IPSEC CONT
Lecture 20

COMPSCI 726
Network Defence and Countermeasures

Nalin Asanka Gamagedara Arachchilage

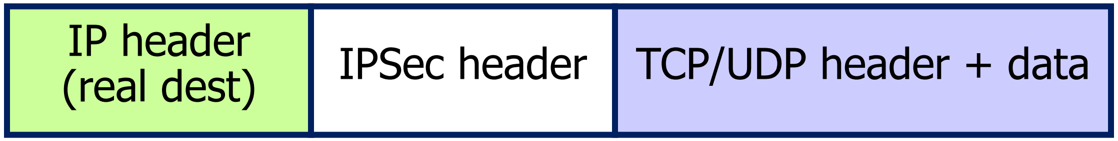
Slides from Muhammad **Rizwan** Asghar

September 15, 2021

Source of some slides: **University of Tennessee** / **Cryptography and Network Security by Behrouz Forouzan**

TRANSPORT VS. TUNNEL MODE

- Transport mode secures packet payload and leaves IP header unchanged

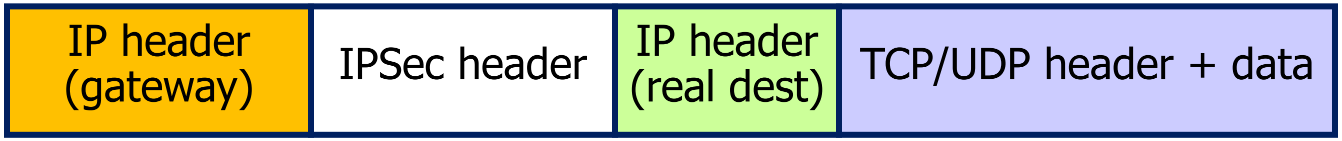


IP header (real dest)

IPSec header

TCP/UDP header + data

- Tunnel mode encapsulates both IP header and payload into IPSec packets



IP header (gateway)

IPSec header

IP header (real dest)

TCP/UDP header + data

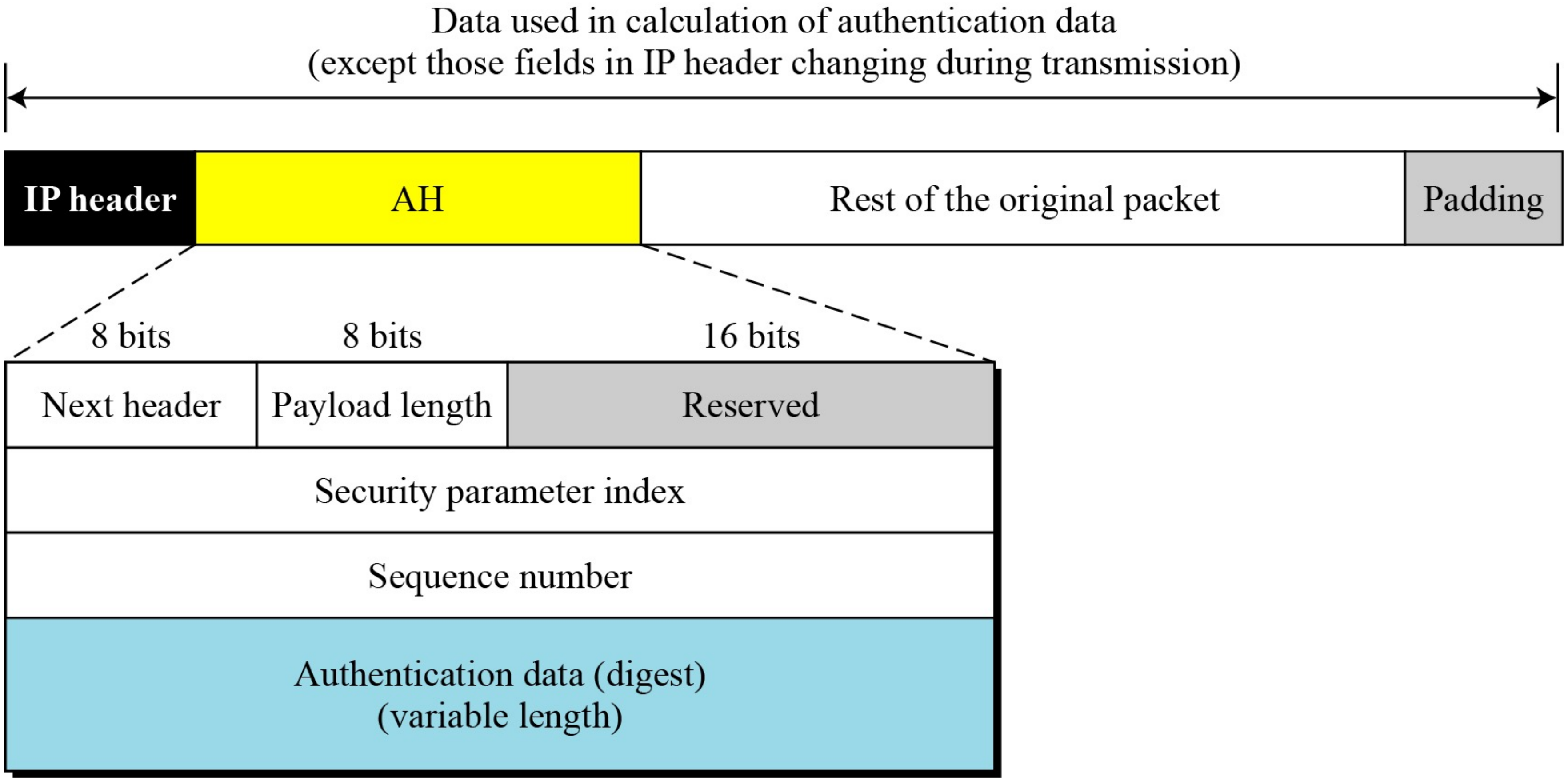
IPSEC BASE PROTOCOLS

- Authentication Header (AH)
  - Authentication
  - Access control
  - Protection against replay attacks
  - Integrity
  - Non-repudiation (depends on algorithm)
- Encapsulating Security Payload (ESP)
  - **Confidentiality**
  - Access control
  - Protection against replay attacks
  - Authentication (depends on algorithm)
  - Integrity (depends on algorithm)
  - Non-repudiation (depends on algorithm)

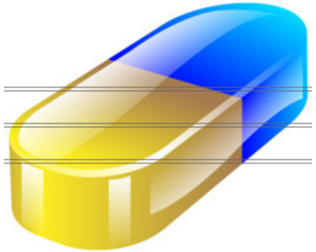
IPSEC BASE PROTOCOLS: AH

- Adds extra field to traditional IP packet
- Provides message authentication and integrity check of IP data payload, but not confidentiality
- Also provides authentication for as much of the IP header as possible
- Sequence number: starts at 1, never recycle (optional)
- Why do we have an authentication-only protocol (AH)?
  - May be used where export/import/use of encryption is restricted
  - Faster implementation

IPSEC BASE PROTOCOLS: AH

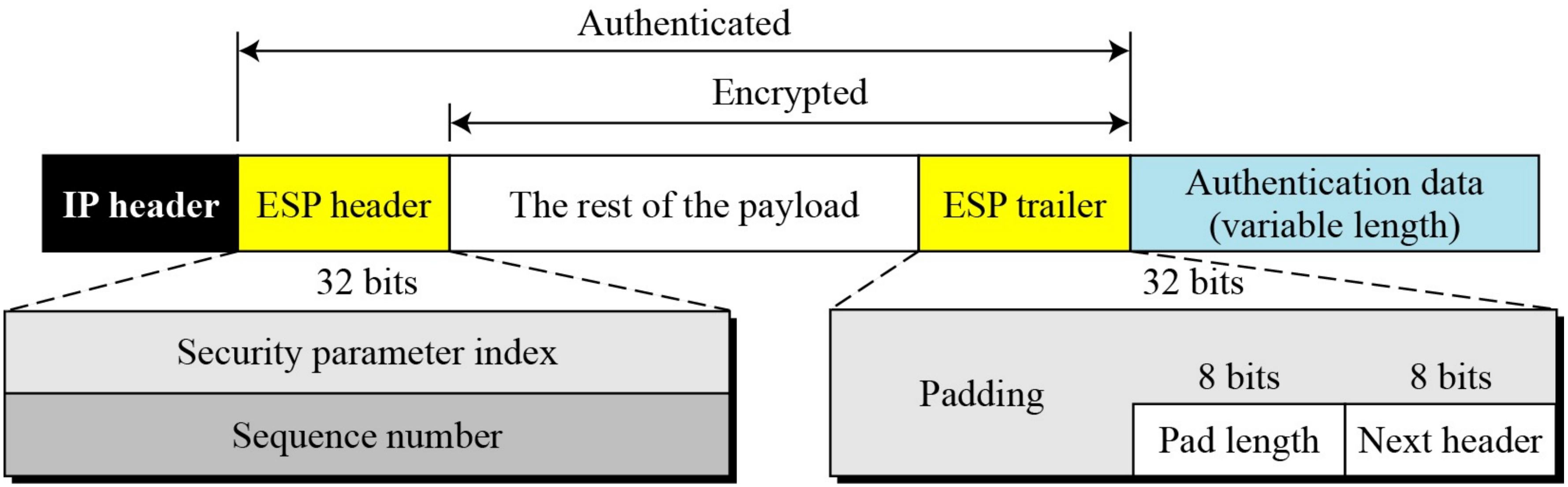

Data used in calculation of authentication data
(except those fields in IP header changing during transmission)
IP header
AH
Rest of the original packet
Padding
8 bits
8 bits
16 bits
Next header
Payload length
Reserved
Security parameter index
Sequence number
Authentication data (digest)
(variable length)

IPSEC BASE PROTOCOLS: ESP



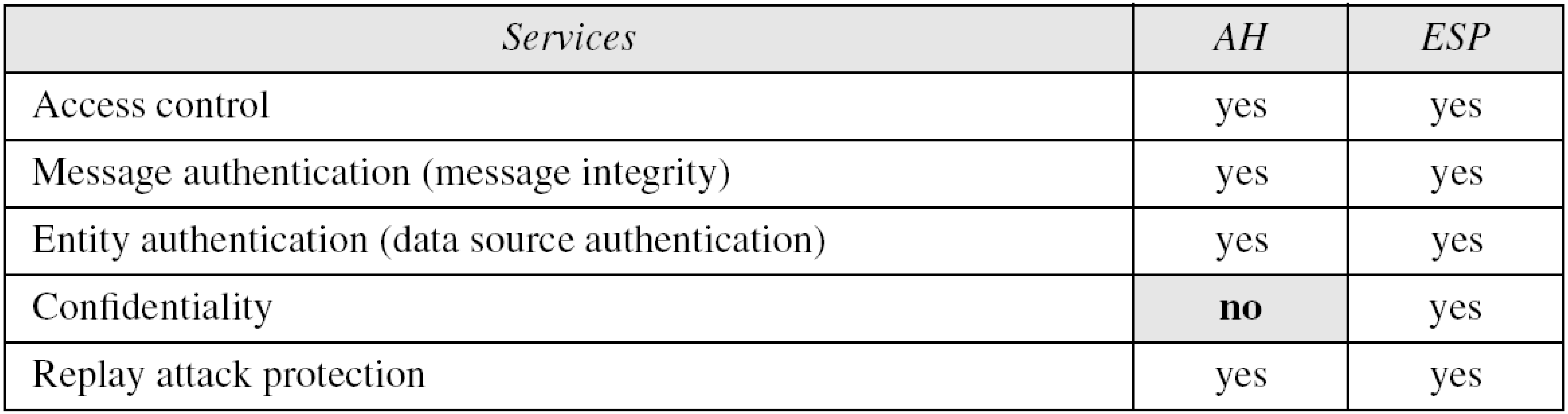
- ESP provides source authentication, data integrity and confidentiality
- Content of IP packet is encrypted and encapsulated between header and trailer fields
- Authentication data optionally added
- Either encryption or authentication (or both) must be enabled
- The authentication trailer must be omitted if not used

IPSEC BASE PROTOCOLS: ESP



AH VS. ESP

- The ESP protocol was designed after the AH protocol was already in use
- ESP does whatever AH does with additional functionality (confidentiality)



Services	*AH*	*ESP*
Access control	yes	yes
Message authentication (message integrity)	yes	yes
Entity authentication (data source authentication)	yes	yes
Confidentiality	**no**	yes
Replay attack protection	yes	yes

RELATIONSHIP BETWEEN IPSEC MODES AND BASE PROTOCOLS

	Transport mode	**Tunnel mode**
AH	Authenticates IP payload and selected portions of IP header	Authenticates entire inner IP packet plus selected portions of outer IP header
ESP	Encrypts IP payload	Encrypts inner IP packet
ESP with Authentication	Encrypts IP payload and authenticates IP payload but not IP header	Encrypts and authenticates inner IP packet

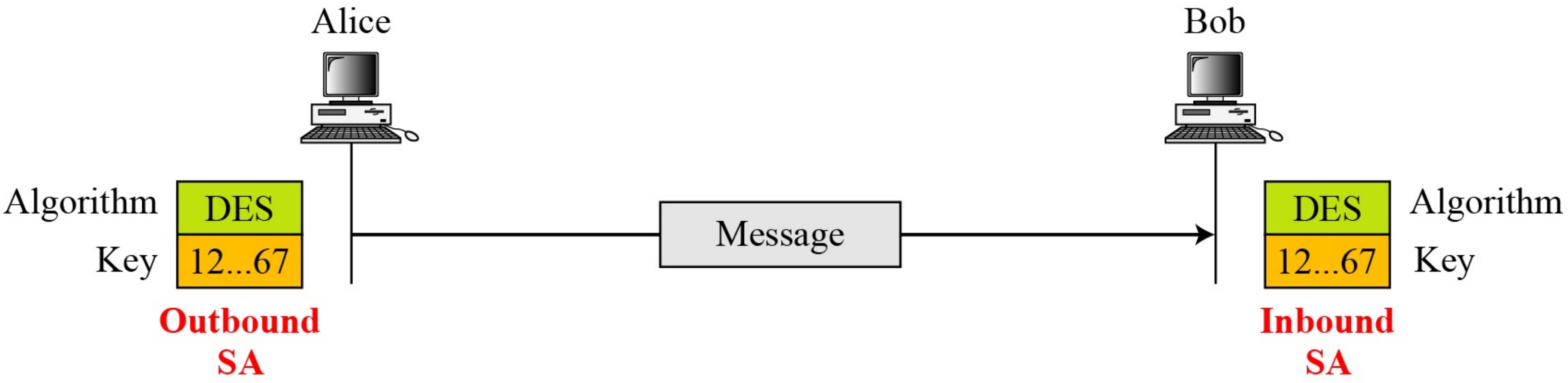
SECURITY ASSOICATION (SA)

- In order to communicate, each pair of hosts must set up SA with each other

- Acts as virtual connection for which various parameters are set:
  - Type of protection
  - Algorithms
  - Keys
  - …

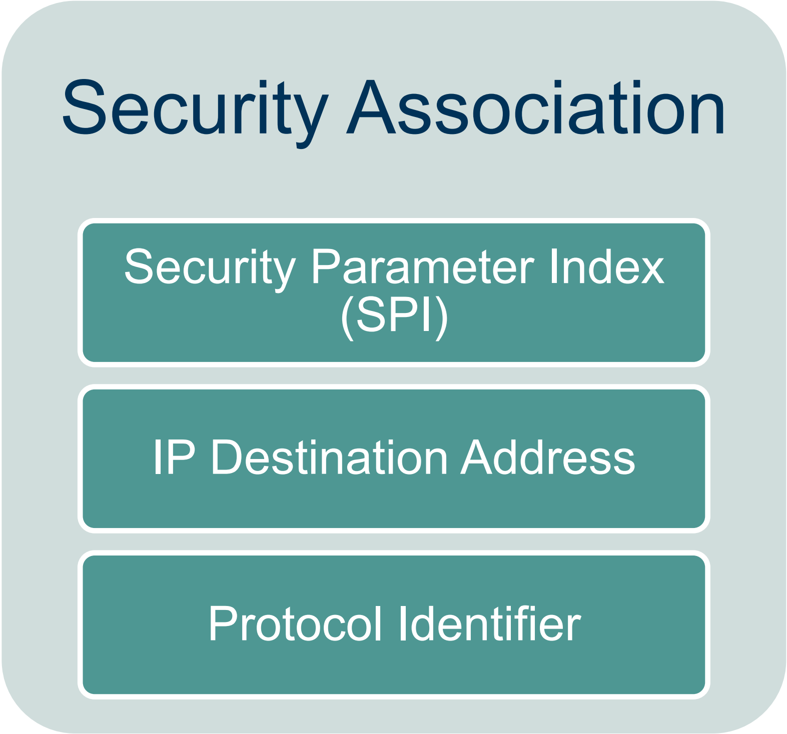
SECURITY ASSOICATION (SA)

- It contains all the security parameters needed for one way communication
- For two-way communications, at least two SAs are needed



AN SA IS UNIQUELY IDENTIFIED BY

- 32-bit string assigned to this SA (local meaning only)
- May be end-user system, or firewall or router
- AH or ESP



Security Association

Security Parameter Index (SPI)

IP Destination Address

Protocol Identifier

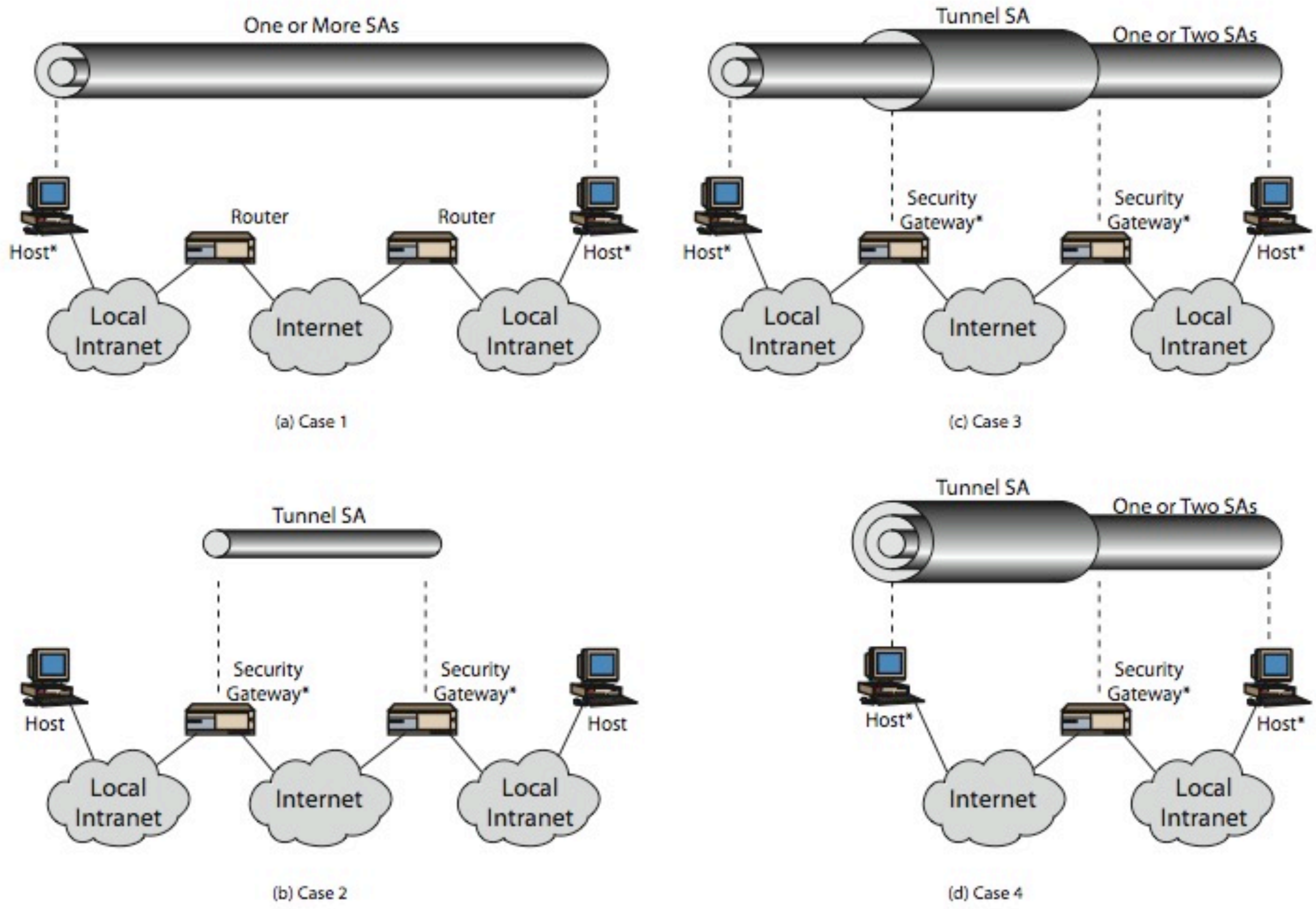
INETERNET KEY EXCHANGE (IKE)

- Generation and distribution of secret keys
- A protocol designed to create both inbound and outbound SAs
- Manual
  - Sysadmin configures keys (does not scale well)
- Automated key management
  - IKE components
    - Internet Security Association and Key Management Protocol (ISAKMP)
    - Oakley
    - SKEME

COMBINING SECURITY ASSOCIATIONS

- SAs can implement either AH or ESP
- To implement both, need to combine SAs
- There are four cases (see next slide)
  - Case 1: host-to-host
  - Case 2: gateway-to-gateway
  - Case 3: pass-through-IPSec
  - Case 4: remote access

COMBINING SECURITY ASSOCIATIONS



(a) Case 1

(c) Case 3

(b) Case 2

(d) Case 4

* Implements IPSec

RESOURCES

- Read Chapter 8 of
  Network Security Essentials – Applications and Standards
  Fourth Edition
  William Stallings
  Prentice Hall
  ISBN 0-13-706792-5

Questions?

Thanks for your attention!