

Network Security: IPsec

CS 239

Computer Software

March 2, 2005

CS 239, Winter 2005

Lecture 13
Page 1

IPsec

- Until recently, the IP protocol had no standards for how to apply security
- Encryption and authentication layered on top
 - Or provided through ad hoc extensions
- Increasing security needs mandated a standard method of securing IP traffic

CS 239, Winter 2005

Lecture 13
Page 2

How Was This Handled?

- The usual way that enhancements to standard Internet protocols are handled
 - The RFC/IETF mechanism
- Smart people worked out a proposal
- They published the proposal and requested comments
- Eventually agreement was reached

CS 239, Winter 2005

Lecture 13
Page 3

IP Security RFCs

- RFC 2401 (originally RFC 1825)
 - Security Architecture for the Internet Protocol
- RFC 2402 (originally RFC 1826)
 - IP Authentication Header
- RFC 2406 (originally RFC 1827)
 - IP Encapsulating Security Payload

CS 239, Winter 2005

Lecture 13
Page 4

Other Related RFCs

- RFC 1828 - IP Authentication Using Keyed MD5
- RFC 1829 - The ESP DES-CBC Transform
- RFC 1851 - The ESP Triple DES Transform
- RFC 1852 - IP Authentication Using Keyed SHA
- RFC 2085 - HMAC-MD5 IP Authentication With Replay Prevention
- And many, many others

CS 239, Winter 2005

Lecture 13
Page 5

RFC 2401

- Defined the basics of security for the Internet Protocol
- Briefly, add per-packet encryption and authentication standards
- Basically, two mechanisms
 - A way to authenticate IP packets
 - A way to encrypt IP packets

CS 239, Winter 2005

Lecture 13
Page 6

What Is Covered

- Message integrity
- Message authentication
- Message confidentiality

What Isn't Covered

- Non-repudiation
- Digital signatures
- Key distribution
- Traffic analysis
- Handling of security associations
- Some of these covered in later RFCs and related standards

Some Important Terms for IPsec

- Security Association - "A Security Association (SA) is a simplex "connection" that affords security services to the traffic carried by it.
 - Basically, a secure channel
- SPI (Security Parameters Index) – Combined with destination IP address and IPsec protocol type, uniquely identifies an SA

General Structure of IPsec

- Really designed for end-to-end encryption
 - Though could do link level
- Designed to operate with either IPv4 or IPv6
- Meant to operate with a variety of different encryption protocols
- And to be neutral to key distribution methods

What IPsec Requires

- Protocol standards
 - To allow messages to move securely between nodes
- Supporting mechanisms at hosts running IPsec
 - E.g., a Security Association Database
- Lots of plug-in stuff to do the cryptographic heavy lifting

The Protocol Components

- Pretty simple
- Necessary to interoperate with non-IPsec equipment
- So everything important is inside an individual IP packet's payload
- No inter-message components to protocol
 - Though some security modes enforce inter-message invariants

The Supporting Mechanisms

- Methods of defining security associations
- Databases for keeping track of what's going on with other IPsec nodes
 - To know what processing to apply to outgoing packets
 - To know what processing to apply to incoming packets

CS 239, Winter 2005

Lecture 13
Page 13

Plug-In Mechanisms

- Designed for high degree of generality
- So easy to plug in:
 - Different crypto algorithms
 - Different hashing/signature schemes
 - Different key management mechanisms

CS 239, Winter 2005

Lecture 13
Page 14

Security Associations

- Groups of entities that legitimately are cooperating in use of IPsec for a particular connection
 - Hosts, applications, gateways, etc.
- Uniquely identified by:
 - Destination address
 - IPsec protocol (to be discussed later)
 - Plus a Security Parameter Index
 - Basically a pseudo-random number

CS 239, Winter 2005

Lecture 13
Page 15

Creating Security Associations

- Setting them up properly is a major task in itself
- Not covered in basic IPsec RFCs
 - But heavily studied
- One way
 - Two way traffic requires two Security Associations
- Sometimes, single packet goes through multiple SAs

CS 239, Winter 2005

Lecture 13
Page 16

New IPSEC Protocols

- The RFCs define two new protocols
 - Authentication Header
 - Encapsulating Security Payload
- Part of the identification of an SA
- These in turn require special headers
- Can be used together

CS 239, Winter 2005

Lecture 13
Page 17

Authentication Header Protocol

- AH
- Provides integrity and authentication
 - Not confidentiality
- The associated header is calculated on payload plus most IP header fields
 - Except those that change in transit
 - So both data and headers are authenticated

CS 239, Winter 2005

Lecture 13
Page 18

Authentication and Backwards Compatibility

- The authentication header is carried in the packet payload
- Non-participating routers can ignore it
- Participating routers know its payload location and can extract and check it as necessary

CS 239, Winter 2005

Lecture 13
Page 19

What's In the Authentication Header?

<i>8 bits</i>	<i>8 bits</i>	<i>16 bits</i>
Next Header	Length	RESERVED
Security Parameters Index		
Sequence Number Field		
Authentication Data (variable number of 32-bit words)		

CS 239, Winter 2005

Lecture 13
Page 20

Authentication Header Fields

- **Next header** identifies the next header in the packet
 - Might be unrelated to IPsec
- **Length** is length of this header's Authentication Data in words (minus two)
- **Reserved** is, well, reserved
- **SPI** identifies the Security Association
- **Sequence Number Field** – monotonically increasing counter value (for each SA)
- **Authentication data** is the actual "signature"

CS 239, Winter 2005

Lecture 13
Page 21

Creating the AH

- Sending site increments per-SA counter and inserts into packet
- Then computes hash
 - Using algorithm specified for SA
 - Based on packet payload, AH header fields, and unchanging or predictable IP header fields

CS 239, Winter 2005

Lecture 13
Page 22

Using the AH

- At receiving site, based on SA, extract AH from packet
- Check that sequence number is higher
 - Optional at this end
- Compute hash on same fields as sender did
- Check if sent hash matches locally computed hash

CS 239, Winter 2005

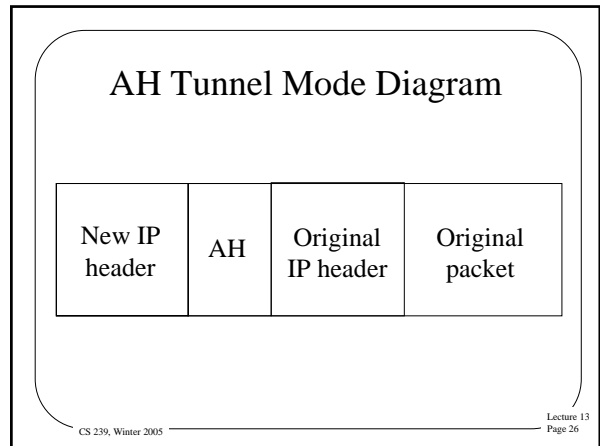
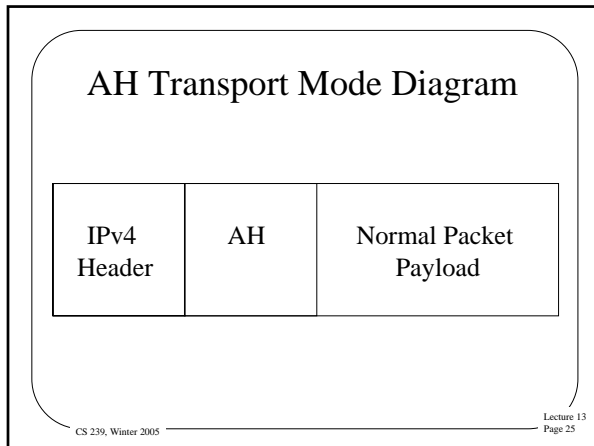
Lecture 13
Page 23

Different AH Modes

- Transport mode
 - Slip the AH between IP header and transport header
- Tunnel mode
 - Put AH in front of entire packet
 - Put new IP header in front of AH

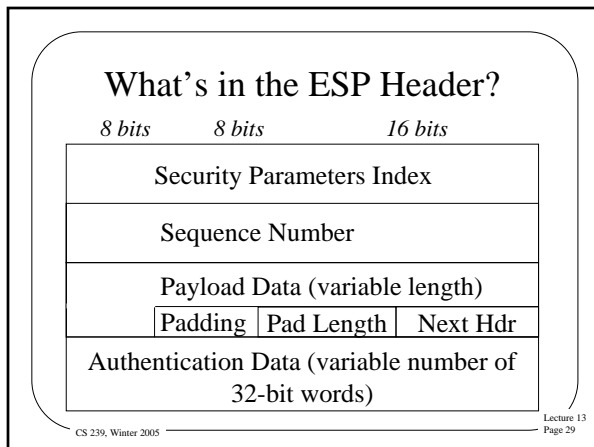
CS 239, Winter 2005

Lecture 13
Page 24

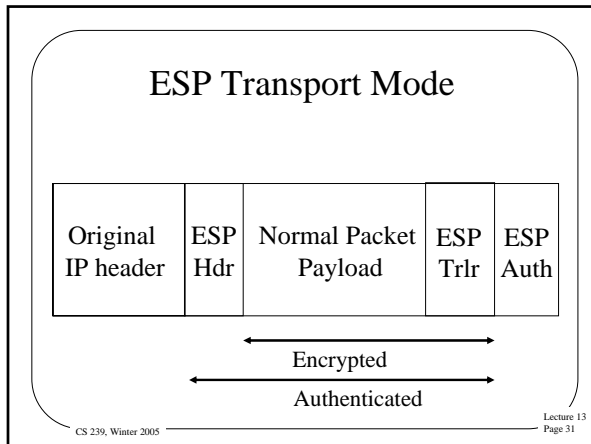


- ### Encapsulating Security Payload (ESP) Protocol
- Encrypt the data and place it within the ESP
 - The ESP has normal IP headers
 - Can be used to encrypt just the payload of the packet
 - Or the entire IP packet
- Lecture 13
Page 27

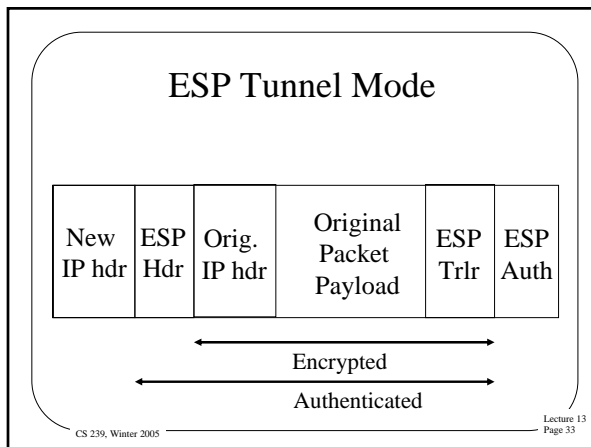
- ### ESP Modes
- Transport mode
 - Encrypt just the transport-level data in the original packet
 - No IP headers encrypted
 - Tunnel mode
 - Original IP datagram is encrypted and placed in ESP
 - Unencrypted headers wrapped around ESP
- Lecture 13
Page 28



- ### ESP in Transport Mode
- Extract the transport-layer frame
 - E.g., TCP, UDP, etc.
 - Encapsulate it in an ESP
 - Encrypt it
 - The encrypted data is now the last payload of a cleartext IP datagram
- Lecture 13
Page 30



- ### Using ESP in Tunnel Mode
- Encrypt the IP datagram
 - The entire datagram
 - Encapsulate it in a cleartext IP datagram
 - Routers not understanding IPsec can still handle it
 - Receiver reverses the process
- Lecture 13
Page 32



- ### Uses and Implications of Tunnel Mode
- Typically used when there are security gateways between sender and receiver
 - And/or sender and receiver don't speak IPsec
 - Outer header shows security gateway identities
 - Not identities of real parties
 - Can thus be used to hide some traffic patterns
- Lecture 13
Page 34

- ### What's the Status of IPsec?
- The standard is done
 - Widely implemented and used
 - Supported in Windows 2000 and XP
 - In Linux 2.6 kernel
 - The architecture doesn't require everyone to use it
 - Generally considered to be a successful extension to IP
- Lecture 13
Page 35

- ### What More Is Needed?
- Key distribution
 - E.g., IKE
 - Security association handling
 - Also dealt with by IKE
 - Implementations of IPsec and IKE are freely available
 - More work on broadcast/multicast use
- Lecture 13
Page 36

IPsec and the AES Ciphers

- RFC 3602 on using AES in IPsec still listed as “proposed”
 - Actually only covers CBC mode
 - But much of content is relevant to any AES mode
- Further drafts looking at different modes/aspects of AES
- Expected that AES will become default for ESP in IPsec