IP LAYER SECURITY: IPSEC

Internet Protocols

CSC / ECE 573

Fall, 2005

N. C. State University

Announcements

I. Figures for HW5

Today's Lecture

I. Security Basics

II. IPSec

III. Authentication Header (AH)

IV. Encapsulating Security Payload (ESP)

SECURITY BASICS

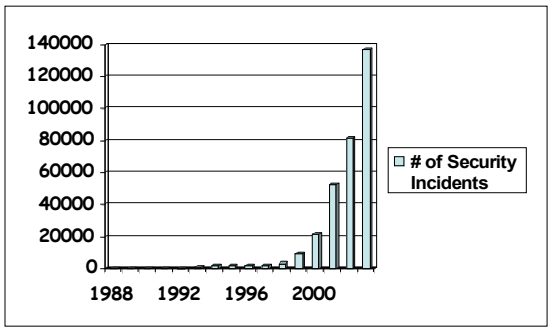
Security Risks

- Why do they attack…?
  - curiosity
  - fun, a challenge
  - financial gain
  - personal (revenge, etc.)
  - political, national
- Targets
  - data
  - infrastructure, operations
  - assets that are accessible electronically

Internet Threats

- Internet protocols were not really designed with security in mind
  - originally: a small community of researchers with a shared mission
- Is "retrofitting" security to TCP/IP protocols viable?
  - some examples: DNSSEC, Secure BGP, …
- In distributed systems, who is reponsible for monitoring, detection, and enforcement?
  - no one entity "owns" or controls the Internet

Internet Under Attack!



Source: http://www.cert.org

Trust (Risk)

- There will always be a need for some servers and communications to be regarded as inherently trustworthy and reliable
- Examples
  - passwords are needed to authenticate individuals, but password server knows all the keys!
  - information provided by a trusted user may turn out to be false
- Goal of security: minimize the amount of trust that is necessary

Where Does Security Belong?

- At…
  - link layer: link encryption
  - network layer: firewalls, IPSec, intrusion detection systems
  - application layer: SSL, authentication protocols
- Advantages / disadvantages of each?

Four Security Goals

- Secrecy of information
- Authentication of identity
- Non-repudiation (of information previously exchanged)
- Message integrity (protection from forgery / modification)

Basic Concepts

- Terminology
  - intruder or attacker
  - ciphers
  - plaintext
  - ciphertext
- Kerchoff's principle: all cryptographic algorithms must be assumed to be public; only keys are secret

Encryption

- Transformation of data from *plaintext* into *ciphertext*
- Strength of encryption
  - casual
  - commercial
  - military
  - "alien"
- Necessary components
  - one or more keys (e.g., password or passphrase)
  - encryption function
  - decryption function

Encryption (cont'd)

- Desired properties
  1. given an encrypted (ciphertext) message, must be difficult to recover the original (plaintext) message
  2. given unencrypted and encrypted versions of a message, must be hard to determine what the key is
- Two types of cryptography
  - secret key
  - public key

IPSEC BASICS

IP Security (IPSEC, RFC2401)

- Encryption and authentication at the IP layer
  - can be used by any higher layer protocol, e.g., TCP, UDP, ICMP, BGP, applications, etc.
- Key management: can be manual or automated
  - Internet Key Exchange (IKE) Protocol (RFC 2409)
  - Internet Security Association and Key Management Protocol (ISAKMP) (RFC2408)
- IPSec protocol supports a choice of cryptographic algorithms that can be used

AH vs. ESP

- Two security protocols
  1. Authentication Header (AH)
  2. Encapsulating Security Payload (ESP)
- AH (authentication) provides authentication and protection from replay attacks for IP datagrams
- ESP (encryption) provides confidentiality for traffic

Security Associations

- *Security association* = a security-enabled uni-directional logical connection
  - two SA's are required for bidirectional communication
- All IP traffic traversing an SA is provided the same security processing
- Each SA is uniquely identified by
  1. Security Parameter Index (SPI)
  2. IP Destination Address
  3. protocol identifier (AH or ESP)

Security Associations (cont'd)

- The *Security Association Database* (SAD) contains parameters associated with each security association
  - sequence number counter
  - anti-replay window
  - lifetime of association
  - keys, cryptographic algorithm, etc.

Security Policies

- Security *policies*: which traffic is processed by which security association
- Traffic mapping
  - selectors (classification patterns) identify traffic types
    - may include "wildcard" entries matching any value
- The *Security Policy Database* (SPD) specifies the policies that apply to all IP traffic from/to a host or security gateway
  - selectors for two entries may overlap (i.e., ambiguous matching)
  - order is important: the first matching entry is selected

Types of Classification Filters

Field	Traffic Value	Possible Filter Values
src addr	single IP addr	single,range,wildcard
dst addr	single IP addr	single,range,wildcard
xpt protocol*	xpt protocol	single,wildcard
src port*	single src port	single,wildcard
dst port*	single dst port	single,wildcard
user ID*	single user ID	single,wildcard
security label	single value	single,wildcard

* entries for these fields could be "OPAQUE" because the traffic value is encrypted

Transport vs. Tunnel Modes

- Each protocol (AH or ESP) supports two modes: transport or tunnel mode
- Transport mode headers
  1. IP header
  2. IPSec header
  3. transport-layer header

Transport vs. Tunnel Modes (cont'd)

- Tunnel mode headers
  - an outer IP header specifies endpoint of the SA
  - IPSec header
  - an inner IP header specifies the ultimate destination for the packet
  - transport layer header
- Steps in tunnel mode processing
  1. Encryption / authentication
  2. Encapsulation
  3. Delivery
  4. Decapsulation
  5. Decryption / verification

Tunnel Mode (cont'd)

- Levels of protection
  - AH: portions of the outer IP header are afforded protection, as well as all of the tunneled IP packet
  - ESP: protection afforded only to the tunneled packet, not to the outer header
- Inner IP header is not changed during transmission, except to decrement the TTL

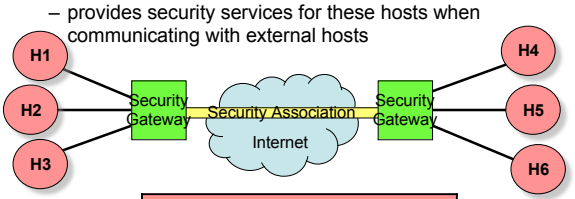
Security Associations Between Hosts

- SA is directly between two hosts
  - either transport mode, or tunnel mode, is allowed

Transport Mode Headers	Tunnel Mode Headers
IP1 + AH	IP2 + AH + IP1
IP1 + ESP	IP2 + ESP + IP1
IP1 + AH + ESP	*(not allowed)*

Security Associations Using Gateways

- A *security gateway* is a device implementing IPSec on behalf of a set of internal hosts
  - provides security services for these hosts when communicating with external hosts



Tunnel Mode Headers
IP2 + AH + IP1
IP2 + ESP + IP1

AUTHENTICATION WITH IPSEC

Authentication Header Protocol (RFC 2402)

- AH provides
  - data origin authentication
  - anti-replay service
  - message integrity
- Provides authentication for as much of the IP header as possible, as well as for higher layer protocol data
  - some IP header fields may change in transit, so cannot be protected by AH
  - called *mutable* fields

AH: Transport Mode

- Before applying AH:

```
-----------------------------
|orig IP hdr  |     |      |
|(any options)| TCP | Data |
-----------------------------
```

- After applying AH:

```
----------------------------------
|orig IP hdr  |     |     |      |
|(any options)| AH  | TCP | Data |
----------------------------------

|<------- authenticated ------->|
except for mutable fields in IP hdr
```


AH: Tunnel Mode

- After applying AH:

```
-------------------------------------------------
|  new IP hdr* |     | orig IP hdr |     |      |
|(+any options)| AH  |(+any options)|TCP | Data |
-------------------------------------------------

|<- authenticated except for mutable fields -->|
|          in the new IP hdr                    |
```


The AH Header

```
                            1             2
0             8             6             4
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Next Header   |  Payload Len  |          RESERVED             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               Security Parameters Index (SPI)                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                   Sequence Number Field                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+               Authentication Data (variable)                  |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

AH Header Fields

- **`Next Header`** identifies the type of the payload after the Authentication Header
- **`Payload Length`** specifies the length of AH in 32-bit words - 2
- **`SPI + destIPaddr + AH`** uniquely identifies the Security Association for this datagram

AH Header Fields (cont'd)

- **`Sequence Number`** is monotonically increasing value
  - for anti-replay purposes, must be present
  - only sequence numbers within a fixed window size *w* of the latest sequence number received are accepted
- **`Authentication Data`**
  - variable-length field (must be multiple of 32 bits)
  - default length is 96 bits
  - Integrity Check Value (ICV) for the packet (i.e., digest)

AH Integrity Check Value (ICV)

- Computed over:
  1. IP header
     - fields that are either immutable, or predictable in value upon arrival
  2. AH header (Authentication Data set to zero) + padding bytes
  3. upper level protocol data (e.g., TCP header, data), which is assumed to be immutable in transit

Which IP Fields Are Protected?

- Immutable
  - Version
  - Internet Header Length
  - Total Length
  - Identification
  - Next Protocol
  - Source Address
  - Destination Address (without source routing)

Which IP Fields are Protected? (cont'd)

- Mutable but predictable
  - Destination Address (with source routing)
- Mutable (zeroed prior to ICV calculation)
  - Type of Service (TOS)
  - Flags
  - Fragment Offset
  - Time to Live (TTL)
  - Header Checksum

Rules Concerning Fragmentation

- Transport mode: AH or ESP applies only to whole IP datagrams (not to IP fragments)
  - prior to performing AH or ESP processing at destination, any IP fragments are reassembled

Fragmentation (cont'd)

- Tunnel mode: AH or ESP applies to IP packets, which may be fragments
- May have to…
  - first reassemble a packet fragmented by the local IP layer
  - then apply IPsec
  - then re-fragment the resulting packet (!)

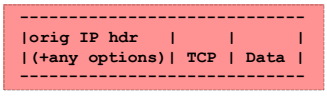
ENCRYPTION WITH IPSEC

IP Encapsulating Security Payload (RFC 2406)

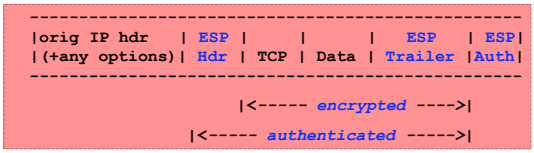
- ESP provides
  - data origin authentication (with authentication)
  - anti-replay service
  - message integrity (with authentication)
  - confidentiality
  - limited traffic analysis confidentiality (via tunnel mode)

ESP: Transport Mode

- Before applying ESP:

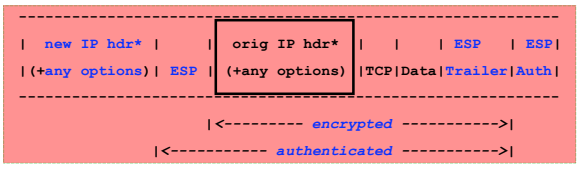


- After applying ESP:

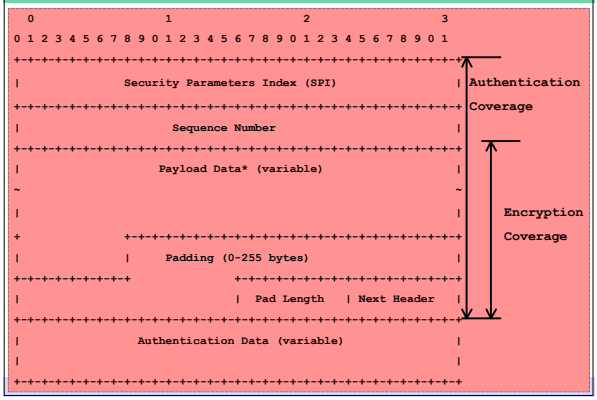


ESP: Tunnel Mode

- ESP does not protect any IP header fields unless tunnel mode is used
- After applying ESP:



ESP Header and Trailer



ESP Header and Trailer Fields

- **`SPI`** uniquely identifies SA (along with destination IP address and ESP)
- **`Sequence Number`**
  - initialized to 0 when SA established
  - no wraparound; must be reset (i.e., establish new SA) prior to transmitting 2^{32}nd packet
- **`Next Header`** identifies the type of data contained in the **`Payload Data`** field
  - how can you find **`Next Header`** and **`Pad Length`** if they come after the **`Payload Data`** and **`Padding`** fields, which are variable length?

ESP Header and Trailer Fields (cont'd)

- **`Payload Data`** = contents of upper layer protocol
- **`Authentication Data`** included only if authentication service has been selected
  - computed over the ESP packet minus the Authentication Data
  - contains ICV
  - variable-length, length is specified by the security association
- **`Padding`** if required by cryptographic algorithm

ESP Packet Encryption

- Encrypts the result using the <key, encryption algorithm, algorithm mode> indicated in the security association
- If authentication is selected...
  - encryption is performed first, before the authentication
  - encryption does not encompass the Authentication Data field

ESP Packet Input Processing

1. Packet reassembly occurs if needed
2. Determine the appropriate SA based on **`Destination IP Address, SPI`**, and protocol (ESP)
3. SA specifies
   - whether to check sequence number
   - whether to expect authentication data
   - what algorithms and keys to use for decryption and authentication

ESP Cryptographic Algorithms

- DES (in CBC mode)
- HMAC with MD5
- HMAC with SHA-1
- NULL Authentication algorithm
- NULL Encryption algorithm
  - authentication and encryption must not both be NULL

Summary

1. IPSec is not perfect, but widely supported and used
2. Provides general encryption and authentication functions for all applications using IP
3. Does not solve the problems of key management and exchange

Next Lecture

- Basic security protocols