

Network Security: Continued
CS 236
On-Line MS Program
Networks and Systems Security
Peter Reiher

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?

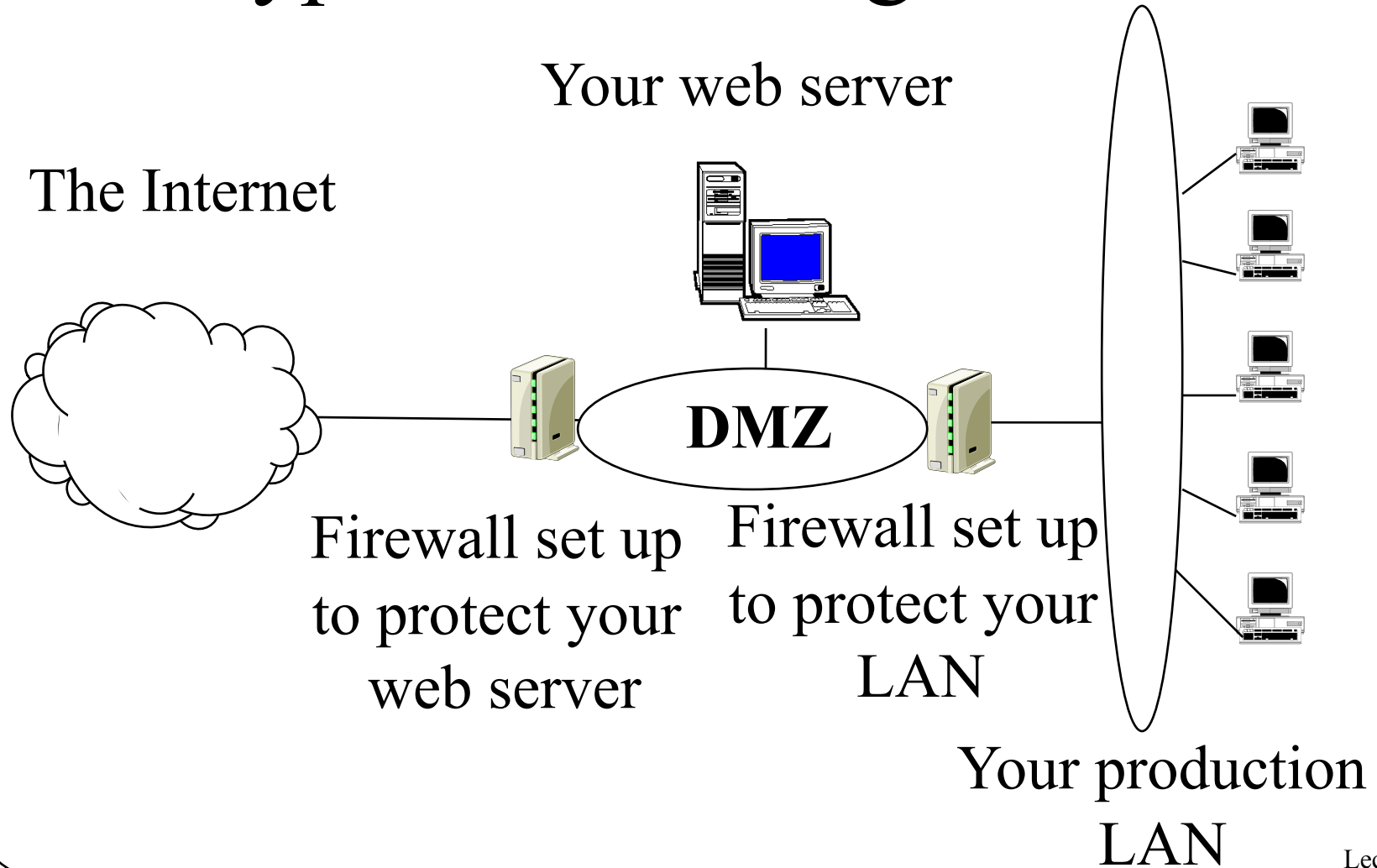
Firewall Location

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

Firewalls and DMZs

- A standard way to configure multiple firewalls for a single organization
- Used when organization runs machines with different openness needs
 - And security requirements
- Basically, use firewalls to divide your network into segments

A Typical DMZ Organization



Advantages of DMZ Approach

- Can customize firewalls for different purposes
- Can customize traffic analysis in different areas of network
- Keeps inherently less safe traffic away from critical resources

Dangers of a DMZ

- Things in the DMZ aren't well protected
 - If they're compromised, provide a foothold into your network
- One problem in DMZ might compromise all machines there
- Vital that main network doesn't treat machines in DMZ as trusted
- Must avoid back doors from DMZ to network

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

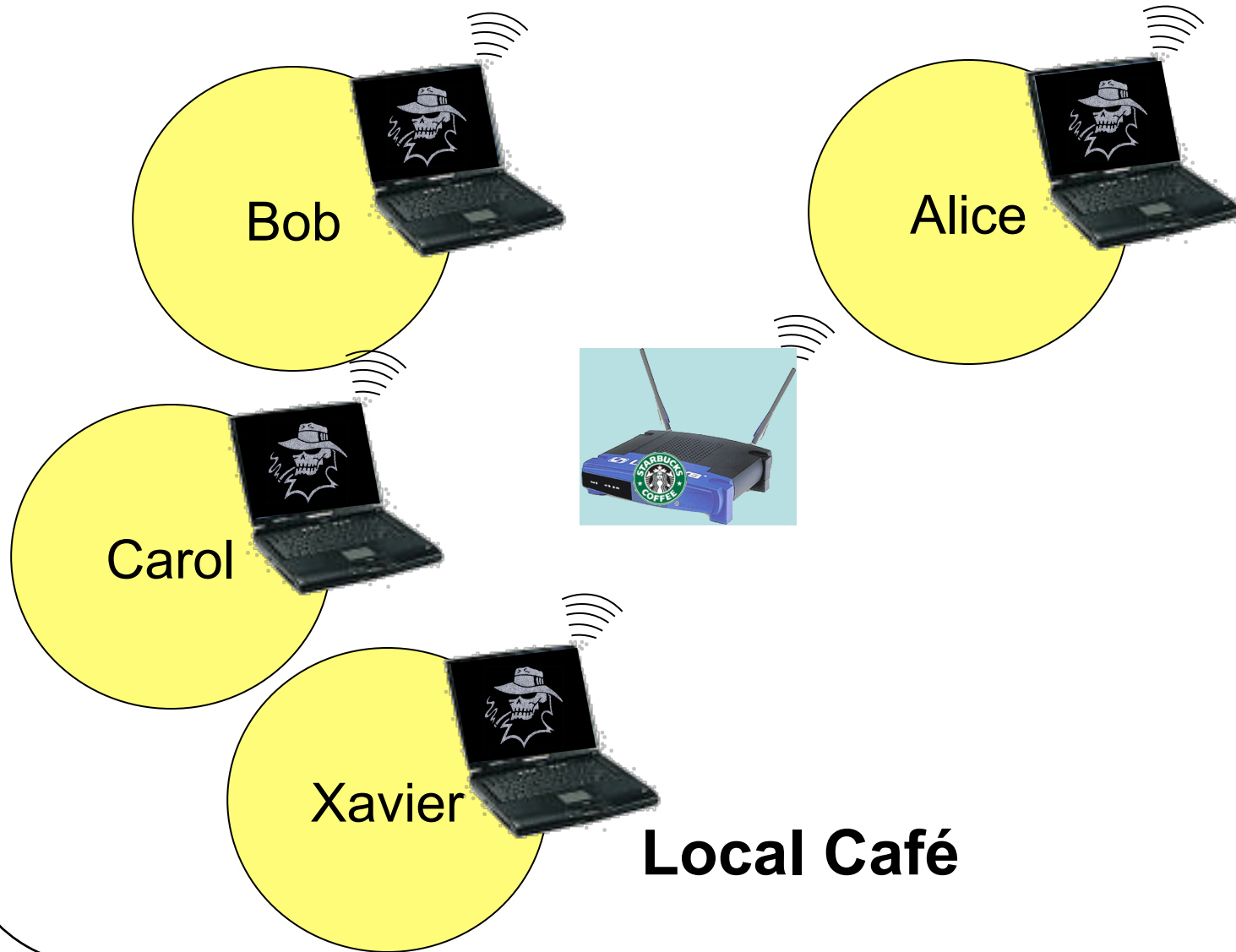
Keep Your Firewall Current

- 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?

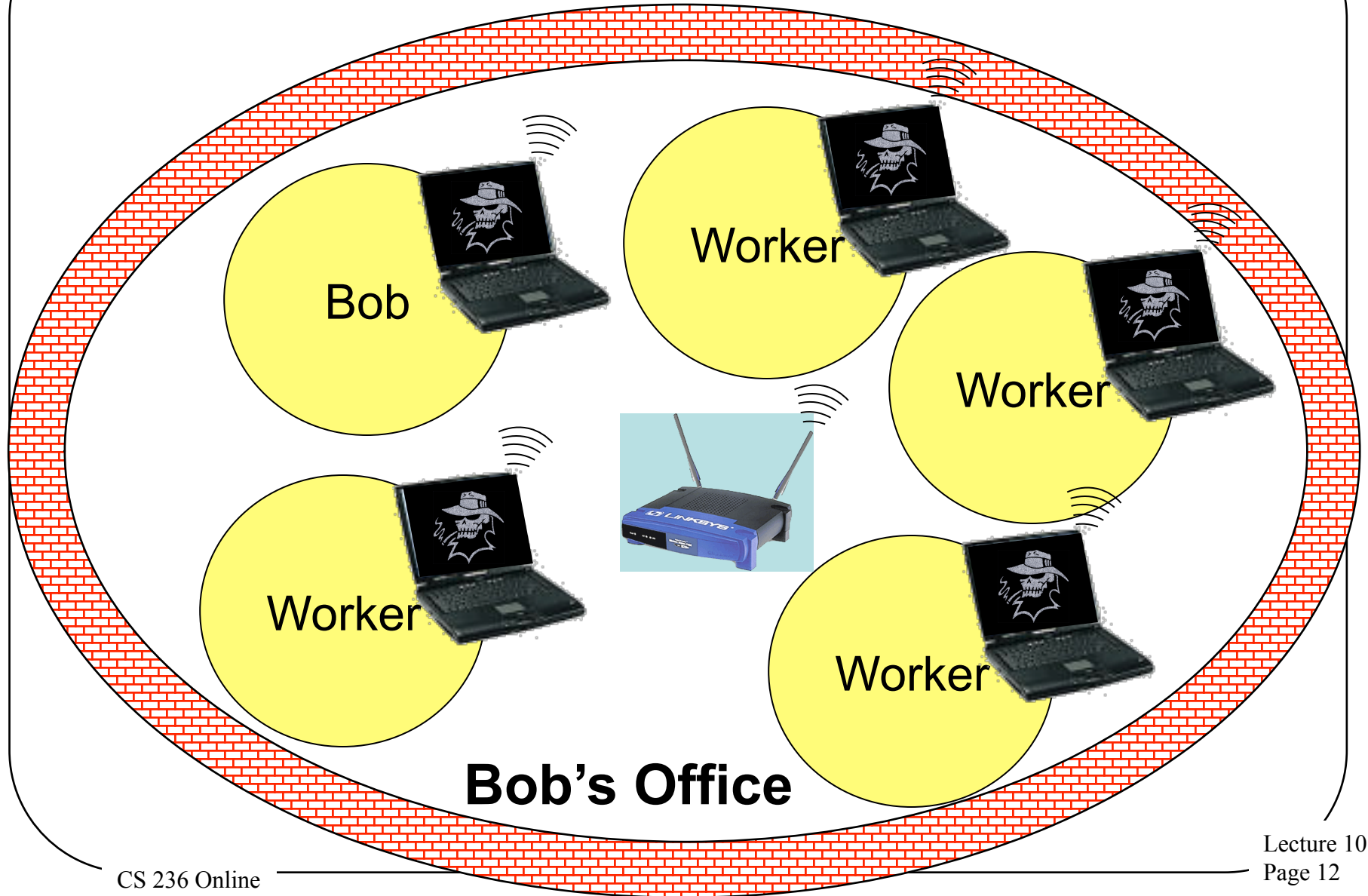
Closing the Back Doors

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

What About Portable Computers?



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
 - Or put them in constrained network
- Common in Cisco, Microsoft, and other companies' products
 - *Network access control*

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
 - Specific to local software and usage
- + Under machine owner's control
- + Can use in-machine knowledge for its decisions
- + May be able to do deeper inspection
- + Provides defense in depth

Cons of Personal Firewalls

- Only protects that machine
- Less likely to be properly configured
 - Since most users don't understand security well
 - And/or don't view it as their job
 - Probably set to the default
- On the whole, generally viewed as valuable