Network Defenses

KAMI VANIEA
26 SEPTEMBER 2017
First the news...

First the news...

Tutorials

• Tutorials start in week 3
• We originally had tutorials and labs, now we just have tutorials
• “Tutorials” are very lab like
Today

• Open System Interconnect (OSI) model
• Firewalls
• Network Address Translation (NAT)
• Intrusion detection systems (IDS)
OSI Network Model
Open Systems Interconnect model

- A good way to think about networking steps logically
- Not how software is actually built

Image from: http://www.tech-faq.com/osi-model.html
OSI in terms of debugging errors

Can your browser open another website?

Do you have a viewer that supports jpg (image format)?

Can you ping the webserver you are trying to reach?

Can you ping the gateway or DNS server?

Do you have an IP address?

Is the light on the modem on?

Is the network cable plugged in?
Data starts at the top of the OSI stack at level 7.

It progresses down the stack with each successive level adding or changing information.

At level 1 it travels across the physical layer to the recipient computer.

The recipient then processes the data up the stack. At level 7 an application processes the data.

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
<th>OSI Stack</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Application</td>
<td>Apache</td>
<td>Firefox user</td>
</tr>
<tr>
<td>6</td>
<td>Presentation</td>
<td>Network</td>
<td>Transport</td>
</tr>
<tr>
<td>5</td>
<td>Session</td>
<td>Data Link</td>
<td>Network</td>
</tr>
<tr>
<td>4</td>
<td>Transport</td>
<td>Physical</td>
<td>Physical</td>
</tr>
<tr>
<td>3</td>
<td>Network</td>
<td>Physical</td>
<td>Data Link</td>
</tr>
<tr>
<td>2</td>
<td>Data Link</td>
<td>Physical</td>
<td>Physical</td>
</tr>
<tr>
<td>1</td>
<td>Physical</td>
<td>Physical</td>
<td>Physical</td>
</tr>
</tbody>
</table>
Information is added to the message as it travels down the OSI levels

- Levels 7 and 6 involve the internal representation of the message
- Levels 5 and 4 involve setting up the connection
- Levels 3, 2, and 1 add header (H) and tail (T) information to each packet

<table>
<thead>
<tr>
<th>Layer</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Application&lt;br/&gt;Network process to application</td>
</tr>
<tr>
<td>6</td>
<td>Presentation&lt;br/&gt;Data representation and encryption</td>
</tr>
<tr>
<td>5</td>
<td>Session&lt;br/&gt;Interhost communication</td>
</tr>
<tr>
<td>4</td>
<td>Transport&lt;br/&gt;End-to-end connection and reliability</td>
</tr>
<tr>
<td>3</td>
<td>Network&lt;br/&gt;Path determination and IP (Logical Addressing)</td>
</tr>
<tr>
<td>2</td>
<td>Data Link&lt;br/&gt;MAC and LLC (Physical Addressing)</td>
</tr>
<tr>
<td>1</td>
<td>Physical&lt;br/&gt;Media, signal, and binary transmission</td>
</tr>
</tbody>
</table>
Header data on a packet

1. Physical
2. Data link
3. Network
4. Transport
... 
6. Transport
7. Application
Frame header data on a packet

1. Physical
2. Data link
3. Network
4. Transport
... 
7. Application

Information needed to physically transport the packet
IP header data on a packet

1. Physical
2. Data link
3. Network
4. Transport
5. Internet
6. Transport
7. Application

Internet Protocol (IP) information

Version 4

Type of the next header

Source and destination IP addresses
Information is added to the message as it travels down the OSI levels

- Levels 7 and 6 involve the internal representation of the message
- Levels 5 and 4 involve setting up the connection
- Levels 3, 2, and 1 add header (H) and tail (T) information to each packet

### OSI Model

<table>
<thead>
<tr>
<th>Layer</th>
<th>Type and Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Application</td>
</tr>
<tr>
<td>6</td>
<td>Presentation</td>
</tr>
<tr>
<td>5</td>
<td>Session</td>
</tr>
<tr>
<td>4</td>
<td>Transport</td>
</tr>
<tr>
<td>3</td>
<td>Network</td>
</tr>
<tr>
<td>2</td>
<td>Data Link</td>
</tr>
<tr>
<td>1</td>
<td>Physical</td>
</tr>
</tbody>
</table>

- **Application**: Network process to application
- **Presentation**: Data representation and encryption
- **Session**: Interhost communication
- **Transport**: End-to-end connection and reliability
- **Network**: Path determination and IP (Logical Addressing)
- **Data Link**: MAC and LLC (Physical Addressing)
- **Physical**: Media, signal, and binary transmission
This is me visiting https://slashdot.org

- 6 packets were sent from my computer to the server
- 50 packets were sent from the server to my computer
This is me visiting http://vaniea.com

- Note the lack of https
- Why does the text look garbled anyway?
Firewalls
Firewalls

- Firewalls divide the untrusted outside of a network from the more trusted interior of a network
- Often they run on dedicated devices
  - Less possibilities for compromise – no compilers, linkers, loaders, debuggers, programming libraries, or other tools an attacker might use to escalate their attack
  - Easier to maintain few accounts
  - Physically divide the inside from outside of a network
Sample Network

- User
  - Mobile Devices
    - Wireless Access Point
  - Personal Devices
  - Home PC
  - Home Router
- Desktop PCs and laptops
- Boundary Firewall
- Email, web and application servers
- Databases
- 3rd party server
  - Card Readers
  - Email, web and application servers
  - Databases
- 3rd party server
Questionable things come from the internet AND from the local network.

Firewall applies a set of rules.

Based on rules, it allows or denies the traffic.

Firewalls can also act as routers deciding where to send traffic.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Type</th>
<th>Source Address</th>
<th>Destination Address</th>
<th>Destination Port</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TCP</td>
<td>*</td>
<td>192.168.1.*</td>
<td>22</td>
<td>Permit</td>
</tr>
<tr>
<td>2</td>
<td>UDP</td>
<td>*</td>
<td>192.1681.*</td>
<td>69</td>
<td>Permit</td>
</tr>
<tr>
<td>3</td>
<td>TCP</td>
<td>192.168.1.*</td>
<td>*</td>
<td>80</td>
<td>Permit</td>
</tr>
<tr>
<td>4</td>
<td>TCP</td>
<td>*</td>
<td>192.168.1.18</td>
<td>80</td>
<td>Permit</td>
</tr>
<tr>
<td>5</td>
<td>UDP</td>
<td>*</td>
<td>192.168.1.*</td>
<td>*</td>
<td>Deny</td>
</tr>
</tbody>
</table>
Sender: Apache server

<table>
<thead>
<tr>
<th>Level</th>
<th>Layer</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Application</td>
<td>Network process to application</td>
</tr>
<tr>
<td>6</td>
<td>Presentation</td>
<td>Data representation and encryption</td>
</tr>
<tr>
<td>5</td>
<td>Session</td>
<td>Interhost communication</td>
</tr>
<tr>
<td>4</td>
<td>Transport</td>
<td>End-to-end connection and reliability</td>
</tr>
<tr>
<td>3</td>
<td>Network</td>
<td>Path determination and IP (Logical Addressing)</td>
</tr>
<tr>
<td>2</td>
<td>Data Link</td>
<td>MAC and LLC (Physical Addressing)</td>
</tr>
<tr>
<td>1</td>
<td>Physical</td>
<td>Media, signal, and binary transmission</td>
</tr>
</tbody>
</table>

Recipient: Firefox user

<table>
<thead>
<tr>
<th>Level</th>
<th>Layer</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Application</td>
<td>Network process to application</td>
</tr>
<tr>
<td>6</td>
<td>Presentation</td>
<td>Data representation and encryption</td>
</tr>
<tr>
<td>5</td>
<td>Session</td>
<td>Interhost communication</td>
</tr>
<tr>
<td>4</td>
<td>Transport</td>
<td>End-to-end connection and reliability</td>
</tr>
<tr>
<td>3</td>
<td>Network</td>
<td>Path determination and IP (Logical Addressing)</td>
</tr>
<tr>
<td>2</td>
<td>Data Link</td>
<td>MAC and LLC (Physical Addressing)</td>
</tr>
<tr>
<td>1</td>
<td>Physical</td>
<td>Media, signal, and binary transmission</td>
</tr>
</tbody>
</table>
A firewall takes in network traffic and compares it to a set of rules. In order to do so it must first process several OSI levels to reach the data it needs.

For example, to filter out all traffic from IP 216.34.181.45 the packet needs to be processed through level 3 where IP addresses can be read.
Firewall ruleset from a custom home router

- Taken from an ARSTechnica article

```
#### Service rules
# OpenVPN
-A INPUT -p udp -m udp --dport 1194 -j ACCEPT

# ssh - drop any IP that tries more than 10 connections per minute
-A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m recent --set --name DEFAULT --mask 255.255.255.255 -m recent --set --name DEFAULT --mask 255.255.255.255 --source
-A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m recent --update --seconds 60 --hitcount 11 --name DEFAULT --mask 255.255.255.255 --source --j LOGDROP
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT

# www - accept from LAN
-A INPUT -i p1p1 -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -i p1p1 -p tcp -m tcp --dport 443 -j ACCEPT

# DNS - accept from LAN
-A INPUT -i p1p1 -p tcp --dport 53 -j ACCEPT
-A INPUT -i p1p1 -p udp --dport 53 -j ACCEPT

# default drop because I'm awesome
-A INPUT -j DROP

#### forwarding ruleset
```

Image: http://arstechnica.co.uk/gadgets/2016/01/numbers-dont-lie-its-time-to-build-your-own-router/
There are many types of Firewalls

Key differences include:

• How implemented
  ◦ Software – slower, easier to deploy on personal computers
  ◦ Hardware – faster, somewhat safer, harder to add in

• Number of OSI levels of processing required
  ◦ Packet size (level 1)
  ◦ MAC (level 2) and IP (level 3) filtering
  ◦ Port filtering (level 3)
  ◦ Deep packet (level 4+)

Today we will talk about:

• Packet filtering gateway
• Stateful inspection firewall
• Application proxy
• Personal firewalls
Packet filtering gateway or screening router

- Simplest – compares information found in the headers to the policy rules
- Operate at OSI level 3
- Source addresses and ports can be forged, which a packet filter cannot detect
- Design is simple, but tons of rules are needed, so it is challenging to maintain
Stateful inspection firewall

- Maintains state from one packet to another
- Similar to a packet filtering gateway, but can remember recent events
- For example, if an outside host starts sending packets to many internal destination ports (aka a port scan) a stateful firewall would record the number of ports probed and once it is over the threshold specified in the policy it would block all further traffic
Port scan

- An attacker is looking for applications listening on ports
- A single IP address (right) is contacting many ports (left) to see if any respond

Firewall ruleset from a custom home router

- Taken from an ARSTechnica article

```
### Service rules
# OpenVPN
-A INPUT -p udp -m udp --dport 1194 -j ACCEPT

# ssh - drop any IP that tries more than 10 connections per minute
-A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m recent --set --name DEFAULT --mask 255.255.255.255 --source
-A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m recent --update --seconds 60 --hitcount 11 --name DEFAULT --mask 255.255.255.255 --source -j LOGDROP
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT

# www - accept from LAN
-A INPUT -i p1p1 -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -i p1p1 -p tcp -m tcp --dport 443 -j ACCEPT

# DNS - accept from LAN
-A INPUT -i p1p1 -p tcp --dport 53 -j ACCEPT
-A INPUT -i p1p1 -p udp --dport 53 -j ACCEPT

# default drop because I'm awesome
-A INPUT -j DROP

### Forwarding ruleset
```

Image: http://arstechnica.co.uk/gadgets/2016/01/numbers-dont-lie-its-time-to-build-your-own-router/
Application proxy

• Simulates the (proper) effects of an application at OSI level 7
• Effectively a protective Man In The Middle that screens information at an application layer (OSI 7)
• Allows an administrator to block certain application requests.
• For example:
  ◦ Block all web traffic containing certain words
  ◦ Remove all macros from Microsoft Word files in email
  ◦ Prevent anything that looks like a credit card number from leaving a database
Personal firewalls

• Runs on the workstation that it protects (software)
• Provides basic protection, especially for home or mobile devices
• Malicious software can disable part or all of the firewall
• Any rootkit type software can disable the firewall
Network Address Translation (NAT)
Looking at the IP address of my laptop which is connected to the University WIFI.
My computer as seen from a remote server
(http://www.hashemian.com/whoami/)

My IP previously showed as:
172.20.106.96

What happened?

HTTP_ACCEPT: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
HTTP_ACCEPT_ENCODING: gzip, deflate
HTTP_ACCEPT_LANGUAGE: en-US,en;q=0.5
HTTP_CONNECTION: keep-alive
HTTP_COOKIE: __utma=145846189.271110778.1474893692.1474893692.1474893692.1; __utmz=1474893692.1.1.utmc=1474893692.1.utmcsr=google|utmcd=organic|utmcmd=organic|utmctr=(not%20provided)|utmcs=organic|utmccn=( organic) PRUM_EPISODES=s=1474893750106&r=ht tp%3A//www.hashemian.com/whoami/
HTTP_HOST: www.hashemian.com
HTTP_REFERER: https://www.google.co.uk/
HTTP_UPGRADE_INSECURE_REQUESTS: 1
HTTP_USER_AGENT: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:49.0) Gecko/20100101 Firefox
REMOTE_ADDR: 192.168.131.255
REMOTE_PORT: 7535
REQUEST_METHOD: GET
REQUEST_TIME: 1474906336
REQUEST_URI: /whoami/
SERVER_ADDR: 173.162.146.61
SERVER_NAME: www.hashemian.com
SERVER_PORT: 80
SERVER_PROTOCOL: HTTP/1.1
SERVER_SIGNATURE:
SERVER_SOFTWARE: Apache
IPv4 and address space exhaustion

• Version 4 of the Internet Protocol
  ◦ 192.168.2.6

• There are less than 4.3 billion IPv4 addresses available

• We do not have enough addresses for every device on the planet

• Answer: Network Address Translation
  ◦ Internal IP different than external IP
  ◦ Border router maps between its own IP and the internal ones
My laptop can have multiple IPs and bridge networks too. Here it shows IPs for both my VirtualBox and my WIF.
Intrusion Detection Systems (IDS)
Firewalls are preventative, IDS detects a potential incident in progress

• At some point you have to let some traffic into and out of your network (otherwise users get upset)
• Most security incidents are caused by a user letting something into the network that is malicious, or by being an insider threat themselves
• These cannot be prevented or anticipated in advance
• The next step is to identify that something bad is happening quickly so you can address it
Signature based

• Perform simple pattern matching and report situations that match the pattern
• Requires that admin anticipate attack patterns in advance
• Attacker may test attack on common signatures
• Impossible to detect a new type of attack
• High accuracy, low false positives
Heuristic based

• Dynamically build a model of acceptable or “normal” behavior and flag anything that does not match
• Admin does not need to anticipate potential attacks
• System needs time to warm up to new behavior
• Can detect new types of attacks
• Higher false positives, lower accuracy
Number of alarms is a big problem

- In the Target breach the IDS did correctly identify that there was an attack on the Target network
- There were too many alarms going off to investigate all of them in great depth
- Some cyberattack insurance policies state that if you know about an attack and do nothing they will not cover the attack.
- Having a noisy IDS can potentially be a liability
Questions