About the Midterm

- Close book; Close notes; Close computer/phone/calculator; No cheat sheet.
- You are NOT allowed to leave the room during the exam.
- There are 6 problems (100 points in total).
- You have **75 minutes**
- Please try to make your hand-writing readable.
- *Student with special need, please contact me after the class.*
Recap: Example Spoofing

Urgent! Response needed immediately.

To: uitest12767@yahoo.com

Dear Mr. Hu,

This email is to inform you that your VISA is going to expire soon. If you don't renew it in 48 hours, your status will be illegal.
[Click Here](mailto:Click Here) to renew your VISA.

Thank you,
The United States Citizenship and Immigration Services (USCIS)
Re-Cap: Email Spoofing

- SMTP has no authentication
  - "MAIL FROM" can be set to anything (e.g., a spoofing target)
    - Also called Return-Path
    - The delivery address of your reply email
  - "From" fields in header can be changed to anything
    - Directly visible to users

- Widely used for spear phishing
Anti-spoofing Protocols Exist, but not widely adopted

- **SPF**: authentication by IP
  - Proposed in 2001, standardized in 2014
  - DNS: specifies the IP range that can send email on behalf of x.com

- **DKIM**: public key based method
  - Drafted in 2004, standardized in 2011
  - Sender domain signs the email

- **DMARC**:
  - Drafted in 2011, standardized in 2015
  - Complementary to SPF and DKIM (addressed the identifier alignment issue)
  - Specific “what to do” when authentication fails
Anti-Spoofing protocols: Technical Weaknesses

- **SPF**: authentication by IP
  - Mail forwarding breaks SPF
  - identifier alignment is not required, deceptive to users

- **DKIM**: public key based method
  - Mailing list often modify content, breaks DKIM signature
  - Identifier alignment is not required, deceptive to users

- **DMARC**:
  - Still not widely used
  - Cannot correctly handle mailing lists
DKIM Weaknesses: Identifier Alignment

Domain that signs the message

DKIM-Signature: v=1; a=rsa-sha256; d=attacker.com; s=pp-dkim1; c=relaxed/relaxed; q=dns/txt; i=@attacker.com; t=1480474251;
  h=From:From:Subject:Date:To:MIME-Version:Content-Type;
  bh=...; b=...

Subject: Urgent! Response needed immediately.

From: visa@uscis.gov

Domain displayed to users

To: uitest12767@yahoo.com

The email sender domain that user sees is different from the one that is actually used to perform DKIM authentication
Email Providers cannot (fully) detect Spoofing

Security indicator?

- Unknown usability
- Do people understand?
Network Scanning
The Problem of Network Security

- The Internet allows an attacker to attack from anywhere in the world
- They just need to find one vulnerability: a security analyst need to close every vulnerability.
Pre-Attack: Network Scanning

Nmap (“Network Mapper”) is an open source tool for network exploration and security auditing.

- Nmap uses raw IP packets to determine
  - what hosts are available on the network,
  - what services (application name and version) those hosts are offering,
  - What operating systems (and OS versions) they are running,
  - what type of packet filters/firewalls are in use
She was using nmap (Matrix Reloaded) to discover that citypower uses vulnerable SSH software

Source: https://nmap.org/movies/matrix/matrix-nmap.mp4
Checkout Z-Map

- **https://zmap.io/**
- Single machine, scan IPv4 address space in under **5 minutes**
- IPv4: 32-bits IP, in total **4,294,967,296 IPv4 addresses**

ZMap is an open-source network scanner that enables researchers to easily perform Internet-wide network studies. With a single machine and a well-provisioned network uplink, ZMap is capable of performing a complete scan of the IPv4 address space in under 5 minutes, approaching the theoretical limit of ten gigabit Ethernet.

ZMap can be used to study protocol adoption over time, monitor service availability, and help us better understand large systems distributed across the Internet.

Check out our [Getting Started Guide](https://zmap.io), read our [Research Paper](https://zmap.io), or go and [Download ZMap](https://zmap.io) yourself.
Network Attack: Gaining Access?

Network Attacks:
- Sniffing (Eavesdropping)
- IP Address Spoofing
- Session Hijacking

System Attacks:
- Buffer Overflow
- Password Cracking
- SQL Injection
- Web Protocol Abuse
- Denial of Service
- Virus, Worm, Trojan

Login: Ginger  Password: Snap
Passive Attacks

- **Eavesdropping (Sniffing)**
  - Listen to packets from other parties

- **Traffic Analysis**
  - Learn about network from observing traffic patterns

- **Footprinting (Network Mapping)**
  - Test to determine software installed on system
Some Active Attacks

Denial of Service
- Message did not make it; or service could not run

Masquerading or Spoofing
- The actual sender is not the claimed sender

Message Modification
- The message was modified in transmission (Man-in-the-middle)

Packet Replay
- A past packet is transmitted again in order to gain access
Man-in-the-Middle Attack

1. Login
2. Login
3. Password
4. Password
Botnets

Attacker

Command and Control
C&C

Botnets: Bots

Bots: Host illegal movies, music, pornography, criminal web sites, …
Forward Spam for financial gain

Zombies
Distributed Denial of Service (DDOS)

Attacker → Command and Control (C&C) → Zombies → Victim

Can barrage a victim server with requests, causing the network to fail to respond to anyone.
Common Attacks & Countermeasures

- Finding a way into the network
  - Firewalls
- Exploiting software vulnerabilities
  - Intrusion Detection Systems (IDS)
- TCP hijacking
  - IPSec
- Denial of Service
  - Ingress filtering, IDS
- Packet sniffing
  - Encryption (SSH, SSL, HTTPS)
- Social engineering problems
  - Education
**Firewalls**

- Isolates organization’s internal net from larger Internet
- Allows some packets to pass, blocking others
- Can help to defend against **port scan**
Firewalls: Why

- Allow only authorized access to inside network
- Prevent illegal modification/access of internal data
  - e.g., attacker replaces CIA’s homepage with something else
- Prevent denial of service attacks:
  - SYN flooding: attacker establishes many bogus TCP connections, no resources left for “real” connections
- 2 types of firewalls:
  - Stateless packet filters
  - Stateful packet filters
TCP 3-Way Handshake
Stateless packet filtering

- Internal network connected to Internet via router firewall
- Router filters packet-by-packet, decision to forward/drop packet based on:
  - source IP address, destination IP address
  - TCP/UDP source and destination port numbers
  - ICMP message type
  - TCP SYN and ACK bits

Should arriving packet be allowed in? Departing packet let out?

TCP 3-way handshake

Stateful FW vs. stateless FW
# Access Control Lists

**ACL**: table of rules, applied top to bottom to incoming packets: (action, condition) pairs

## Table of Access Control List Rules

<table>
<thead>
<tr>
<th>action</th>
<th>source address</th>
<th>dest address</th>
<th>protocol</th>
<th>source port</th>
<th>dest port</th>
<th>flag bit</th>
</tr>
</thead>
<tbody>
<tr>
<td>allow</td>
<td>222.22/16</td>
<td>outside of 222.22/16</td>
<td>TCP</td>
<td>&gt; 1023</td>
<td>80</td>
<td>any</td>
</tr>
<tr>
<td>allow</td>
<td>outside of 222.22/16</td>
<td>222.22/16</td>
<td>TCP</td>
<td>80</td>
<td>&gt; 1023</td>
<td>ACK</td>
</tr>
<tr>
<td>allow</td>
<td>222.22/16</td>
<td>outside of 222.22/16</td>
<td>UDP</td>
<td>&gt; 1023</td>
<td>53</td>
<td>---</td>
</tr>
<tr>
<td>allow</td>
<td>outside of 222.22/16</td>
<td>222.22/16</td>
<td>UDP</td>
<td>53</td>
<td>&gt; 1023</td>
<td>----</td>
</tr>
<tr>
<td>deny</td>
<td>all</td>
<td>all</td>
<td>all</td>
<td>all</td>
<td>all</td>
<td>all</td>
</tr>
</tbody>
</table>

- **Allow HTTP initiated from inside**
- **Allow DNS inbound & outbound**
## Stateless packet filtering examples

<table>
<thead>
<tr>
<th>Policy</th>
<th>Firewall Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>No outside Web access.</td>
<td>Drop all outgoing packets to any IP address, port 80</td>
</tr>
<tr>
<td>No incoming TCP connections, except those for institution’s public Web server only.</td>
<td>Drop all incoming TCP SYN packets to any IP except 130.207.244.203, port 80</td>
</tr>
<tr>
<td>Prevent streaming audio/video from eating up the available bandwidth.</td>
<td>Drop all incoming UDP packets - except DNS and router broadcasts.</td>
</tr>
<tr>
<td>Prevent your network from being used for a smurf DoS attack.</td>
<td>Drop all ICMP packets going to a “broadcast” address (eg 130.207.255.255).</td>
</tr>
<tr>
<td>Prevent your network from being tracerouted</td>
<td>Drop all outgoing ICMP TTL expired traffic</td>
</tr>
</tbody>
</table>
Stateful packet filtering
(Protocol state analysis)

- Stateless packet filter:
  - admits packets that “make no sense” e.g., dest port = 80, ACK bit set, even though no TCP connection established:

<table>
<thead>
<tr>
<th>Action</th>
<th>Source Address</th>
<th>Dest Address</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Dest Port</th>
<th>Flag Bit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow</td>
<td>outside of 222.22/16</td>
<td>222.22/16</td>
<td>TCP</td>
<td>80</td>
<td>&gt; 1023</td>
<td>ACK</td>
</tr>
</tbody>
</table>

- Stateful packet filter: track status of every TCP connection
  - track connection setup (SYN), teardown (FIN)
  - determine whether incoming, outgoing packets “makes sense”
  - timeout inactive connections at firewall: no longer admit packets
**Stateful packet filtering**

ACL augmented to indicate need to check connection state table before admitting packet

<table>
<thead>
<tr>
<th>action</th>
<th>source address</th>
<th>dest address</th>
<th>proto</th>
<th>source port</th>
<th>dest port</th>
<th>flag bit</th>
<th>check conn. table</th>
</tr>
</thead>
<tbody>
<tr>
<td>allow</td>
<td>222.22/16</td>
<td>outside of 222.22/16</td>
<td>TCP</td>
<td>&gt; 1023</td>
<td>80</td>
<td>any</td>
<td></td>
</tr>
<tr>
<td>allow</td>
<td>outside of 222.22/16</td>
<td>222.22/16</td>
<td>TCP</td>
<td>80</td>
<td>&gt; 1023</td>
<td>ACK</td>
<td>✗</td>
</tr>
<tr>
<td>allow</td>
<td>222.22/16</td>
<td>outside of 222.22/16</td>
<td>UDP</td>
<td>&gt; 1023</td>
<td>53</td>
<td></td>
<td></td>
</tr>
<tr>
<td>allow</td>
<td>outside of 222.22/16</td>
<td>222.22/16</td>
<td>UDP</td>
<td>53</td>
<td>&gt; 1023</td>
<td>----</td>
<td>✗</td>
</tr>
<tr>
<td>deny</td>
<td>all</td>
<td>all</td>
<td>all</td>
<td>all</td>
<td>all</td>
<td>all</td>
<td>all</td>
</tr>
</tbody>
</table>

Source address | Dest address | Source port | Dest port
--- | --- | --- | ---
222.22.17 | 37.96.87.123 | 12699 | 80
222.22.93.2 | 199.1.205.23 | 37654 | 80

Reject if not part of ongoing connections

Ongoing connections
Limitations of firewalls

- **IP spoofing**: router can’t know if data “really” comes from claimed source

- If multiple applications need special treatment, each has own app gateway

- Client software must know how to contact gateway.
  - set IP address of proxy in Web browser

- **Tradeoff**: degree of communication with outside world, level of security

- Many highly protected sites still suffer from attacks.
Intrusion Detection Systems (IDS)
Intrusion Detection Systems

- Packet filtering in firewalls:
  - Operates on TCP/IP headers only
  - No correlation check among sessions
- **IDS: intrusion detection system**
  - *Deep packet inspection*: look at packet contents (e.g., check strings in packet against database of known virus)
  - Examine correlation among multiple packets
    - port scanning, network mapping, DoS attack
- Generate alerts when it observes potentially malicious traffic
- **Passive** monitoring
A different method: Intrusion Prevention System

- IPS: **actively** filters out suspicious traffic
- Terminate connections, blocking access of user accounts, IP addresses
- Respond to detected threats at a real time
  - Delete malicious content
  - Apply patches
  - Reconfigure a firewall or router
  - Run executables in virtual environments
- Cisco global correlation IPS
  - Reputation scores for the sources
  - Reputation obtained from centralized databases
Signature based IDS

- Signature based IDS maintains a database of attack signatures.
- Each signature is a set of rules pertaining to an intrusion activity.
- A list of characteristics of a single or a series of packets:
  - Packet size, source, destination port numbers, protocol type, payload.
- Limitations:
  - Blind to new attacks (false negatives).
  - False alarms (false positives).
  - High Costs – every packet is compared to a large collection of signatures.

<table>
<thead>
<tr>
<th>False positive rate</th>
<th>False negative rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>True positive rate = 1 - FP</td>
<td>True negative rate = 1 - FN</td>
</tr>
</tbody>
</table>
How to detect previously unknown attacks
Anomaly based IDS [Dorothy Denning 86]

- Observe normal traffic first, then,
- Look for packet streams that are statistically unusual
  - Unusual percentage of ICMP packets
  - Sudden exponential growth in port scans and ping echo requests

- Advantage: can detect new attacks (in theory)
- Disadvantage:
  - Need to have a lot of training data to see what normal is
  - Hard to distinguish normal from abnormal activities (e.g., stealthy malware)
IPSec

- Network layer security protocol
- Designed for IPv6, backwards-compatible for IPv4
Attack models and security goals in IP protocol

- IP forgery attacks
  - Attacker forges an IP address
- Eavesdropping attacks
  - Attacker learns the content of IP packets

[Goal 1] Authenticity of IP addresses (AH and ESP)
[Goal 2] Confidentiality of IP packets
  - Payload of IP packets (ESP)
  - Header of IP packets (tunneling mode in IPSec)
**Authentication Header (AH)**

**Encapsulating Security Payload (ESP)**

**AH protocol [Light mode]:**
- Source authentication, data integrity
- No confidentiality
- AH header inserted between IP header and data field.
- ICV (integrity check value)

**ESP Protocol [Full mode]**
- Source authentication, data integrity, and confidentiality
- Payload encrypted
- More complex than AH

---

**IP header**

**AH header**

**data (e.g., TCP, UDP segment)**

**IP datagram with an AH header**
Tunneling Mode vs. Transport Mode

**Tunneling mode** encapsulates the IP header
- generates a new IP header, treats the old one as part of datagram payload
- for **anonymity** purpose (hides real destination IP addresses)

**Transport mode** is simpler (does not generate new IP header)

<table>
<thead>
<tr>
<th></th>
<th>Transport Mode</th>
<th>Tunneling Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication header (AH)</td>
<td>AH+Transport (new AH header)</td>
<td>AH+Tunneling (new AH header, new IP header)</td>
</tr>
<tr>
<td>Encapsulating security payload (ESP)</td>
<td>ESP+Transport (payload encryption)</td>
<td>ESP+Tunneling (payload encryption)</td>
</tr>
</tbody>
</table>
ESP with Tunnel mode or Transport mode

http://docs.hp.com/en/J4255-90011/ch04s03.html
Key management in IPSec

- **Manual:** system admins manually configure crypto algorithms and secret keys
  - Pre-shared keys
  - Only suitable for small, low-risk environments

- **Automated:** crypto algorithms and keys are obtained automatically
  - Internet Key Exchange protocol (IKE)
  - Uses public key cryptography to distribute keys
  - Suitable for large, high-risk environments
VPN
Virtual private networks (VPN)

- VPN: end-to-end secure connections over public Internet
  - Using authentication and encryption to protect payload

- Creates virtual channels of connected entities
  - host-to-host, Host-gateway, Gateway-to-gateway

- VPN can work on different network layers
  - PGP (application layer)
  - SSL (transport layer)
  - IPSec (network layer)
  - PPTP (data link layer)

Tunneling

- Tunneling is to encapsulate one type of packet into another
  - DNS tunneling: e.g., encapsulating arbitrary data into DNS packets
  - HTTP tunneling: e.g., encapsulating SMTP traffic in HTTP traffic

- Sender and receiver agree on format, interpretation
- Deep packet inspection may detect tunnels
  - Probability distribution of payload
- E.g., firewall only allows HTTP traffic,
- Encapsulate SMTP traffic in HTTP packets
Encapsulate SMTP into HTTP packet

SMTP packet For 9.3.1.1

HTTP packet for 9.3.1.1

4.2.1.8

Internet

9.3.1.1

SMTP packet For 9.3.1.1

payload

HTTP packet for 9.3.1.1
PPTP (point-to-point tunneling protocol)

VPN at data link layer

- Protects frames on the network
  - Create tunnel to hide entire payload of frames
  - Encapsulation of data-link frame & IP datagram

- No inherent encryption capabilities
  - Encryption can be added to obtain data confidentiality
  - (in true VPN)

Alternative: L2TP (layer-2 tunneling protocol)
PPTP (point-to-point tunneling protocol)
**PPTP (point-to-point tunneling protocol)**

**Without VPN:**
- IP datagram (to final-destination)
- Ethernet MAC (to ISP’s router)

**Encryption with shared key with VT VPN server:**
- IP datagram (to VT’s LAN router)
- Ethernet MAC (to VT’s LAN router)
- IP datagram (to final-destination)
- Ethernet MAC (to ISP’s router)

**For getting out of the ISP’s network:**
- Encryption with shared key with VT VPN server
- IP datagram (to VT’s VPN server)
- Ethernet MAC (to ISP’s router)

**payload**
VPN pros and cons

- Advantages of VPN
  - Security - confidentiality, integrity, authentication
  - Leverage existing network infrastructure – ease of deployment

- Disadvantage of VPN
  - Process overhead: to encrypt, encapsulate every packet
  - High workload for VPN gateways
  - Each frame contains few useful payload bytes
  - Incompatible with network address translation (NAT)