A Brief Review of AH and ES

Steve Kent, BBN

39th IETF Meeting

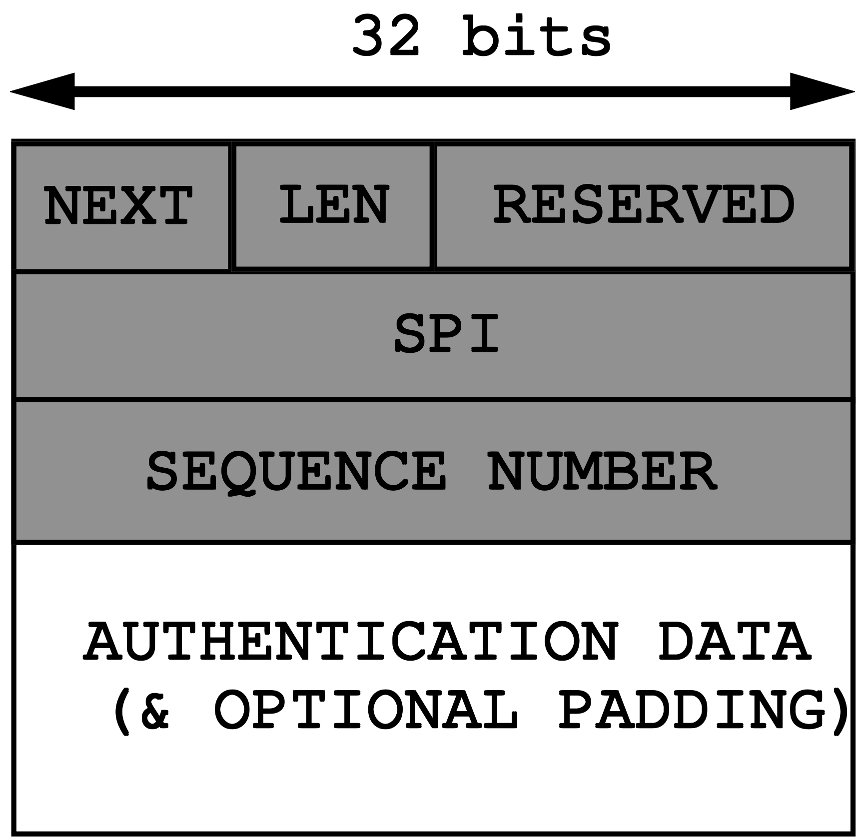
Munich, Germany

August 15, 1997

AH & ESP Status

- A few minor edits required, based on feedback weeks, e.g., AH positioning relative to desti IPv6 header
- Keep default algorithm references in ESP and another document?
- Resolution of default IV choice for DES CBC i default algorithm discussion inline)
- **Note: linkage to Architecture Document requir publication of all three, plus algorithm spec**

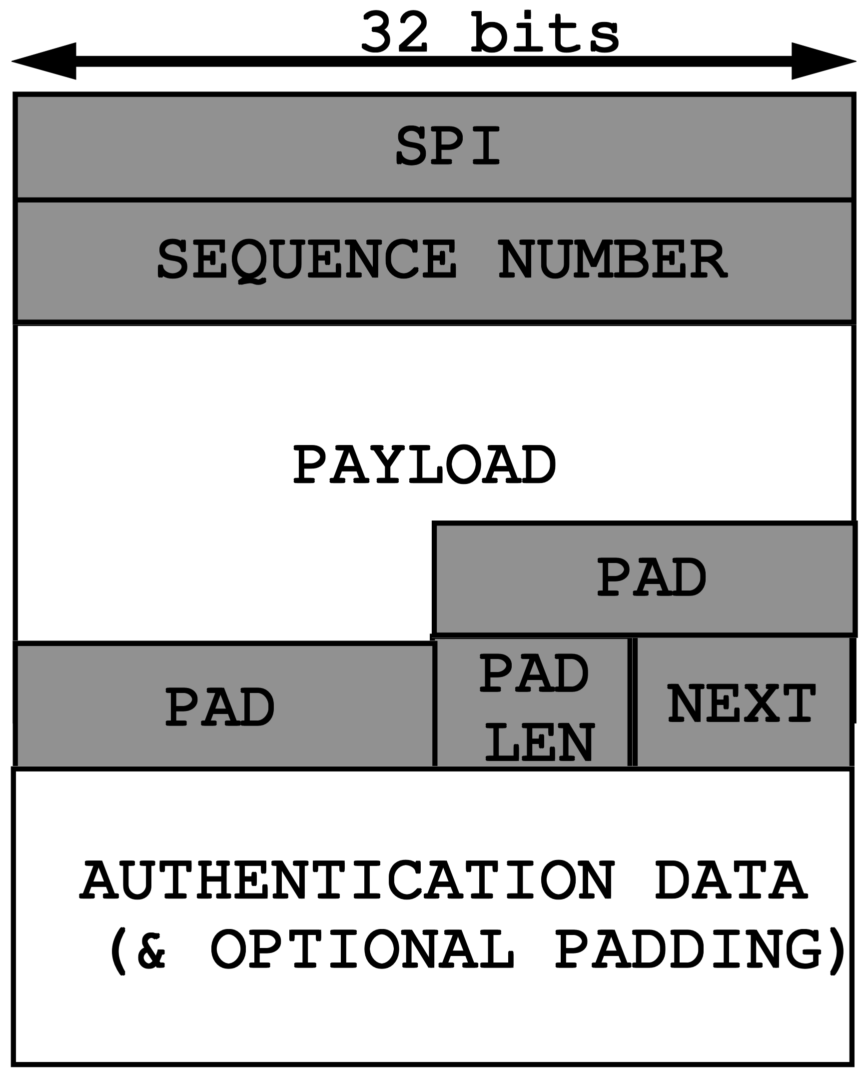
AH Format


32 bits
NEXT
LEN
RESERVED
SPI
SEQUENCE NUMBER
AUTHENTICATION DATA
(& OPTIONAL PADDING)

AH Format Features

- NEXT is the 8-bit next protocol field from I
- LENGTH is the length of this header in 32-bit
- SPI is a 32-bit field identifying this security
- SEQUENCE NUMBER is a 32-bit counter used to de reject replayed packets
- RESERVED is a 16-bit field, currently all zero
- AUTHENTICATION DATA contains the value compute authentication algorithm, padded to an integra bits

ESP Format


32 bits
SPI
SEQUENCE NUMBER
PAYLOAD
PAD
PAD
PAD LEN
NEXT
AUTHENTICATION DATA
(& OPTIONAL PADDING)

ESP Format Features

- SPI identifies the security association
- SEQUENCE NUMBER is a 32-bit counter used to de
  reject replayed packets
- PAYLOAD is the subscriber data protected by E
  an IV if required
- PAD is a field used to extend the plaintext pa
  length equal to 6 mod 8 (to meet IPv6 alignmen
- PAD LEN indicates the pad length, in bytes (0-
- NEXT identifies the protocol encapsulated by E
- AUTHENTICATION DATA contains the value compute
  authentication algorithm, padded to an integra

AH & ESP Default Algorithms

- HMAC with MD5 or SHA-1 for integrity and authe
- DES-CBC for confidentiality
- Anti-replay sequence nuber receive window size
  - recommended size is 64
  - minimum of 32 required
  - larger sizes optional, in multiples of 32