Week 10 - Monday

COMP 4290

Last time

- Network reconnaissance
- Eavesdropping
- Wireless vulnerabilities
- Started denial of service attacks

Questions?

Project 3

Colm Oneacre Presents

Denial of Service

Denial of service

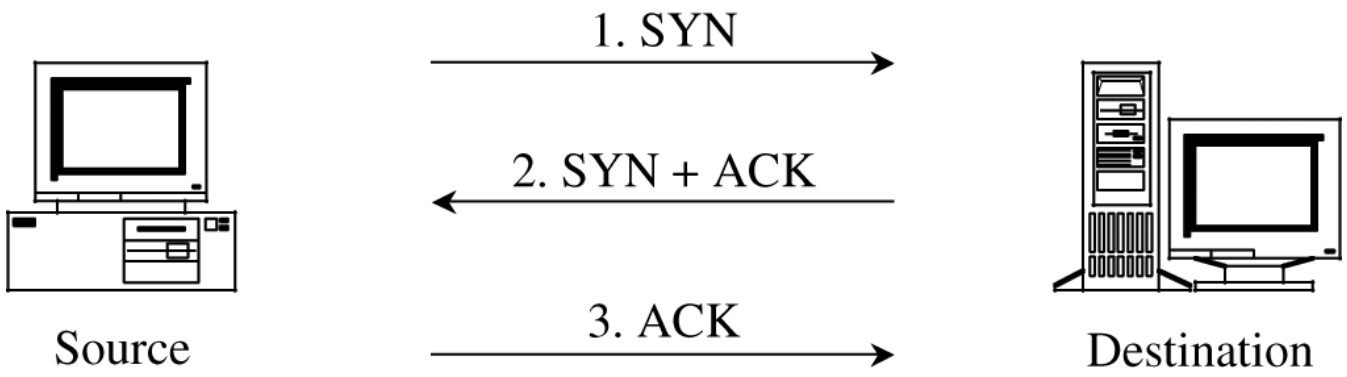
- Networks are one of the best places to launch an attack on availability
- In this setting, these are usually called **denial of service** (DoS) attacks
- DoS attacks are very hard to avoid

Ways to make DoS happen

- Flooding overloads capacity
  - Ask for too many connections
  - Request too many of some other service
- Blocking access
  - Crash an application
  - Interfere with network routing protocols
- Access failure
  - Hardware or software fails

SYN flood

- TCP is built on a three-way handshake
  - Client requests a connection by sending a **SYN** packet
  - The server acknowledges the request by sending a **SYN-ACK** packet back
  - The client responds with an **ACK**, establishing the connection
- An attacker can just keep sending **SYN** packets
- The server will allocate some resources, wait for the **ACK**, and never get it
- A clever attacker will spoof at least his own IP so that the **SYN-ACK** is sent elsewhere
- A more sophisticated attacker will spoof many different IP addresses (or have many bots in a botnet) sending all these **SYN**'s

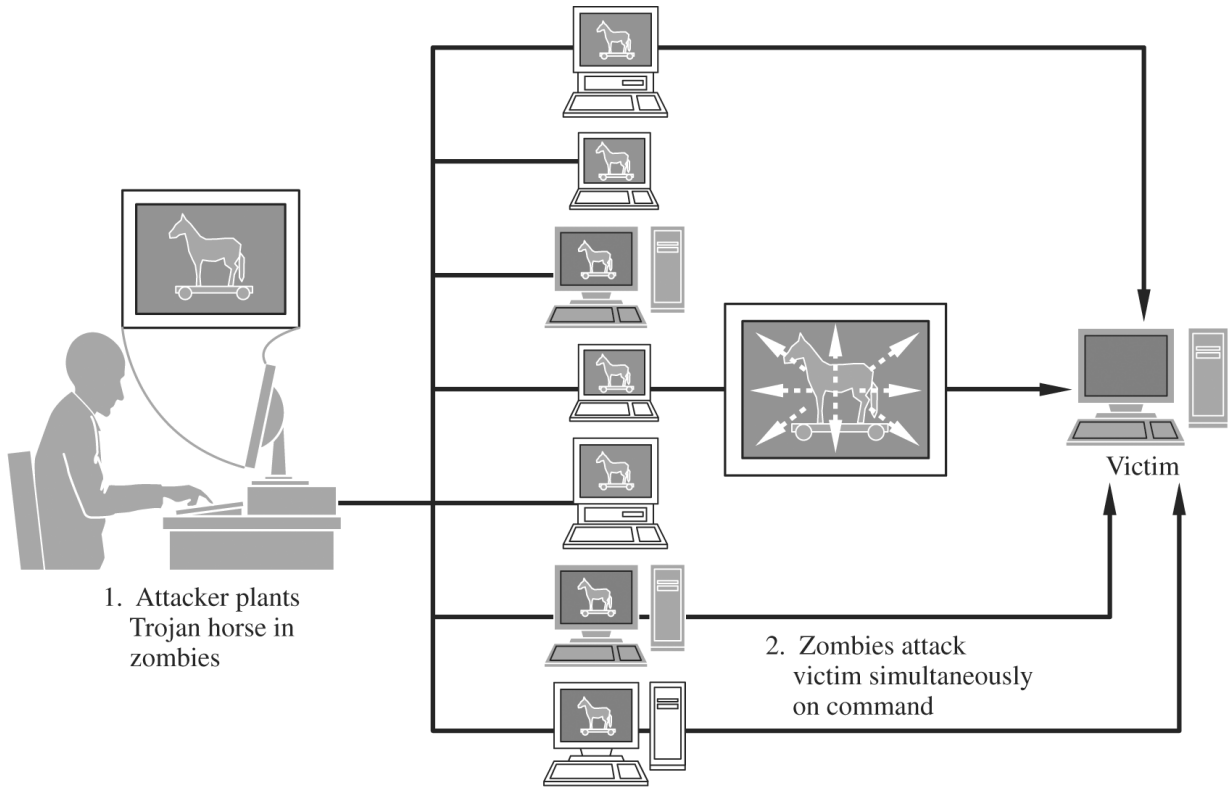


Other denial of service attacks

- Echo-chargen
  - Chargen sets up a stream of packets for testing
  - Echo packets are supposed to be sent back to the sender
  - If you can trick a server into sending echo packets to itself, it will respond to its own packets forever
- Ping of death
  - A ping packet requests a reply
  - If you can send more pings than a server can handle, it goes down
  - Only works if the attacker has more bandwidth than the victim (DDoS helps)
- Smurf
  - A ping packet is broadcast to everyone, with the victim spoofed as the originator
  - All the hosts try to ping the victim
  - The real attacker is hidden
- Teardrop
  - A teardrop attack uses badly formed IP datagrams
  - They claim to correspond to overlapping sequences of bytes in a packet
  - There's no way to put them back together and the system can crash

Distributed denial of service

- **Distributed denial of service** (DDoS) attacks use many machines to perform a DoS attack
- Usually, many targets have been compromised with a Trojan horse making them **zombies** or **bots**
- These zombie machines are controlled by the attacker, performing flooding or other attacks on a victim
  - A network of zombies is called a **botnet**
- The attacker is hard to trace



Stopping DDoS attacks

- The best defense is prevention
  - DDoS attacks are usually mounted by bots that were compromised by known vulnerabilities
  - Patch your stuff!
- Defense against DoS attacks:
  - Tuning: adjusting the number of active servers
  - Load balancing: redirecting traffic to servers that aren't getting used
  - Shunning: reducing service given to certain IP addresses
  - Blacklisting: ignoring traffic from known bad IP addresses

DNS attacks

- The Domain Name System (DNS) uses Domain Name Servers (also DNS) to convert user readable URLs like **`google.com`** to IP addresses
- Taking control of a server means that you get to say where google.com is
  - Called **DNS spoofing**
- For efficiency, servers cache results from other servers if they didn't know the IP
  - **DNS cache poisoning** is when an attacker gives a good server a bad IP address

Summary of vulnerabilities

Target	Vulnerability	Target	Vulnerability
Precursors to attack	• Port scan • Social engineering • Reconnaissance • OS and application fingerprinting	**Confidentiality**	• Protocol flaw • Eavesdropping • Passive wiretap • Misdelivery • Exposure • Traffic flow analysis
Authentication failures	• Impersonation • Guessing • Eavesdropping • Spoofing • Session hijacking • Man in the middle attack	**Integrity**	• Protocol flaw • Active wiretap • Impersonation • Falsification • Noise • Web site defacement • DNS attack
Programming flaws	• Buffer overflow • Addressing errors • Server-side include • Malicious Java or ActiveX • Worms, viruses, Trojan horses	**Availability**	• Protocol flaw • Transmission failure • Flooding • DNS attack • Traffic redirection • DDoS

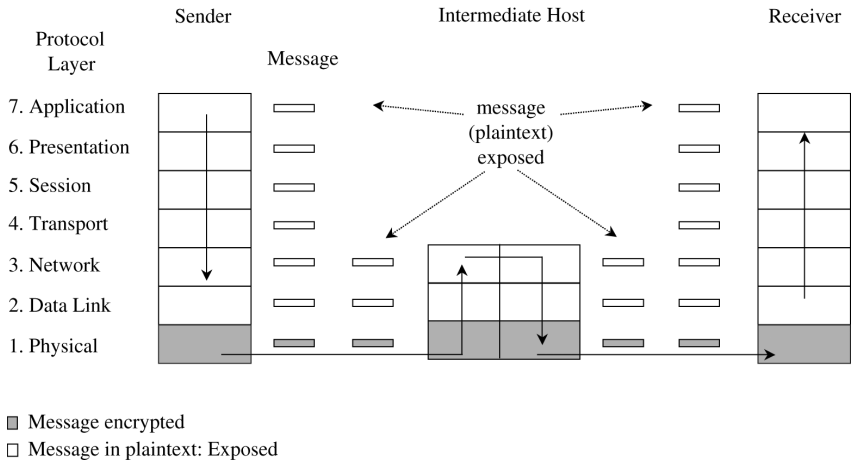
Network Security Controls

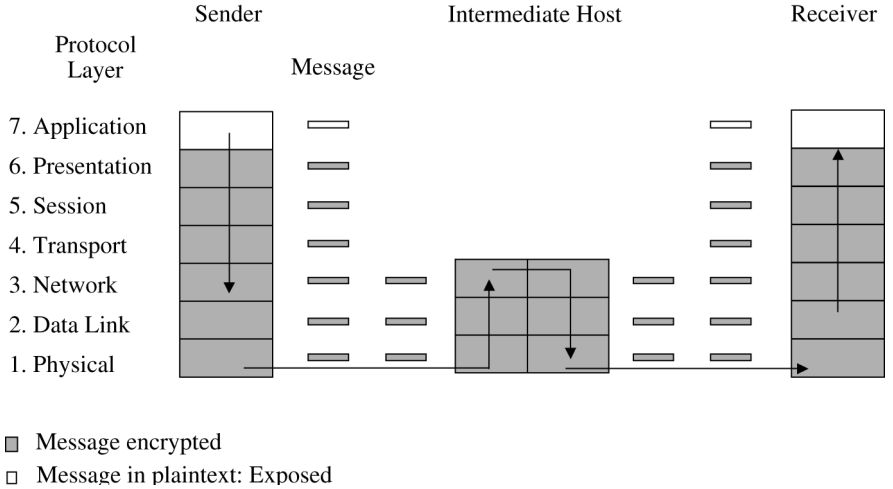
Architecture

- Good network architecture can make security better
- Segmentation means separating the network into different parts
  - Web server
  - Database server
  - Application servers
- Redundancy is important
  - Multiple servers that check if each other have gone down
- Avoid single points of failure

Encryption

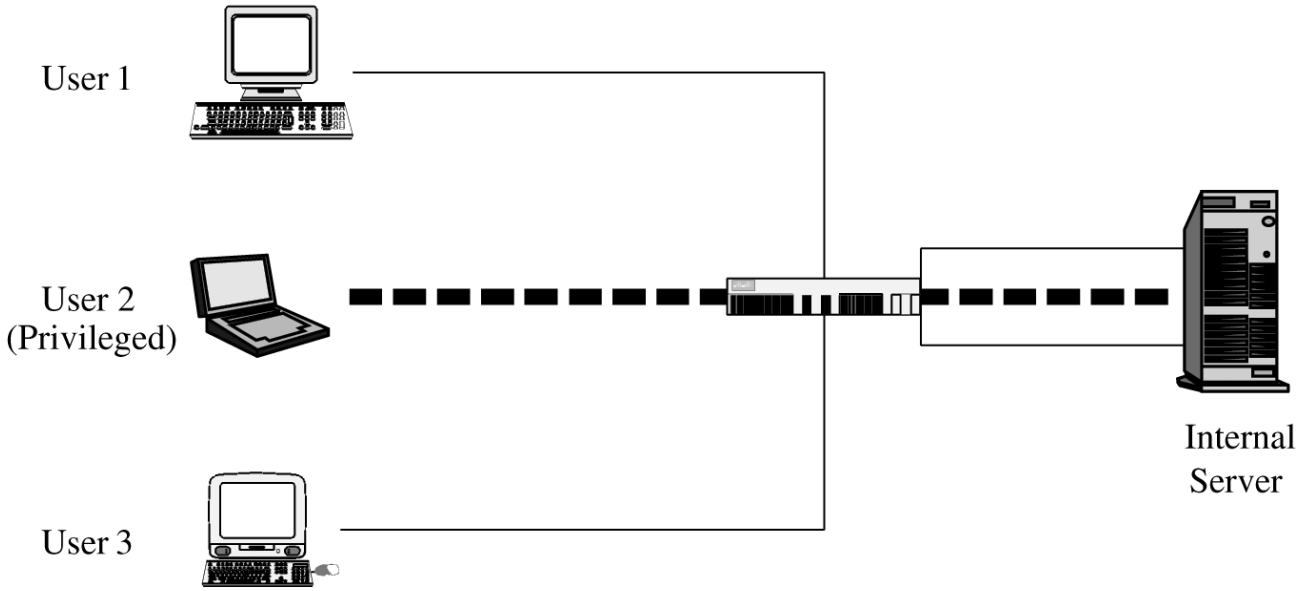
- Encryption is important for network security
- **Link encryption** encrypts data just before going through the physical communication layer
  - Each link between two hosts could have different encryption
  - Message are in plaintext within each host
  - Link encryption is fast and transparent
- **End-to-end encryption** provides security from one end of the transmission to the other
  - Slower
  - Responsibility of the user
  - Better security for the message in transit





Virtual private networks

- Encryption that allows people in a public network to communicate securely with a private network creates a virtual private network (VPN)
- A user's system negotiates a key with a firewall that guards a private network
  - Communication takes place in a tunnel



Public key infrastructure

- As we discussed before, the big problem with public keys is making sure you get the right one
- **Public key infrastructure** (**PKI**) is the solution to this problem
- A PKI sets up **certificate authorities** who certify that keys belong to who they're supposed to
- Their jobs include:
  - Managing public key certificates
  - Issuing certificates that connect a user to a key
  - Scheduling certificate expiration
  - Publishing certificate revocation lists

Secure protocols

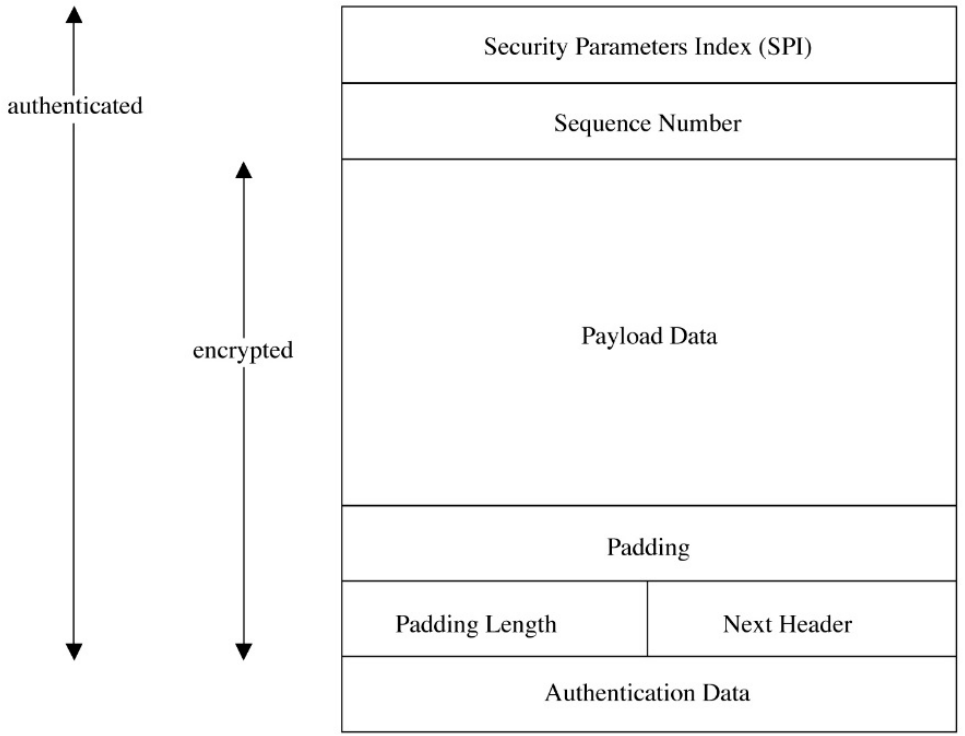
- **SSH** (secure shell) is a protocol for encrypted communication between computers
  - Designed for Unix/Linux, but available on Windows
  - Telnet, rlogin, and rsh should be replaced by SSH
  - Negotiates symmetric key encryption usually using public key encryption, similar to Project 2
- **TLS** (**transport layer security**) creates a secure session (golden lock) between a web browser and a web server

Onion routing

- With link and end-to-end encryption, the data is encrypted, but the addresses are not
- **Onion routing** uses forwarding hosts where only the first host knows where the data came from and only the last host knows where the data is going
  - It uses public key cryptography to work
- It's inefficient, but traffic analysis is nearly impossible
- Tor is a system developed to do onion routing
- Such systems allow bad guys to keep their communications untraceable as well

IPSec

- **IPSec** (**IP Security Protocol Suite**) is a group of protocols designed to provide security for general IP communication
- There is an **Authentication Header** (**AH**) mode that provides authentication and integrity by supplying a cryptographic hash of the message and its addresses
- There is an **Encapsulated Security Payload** (**ESP**) mode that can provide encryption, authentication, or both
- In **transport mode**, IPSec encrypts only the payload of the packet
- In **tunnel mode**, IPSec encrypts the entire packet and puts it inside of another packet, hiding its final destination inside of a private network

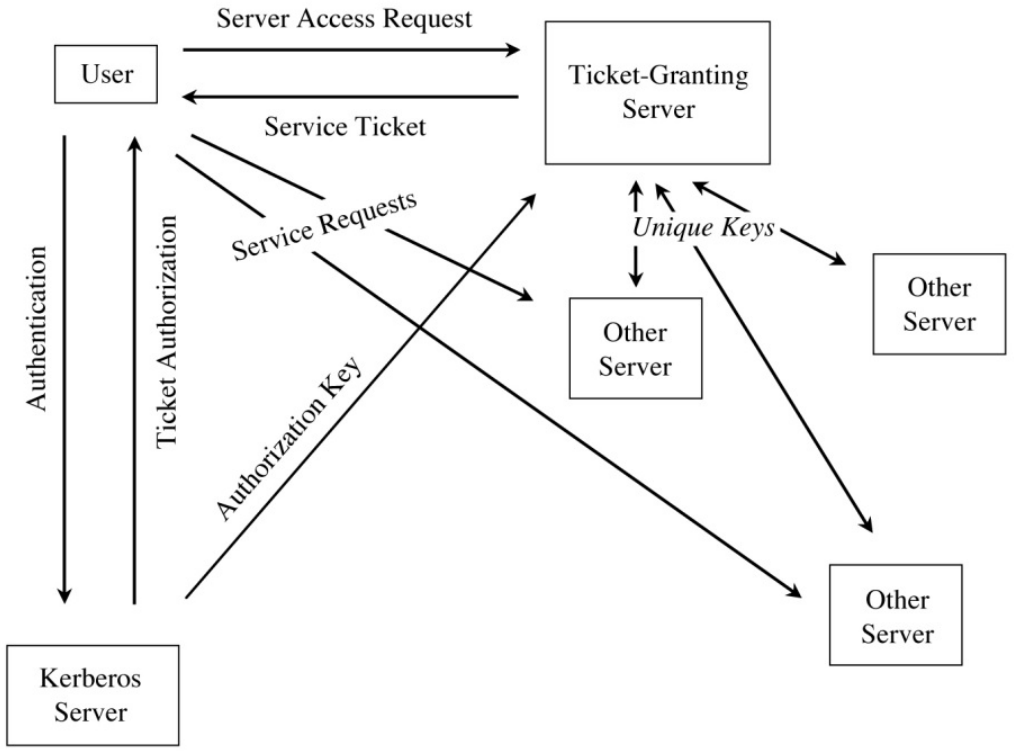


Content integrity

- Encryption helps protect integrity from malicious attackers
- Error correcting codes (like parity checks) can help prevent non-malicious problems with integrity
- Cryptographic checksums (AKA cryptographic hash digests) protect from both malicious and non-malicious threats to integrity

Strong authentication

- Who are you talking to? Passwords can be stolen
- **One-time passwords** prevent the problem of stolen passwords
  - RSA SecurIDs and other password tokens generate one-time passwords
- **Challenge-response systems** serve a similar role
- **Kerberos** is a system designed at MIT
  - Users interact with an authentication server who authenticates them
  - They get a ticket to access a file from a ticket granting server
  - The ticket lets you use a file
  - Everything is time-stamped



Access controls on routers

- Routers want to block packet floods from affecting the servers behind the router
- We can have ACLs that list all the legal (or all the illegal) hosts that can send (or are not allowed to send) packets into the network
- But, checking packets against ACLs slows down the system, making the router easier to flood
- Since it is possible to forge source addresses, the ACLs might not correctly block the packets

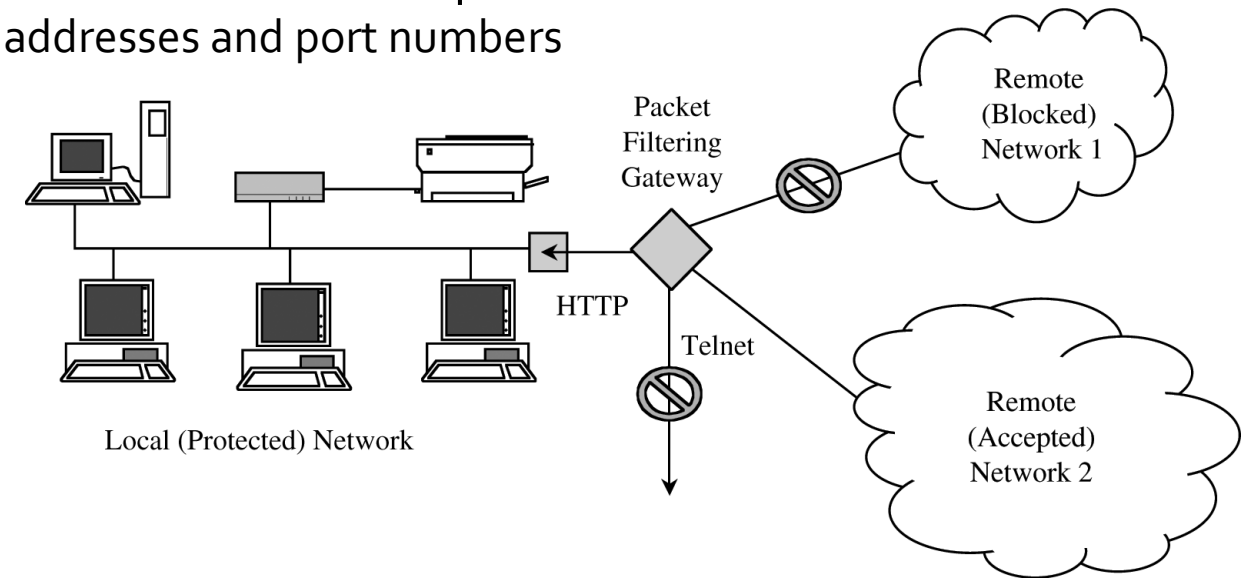
Firewalls

Firewalls

- A firewall filters traffic between an inside network and an outside network
  - The inside is more trusted and needs to be protected from the outside
- Kinds of firewalls:
  - Packet filtering gateway or screening routers
  - Stateful inspection firewalls
  - Application proxies
  - Guards
  - Personal firewalls

Packet filtering gateway

- Packet filtering gateways are simple
- They only allow certain packets to get by
  - Based on source or destination address
  - Based on protocol (HTTP on port 80, for example)
- A packet filter can be used in combination with other firewalls
  - The packet filter can remove a lot of traffic so that a more complex firewall has to worry about checking fewer packets
- Packet filters ignore the data inside the packets
  - They only use the addresses and port numbers



Stateful inspection firewall

- A **stateful inspection firewall** keeps track of data inside of packets
- For example, if a host inside the firewall initiates a TCP connection with a host outside, a stateful inspection firewall can remember this and let only that particular outside host's packets in

Application proxies and guards

- An **application proxy gateway** (or **bastion host**) appears to function like a host running a particular application
- The outside world sends date to the application proxy's IP address
- The application proxy changes the addresses and forwards the data on to the real server
- Only appropriate requests and responses are allowed through
- All accesses can also be logged
- A **guard** is really the same thing, just with more functionality
  - For example, a guard might reassemble a file and run it through a virus scanner

Personal firewalls

- A **personal firewall** is software that runs on a workstation
- These firewalls can give additional protection
- The user and OS can have very fine grained control over what kind of connections can be made and what kind of applications can send and receive data

Network address translation

- Firewalls generally do **network address translation (NAT)**
- Outsiders direct all traffic to the firewall
- The firewall keeps track of which internal host is sending traffic on a particular port
- Thus, outsiders don't even know which machines or addresses exist behind the firewall

Upcoming

Next time…

- Intrusion detection
- Database background
- Security requirements of databases
- Database reliability and integrity
- Aidan Kent presents

Reminders

- Reading Sections 7.1 through 7.3
- Form teams for Project 3
  - I need the name of the leader
  - You will need to create passwords and secret messages for **every** team in class