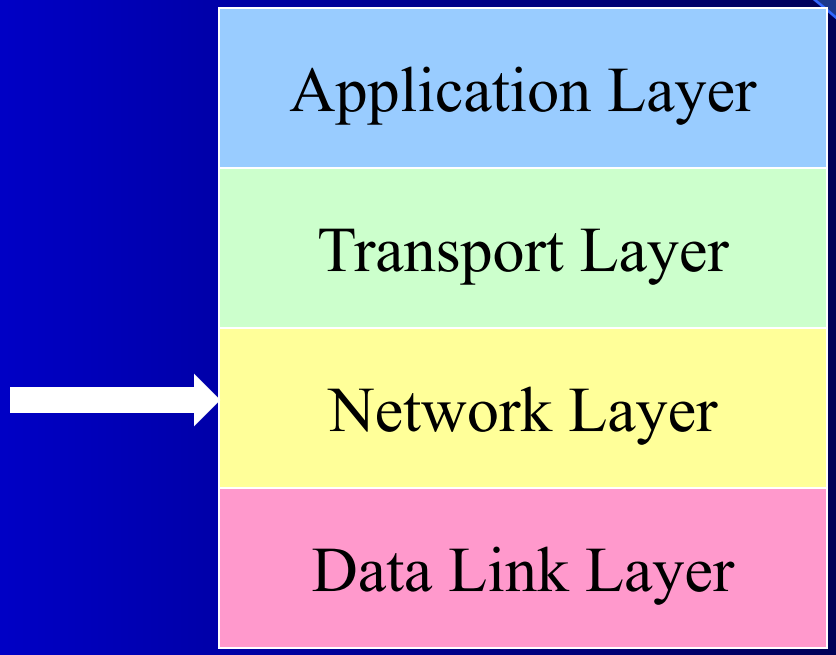
Internet Security
CSCE 813

IPsec

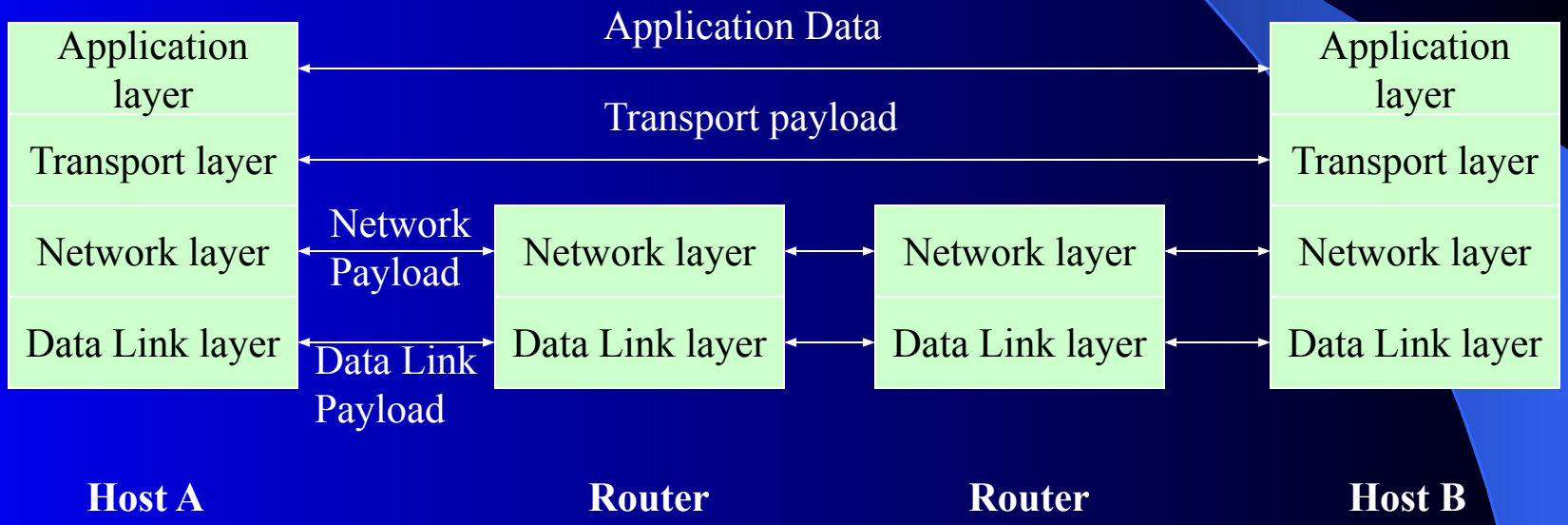
TCP/IP Protocol Stack



Network Layer

- Provides connectionless service
- Routing (routers): determine the path a path has to traverse to reach its destination
- Defines addressing mechanism
  - Hosts should conform to the addressing mechanism

Communication Between Layers



Network Layer and Security

In most network architecture and corresponding communication protocol stack: *network layer protocol data units are transmitted in the clear*:

- Easy to inspect the data content
- Easy to forge source or destination address
- Easy to modify content
- Easy to replay data

Need network layer security protocol

Network Layer Protocols

Several protocols have been proposed:

- *Security Protocol 3 (SP3):* U.S. NSA and NIST as part of the secure data network system (SDNS)
- *Network Layer Security Protocol (NLSP):* ISO for Connectionless Network Protocol (CLNP)
- *Integrated NLSP (I-NLSP):* NIST, for both IP and CLNP
- *swIPe:* John Ioannidis and Matt Blaze at Berkley Univ. Used in Unix environment

Internet Engineering Task Force Standardization

- IPv6 development requirements: Strong security features
  - Security features algorithm-independent
  - Must enforce wide variety of security policies
  - Avoid adverse impact on Internet users who do not need security
- 1992: IPSEC WG (IETF)
  - Define security architecture
  - Standardize IP Security Protocol and Internet Key Management Protocol
- **1998: revised version of IP Security Architecture**
  - *IPsec protocols* (two sub-protocols AH and ESP)
  - *Internet Key Exchange* (IKE)

IPsec

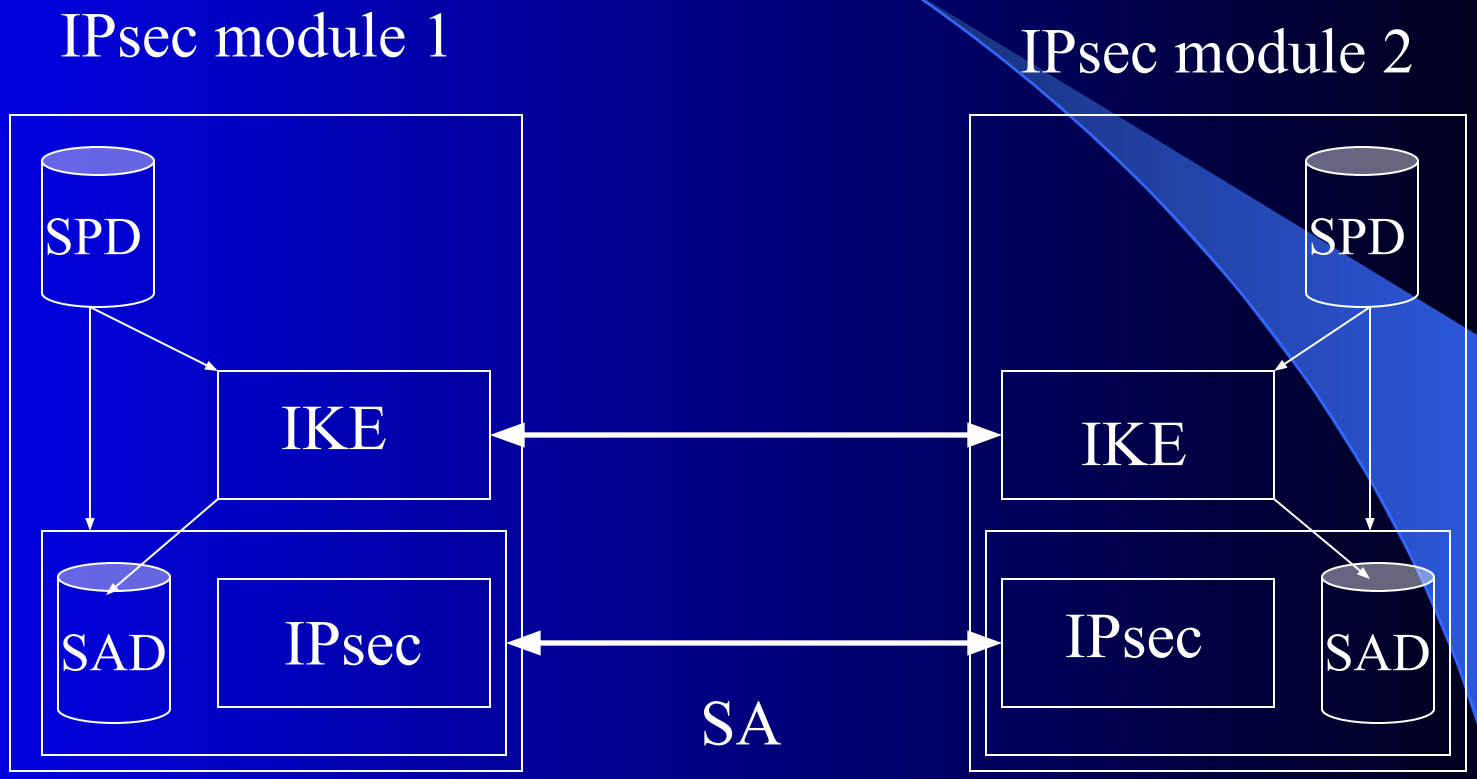
- Provides security for IP and upper layer protocols
- Suit of algorithms:
  - Mandatory-to-implement
  - Assures interoperability
  - Easy to add new algorithms

IP Security Overview

IPSec: method of protecting IP datagrams

- Data origin authentication
- Connectionless data integrity authentication
- Data content confidentiality
- Anti-replay protection
- Limited traffic flow confidentiality

IP Security Architecture



Security Association

- Associates security services and keys with the traffic to be protected
  - Identified by Security Parameter Index (SPI) retrieve correct SA parameters from Security Association Database (SAD)
  - Ipsec protocol identifier
  - Destination address (direction)
- Simplex connection need to establish two SAs for secure bidirectional communication

Security Association

- Defines *security services* and *mechanisms* between two end points (or IPsec modules):
  - Hosts
  - Network security gateways (e.g., routers, application gateways)
  - Hosts and security gateways
- Security service, parameters, mode of operation, and initialization vector
  - e.g., Confidentiality using ESP with DES in CBC mode with IV initialization vector

Security Association

- May use either Authentication Header (AH) or Encapsulating Security Payload (ESP) but not both if both AH and ESP are applied, need two SAs
- Bundle: set of SAs through which traffic must be processed

SA -- Lifetime

- Amount of traffic protected by a key and time frame the same key is used
  - Manual creation: no lifetime
  - Dynamic creation: may have a lifetime

SA -- Security Granularity

User (SSO) specified

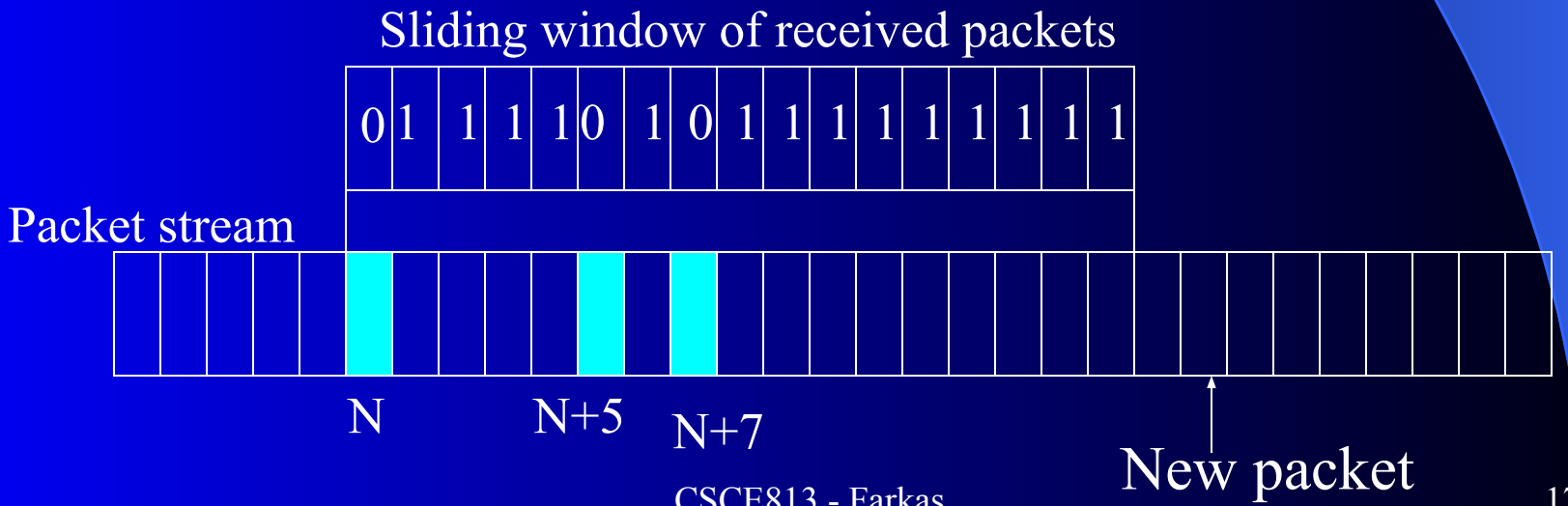
- Host-oriented keying
  - All users on one host share the same session key
  - Not recommended!
- User-oriented keying
  - Each user on one host have one or of more unique session keys
- Session-unique keying
  - Single session key is assigned to a give IP address, upper-layer protocol, and port number

Security Policy Database (SPD)

- Defines:
  - What traffic to be protected
  - How to protect
  - With whom the protection is shared
- For each packet entering or leaving an IPsec implementation SPD is used to determine security mechanism to be applied
- Actions:
  - Discard: do not let packet in or out
  - Bypass: do not apply or expect security services
  - Protect: apply/expect security services on packets

Anti-replay Protection

- Not explicitly part of the architecture
- Protection by sequence number (32-bits) and sliding receive window (64-bits)
- When SA is created: sequence number is initiated to zero
- Prior to IPsec output processing: sequence number is incremented



IPSec

- Protection for IP and upper layer protocols
- IPSec protocols
  - *Encapsulating Security Payload (ESP)*
    - Proof of data origin, data integrity, anti-replay protection
    - Data confidentiality and limited traffic flow confidentiality
  - *Authentication Header (AH)*
    - Proof of data origin, data integrity, anti-replay protection

IPsec

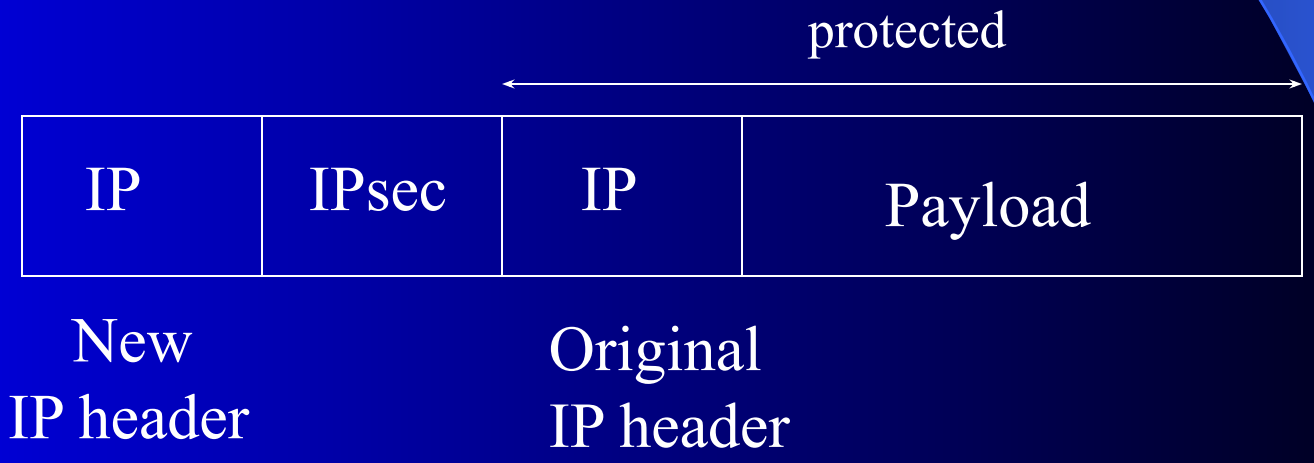
- Security provided by ESP or AH is dependent on the cryptographic algorithms applied to them
- Default encryption algorithm: DES CBC
  - Not suited for highly sensitive data or
  - For data that must remain secure for extended period of time
- Authentication and/or confidentiality requires shared keys
- Manual key addition is supported but scales poorly
- Internet Key Exchange (IKE): key management protocol

AH and ESP

- Transport mode: protect upper layer protocols
  - IPSec header is inserted between the IP header and the upper-layer protocol header
  - Communication endpoints must be cryptographic endpoints

AH and ESP

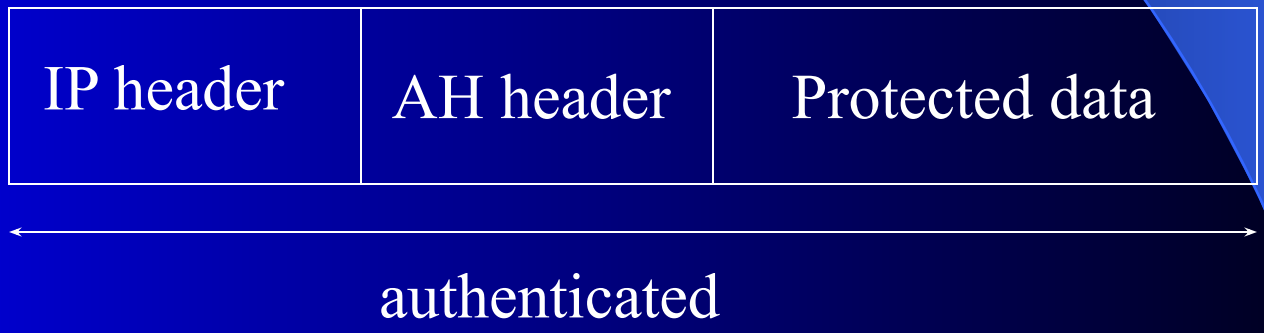
- Tunnel mode: protect entire IP datagram
  - Entire IP packet to be protected is encapsulated in another IP datagram and an IPsec header is inserted between the outer and inner IP headers



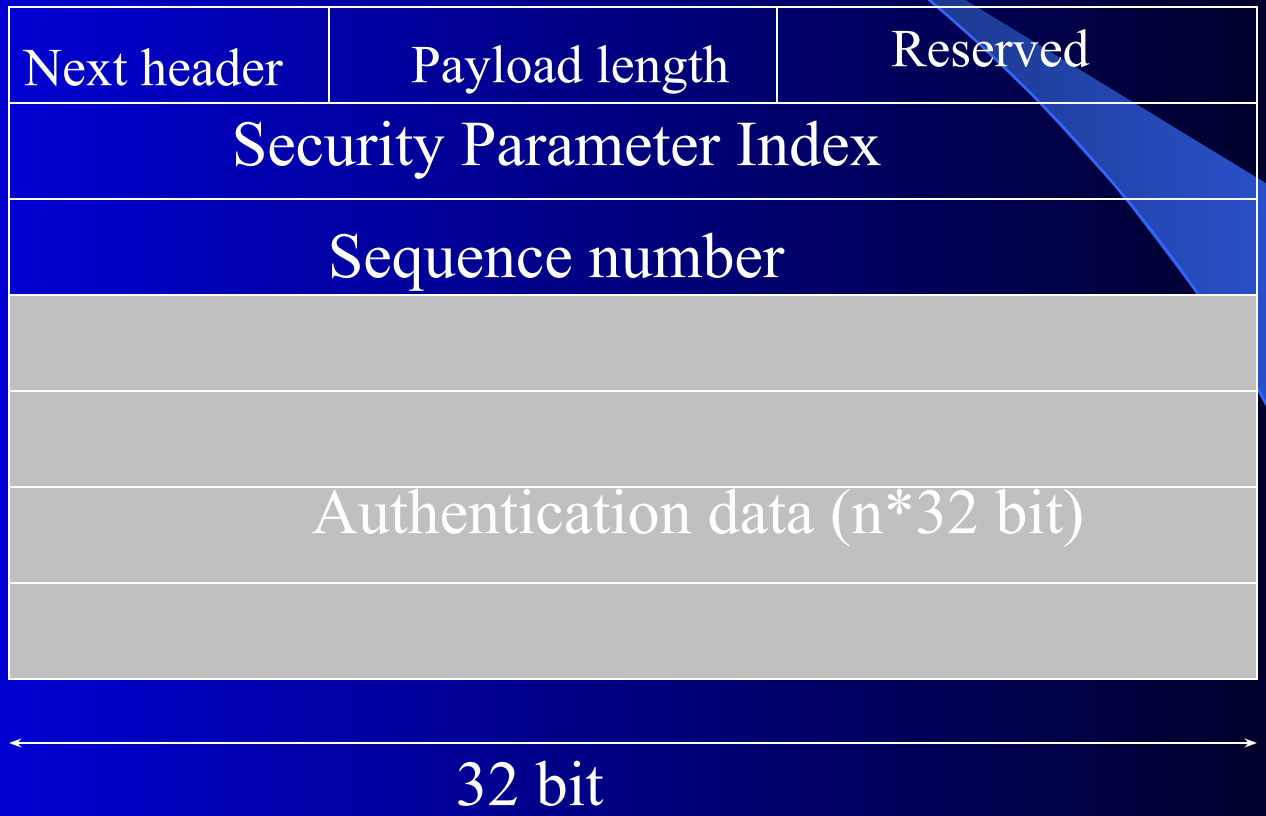
Authentication Header (AH)

- Does NOT provide confidentiality
- Provides:
  - Data origin authentication
  - Connectionless data integrity
- May provide:
  - Non-repudiation (depends on cryptographic alg.)
  - Anti-replay protection
- Precision of authentication: granularity of SA
- Protocol number: 51

AH Protected IP packet



AH Header


Next header
Payload length
Reserved
Security Parameter Index
Sequence number
Authentication data (n*32 bit)
32 bit

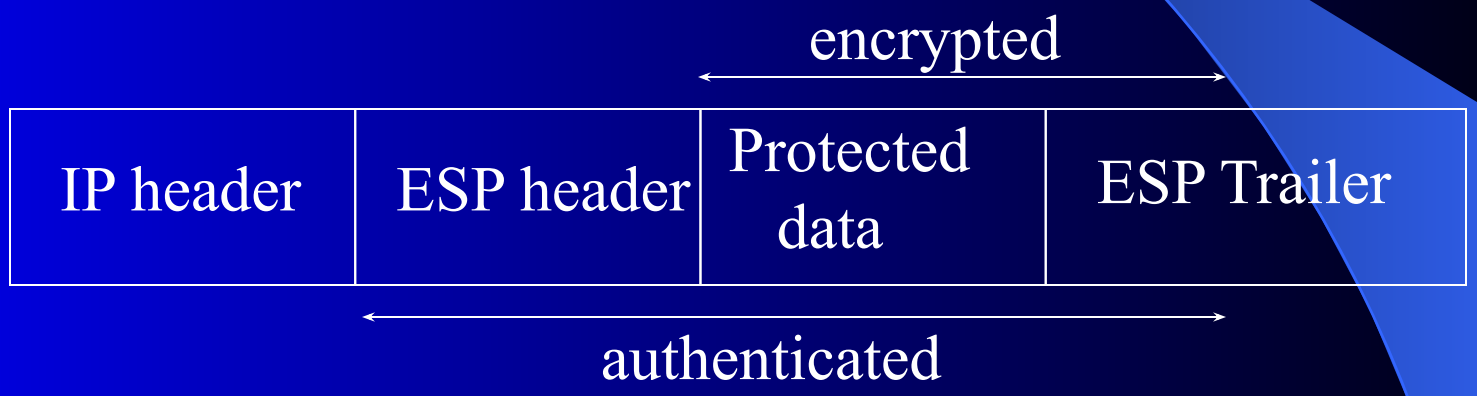
Authentication Data

- Computed by using
  - authentication algorithm (MD5, SHA-1)
  - cryptographic key (secret key)
- Sender: computes authentication data
- Recipient: verifies data

Encapsulating Security Payload (ESP)

- Provides:
  - Confidentiality
  - Authentication (not as strong as AH: IP headers below ESP are not protected)
  - Limited traffic flow confidentiality
  - Anti-replay protection
- Protocol number: 50

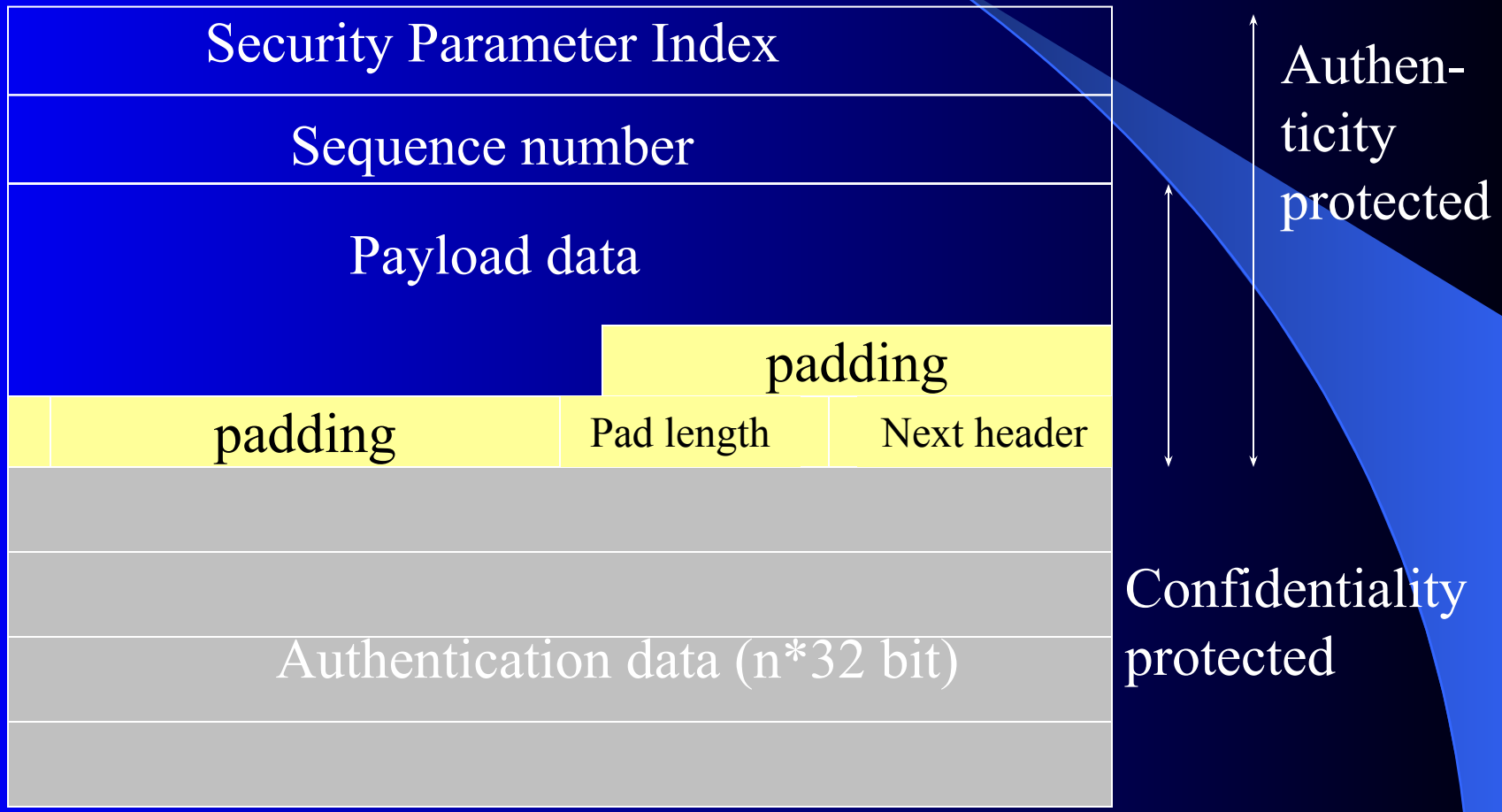
ESP Protected IP packet



ESP header and trailer

- ESP packet processing:
  1. Verify sequence number
  2. Verify integrity
  3. Decrypt
- ESP header: not encrypted
  - Contains: SPI and sequence number
- ESP trailer: partially encrypted
  - Contains: padding, length of padding, next protocol, authentication data

ESP Format


Security Parameter Index
Sequence number
Payload data
padding
padding
Pad length
Next header
Authentication data (n*32 bit)
Authen-
ticity
protected
Confidentiality
protected

ESP

- SA has multiple algorithms defined:
  - Cipher: for confidentiality
  - Authenticator: for authenticity
  - Each ESP has at most:
    - one cipher and one authenticator or
    - one cipher and zero authenticator or
    - zero cipher and one authenticator or
    - Disallowed: zero cipher and zero authenticator or

Encryption

- Block ciphers in Cipher Block Chain (CBC) mode
- Need
  - Padding at the end of data
  - Initialization vector (IV) – contained in the packet

Encryption and Compression

- Interdependence between encryption and compression
  - When encryption is applied at Internet layer prevents effective compression by lower protocol layers
  - IPsec: does not provide data compression

Key Management Protocols

- IP security architecture supports manual and automated SA and key agreement
- Key management protocol: e.g., IKE
- Proposals for automated key management protocol