

CS 4803

Computer and Network Security

Alexandra (Sasha) Boldyreva
IPsec

1

Network layers

- Application
- Transport
- Network
- Lower level

2

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

3

Examples

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

4

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.

5

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

6

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...

7

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

8

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...)

9

Overview

IPSec = AH + ESP + IKE

Protection for IP traffic
AH provides integrity and
origin authentication
ESP also confidentiality

Sets up keys and algorithms
for AH and ESP

10

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

11

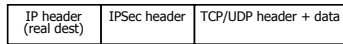
AH vs. ESP

- 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

12

Transport vs. tunnel mode

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



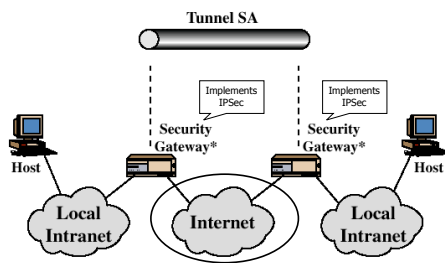
13

Transport vs. tunnel mode

- Tunnel mode: keep original IP packet intact; add new header information
- | | | | |
|------------------------|--------------|--------------------------|-----------------------|
| IP header
(gateway) | IPSec header | IP header
(real dest) | TCP/UDP header + data |
|------------------------|--------------|--------------------------|-----------------------|
- Can be used when IPsec is applied at intermediate point along path (e.g., for firewall-to-firewall traffic)
 - E.g., change source/destination info...
- Results in slightly longer packet

14

Tunnel mode illustration



15

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

16

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...

17

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

18