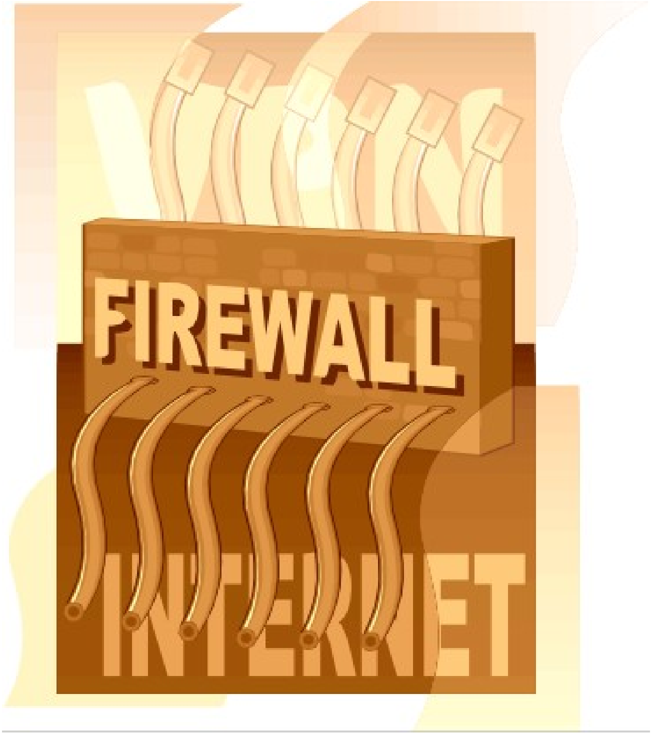
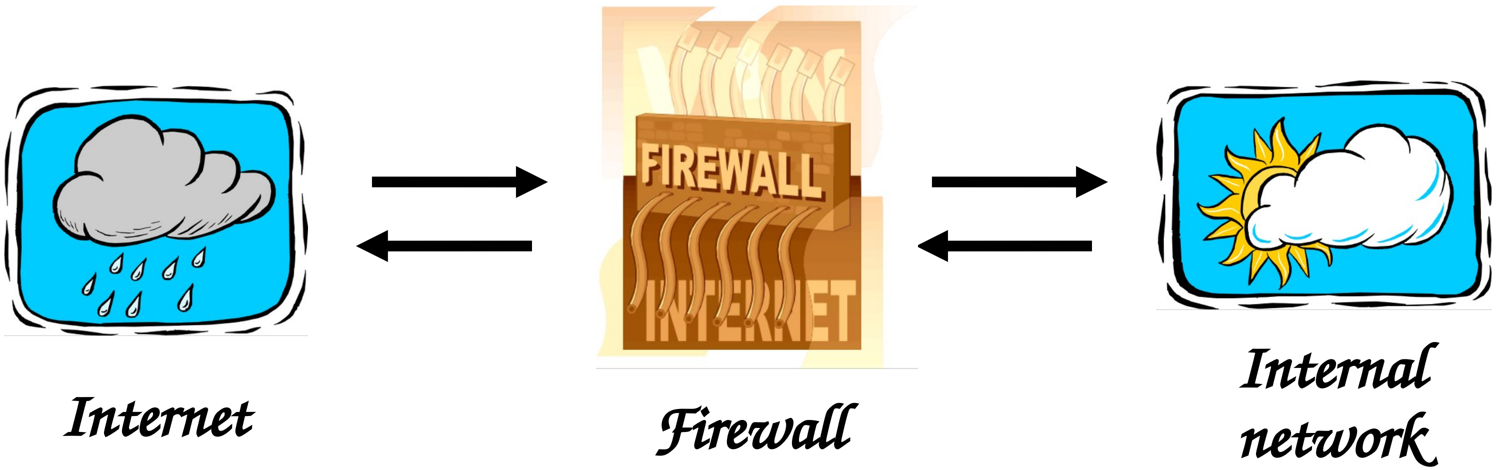
Firewalls



Firewalls



- Firewall decides what to let in to internal network and/or what to let out
- **Access control** for the network

Firewall as Secretary

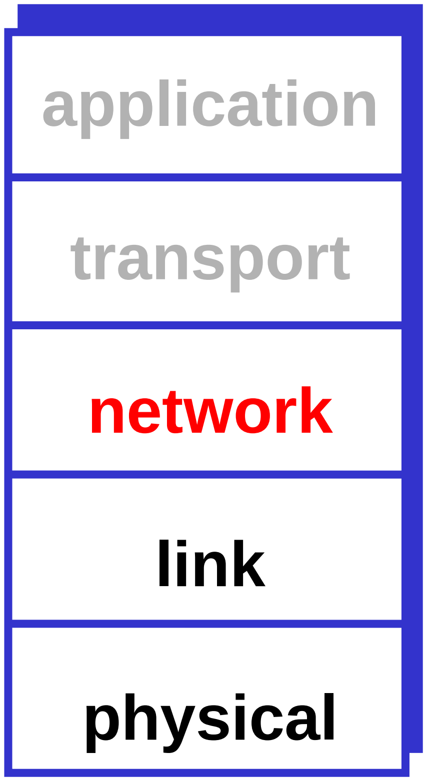
- A firewall is like a **secretary**
- To meet with an executive
  - First contact the secretary
  - Secretary decides if meeting is important
  - So, secretary filters out many requests
- You want to meet chair of CS department?
  - Secretary does some filtering
- You want to meet POTUS?
  - Secretary does lots of filtering

Firewall Terminology

- No standard firewall terminology
- Types of firewalls
  - **Packet filter** works at network layer
  - **Stateful packet filter** transport layer
  - **Application proxy** application layer
- Lots of other terms often used
  - E.g., "deep packet inspection"

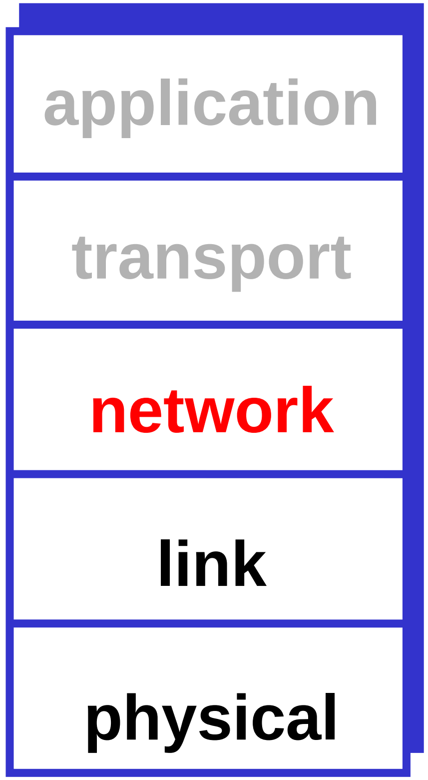
Packet Filter

- Operates at network layer
- Can filters based on…
  - Source IP address
  - Destination IP address
  - Source Port
  - Destination Port
  - Flag bits (SYN, ACK, etc.)
  - Egress or ingress



Packet Filter

- Advantages?
  - Speed
- Disadvantages?
  - No concept of state
  - Cannot see TCP connections
  - Blind to application data



Packet Filter

- Configured via Access Control Lists (ACLs)
  - Different meaning than at start of Chapter 8

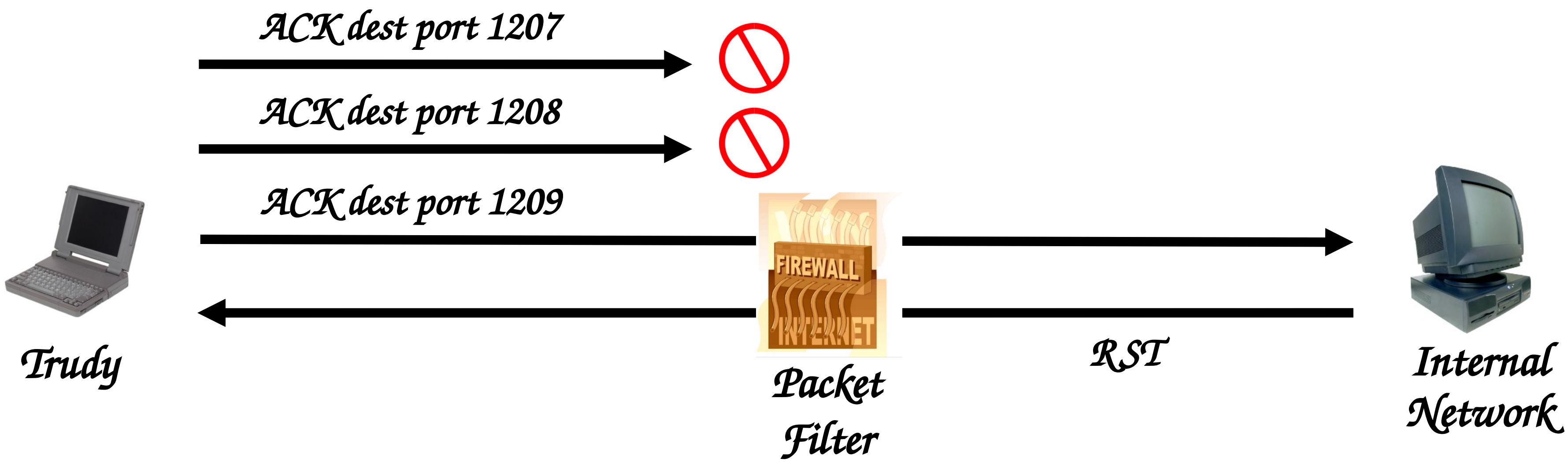
Action	Source IP	Dest IP	Source Port	Dest Port	Protocol	Flag Bits
Allow	Inside	Outside	Any	80	HTTP	Any
Allow	Outside	Inside	80	> 1023	HTTP	ACK
Deny	All	All	All	All	All	All

- **Q: Intention?**
- **A: Restrict traffic to Web browsing**

TCP ACK Scan

- Attacker scans for open ports thru firewall
  - Port scanning often first step in network attack
- Attacker sends packet with ACK bit set, **without** prior 3-way handshake
  - Violates TCP/IP protocol
  - ACK packet pass thru packet filter firewall
  - Appears to be part of an ongoing connection
  - RST sent by recipient of such packet

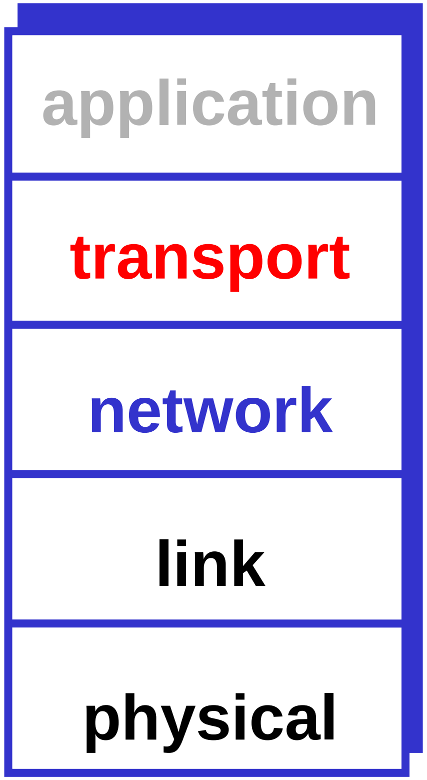
TCP ACK Scan



- Attacker knows port 1209 open thru firewall
- A **stateful packet filter** can prevent this
  - Since scans not part of established connections

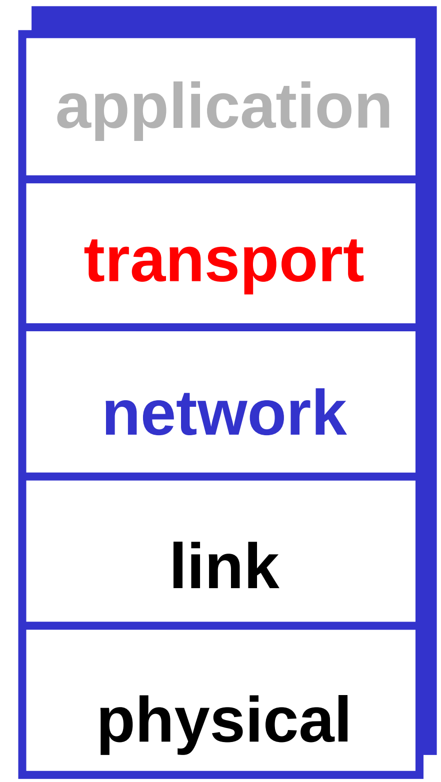
Stateful Packet Filter

- Adds **state** to packet filter
- Operates at transport layer
- ***Remembers*** TCP connections, flag bits, etc.
- Can even remember UDP packets (e.g., DNS requests)



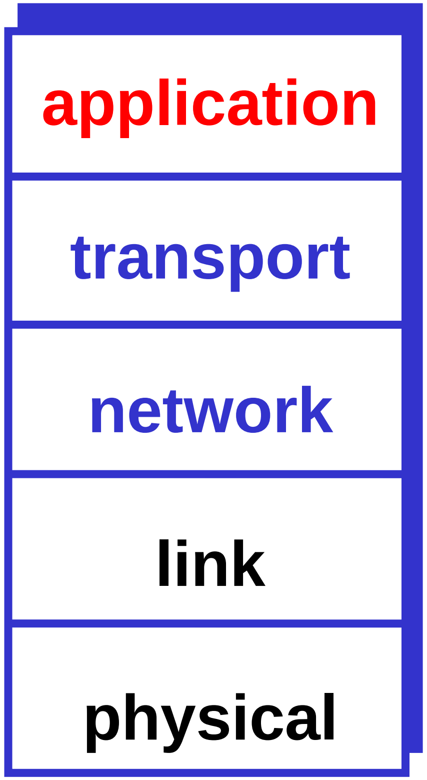
Stateful Packet Filter

- Advantages?
  - Can do everything a packet filter can do plus…
  - Keep track of ongoing connections (e.g., prevents TCP ACK scan)
- Disadvantages?
  - Cannot see application data
  - Slower than packet filtering



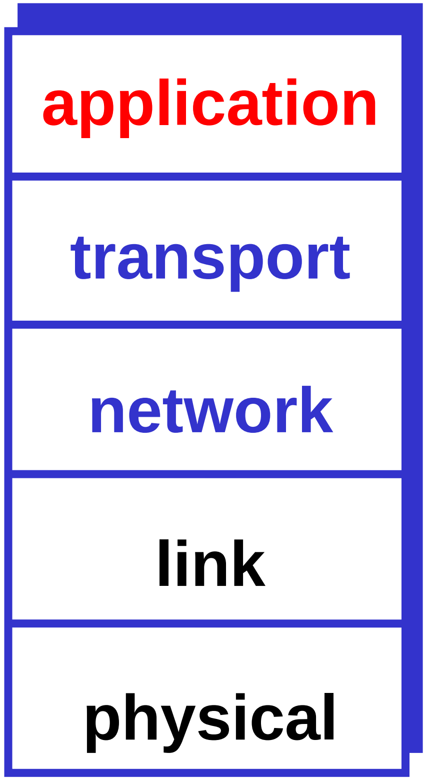
Application Proxy

- A **proxy** is something that acts on your behalf
- Application proxy looks at incoming application data
- Verifies that data is safe before letting it in



Application Proxy

- Advantages?
  - Complete view of connections and applications data
  - Filter bad data at application layer (viruses, Word macros)
- Disadvantages?
  - Speed



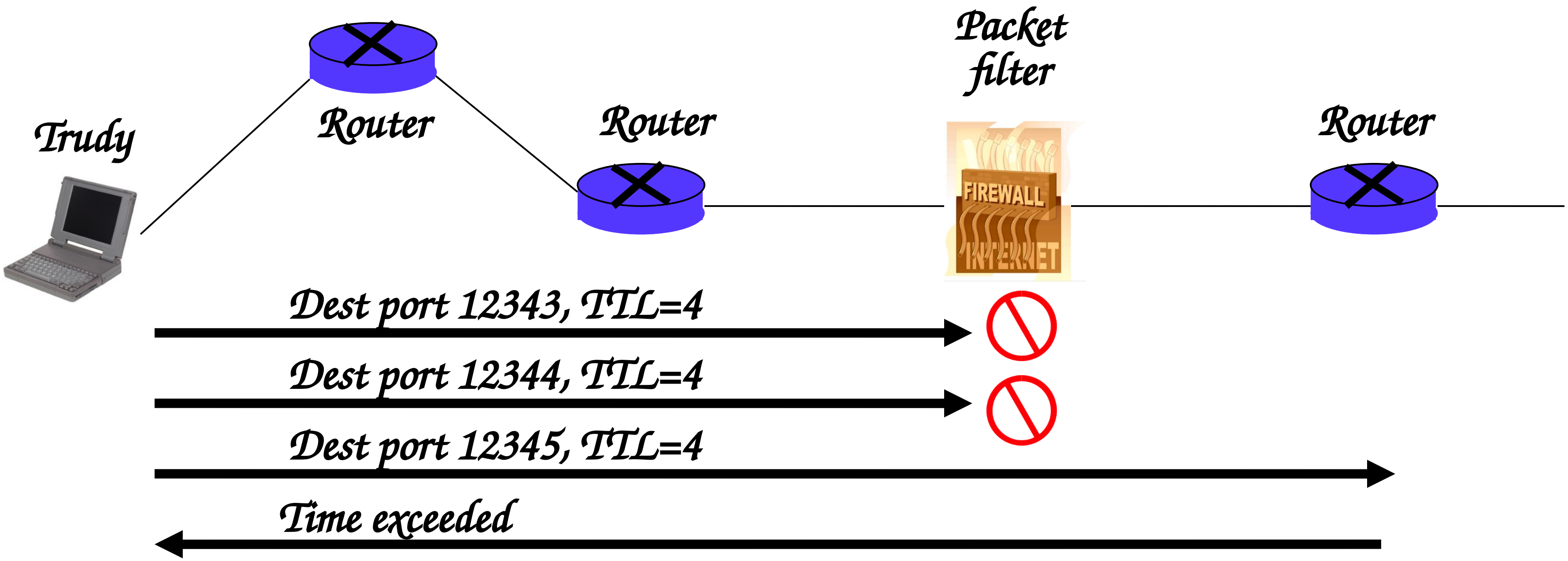
Application Proxy

- Creates a new packet before sending it thru to internal network
- Attacker must talk to **proxy** and convince it to forward message
- Proxy has complete view of connection
- Can prevent some scans stateful packet filter cannot next slides

Firewalk

- Tool to scan for open ports thru firewall
- Attacker knows IP address of firewall and IP address of one system inside firewall
  - Set TTL to 1 more than number of hops to firewall, and set destination port to N
- If firewall allows data on port N thru firewall, get ***time exceeded*** error message
  - Otherwise, no response

Firewalk and Proxy Firewall



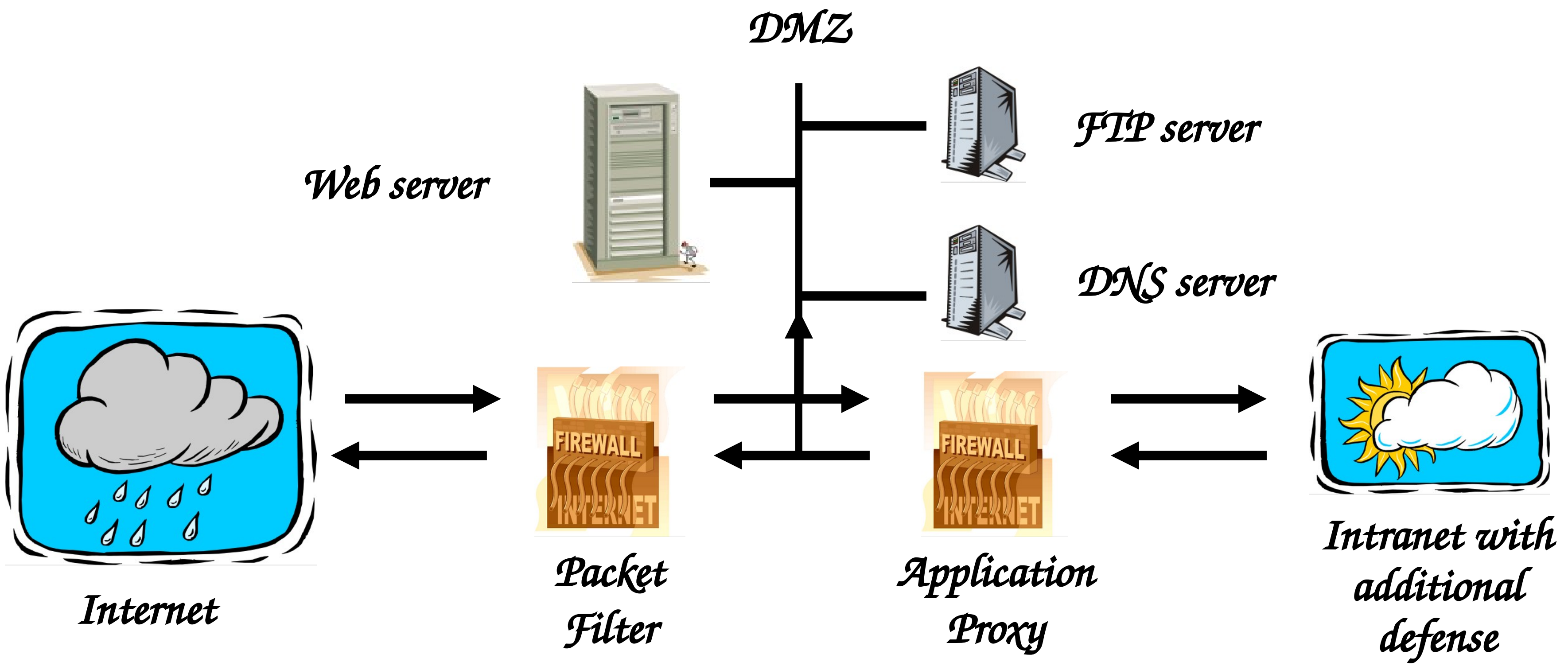
- This will **not** work thru an application proxy (why?)
- The proxy creates a new packet, destroys old TTL

Deep Packet Inspection

- Many buzzwords used for firewalls
  - One example: **deep packet inspection**
- What could this mean?
- Look into packets, but don't really "process" the packets
  - Like an application proxy, but faster

Firewalls and Defense in Depth

- Typical network security architecture



Intrusion Detection Systems

Intrusion Prevention

- Want to keep bad guys out
- **Intrusion prevention** is a traditional focus of computer security
  - Authentication is to prevent intrusions
  - Firewalls a form of intrusion prevention
  - Virus defenses aimed at intrusion prevention
  - Like locking the door on your car

Intrusion Detection

- In spite of intrusion prevention, bad guys will sometime get in
- Intrusion detection systems (**IDS**)
  - Detect attacks in progress (or soon after)
  - Look for unusual or suspicious activity
- IDS evolved from log file analysis
- IDS is currently a **hot** research topic
- How to respond when intrusion detected?
  - We don't deal with this topic here…

Intrusion Detection Systems

- Who is likely intruder?
  - May be outsider who got thru firewall
  - May be evil insider
- What do intruders do?
  - Launch well-known attacks
  - Launch variations on well-known attacks
  - Launch new/little-known attacks
  - "Borrow" system resources
  - Use compromised system to attack others. etc.

IDS

- Intrusion detection **approaches**
  - Signature-based IDS
  - Anomaly-based IDS
- Intrusion detection **architectures**
  - Host-based IDS
  - Network-based IDS
- Any IDS can be classified as above
  - In spite of marketing claims to the contrary!

Host-Based IDS

- Monitor activities on hosts for
  - Known attacks
  - Suspicious behavior
- Designed to detect attacks such as
  - Buffer overflow
  - Escalation of privilege, …
- Little or no view of network activities

Network-Based IDS

- Monitor activity on the network for…
  - Known attacks
  - Suspicious network activity
- Designed to detect attacks such as
  - Denial of service
  - Network probes
  - Malformed packets, etc.
- Some overlap with firewall
- Little or no view of host-base attacks
- Can have both host and network IDS

Signature Detection Example

- Failed login attempts may indicate password cracking attack
- IDS could use the rule "N failed login attempts in M seconds" as **signature**
- If N or more failed login attempts in M seconds, IDS warns of attack
- Note that such a warning is specific
  - Admin knows what attack is suspected
  - Easy to verify attack (or false alarm)

Signature Detection

- Suppose IDS warns whenever N or more failed logins in M seconds
  - Set N and M so false alarms not common
  - Can do this based on "normal" behavior
- But, if Trudy knows the signature, she can try N – 1 logins every M seconds…
- Then signature detection slows down Trudy, but might not stop her

Signature Detection

- Many techniques used to make signature detection more robust
- Goal is to detect "almost" signatures
- For example, if "about" N login attempts in "about" M seconds
  - Warn of possible password cracking attempt
  - What are reasonable values for "about"?
  - Can use statistical analysis, heuristics, etc.
  - Must not increase false alarm rate too much

Signature Detection

- Advantages of signature detection
  - Simple
  - Detect known attacks
  - Know which attack at time of detection
  - Efficient (if reasonable number of signatures)
- Disadvantages of signature detection
  - Signature files must be kept up to date
  - Number of signatures may become large
  - Can only detect known attacks
  - Variation on known attack may not be detected

Anomaly Detection

- Anomaly detection systems look for unusual or abnormal behavior
- There are (at least) two challenges
  - What is normal for this system?
  - How "far" from normal is abnormal?
- No avoiding statistics here!
  - **mean** defines normal
  - **variance** gives distance from normal to abnormal

How to Measure Normal?

- How to measure normal?
  - Must measure during "representative" behavior
  - Must not measure during an attack…
  - …or else attack will seem normal!
  - Normal is statistical **mean**
  - Must also compute **variance** to have any reasonable idea of abnormal

How to Measure Abnormal?

- Abnormal is relative to some "normal"
  - Abnormal indicates possible attack
- Statistical discrimination techniques include
  - Bayesian statistics
  - Linear discriminant analysis (LDA)
  - Quadratic discriminant analysis (QDA)
  - Neural nets, hidden Markov models (HMMs), etc.
- Fancy modeling techniques also used
  - Artificial intelligence
  - Artificial immune system principles
  - Many, many, many others

Anomaly Detection (1)

- *Spse we monitor use of three commands:*

  open, read, close
- *Under normal use we observe Alice:*

  open, read, close, open, open, read, close, …
- *Of the six possible ordered pairs, we see four pairs are normal for Alice,*

  (open,read), (read,close), (close,open), (open,open)
- *Can we use this to identify unusual activity?*

Anomaly Detection (1)

- We monitor use of the three commands

  open, read, close

- If the ratio of abnormal to normal pairs is "too high", warn of possible attack
- Could improve this approach by
  - Also use expected frequency of each pair
  - Use more than two consecutive commands
  - Include more commands/behavior in the model
  - More sophisticated statistical discrimination

Anomaly Detection (2)

- *Over time, Alice has accessed file F_n at rate H_n*

H_0	H_1	H_2	H_3
.10	.40	.40	.10

- ***Recently, "Alice" has accessed F_n at rate A_n***

A_0	A_1	A_2	A_3
.10	.40	.30	.20

- ***Is this normal use for Alice?***
- ***We compute*** $\mathbf{S = (H_0 - A_0)^2+(H_1 - A_1)^2+\ldots+(H_3 - A_3)^2 = .02}$
  - ***We consider*** $\mathbf{S < 0.1}$ ***to be normal, so this is normal***
- ***How to account for use that varies over time?***

Anomaly Detection (2)

- *To allow "normal" to adapt to new use, we update averages:* $H_n = 0.2A_n + 0.8H_n$
- *In this example,* H_n *are updated…* $H_2 = .2 \times .3 + .8 \times .4 = .38$ *and* $H_3 = .2 \times .2 + .8 \times .1 = .12$
- *And we now have*

H_0	H_1	H_2	H_3
.10	.40	.38	.12

Anomaly Detection (2)

- The updated long term average is

H_0	H_1	H_2	H_3
.10	.40	.38	.12

- Suppose new observed rates…

A_0	A_1	A_2	A_3
.10	.30	.30	.30

- Is this normal use?
- Compute $S = (H_0 - A_0)^2 + \ldots + (H_3 - A_3)^2 = .0488$
  - Since $S = .0488 < 0.1$ we consider this normal
- And we again update the long term averages:

$$H_n = 0.2A_n + 0.8H_n$$

Anomaly Detection (2)

- The starting averages were:

H_0	H_1	H_2	H_3
.10	.40	.40	.10

- **After 2 iterations, averages are:**

H_0	H_1	H_2	H_3
.10	.38	.364	.156

- **Statistics slowly evolve to match behavior**
- **This reduces false alarms for SA**
- **But also opens an avenue for attack…**
  - **Suppose Trudy *always* wants to access F_3**
  - **Can she convince IDS this is normal for Alice?**

Anomaly Detection (2)

- To make this approach more robust, must incorporate the variance
- Can also combine N stats S_i as, say,

  $$T = (S_1 + S_2 + S_3 + \ldots + S_N) / N$$

  to obtain a more complete view of "normal"
- Similar (but more sophisticated) approach is used in an IDS known as **NIDES**
- NIDES combines anomaly & signature IDS

Anomaly Detection Issues

- Systems constantly evolve and so must IDS
  - Static system would place huge burden on admin
  - But evolving IDS makes it possible for attacker to (slowly) convince IDS that an attack is normal
  - Attacker may win simply by "going slow"
- What does "abnormal" really mean?
  - Indicates there may be an attack
  - Might not be any specific info about "attack"
  - How to respond to such vague information?
  - In contrast, signature detection is very specific

Anomaly Detection

- Advantages?
  - Chance of detecting unknown attacks
- Disadvantages?
  - Cannot use anomaly detection alone…
  - …must be used with signature detection
  - Reliability is unclear
  - May be subject to attack
  - Anomaly detection indicates "something unusual", but lacks specific info on possible attack

Anomaly Detection: The Bottom Line

- Anomaly-based IDS is active research topic
- Many security experts have high hopes for its ultimate success
- Often cited as key future security technology
- Hackers are not convinced!
  - Title of a talk at Defcon: "Why Anomaly-based IDS is an Attacker's Best Friend"
- Anomaly detection is difficult and tricky
- As hard as AI?