Topics in Network Security
CS 136
Computer Security
Peter Reiher
March 13, 2008

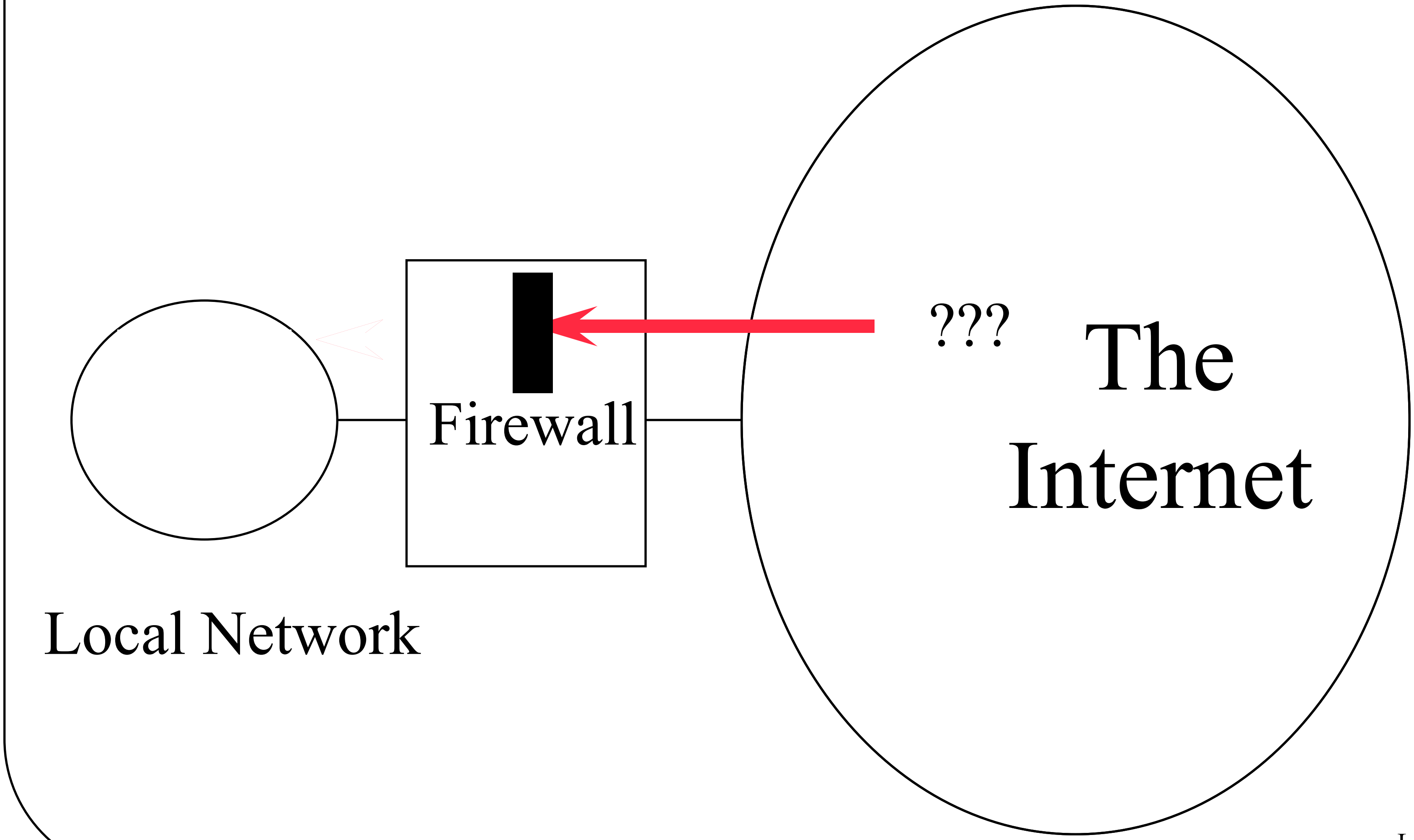
Outline

- Firewalls
- VPNs
- Internet security threats

Firewalls

- "A system or combination of systems that enforces a boundary between two or more networks" - NCSA Firewall Functional Summary
- Usually, a computer that keeps the bad guys out

Typical Use of a Firewall



What Is a Firewall, Really?

- Typically a machine that sits between a LAN/WAN and the Internet
- Running special software
- That somehow regulates network traffic between the LAN/WAN and the Internet

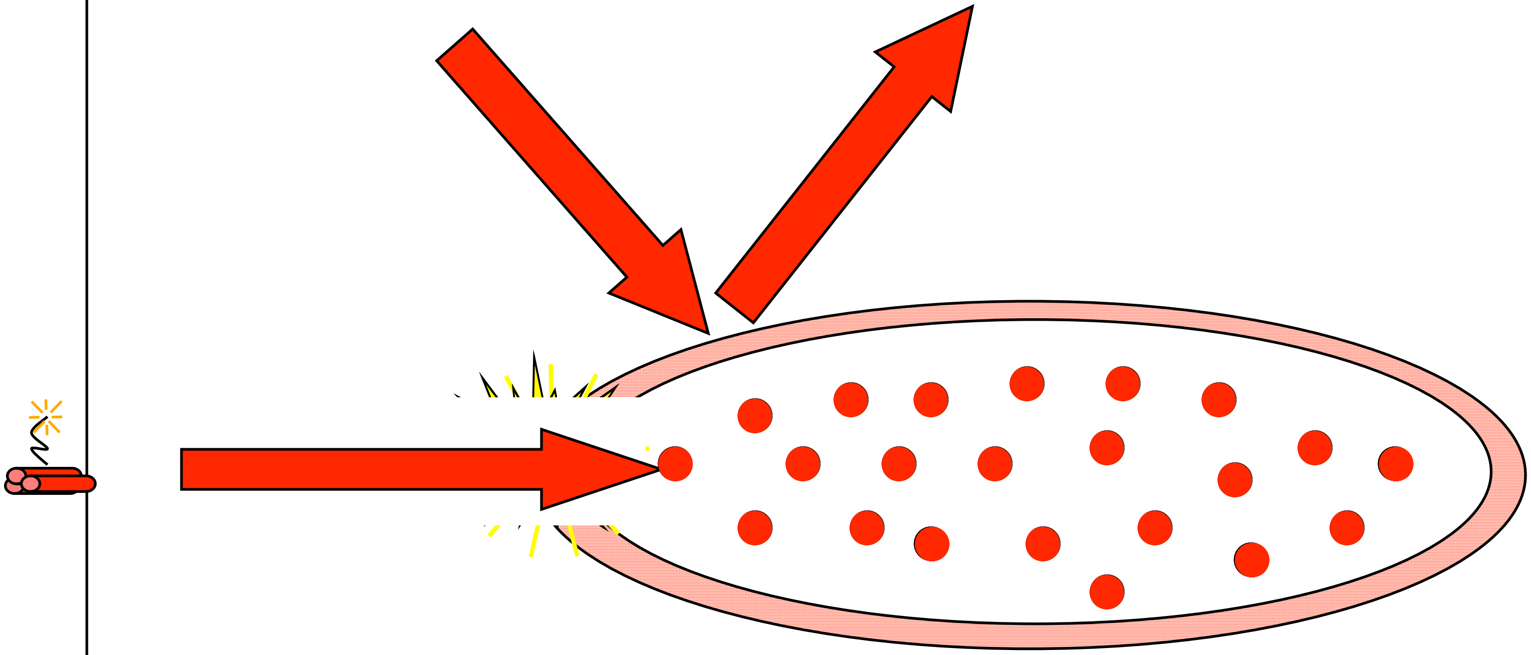
Firewalls and Perimeter Defense

- Firewalls implement a form of security called *perimeter defense*
- Protect the inside of something by defending the outside strongly
  - The firewall machine is often called a *bastion host*
- Control the entry and exit points
- If nothing bad can get in, I'm safe, right?

Weaknesses of Perimeter Defense Models

- Breaching the perimeter compromises all security
- Windows passwords are a form of perimeter defense
  - If you get past the password, you can do anything
- Perimeter defense is part of the solution, not the entire solution

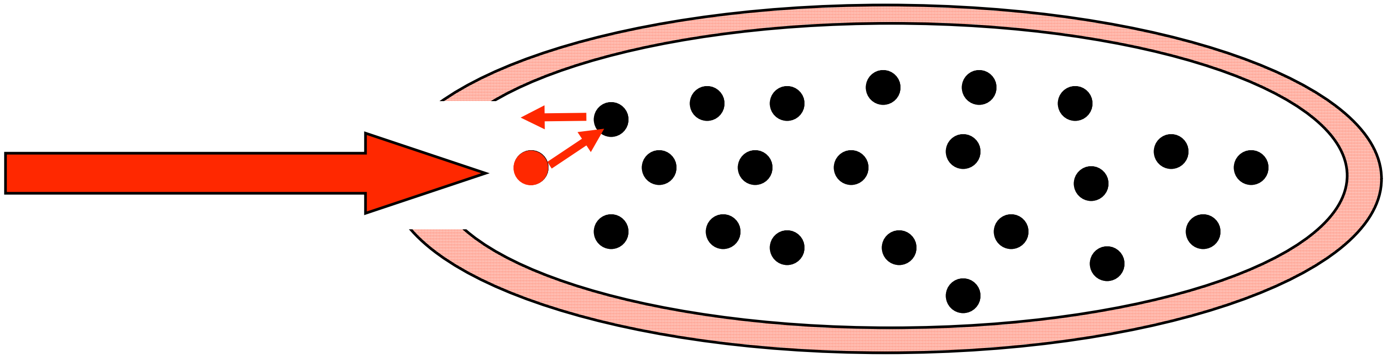
Weaknesses of Perimeter Defense



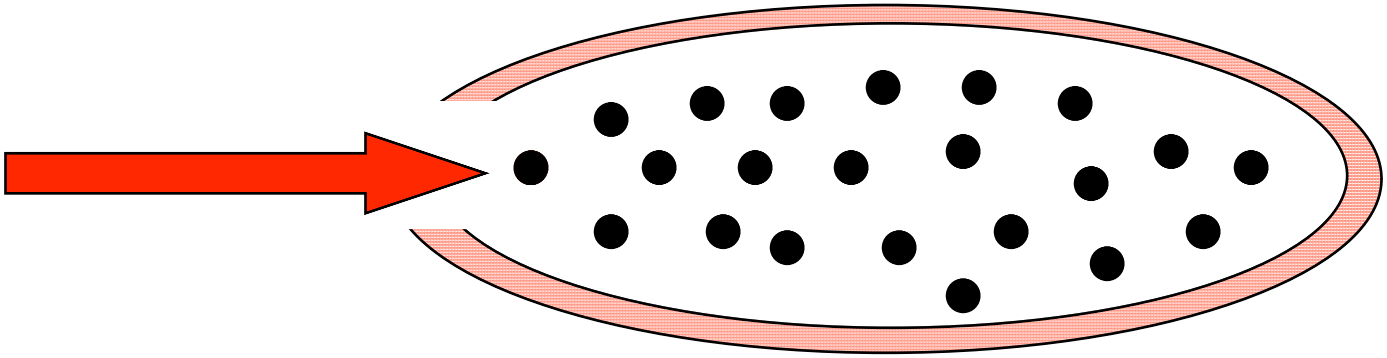
Defense in Depth

- An old principle in warfare
- Don’t rely on a single defensive mechanism or defense at a single point
- Combine different defenses
- Defeating one defense doesn’t defeat your entire plan

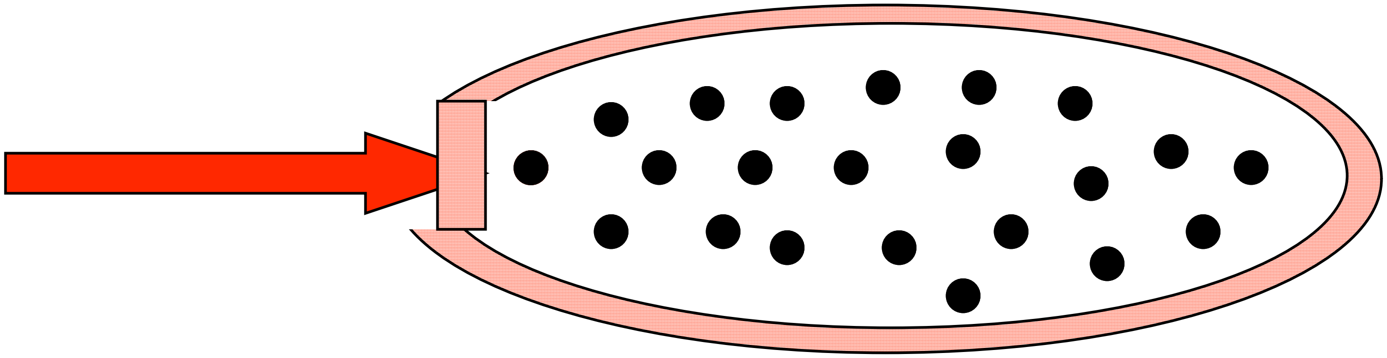
So What Should Happen?



Or, Better



Or, Even Better



So Are Firewalls Any Use?

- Definitely!
- They aren’t the full solution, but they are absolutely part of it
- Anyone who cares about security needs to run a decent firewall
- They just have to do other stuff, too
- 97% of respondents in 2007 CSI survey say they use firewalls

Types of Firewalls

- Filtering gateways
  - AKA screening routers
- Application level gateways
  - AKA proxy gateways

Filtering Gateways

- Based on packet routing information
- Look at information in the incoming packets' headers
- Based on that information, either let the packet through or reject it

Example Use of Filtering Gateways

- Allow particular external machines to connect to specific internal machines
  - Denying connections to other machines
- Or allow full access to some external machines
- And none to others

Filtering Based on Ports

- Most incoming traffic is destined for a particular machine and port
  - Which can be derived from the IP and TCP headers
- Only let through packets to select machines at specific ports
- Makes it impossible to externally exploit flaws in little-used ports
  - If you configure the firewall right . . .

Pros and Cons of Filtering Gateways

+ Fast
+ Cheap
+ Flexible
+ Transparent

– Limited capabilities
– Dependent on header authentication
– Generally poor logging
– May rely on router security

Application Level Gateways

- Also known as proxy gateways and stateful firewalls
- Firewalls that understand the application-level details of network traffic
  - To some degree
- Traffic is accepted or rejected based on the probable results of accepting it

How Application Level Gateways Work

- The firewall serves as a general framework
- Various proxies are plugged into the framework
- Incoming packets are examined
  - And handled by the appropriate proxy

Firewall Proxies

- Programs capable of understanding particular kinds of traffic
  - E.g., FTP, HTTP, videoconferencing
- Proxies are specialized
- A good proxy must have deep understanding of the network application

An Example Proxy

- A proxy to audit email
- What might such a proxy do?
  – Only allow email from particular users through
  – Or refuse email from known spam sites
  – Or filter out email with unsafe inclusions (like executables)

What Are the Limits of Proxies?

- Proxies can only test for threats they understand
- Either they must permit a very limited set of operations
- Or they must have deep understanding of the program they protect
  - If too deep, they may share the flaw
- Performance limits on how much work they can do on certain types of packets

Pros and Cons of Application Level Gateways

+ Highly flexible
+ Good logging
+ Content-based filtering
+ Potentially transparent
– Slower
– More complex and expensive
– A good proxy is hard to find

More Firewall Topics

- Statefulness
- Transparency
- Handling authentication
- Handling encryption

Stateful Firewalls

- Much network traffic is connection-oriented
  - E.g., ssh and videoconferencing
- Proper handling of that traffic requires the firewall to maintain state
- But handling information about connections is more complex

Firewalls and Transparency

- Ideally, the firewall should be invisible
  - Except when it vetoes access
- Users inside should be able to communicate outside without knowing about the firewall
- External users should be able to invoke internal services transparently

Firewalls and Authentication

- Many systems want to allow specific sites or users special privileges
- Firewalls can only support that to the extent that strong authentication is available
  - At the granularity required
- For general use, may not be possible
  - In current systems

Firewalls and Encryption

- Firewalls provide no confidentiality
- Unless the data is encrypted
- But if the data is encrypted, the firewall can't examine it
- So typically the firewall must be able to decrypt
  - Or only work on unencrypted parts of packets
- Can decrypt, analyze, and re-encrypt

Firewall Configuration and Administration

- Again, the firewall is the point of attack for intruders
- Thus, it must be extraordinarily secure
- How do you achieve that level of security?

Firewall Location

- Clearly, between you and the bad guys
- But you may have some very different types of machines/functionalities
- Sometimes makes sense to divide your network into segments
  - Most typically, less secure public network and more secure internal network
  - Using separate firewalls

Firewall Hardening

- Devote a special machine only to firewall duties
- Alter OS operations on that machine
  - To allow only firewall activities
  - And to close known vulnerabilities
- Strictly limit access to the machine
  - Both login and remote execution

Firewalls and Logging

- The firewall is the point of attack for intruders
- Logging activities there is thus vital
- The more logging, the better
- Should log what the firewall allows
- And what it denies
- Tricky to avoid information overload

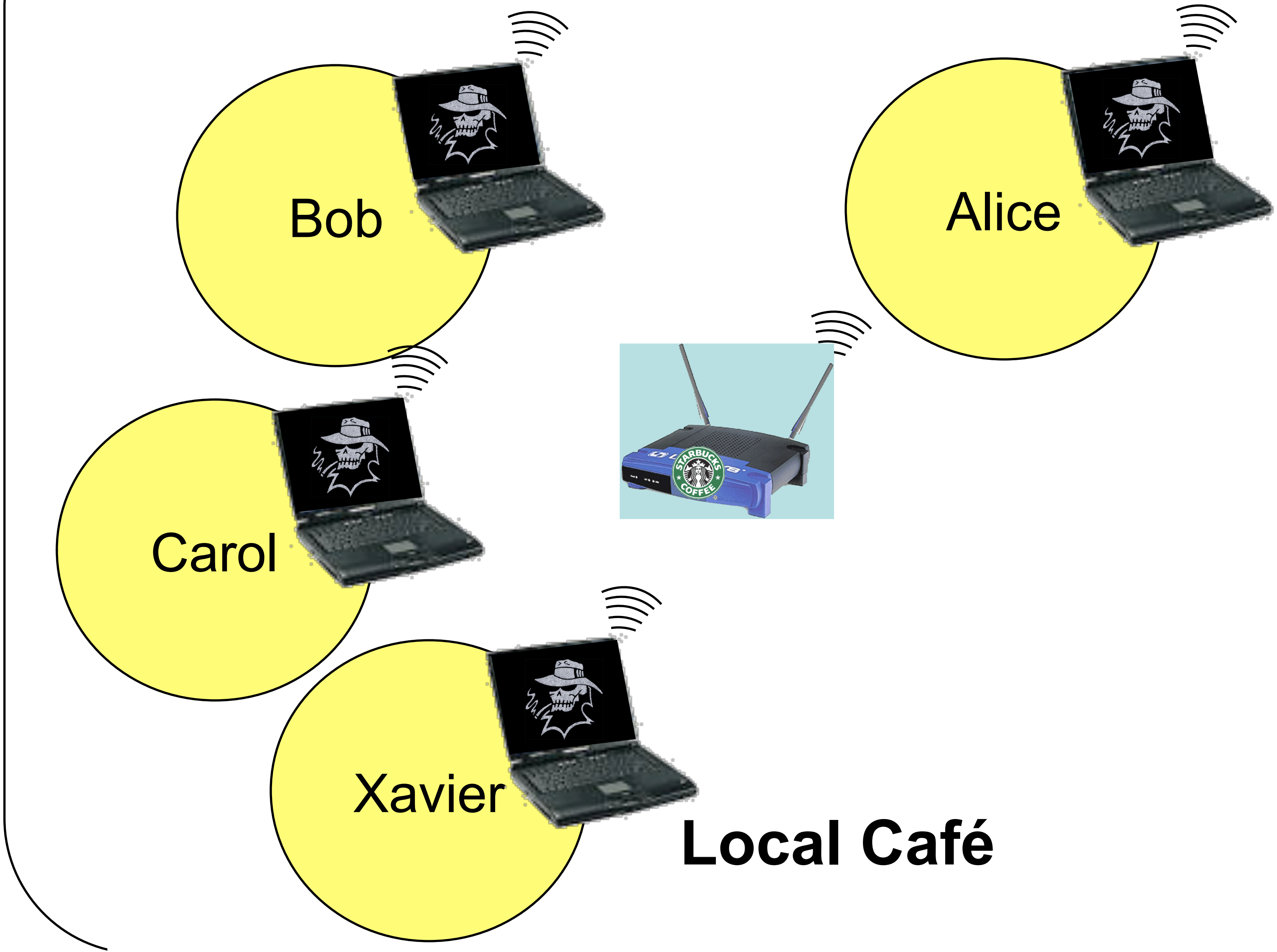
Keep Your Firewall Current

- New vulnerabilities are discovered all the time
- Must update your firewall to fix them
- Even more important, sometimes you have to open doors temporarily
  - Make sure you shut them again later
- Can automate some updates to firewalls
- How about getting rid of old stuff?

Closing the Back Doors

- Firewall security is based on assumption that all traffic goes through the firewall
- So be careful with:
  - Modem connections
  - Wireless connections
  - Portable computers
- Put a firewall at every entry point to your network
- And make sure all your firewalls are up to date

What About Portable Computers?



Bob

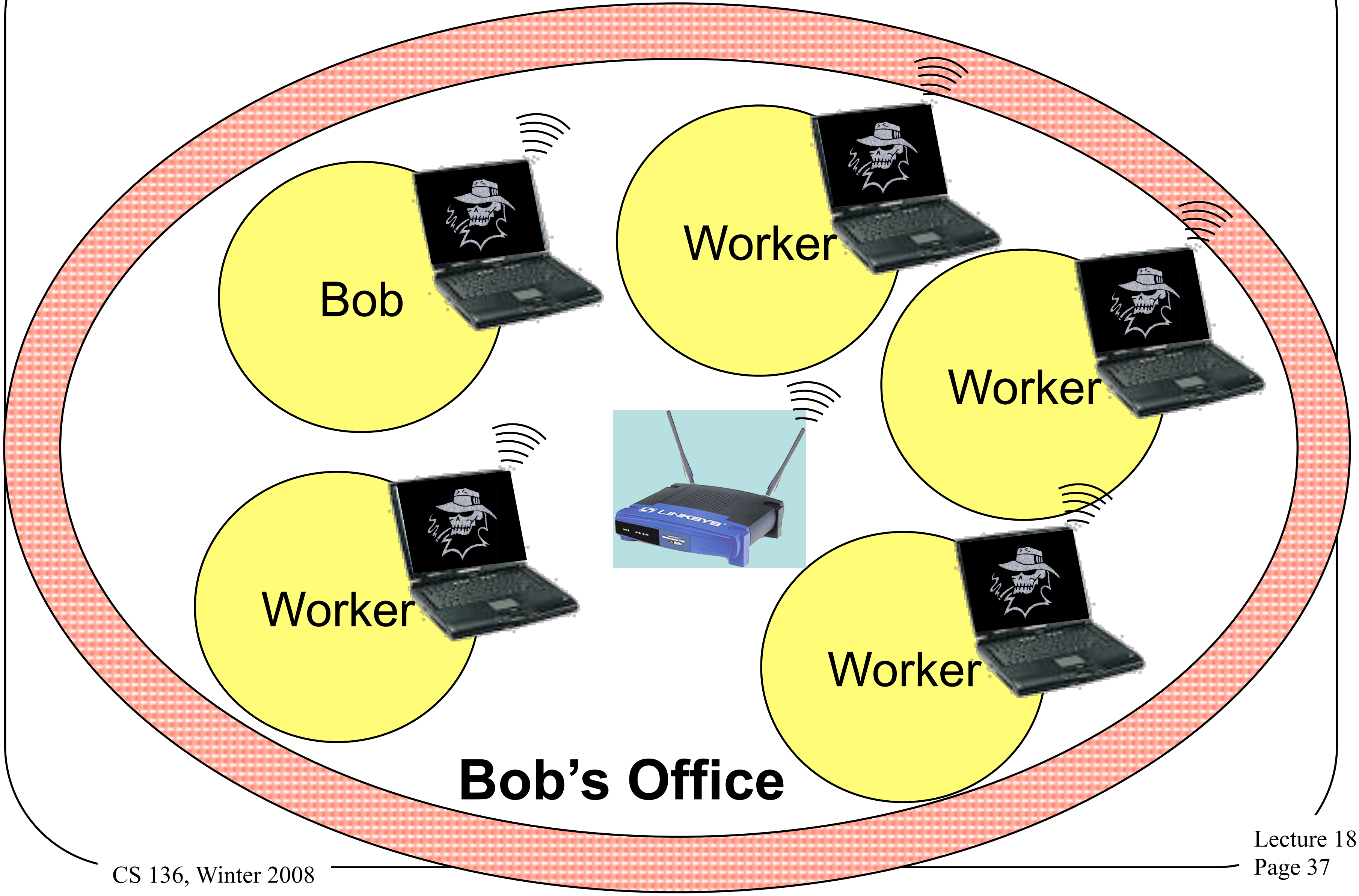
Alice

Carol

Xavier

Local Café

Now Bob Goes To Work . . .



How To Handle This Problem?

- Essentially *quarantine* the portable computer until it’s safe
- Don’t permit connection to wireless access point until you’re satisfied that the portable is safe
- UCLA did it first with QED
- Now very common in Cisco, Microsoft, and other companies’ products

How To Tell When It’s Safe?

- Local network needs to *examine* the quarantined device
- Looking for evidence of worms, viruses, etc.
- If any are found, require *decontamination* before allowing the portable machine access

Single Machine Firewalls

- Instead of separate machine protecting network,
- A machine puts software between the outside world and the rest of machine
- Under its own control
- To protect itself
- Available on most modern systems

Pros and Cons of Individual Firewalls

+Customized to particular machine

+Under machine owner’s control

+Provides defense in depth

–Only protects that machine

–Less likely to be properly configured

- Generally considered a good idea

Virtual Private Networks

- VPNs
- What if your company has more than one office?
- And they’re far apart?
  - Like on opposite coasts of the US
- How can you have secure cooperation between them?

Leased Line Solutions

- Lease private lines from some telephone company
- The phone company ensures that your lines cannot be tapped
  - To the extent you trust in phone company security
- Can be expensive and limiting

Another Solution

- Communicate via the Internet
  - Getting full connectivity, bandwidth, reliability, etc.
  - At a lower price, too
- But how do you keep the traffic secure?
- Encrypt everything!

Encryption and Virtual Private Networks

- Use encryption to convert a shared line to a private line
- Set up a firewall at each installation’s network
- Set up shared encryption keys between the firewalls
- Encrypt all traffic using those keys

Actual Use of Encryption in VPNs

- VPNs run over the Internet
- Internet routers can't handle fully encrypted packets
- Obviously, VPN packets aren't entirely encrypted
- They are encrypted in a tunnel mode

Is This Solution Feasible?

- A VPN can be half the cost of leased lines (or less)
- And give the owner more direct control over the line's security
- Ease of use improving
  - Often based on IPsec

Key Management and VPNs

- All security of the VPN relies on key secrecy
- How do you communicate the key?
  - In early implementations, manually
  - Modern VPNs use something like IKE
- How often do you change the key?
  - IKE allows frequent changes

VPNs and Firewalls

- VPN encryption is typically done between firewall machines
- Do I need the firewall for anything else?
- Probably, since I still need to allow non-VPN traffic in and out

Internet Security Problems

- Problems related to the Internet as a whole
- Either its core infrastructures
- Or problems based on its fundamental characteristics

Some Internet Security Problems

- Routing security
- DNS security
- Distributed denial of service attacks
- IP spoofing
  - Already discussed in previous lecture

Routing Security

- Routing protocols control how packets flow through the Internet
- If they aren’t protected, attackers can alter packet flows at their whim
- Most routing protocols were not built with security in mind

Routing Protocol Security Threats

- Packets could be routed through an attacker
- Packets could be dropped
  - Routing loops, blackhole routing, etc.
- Some users' service could be degraded
- The Internet's overall effectiveness could be degraded
  - Slow response to failures
  - Total overload of some links
- Many types of defenses against other attacks presume correct routing

Where Does the Threat Occur?

- At routers, mostly
- Most routers are well-protected
  - But . . .
  - Several recent vulnerabilities have been found in routers
- Also, should we always trust those running routers?

How Do We Solve These Problems?

- Advertising routers must prove ownership and right to advertise
- Paths must be signed by routers on them
- Must avoid cut-and-paste attacks
- S-BGP addresses these issues
  - Not in wide use

DNS Security

- The Domain Name Service (DNS) translates human-readable names to IP addresses
  - E.g., thesiger.cs.ucla.edu translates to 131.179.192.144
  - DNS also provides other similar services
- It wasn’t designed with security in mind

DNS Threats

- Threats to name lookup secrecy
  - Definition of DNS system says this data isn’t secret
- Threats to DNS information integrity
  - Very important, since everything trusts that this translation is correct
- Threats to DNS availability
  - Potential to disrupt Internet service

What Could Really Go Wrong?

- DNS lookups could be faked
  - Meaning packets go to the wrong place
- The DNS service could be subject to a DoS attack
  - Or could be used to amplify one
- Attackers could “bug” a DNS server to learn what users are looking up

Where Does the Threat Occur?

- Unlike routing, threat can occur in several places
  - At DNS servers
  - But also at DNS clients
    - Which is almost everyone
- Core problem is that DNS responses aren’t authenticated

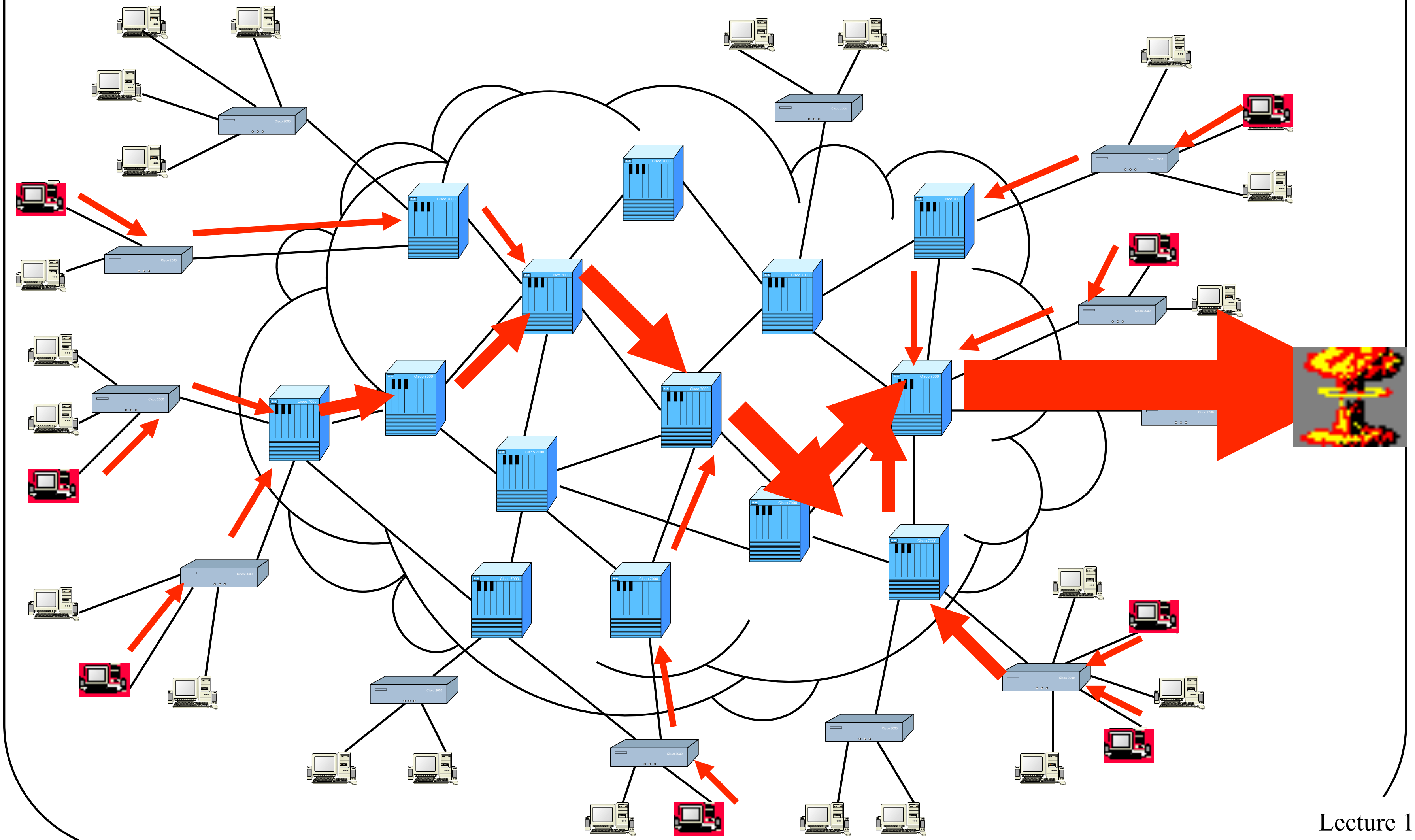
General Solution

- Authenticate DNS responses
- DNSSEC does that
- But there are significant technical issues in doing it properly
  - At an acceptable cost
  - While maintaining traditional DNS capabilities

Distributed Denial of Service Attacks

- Goal: Prevent a network site from doing its normal business
- Method: overwhelm the site with attack traffic
- Response: ?

The Problem



Why Are These Attacks Made?

- Generally to annoy
- Sometimes for extortion
- If directed at infrastructure, might cripple parts of Internet

Attack Methods

- Pure flooding
  - Of network connection
  - Or of upstream network
- Overwhelm some other resource
  - SYN flood
  - CPU resources
  - Memory resources
  - Application level resource
- Direct or reflection

Why "Distributed"?

- Targets are often highly provisioned servers
- A single machine usually cannot overwhelm such a server
- So harness multiple machines to do so
- Also makes defenses harder

How to Defend?

- A vital characteristic:
  - Don’t just stop a flood
  - ENSURE SERVICE TO LEGITIMATE CLIENTS!!!
- If you deliver a manageable amount of garbage, you haven’t solved the problem

Complicating Factors

- High availability of compromised machines
  - At least tens of thousands of zombie machines out there
- Internet is designed to deliver traffic
  - Regardless of its value
- IP spoofing allows easy hiding
- Distributed nature makes legal approaches hard
- Attacker can choose all aspects of his attack packets
  - Can be a lot like good ones

Basic Defense Approaches

- Overprovisioning
- Dynamic increases in provisioning
- Hiding
- Tracking attackers
- Legal approaches
- Reducing volume of attack
- None of these are totally effective