Network Layer Security – Structure and Challenges

Steven M. Bellovin
smb@research.att.com
What is Network Layer Security?

- Encrypt (or authenticate) everything above the network layer header.
- Completely transparent to applications.
- TCP- or application-level retransmissions handle deleted or damaged packets.
- Generally must modify protocol stack or kernel; out of reach of application writers or users.
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 per-user keying.
- Works with IPv4 and IPv6.
Authentication Header (AH)

- Uses HMAC algorithm to combine secret key and data via a cryptographic hash function.
- Covers payload and portion of preceding IP header.
- Uses Security Parameter Index (SPI) to identify key, algorithm, etc.
- Optionally provides replay protection.
Encapsulating Security Protocol (ESP)

- Carries encrypted packet.
- Uses SPI.
- Provides confidentiality, authentication and integrity protection, and replay protection.
Key Management

- Dynamically negotiate session key between peers.
- Use digital signature algorithm to sign Diffie-Hellman exchange.
- Many different flavors.
Uses for IPSEC

- Virtual Private Networks (VPNs)
- “Phone home” for laptops, telecommuters
- General Internet security.
Virtual Private Networks

- Extend boundary of physically-secure network.
- Use cryptography to protect links across public Internet.
- Encrypting gateway (often a firewall) protects all traffic into/out of the network.
- Parties must *know* proper IPSEC gateway.
Open Issues

• Gateway discovery.
• API
• Multicast
IPSEC Gateways

• Often manually configured – doesn’t scale.
• DNS-based proposal: KX records, similar to MX records.
• What about complex topologies?
• Pathfinder packets: see who bounces the packet.
  - Do they have the right to? Must be digitally signed by destination.
IPSEC API

• How can an application request cryptographic protection?
• How can an application determine the protection level? The peer’s identity?
• How are different cryptographic strengths indicated?
• How is certificate selection done?
Multicast

• What type of multicast? Broadcast? Private conference?
• How can we do key management? Does it scale?
• Who controls group membership? How? Can the membership change dynamically?
• Do we need to be able to revoke keys?
How Can We Secure the Internet?

• Hard to deploy host-to-host IPSEC.
• When can it be used? When should it be used?
• Is it the right mechanism for general Internet security?