IPsec

IPsec

Encryption at Different Layers

- Most layers have control information that must be decoded before decryption is possible — this must always be sent in the clear
- If the layer does demultiplexing, the information for that must be in the clear, too, to permit different keys for different destinations
- Anything higher-level is hidden

Link Layer

- Framing information must be in cleartext
- Link layer (if used) addresses must be cleartext, to permit proper delivery
- Link layer type field must be cleartext
- Protects IP source and destination addresses — but only for that hop
- Common for especially-vulnerable links: WiFi, satellite downlinks, etc.
- Often used for access control

IPsec

- Network-layer security protocol for the Internet.
- Operates at the IP layer — has a cleartext IP header
- Completely transparent to applications.
- Generally must modify protocol stack or kernel; out of reach of application writers or users.

History

SP3	Layer 3 security protocol for SDNS.
NLSP	OSIfied version of SP3, with an incomprehensible spec.
swIPe	UNIX implementation by Ioannidis and Blaze (1993).
ka9q	Phil Karn's proto-IPsec
IPsec	Many years of design in the IETF
1995	First IETF version of IPsec
1998	Revised version with sequence numbers and authentication
2005	IPsec v3, for newer algorithms and larger sequence numbers

Why IPsec?

- SSL doesn't protected against certain attacks
- Example: enemy sends forged packet with RST bit set; tears down connection
- Example: enemy sends bogus data for connection — SSL detects that, but can't recover, since TCP has accepted the data
- Also — SSL can't (easily) protect UDP

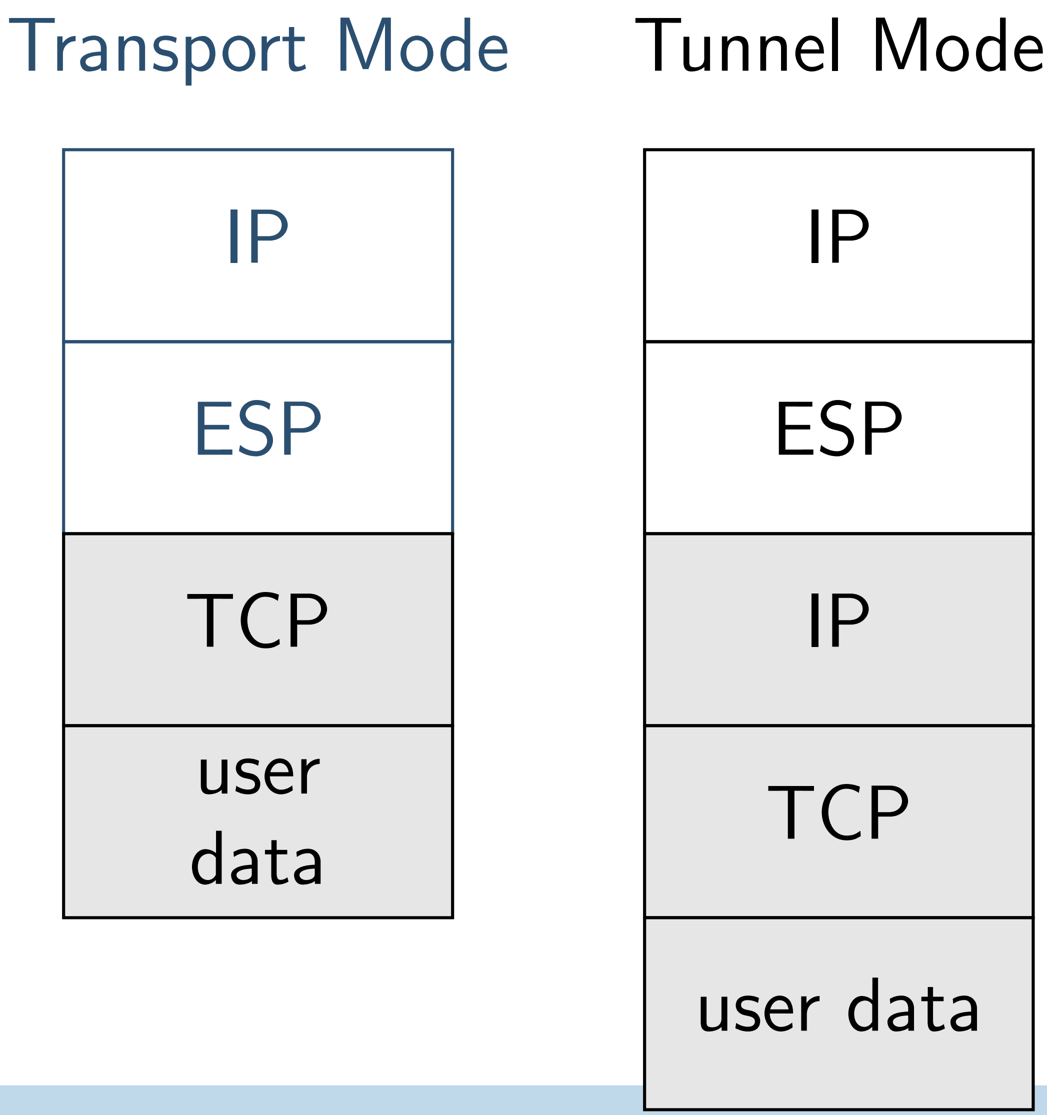
Protects All Applications

- To protect an application that uses TLS, you have to change its code
- IPsec protects *all* traffic
- But — how does an application know if IPsec is present?
- Can it request IPsec protection?

IPsec Structure

- Nested headers: IP; ESP or AH; maybe another IP; TCP or UDP; then data.
- Cryptographic protection can be host to host, host to firewall, or firewall to firewall.
- Option for user-granularity keying.
- Works with IPv4 and IPv6.
- Implements *Virtual Private Networks* (VPNs)

Some Packet Layouts



Tunnel and Transport Mode

- Transport mode protects end-to-end connections
- Tunnel mode — much more common — is used for VPNs and telecommuter-to-firewall
- The inner IP header can have site-local addresses

Implementation Choices

- "Bump in the stack" — host-resident
- In network hardware; explicitly controlled by the host
- "Bump in the wire" — external device in the network cable; not known to the host
- Gateway- or firewall-resident — not known to any hosts within the protected net

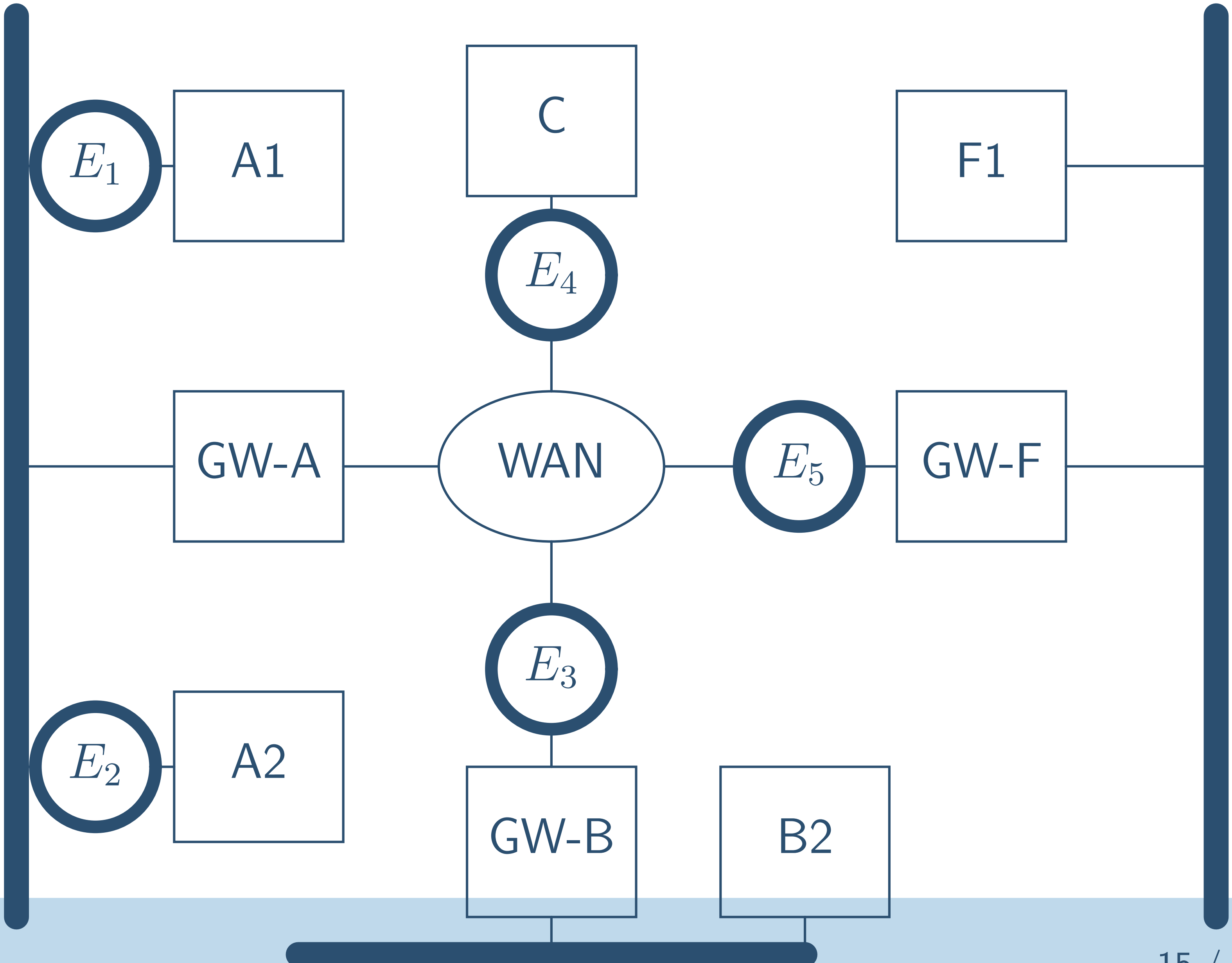
IPsec Addressing

- Packets are always addressed to the decryptor
- No need for “snooping”
- May be further forwarded

Security Associations

- SA: *Security Association*
- Think of it as an IPsec connection
- All of the parameters needed for an IPsec session: crypto algorithms (AES, SHA1, etc.), modes of operation (CBC, HMAC, etc.), key lengths, digest lengths, traffic to be protected, etc.
- Both sides must agree on the SA for secure communications to work

Topologies



Paths

- A1 to F1:
  Encryptors E_1, E_5 (tunnel mode)
- B2 to F1:
  Encryptors E_3, E_5 (tunnel mode)
- A2 to C:
  Encryptors E_2, E_4 (transport mode)

Uses for IPsec

- Virtual Private Networks.
- "Phone home" for laptops, telecommuters.
- General Internet security?

Outbound Packet Processing

- Compare packet — src and dst addr, src and dst port numbers — against *Security Policy Database* (SPD)
- If packet should be protected, consult *Security Association Database* (SADB) to find SA
- Add appropriate IPsec header

Inbound Packet Processing

- If IPsec-protected, look up SA, authenticate, and decrypt
- Compare packet — src and dst addr, src and dst port numbers, as before — against SPD to see if it *should* have been protected, and by which SA
- If the protection characteristics match, accept the packet
- If they do not match, discard it

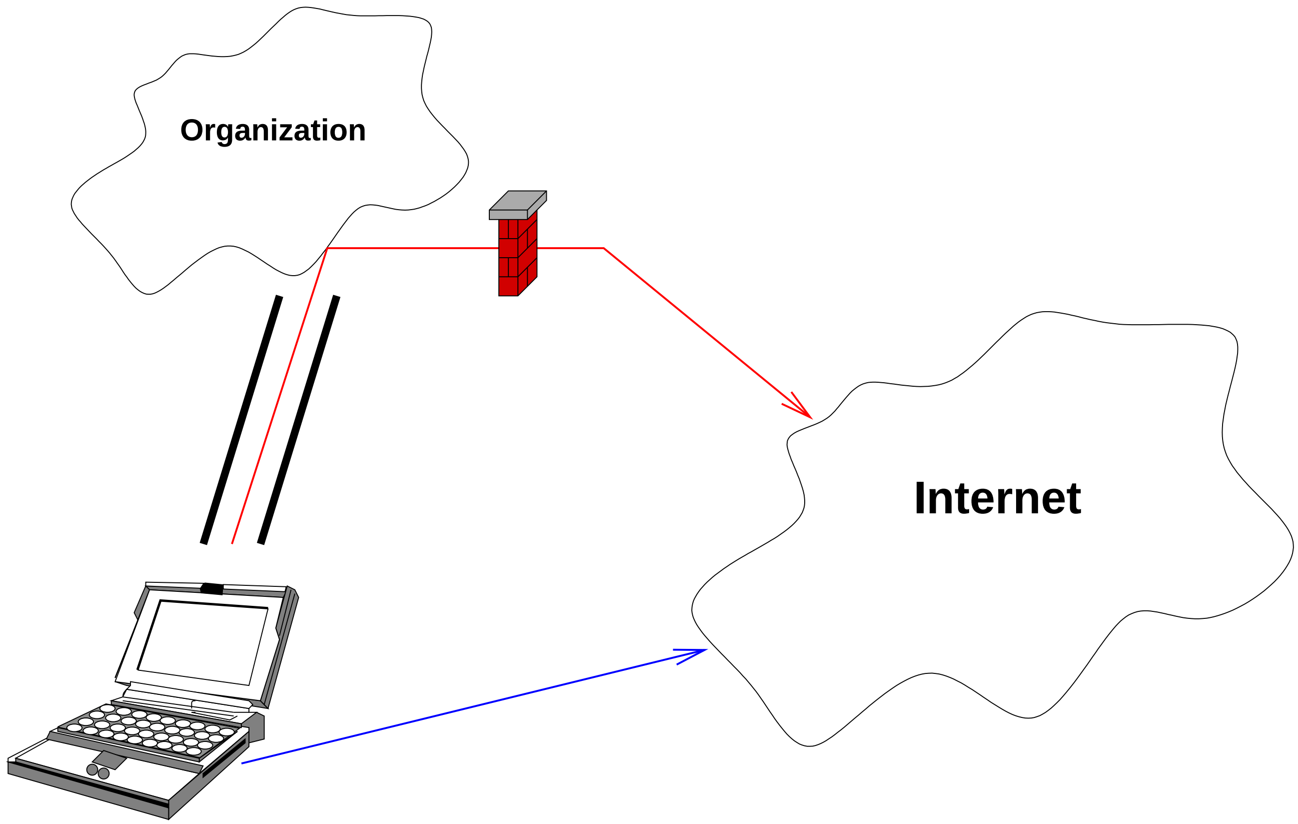
Security Policy Database: Theory

- IP address range or subnet: protect everything going to 128.59.0.0/16
- Port number list or range: 25,110,143
- Protect all addresses and/or all port numbers: full protection
- Multiple sets of the above

Security Policy Database: Reality

- Most IPsec usage is for VPNs
- Two options: send all traffic to the main site for relaying (triangle routing) or send Internet-bound traffic directly to the Internet
- Tradeoff: performance and reliability versus protection and policy enforcement by the organizational firewall

Triangle Routing



For Triangle Routing, the SPD says "protect everything". For Direct Routing, the SPD says "protect traffic destined for the organization".

End-to-End ESP vs. Firewalls

- Suppose you have a firewall that allows some outgoing connections
- Further suppose that some internal host wishes to talk end-to-end (transport mode) ESP to the outside
- When the firewall sees the encrypted packet, it can't tell if it's a new connection (SYN bit set) or not
- It also can't tell what port number it's going to, or even if it's transport mode or tunnel mode

IPsec Details

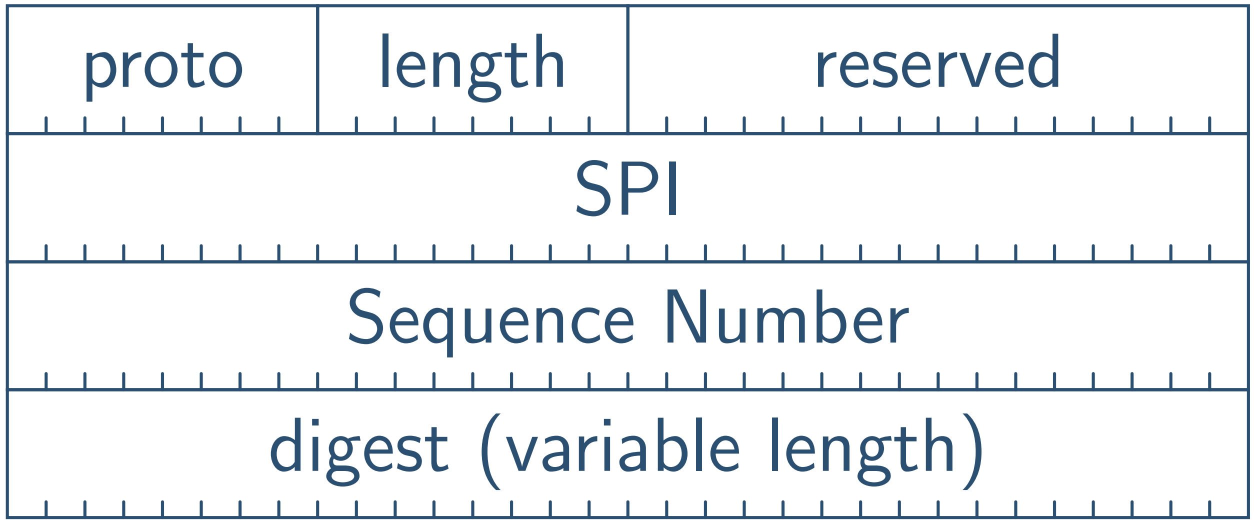
Authentication Header (AH)

- Based on keyed cryptographic hash function.
- Covers AH header, payload and immutable portion of preceeding IP header.
- Not that useful today, compared to ESP with null encryption
- Usually used with HMAC-SHA1 or HMAC-MD5
- HMAC output is frequently truncated
- Details: see RFC 4302

Truncating HMACs

- It is not necessary to send the full HMAC
- Tradeoff between packet size (i.e., network performance) and probability of forgery
- 8 or 12 bytes is generally enough: forgery probability is 2^{-64} or 2^{-96}
- Also — makes it harder to verify a possibly-recovered key

AH Layout


proto
length
reserved
SPI
Sequence Number
digest (variable length)

What is an SPI?

- SPI — Security Parameter Index
- Identifies *Security Association*
- Each SA has its own keys, algorithms, policy rules
- On packet receipt, look up SA from $\langle$SPI, dstaddr$\rangle$ pair

Other AH Fields

- "Proto" — what transport protocol header is next (i.e., TCP, UDP, etc.)
- "length" — length of AH header in 32-bit words, minus 2
- Actually, length is implicit in the security association; putting it in the header permits context-free (and unkeyed) examination of the packet
- "Sequence" — prevents replay attacks

Why a Sequence Number?

- Prevent packet replays
- Permitted by the IP model — but accidents are not the same as malice
- Many attacks possible if replays are permitted

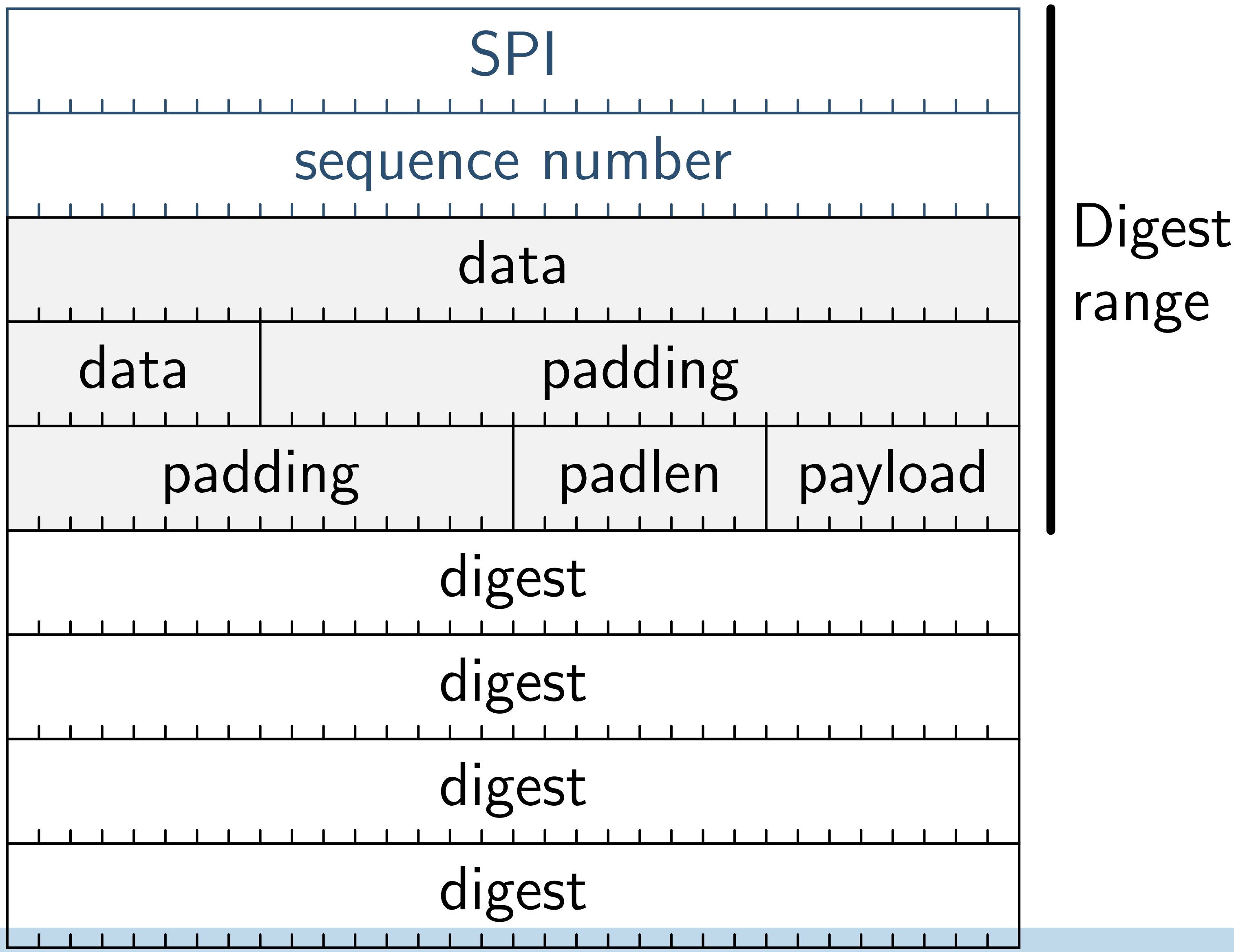
Mutable Parts of the IP Header

- Some parts of the IP header change in transit
- Obvious: TTL (and hence IP checksum)
- Fragmentation? You generally reassemble fragments before doing AH processing
- DSCP (previously known as ToS)
- IP options — some change in flight (record route, source route); others do not. See RFC 4302 for details

Encapsulating Security Payload (ESP)

- Carries encrypted packet.
- An SPI is used, as with AH.
- Preferred use of ESP is for AES in CBC mode with HMAC-SHA1

ESP Layout



SPI
sequence number
data
data
padding
padding
padlen
payload
digest
digest
digest
digest
Digest range

Padding

- "padlen" says how many bytes of padding should be removed from the packet
- Primary purpose: handle CBC blocksize issue
- Secondary purpose: add random extra padding, to confuse *traffic analysts* (but it doesn't do a very good job of that)

Traffic Analysis of IP Packets

- What can you learn from encrypted packets?
- Source address
- Destination address
- Length
- Time
- Hard to hide these things, even with crypto

Using ESP

- Can be used with null authentication or null encryption
- With null encryption, provides authentication only
- Easier to implement than AH
- Note: you should *virtually always* use authentication with ESP
- Similarly, sequence numbers should be used whenever possible

Nested IPsec

- In theory, can nest IPsec headers
- Outer layer: tunnel mode for VPN
- Inner layer: transport mode for host-to-host protection
- Rarely implemented

Issues

IPsec and Firewalls

- Encryption is not authentication or authorization
- Access controls may need to be applied to encrypted traffic, depending on the source.
- The source IP address is only authenticated if it is somehow bound to the certificate.
- Encrypted traffic can use a different firewall; however, co-ordination of policies may be needed.

IPsec and the DNS

- IPsec often relies on the DNS.
  - Users specify hostnames.
  - IPsec operates at the IP layer, where IP addresses are used.
  - An attacker could try to subvert the mapping.
- We need to protect the DNS, via DNSSEC (later in the term)
- DNSSEC may not meet some organizational security standards.
- DNSSEC — which isn't deployed yet, either — uses its own certificates, not X.509.

Implementation Issues

- How do applications request cryptographic protection? How do they verify its existence?
- How do adminstrators mandate cryptography between host or network pairs?
- We need to resolve authorization issues.

Requesting Protection

- Some stacks permit applications to request IPsec protection
- Creates temporary SPD entry
- May cause key management negotiation or SA change (wait till next class)
- But — what about bump-in-the-wire or gateway-resident IPsec implementations?
- Would need marking in the packets, but no mechanism for that has ever been defined

Implementation Status

- IPsec is available for all major operating systems
- Not all of them support all of the many options
- Hard to use for specific application protection
- Nested IPsec rarely available