path attacker knows ports and sequence numbers, can inject data into the TCP connection.
- RST injection: Attacker can inject RST into connection to immediately stop it, will be accepted if sequence number is within acceptable window.
    - China’s great firewall famously does this to block traffic.

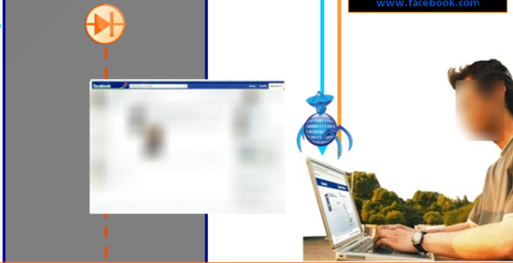
1. A target requests connection to www.facebook.com

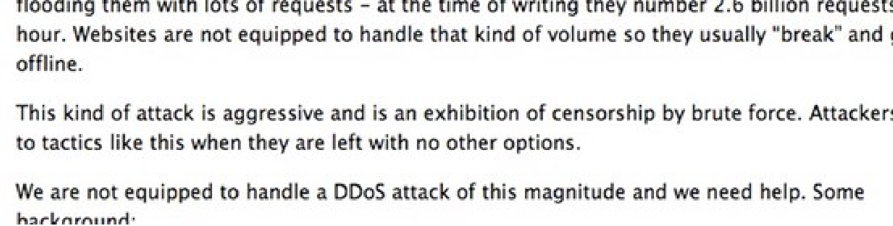
2. The target initiates frequent, periodic data pushes requests from the Facebook server.

3. Passive collection site detects data push requests and tips TURBINE.

4. TURBINE redirects the target to a TAO server by beating the Facebook server response. Response window can be as long as 55 seconds.

5. TAO server attempts to implant the target.

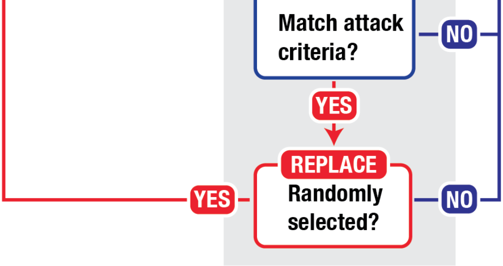




flooding them with lots of requests – at the time of writing they number 2.6 billion requests
hour. Websites are not equipped to handle that kind of volume so they usually "break" and
offline.

This kind of attack is aggressive and is an exhibition of censorship by brute force. Attackers
to tactics like this when they are left with no other options.

We are not equipped to handle a DDoS attack of this magnitude and we need help. Some
background:


Match attack criteria?
NO
YES
REPLACE
Randomly selected?
YES
NO

TCP threats

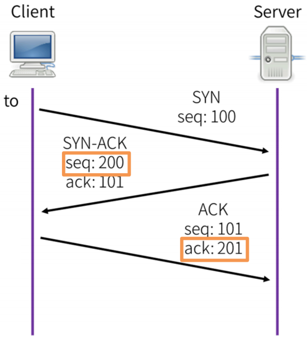
Blind spoofing: Can an off-path attacker convince a victim to open a TCP connection with a spoofed host?

- Attacker forges the initial TCP handshake SYN message from an arbitrary source.
- The attacker cannot see the SYN-ACK response so does not learn the responder’s sequence number.

TCP threats

Blind spoofing: Can an off-path attacker convince a victim to open a TCP connection with a spoofed host?

- Attacker forges the initial TCP handshake SYN message from an arbitrary source.
- The attacker cannot see the SYN-ACK response so does not learn the responder's sequence number.
- Initial TCP spec: initial sequence number based on local clock.
- Now should be random: 2^{-32} chance of guessing correctly.



Application layer threats: DNS spoofing

Recall:

- DNS maps between domain names and IP addresses.
- Responses cached to avoid query times.

DNS Threat Models:

- **Malicious DNS server:** Any DNS server in query chain can lie about responses.

Application layer threats: DNS spoofing

Recall:

- DNS maps between domain names and IP addresses.
- Responses cached to avoid query times.

DNS Threat Models:

- **Malicious DNS server:** Any DNS server in query chain can lie about responses.
- **Local/on-path attacker**: Can impersonate DNS server and send a fake response.

Application layer threats: DNS spoofing

Recall:

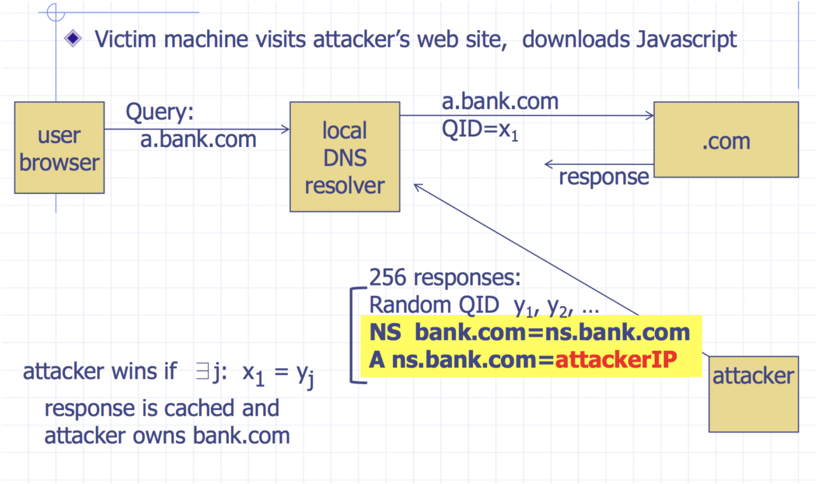
- DNS maps between domain names and IP addresses.
- Responses cached to avoid query times.

DNS Threat Models:

- **Malicious DNS server:** Any DNS server in query chain can lie about responses.
- **Local/on-path attacker**: Can impersonate DNS server and send a fake response.
- **Off-path attacker:** Can try to forge response: needs to match 16-bit query ID.
  - Original spec: query ID increments with each request.
  - Now: Random query ID.

DNS spoofing: 2008 Kaminsky attack

DNS spoofing: 2008 Kaminsky attack



- Victim machine visits attacker’s web site, downloads Javascript

user browser

Query: a.bank.com

local DNS resolver

a.bank.com QID=x_1

.com

response

256 responses:
Random QID y_1, y_2, …
NS bank.com=ns.bank.com
A ns.bank.com=attackerIP

attacker

attacker wins if $\exists j$: $x_1 = y_j$

response is cached and
attacker owns bank.com

- Birthday bound: attacker expects to succeed after $2^8 = 256$ lookups
- Mitigation: randomize source port

- (TS//SI//REL) QUANTUMBOT2
  - Combination of Q-BOT/Q-BISCUIT for web based Command and controlled botnets

Conclusion:

- Internet built from protocols that assumed trustworthy network operators.
- Next lecture: How to add security after the fact.