Network layers
- Application
- Transport
- Network
- Lower level

Roughly...
- Application layer: the communicating processes themselves and the actual messages transmitted
- Transport layer: handles transmissions on an “end-to-end” basis
- Network layer: handles transmissions on a “hop-by-hop” basis

Examples
- Application layer: PGP, SSH
- Transport layer: SSL/TLS
- Network layer: IPsec
- Security at the lower layer?
Security in what layer?

- Depends on the purpose...
  - What information needs to be protected?
  - What is the attack model?
  - Who shares keys in advance?
  - Should the user be involved?
- E.g., a network-layer protocol cannot authenticate two end-users to each other
- An application-layer protocol cannot protect IP header information
- Also affects efficiency, ease of deployment, etc.

Example: PGP vs. SSL vs. IPsec

- PGP is an application-level protocol for "secure email"
  - Can provide security on "insecure" systems
  - Users choose when to use PGP; user must be involved
  - Alice’s signature on an email proves that Alice actually generated the message, and it was received unaltered; also non-repudiation
  - In contrast, SSL would secure "the connection" from Alice’s computer

Example: PGP vs. SSL vs. IPsec

- SSL sits “on top of” the transport layer
  - End-to-end security, best for connection-oriented sessions
  - User does not need to be involved
  - The OS does not have to be changed
  - Easy to modify applications to use SSL
  - If SSL rejects packet accepted by TCP, then TCP rejects “correct” packet when it arrives!
    - SSL must then close the connection...

Example: PGP vs. SSL vs. IPsec

- IPsec sits “on top of” the network layer
  - End-to-end or hop-by-hop security
    - Best for connectionless channels
    - Need to modify OS
  - All applications are “protected” by default, without requiring any change to applications or actions on behalf of users
  - Can only authenticate hosts, not users
  - User completely unaware that IPsec is running
Take home message...

- Best solution may involve changes at both the OS and applications layers
  - The "best" solution is not to run SSL and IPsec!
  - Would have been better to design system with security in mind from the beginning...
  - (Keep in mind for future systems...)

Security associations (SAs)

- An SA is a crypto-protected connection
  - One SA in each direction...
  - At each end, the SA contains a key, the identity of the other party, the sequence number, and crypto parameters
  - IPsec header indicates which SA to use
  - Parties will maintain a database of SAs for currently-open connections
  - Used both to send and receive packets

Overview

IPSec = AH + ESP + IKE

- IPSec = Authentication header (AH) + Encapsulating security payload (ESP) + Internet Key Exchange (IKE)
  - AH provides integrity and origin authentication
  - ESP also provides confidentiality
  - IKE sets up keys and algorithms for AH and ESP

AH vs. ESP

- Authentication header (AH)
  - Provides integrity only
  - Encapsulating security payload (ESP)
  - Provides encryption and/or integrity
  - Both provide cryptographic protection of everything beyond the IP headers
  - AH additionally provides integrity protection of some fields of the IP header
Transport vs. tunnel mode

- Transport mode: add IPsec information between IP header and rest of packet
- Most logical when IPsec used end-to-end

| IP header (real dest) | IPsec header | TCP/UDP header + data |

Tunnel mode illustration

More on AH

- AH provides integrity protection on header
- But some fields change *en route*!
- Only immutable fields are included in the integrity check
- Mutable but predictable fields are also included in the integrity check
- E.g., payload length
- The *final* value of the field is used
More on AH vs. ESP

- Recall that ESP provides encryption and/or authentication
- So why do we need AH?
  - AH also protects the IP header
  - Export restrictions
  - Firewalls need some high-level data to be unencrypted
- None of these are compelling...

The future of IPsec?

- In the long run, it seems that AH will become obsolete
- Better to encrypt everything anyway
- No real need for AH
- Certain performance disadvantages
- AH is complex...
  - Etc.
- IPsec is still evolving