Last Time

- Internet Application Security and Privacy
  - Link-layer security: WEP, WPA, WPA2

This time

[Stinson, Shmatikov-Boneh]

- Internet Application Security and Privacy
  - Network-layer security: VPN, IPSec
  - Transport-layer security and privacy: TLS / SSL

WEP access control

- Adversary can inject a new message *F* onto a WEP-protected network
  - All he needs is a single plaintext/ciphertext pair
  - This gives him a value of *v* and the corresponding keystream *RC4(v,k)*
  - Then *C′* = <*F,c(F)*> XOR *RC4(v,k)*, and he transmits *v,C′*.
  - *C′* is in fact a correct encryption of *F*, so the message must be accepted.
- Just replace F with the plaintext that adversary get from the access point for authentication

Network-layer security

- Suppose every link in our network had strong link-layer security
- Why would this not be enough?

- We need security across networks
  - Ideally, end-to-end

- At the network layer, this is usually accomplished with a Virtual Private Network (VPN)

Virtual Private Networks

- Connect two (or more) networks that are physically isolated, and make them appear to be a single network
  - Alternately: connect a single remote host (often a laptop) to one network
- Virtual Private Network is a type of private network that uses public telecommunication, such as the Internet, instead of leased lines to communicate.
- Goal: adversary between the networks should not be able to read or modify the traffic flowing across the VPN

Four Critical Functions

- Authentication – validates that the data was sent from the sender.
- Access control – limiting unauthorized users from accessing the network.
- Confidentiality_– preventing the data to be read or copied as the data is being transported.
- Data Integrity – ensuring that the data has not been altered

Setting up a VPN

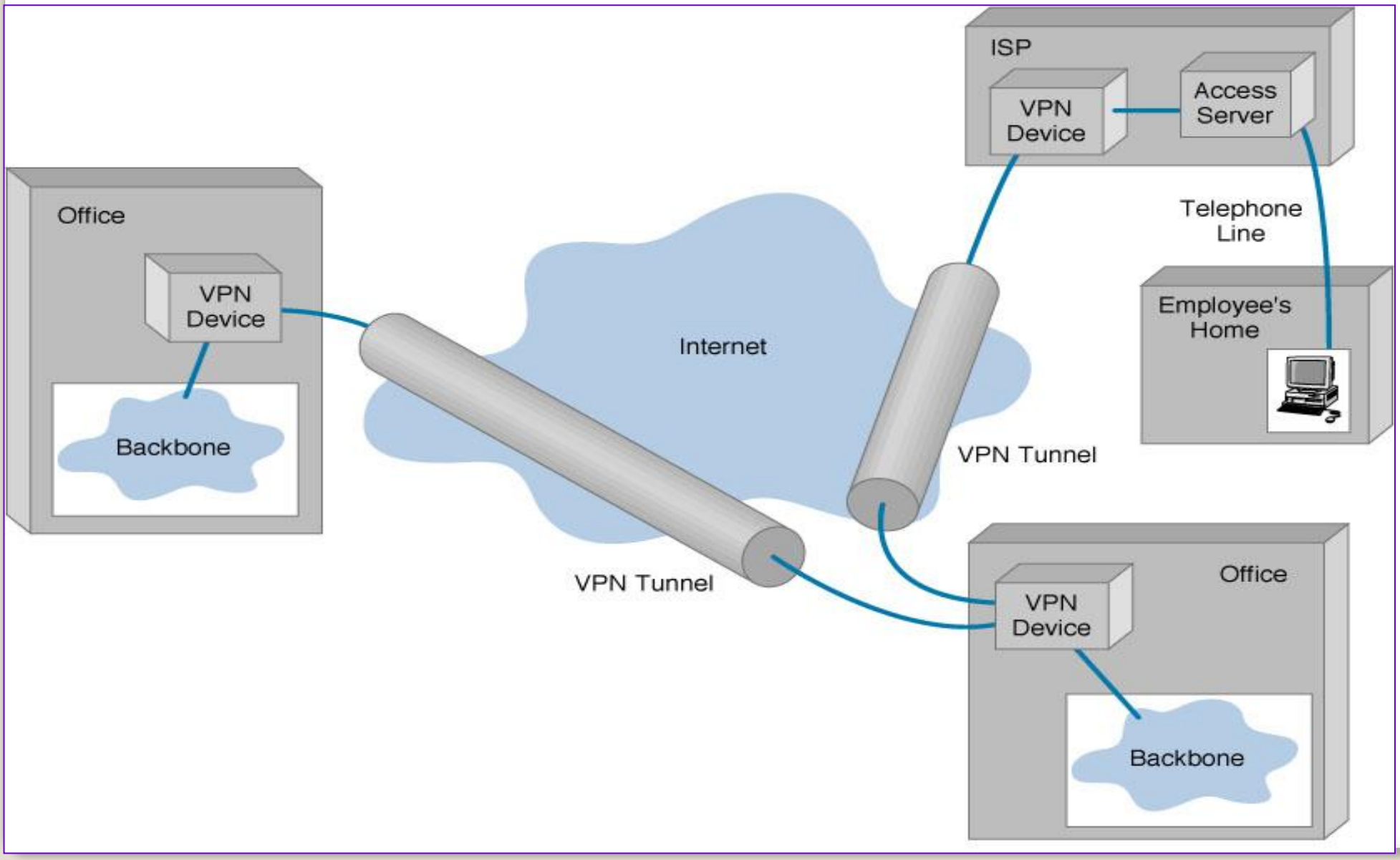
- One host on each side is the VPN gateway
  - Could be the firewall itself, or could be in DMZ
  - In the laptop scenario, it will of course be the laptop itself on its side

- Traffic destined for the "other side" is sent to the local VPN gateway

**DMZ (DeMilitarized Zone): is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger untrusted network.

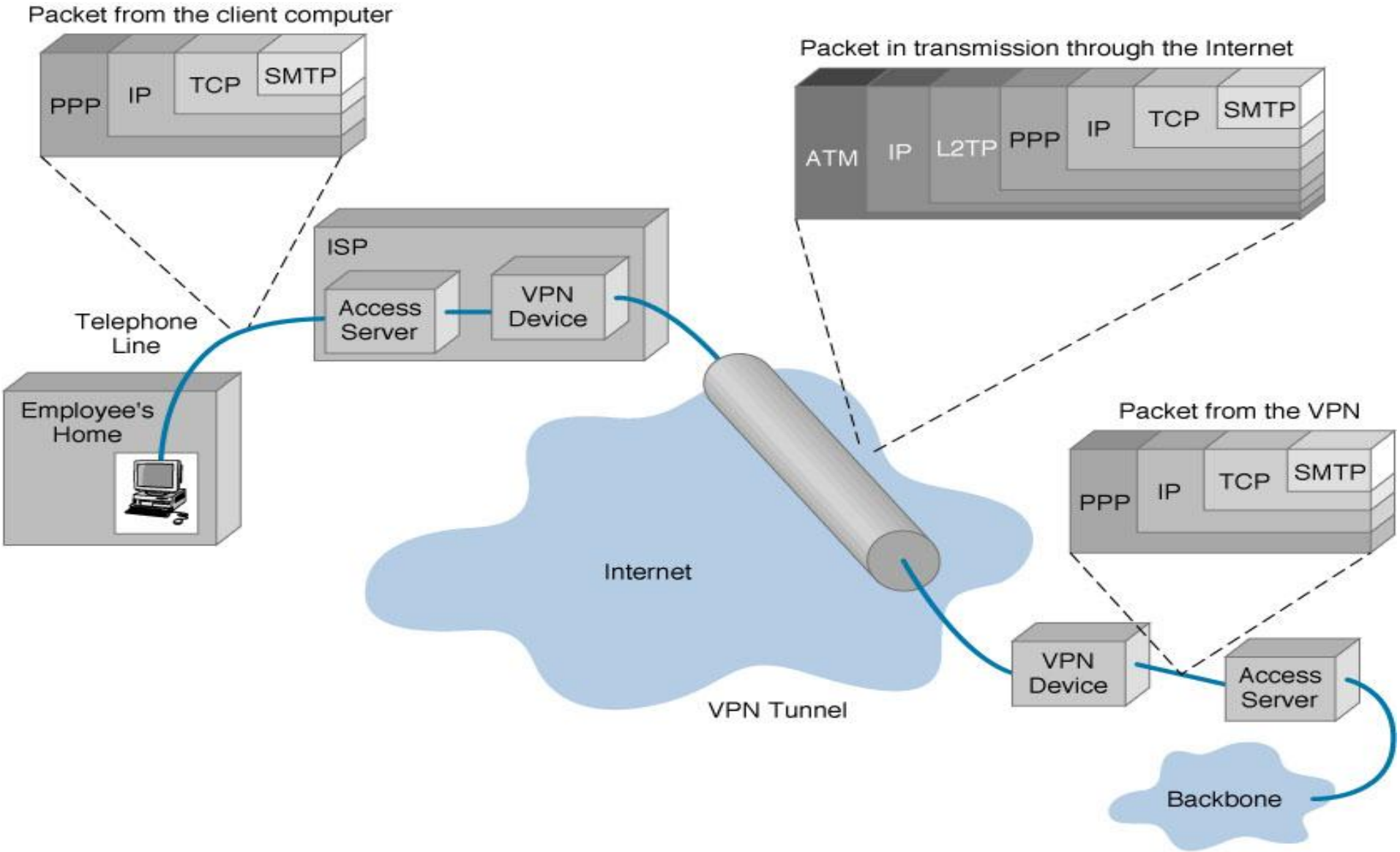
Setting up a VPN

- The local VPN gateway uses cryptography (encryption and integrity techniques) to send the traffic to the remote VPN gateway
  - Often by tunnelling
- The remote gateway decrypts the messages and sends them on to their appropriate destinations


ISP
VPN Device
Access Server
Telephone Line
Office
VPN Device
Backbone
Internet
VPN Tunnel
Employee's Home
VPN Tunnel
Office
VPN Device
Backbone

Tunnelling

- Tunnelling is the sending of messages of one protocol inside (that is, as the payload of) messages of another protocol, out of their usual protocol nesting sequence
  - So TCP-over-IP is not tunnelling, since you're supposed to send TCP (a transport protocol) over IP (a network protocol; one layer down in the stack)
  - But IP-over-TCP is tunnelling (going up the stack instead of down), as are IP-over-IP (same place in the stack)


Packet from the client computer
PPP
IP
TCP
SMTP
Packet in transmission through the Internet
ATM
IP
L2TP
PPP
IP
TCP
SMTP
ISP
Access Server
VPN Device
Telephone Line
Employee's Home
Internet
Packet from the VPN
PPP
IP
TCP
SMTP
VPN Device
Access Server
VPN Tunnel
Backbone

IPSec

- One standard way to set up a VPN is by using IPSec
- Many corporate VPNs use this (open) protocol
- Two modes:
  - Transport mode
  - Tunnel mode

IPSec

- Transport mode
  - Useful for connecting a single laptop to a home network
  - Only the contents of the original IP packet are encrypted and authenticated
- Tunnel mode
  - Useful for connecting two networks
  - The contents and the header of the original IP packet are encrypted and authenticated; result is placed inside a new IP packet destined for the remote VPN gateway

Four Protocols used in VPN

- In addition to IPSec, there are a number of other standard ways to set up a VPN
- PPTP -- Point-to-Point Tunneling Protocol
  - Microsoft's PPTP was an older protocol
  - It had about as many design flaws as WEP
  - Most users now migrating to IPSec
- L2TP -- Layer 2 Tunneling Protocol

- SOCKS – is not used as much as the ones above

Transport-layer security and privacy

- Network-layer security mechanisms arrange to send individual IP packets securely from one network to another
- **Transport-layer security** mechanisms transform arbitrary TCP connections to add security
  - And similarly for "privacy" instead of "security"
- The main transport-layer security mechanism:
  - TLS (formerly known as SSL)
- The main transport-layer privacy mechanism
  - Tor

TLS / SSL

- In the mid-1990s, Netscape invented a protocol called **Secure Sockets Layer (SSL)** meant for protecting HTTP (web) connections
  - The protocol, however, was general, and could be used to protect any TCP-based connection
  - HTTP + SSL = HTTPS
- Historical note: there was a competing protocol called S-HTTP. But Netscape and Microsoft both chose HTTPS, so that's the protocol everyone else followed

TLS / SSL

- SSL went through a few revisions, and was eventually standardized into the protocol known as TLS (Transport Layer Security)

TLS at a high level

- Client connects to server, indicates it wants to speak TLS, and which cipher suites it knows
- Server sends its certificate to client, which contains:
  - Its host name
  - Its public key
  - Some other administrative information
  - A signature from a Certificate Authority
- Server also chooses which cipher suite to use
- Client sends symmetric encryption key *K, encrypted with server's public key*
- *Communication now proceeds using K and the chosen ciphersuite*

Privacy Enhancing Technologies

- So far, we've only used encryption to protect the *contents* of messages
- *But there are other things we might want to protect as well!*
- *We may want to protect the metadata*
  - *Who is sending the message to whom?*
  - *If you're seen sending encrypted message to Human Rights Watch, bad things may happen*
- *We may want to hide the existence of the message*
  - *If you're seen sending encrypted messages at all, bad things may happen*

Tor

- Tor is another successful privacy enhancing technology that works at the transport layer
  - Hundreds of thousands of users
- Normally, any TCP connection you make on the Internet automatically reveals your IP address
  - Why?
- Tor allows you to make TCP connections without revealing your IP address
- It's most commonly used for HTTP (web) connections

Recap

- Internet Application Security and Privacy
  - Network-layer security: VPN, IPSec
  - Transport-layer security and privacy: TLS / SSL

Next time

- Internet Application Security and Privacy
  - Transport-layer security and privacy: Tor
  - Application-layer security and privacy: SSH, remailers, PGP/gpg, OTR