Network Security, Continued
Computer Security
Peter Reiher
April 28, 2016

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

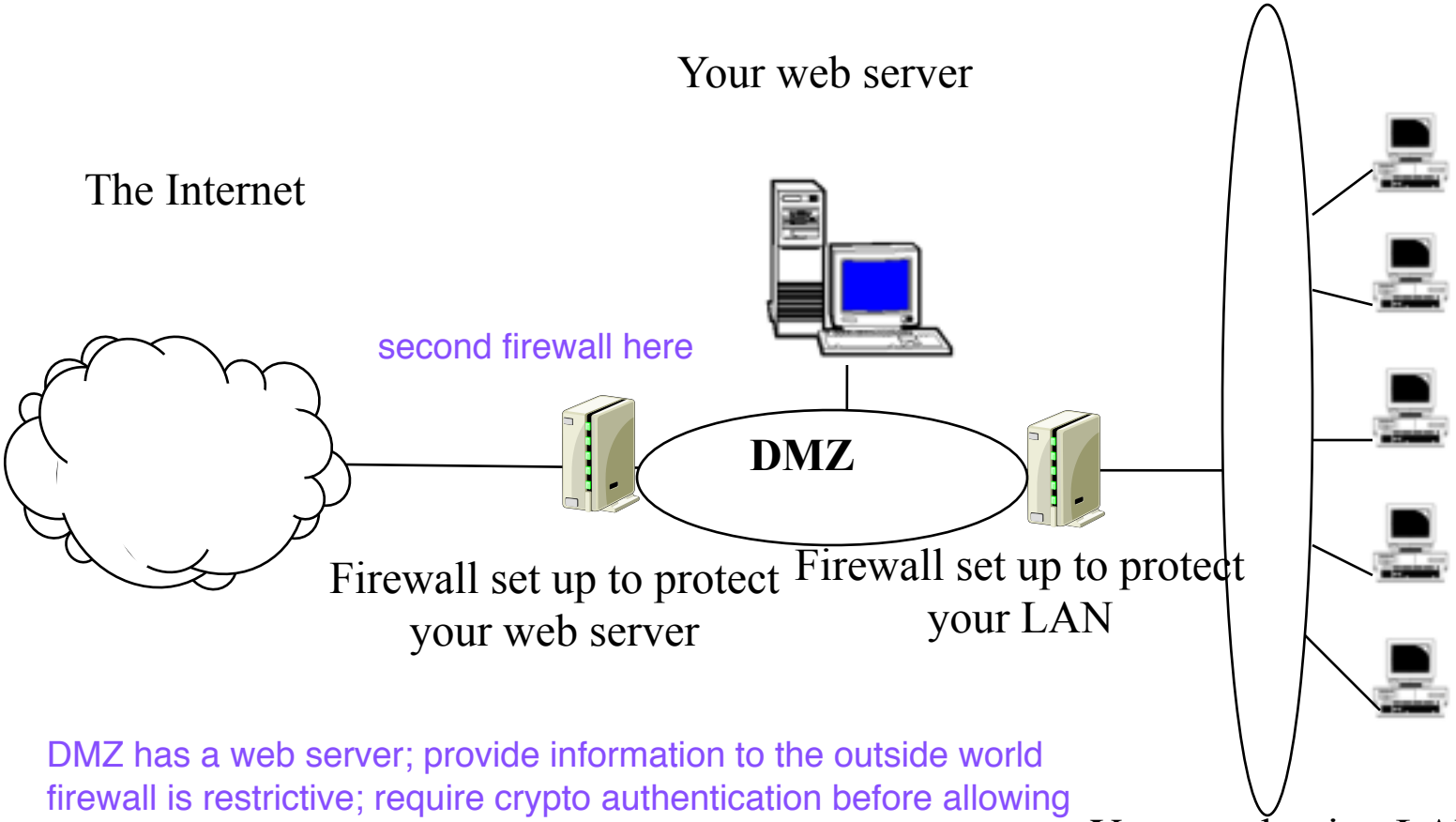
have a lot of interactions - how to protect when you have private and public information?
the right way to do this is to divide network into segment

- Clearly, between you and the bad guys
- But you may have some different types of machines/functionalities private and public segments
- 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



DMZ has a web server; provide information to the outside world
firewall is restrictive; require crypto authentication before allowing flow to go through the firewall

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

If I don't use web server, and I see HTTP request in my private network, then I know I have a problem

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

  anything else sitting in the DMZ; once he compromised one of them, he will compromise all of them
- Vital that main network doesn't treat machines in DMZ as trusted
- Must avoid back doors from DMZ to network

  sys admin takes care of the DMZ; he is a privileged user, he may want to bop back and forth between DMZ and his machine in a very backdoorish way; he could be compromised

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

turn off all background apps running

- Strictly limit access to the machine
  - Both login and remote execution

only sys and network admin should be able to login

making firewall a harder surface that makes it harder to be attacked
the less software you are running on your machines, the less flaws
(not to self, take out unnecessary programs)

Keep Your Firewall Current

you want to have someone who is in your organization who is aware of what kind of vulnerabilities is there

- New vulnerabilities are discovered all the time
  if student want to create new protocol: use open ports to do testing and development those ports after student finish, those ports can be a vulnerability as well
- 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

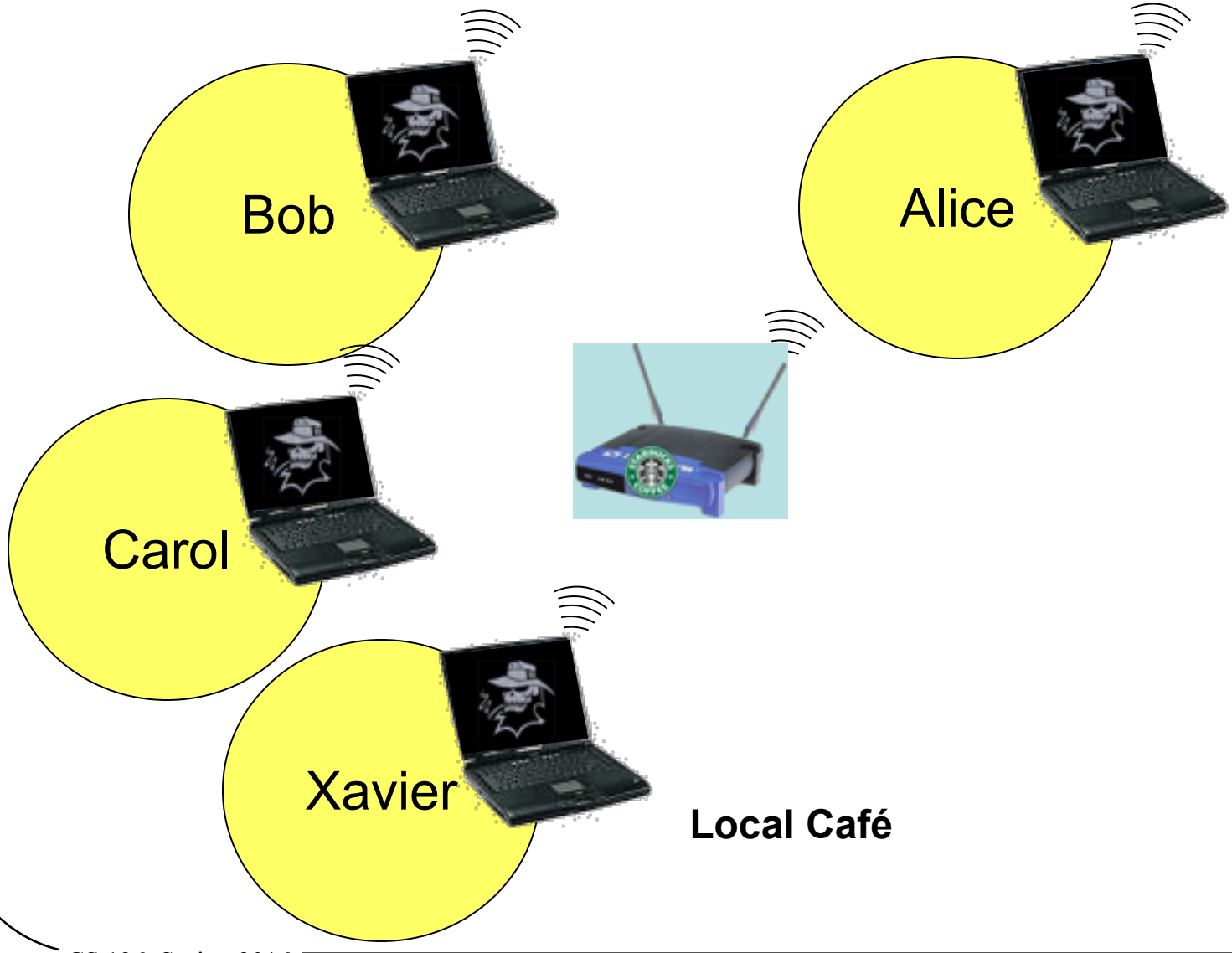
- Firewall security is based on assumption that all traffic goes through the firewall
- So be careful with:
  - Wireless connections
  - Portable computers
  - Sneakernet mechanisms and other entry points
- Put a firewall at every entry point to your network
- And make sure all your firewalls are up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

hard to force through your firewall
you can configure network to be safer

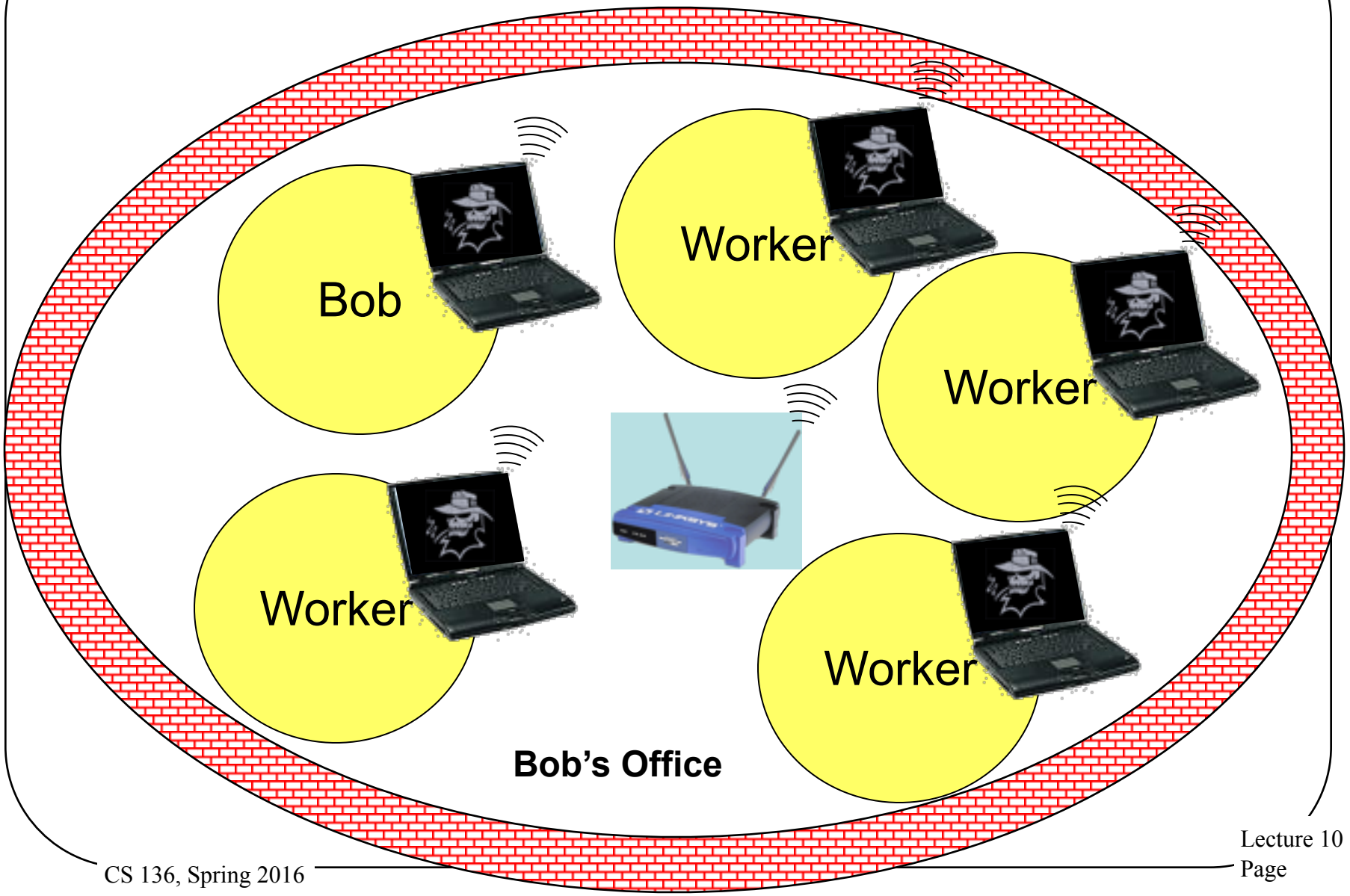
flash drives are sneakernets

a common way was to use the modem to connect to a coptier (dev

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 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

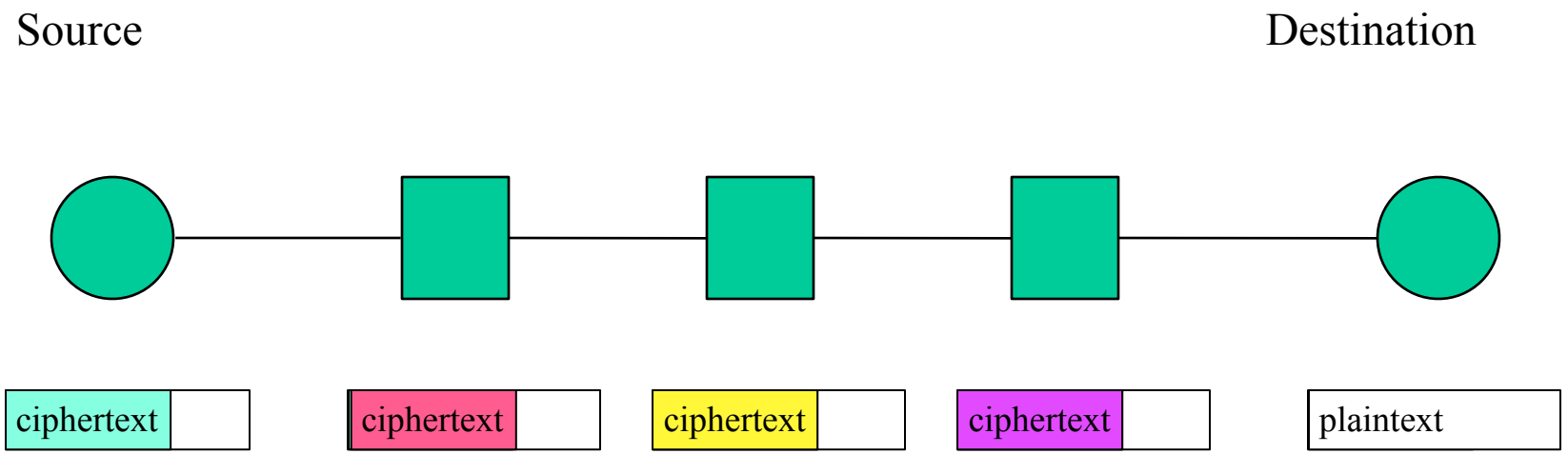
Cons of Personal Firewalls

- 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

Encryption and Network Security

- Relies on the kinds of encryption algorithms and protocols discussed previously
- Can be applied at different places in the network stack
- With different effects and costs

Link Level Encryption



Let's say we want to send a message using encryption

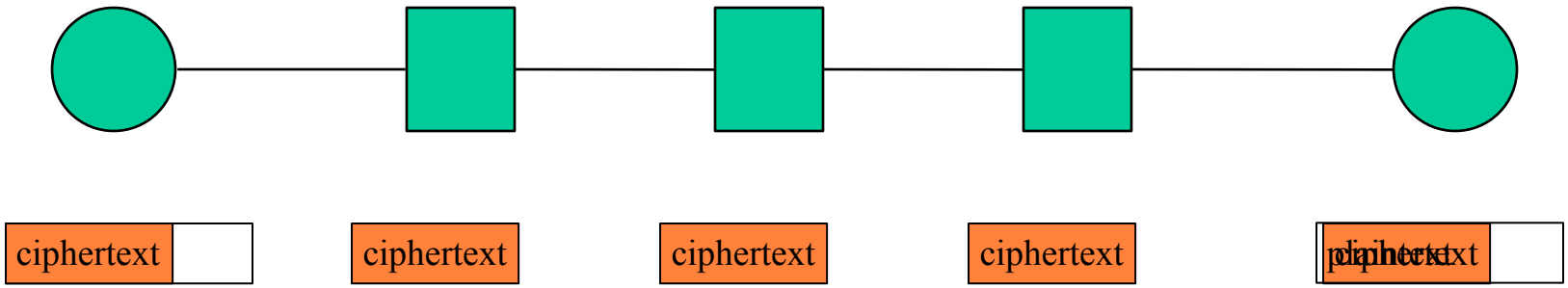
Different keys (maybe even different ciphers) used at each hop

End-to-End Encryption

link encrupton

Source

Destination



When would link encryption be better?

Cryptography only at the end points

Only the end points see the plaintext

Normal way network cryptography done

Where Are the Endpoints, Anyway?

- If you do end-to-end encryption, where are the endpoints?
- The network layer end points?
- The transport layer end points?
- The application layer end points?
- Maybe not even end machine to end machine (e.g., VPNs)?
- Has serious implications for where you do cryptography
  - And keying and trust issues

IPsec

- Standard for applying cryptography at the network layer of IP stack
- Provides various options for encrypting and authenticating packets
  - On end-to-end basis
  - Without concern for transport layer (or higher)

What IPsec Covers

- Message integrity
- Message authentication
- Message confidentiality

What Isn't Covered

- Non-repudiation
- Digital signatures
- Key distribution
- Traffic analysis
- Handling of security associations
- Some of these covered in related standards

Some Important Terms for IPsec

- Security Association - "A Security Association (SA) is a simplex 'connection' that affords security services to the traffic carried by it."
  - Basically, a secure one-way channel
- SPI (Security Parameters Index) – Combined with destination IP address and IPsec protocol type, uniquely identifies an SA

General Structure of IPsec

- Really designed for end-to-end encryption
  - Though could do link level
- Designed to operate with either IPv4 or IPv6
- Meant to operate with a variety of different ciphers
- And to be neutral to key distribution methods
- Has sub-protocols
  - E.g., Encapsulating Security Payload

Encapsulating Security Payload (ESP) Protocol

- Encrypt the data and place it within the ESP
- The ESP has normal IP headers
- Can be used to encrypt just the payload of the packet
- Or the entire IP packet

ESP Modes

- Transport mode
  - Encrypt just the transport-level data in the original packet
  - No IP headers encrypted
- Tunnel mode
  - Original IP datagram is encrypted and placed in ESP
  - Unencrypted headers wrapped around ESP

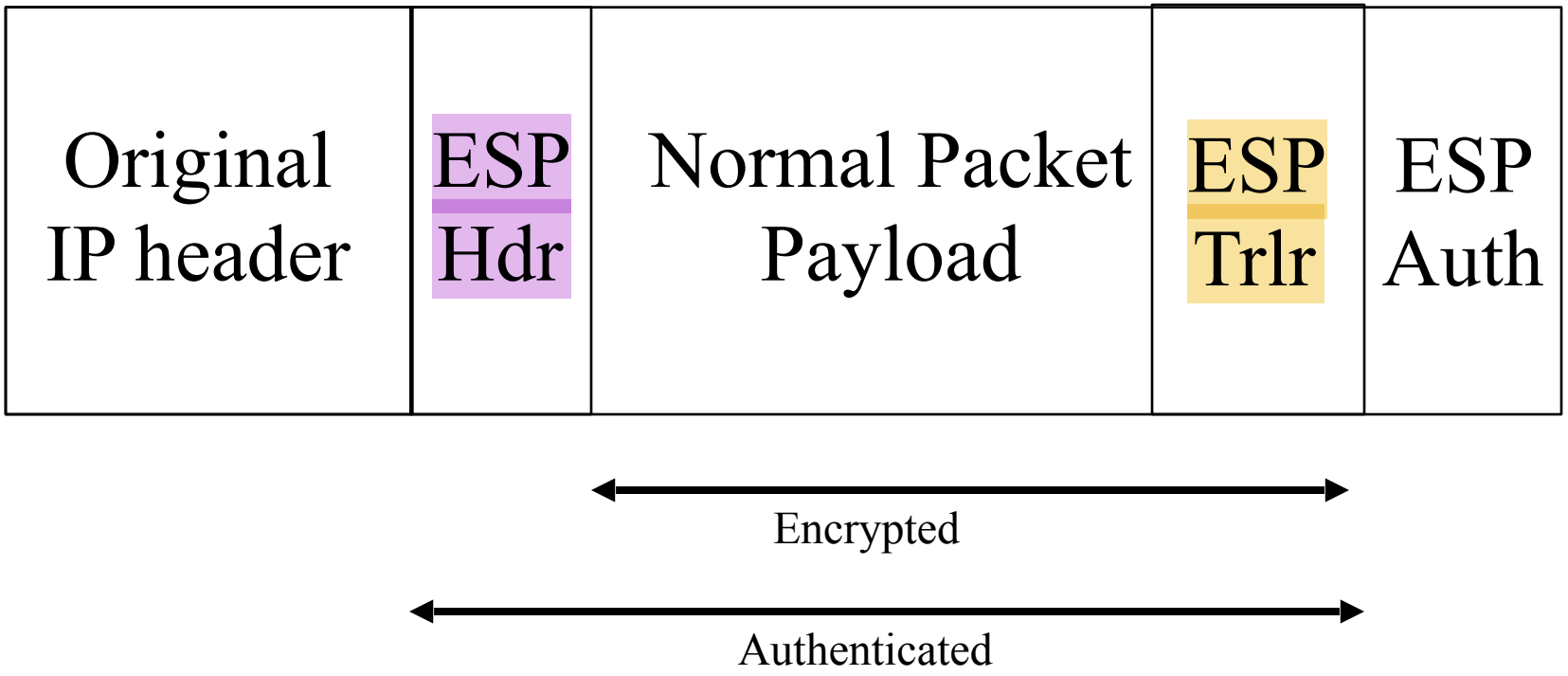
ESP in Transport Mode

- Extract the transport-layer frame
  - E.g., TCP, UDP, etc.
- Encapsulate it in an ESP
- Encrypt it
- The encrypted data is now the last payload of a cleartext IP datagram

ESP Transport Mode

orignal IP header has the original
it doesn't have information about other ip headers
IPsec and ESP transport mode
these information are there, so they have to be unencrypted

ESP auth is also unencrypted

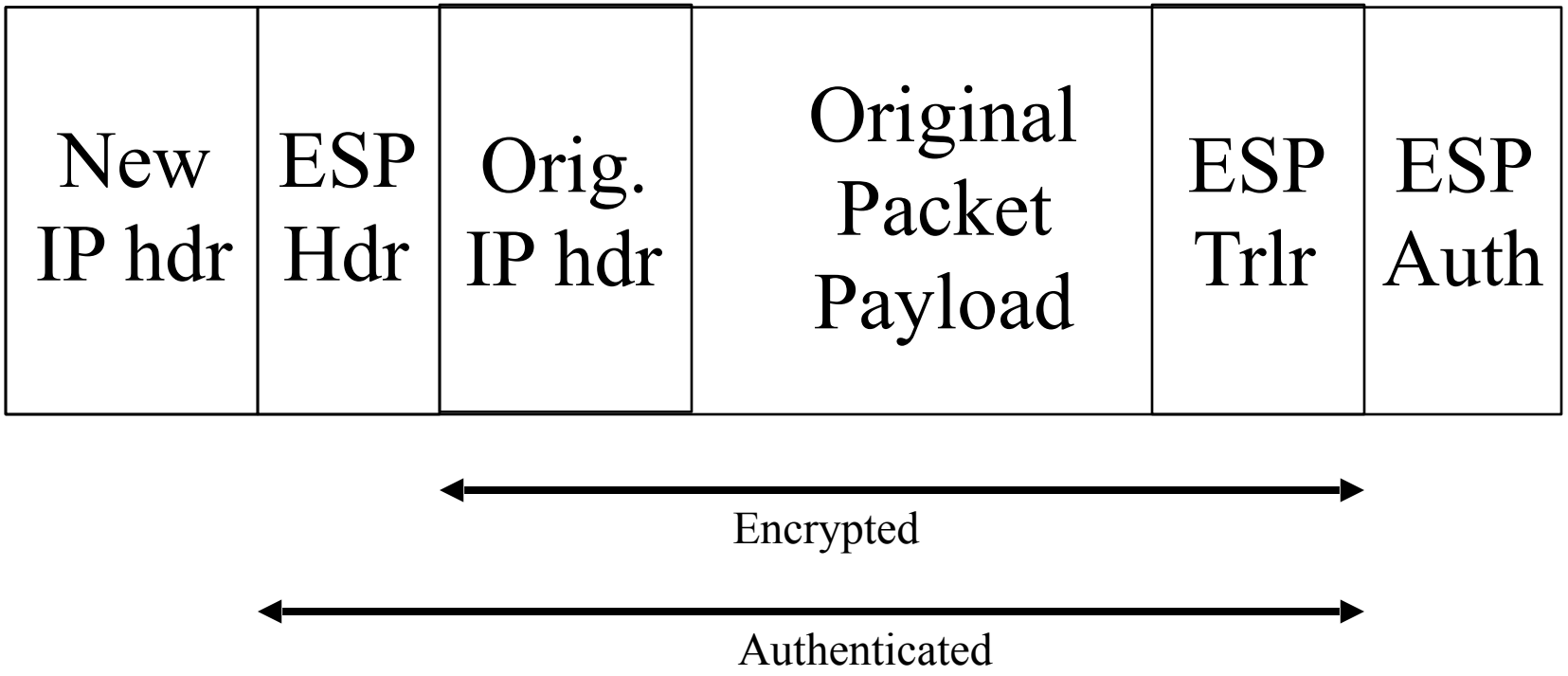


Using ESP in Tunnel Mode

encrypt the whole thing - place cleartext IP datagram outside of it

- Encrypt the IP datagram
  - The entire datagram
- Encapsulate it in a cleartext IP datagram
- Routers not understanding IPsec can still handle it
- Receiver reverses the process

ESP Tunnel Mode



Uses and Implications of Tunnel Mode

- Typically used when there are security gateways between sender and receiver
  - And/or sender and receiver don't speak IPsec
- Outer header shows security gateway identities
  - Not identities of real parties
- Can thus be used to hide some traffic patterns

What IPsec Requires

IPsec has no ciphers!

- Protocol standards
  - To allow messages to move securely between nodes
- Supporting mechanisms at hosts running IPsec
  - E.g., a Security Association Database
- Lots of plug-in stuff to do the cryptographic heavy lifting

The Protocol Components

- Pretty simple
- Necessary to interoperate with non-IPsec equipment
- So everything important is inside an individual IP packet's payload
- No inter-message components to protocol
  - Though some security modes enforce inter-message invariants

The Supporting Mechanisms

above network layer, below transport layer

- Methods of defining security associations
- Databases for keeping track of what's going on with other IPsec nodes
  - To know what processing to apply to outgoing packets
  - To know what processing to apply to incoming packets

Plug-In Mechanisms

- Designed for high degree of generality
- So easy to plug in:
  - Different crypto algorithms
  - Different hashing/signature schemes
  - Different key management mechanisms

these can be plugged in, so they are more convenient

Status of IPsec

- Accepted Internet standard
- Widely implemented and used
  - Supported in Windows 2000 and later
  - In Linux 2.6 (and later) kernel
  - Mac OS 10.6 and later
- The architecture doesn't require everyone to use it
- RFC 3602 on using AES in IPsec still listed as "proposed"
- AES will become default for ESP in IPsec

SSL and TLS

- SSL – Secure Socket Layer
- TLS – Transport Layer Security
- The common standards for securing network applications in Internet
  - E.g., web browsing
- Essentially, standards to negotiate, set up, and apply crypto

The Basics of SSL

- Usually a client/server operation
- Client contacts server negotiation can fail sometimes
- A negotiation over authentication, key exchange, and cipher takes place
- Authentication is performed and key agreed upon
- Then all packets are encrypted with that key and cipher at application level

Common Use

- Server authenticates to client using an X.509 certificate
  - Typically, client not authenticated
    - Though option allows it

server doesn't care who the client is

- Client provides material to server to derive session key
- Client and server derive same session key, start sending encrypted packets

Crypto in TLS/SSL

- Several options supported
- RSA or elliptic curve for PK part
- AES, DES, 3DES, or others for session cryptography use three different keys - get the effect of 128 bit key
- Not all are regarded as still secure
- Chosen by negotiation between client and server

Use of SSL/TLS

- The core crypto for web traffic
- Commonly used for many other encrypted communications
- Used in all major browsers
- Usually not part of OS per se
  - But all major OSes include libraries or packages that implement it

Security Status of SSL/TLS

- Kind of complex
- SSL is not very secure
- Early versions of TLS not so secure
- Later versions of TLS fairly secure
  - Depending on cipher choice
- Recent chosen-plaintext attacks shown to work on all versions
  - In special circumstances

don't build your own cryptography

Virtual Private Networks

- VPNs

if you had a trusted network that worked with the enclave, then you are good.

VPN: tunneling encrypt everyting from one head to another.

- 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?
- Could use leased lines, but . . .

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 all packets are iugin go address=null
- 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
  - Often using IPSec
- Gives owners flexibility and control

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 IKE or proprietary key servers
- How often do you change the key?
  - IKE allows frequent changes

VPNs and Firewalls

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

frewall doesn't work thatwell on incepted aa

- Need firewall "inside" VPN
  - Since VPN traffic encrypted
  - Including stuff like IP addresses and ports
  - "Inside" means "later in same box" usually

VPNs and Portable Computing

- Increasingly, workers connect to offices remotely

exchange etiqio often

  - While on travel
  - Or when working from home
- VPNs offer a secure solution
  - Typically as software in the portable computer
- Usually needs to be pre-configured

downloaded code

VPN Deployment Issues

- Desirable not to have to pre-deploy VPN software
  - Clients get access from any machine
- Possible by using downloaded code
  - Connect to server, download VPN applet, away you go
  - Often done via web browser
  - Leveraging existing SSL code
  - Authentication via user ID/password
  - Implies you trust the applet . . .
- Issue of compromised user machine

GPA -g= I wll slwf oya

Wireless Network Security

- Wireless networks are "just like" other networks
- Except . . .
  - Almost always broadcast
  - Generally short range
  - Usually supporting mobility
  - Often very open

Diffie-Helman Ke Isuad

Types of Wireless Networks

- 802.11 networks
  - Variants on local area network technologies
- Bluetooth networks
  - Very short range
- Cellular telephone networks
- Line-of-sight networks
  - Dedicated, for relatively long hauls
- Satellite networks

The General Solution For Wireless Security

- Wireless networks inherently less secure than wired ones
- So we need to add extra security
- How to do it?
- Link encryption
  - Encrypt traffic just as it crosses the wireless network
    Decrypt it before sending it along

Why Not End-to-End Encryption?

- Some non-wireless destinations might not be prepared to perform crypto
  - What if wireless user wants protection anyway?
- Doesn't help wireless access point provide exclusive access
  - Any eavesdropper can use network

802.11 Security

- Originally, 802.11 protocols didn't include security
- Once the need became clear, it was sort of too late
  - Huge number of units in the field
  - Couldn't change the protocols

using a portion of electromagi F d

- So, what to do?

wire equivalency protocl

WEP

- First solution to the 802.11 security problem
- Wired Equivalency Protocol
- Intended to provide encryption in 802.11 networks
  - Without changing the protocol
  - So all existing hardware just worked
- The backward compatibility worked
- The security didn't

What Did WEP Do?

- Used stream cipher (RC4) for confidentiality
  - With 104 bit keys
  - Usually stored on the computer using the wireless network
  - 24 bit IV also used
- Used checksum for integrity

What Was the Problem With WEP?

- Access point generates session key from its own permanent key plus IV
  - Making replays and key deduction attacks a problem
- IV was intended to prevent that
- But it was too short and used improperly
- In 2001, WEP cracking method shown
  - Took less than 1 minute to get key

WPA and WPA2

AES or disfe

- Generates new key for each session
- Can use either TKIP or AES mode
- Various vulnerabilities in TKIP mode
- AES mode hasn't been cracked yet
  - May be available for some WPA
  - Definitely in WPA2

Honeypots and Honeynets

- A *honeypot* is a machine set up to attract attackers
- Classic use is to learn more about attackers
- Ongoing research on using honeypots as part of a system's defenses

Setting Up A Honeypot

- Usually a machine dedicated to this purpose
- Probably easier to find and compromise than your real machines
- But has lots of software watching what's happening on it
- Providing early warning of attacks

What Have Honeypots Been Used For?

- To study attackers' common practices
- There are lengthy traces of what attackers do when they compromise a honeypot machine
- Not clear these traces actually provided much we didn't already know

Honeynets

- A collection of honeypots on a single network
  - Maybe on a single machine with multiple addresses
  - More often using virtualization
- Typically, no other machines are on the network
- Since whole network is phony, all incoming traffic is probably attack traffic

What Can You Do With Honeynets?

- Similar things to honeypots
  - But at the network level
- Also good for tracking the spread of worms
  - Worm code typically visits them repeatedly
- Main tool for detecting and analyzing botnets
- Gives evidence of DDoS attacks
  - Through *backscatter*
  - Based on attacker using IP spoofing

Honeynets and Botnets

- Honeynets widely used by security researchers to "capture" bots
- Honeynet is reachable from Internet
- Intentionally weakly defended
- Bots tend to compromise them
- Researcher gets a copy of the bot

Issues With Honeynet Research

- Don't want captured bot infecting others
  - Or performing other attack activities
- So you need to prevent it from attacking out
- But you also need to see its control traffic

What To Do With a Bot?

- When the bot is captured, what do you do with it?
- Typically, analyze it
  - Especially for new types of bots
  - To find weaknesses
  - And to track rest of botnet
- Analysis helpful for tracing "ancestry"

honeypot is useful for providing youw

Do You Need A Honeypot?

- Not in the same way you need a firewall
- Only useful if your security administrator spending a lot of time watching things
  - E.g., very large enterprises
- Or if your job is observing hacker activity
- Something that someone needs to be doing
  - Particularly, security experts watching the overall state of the network world
  - But not necessarily you