IP Security

Professor Yeali S. Sun

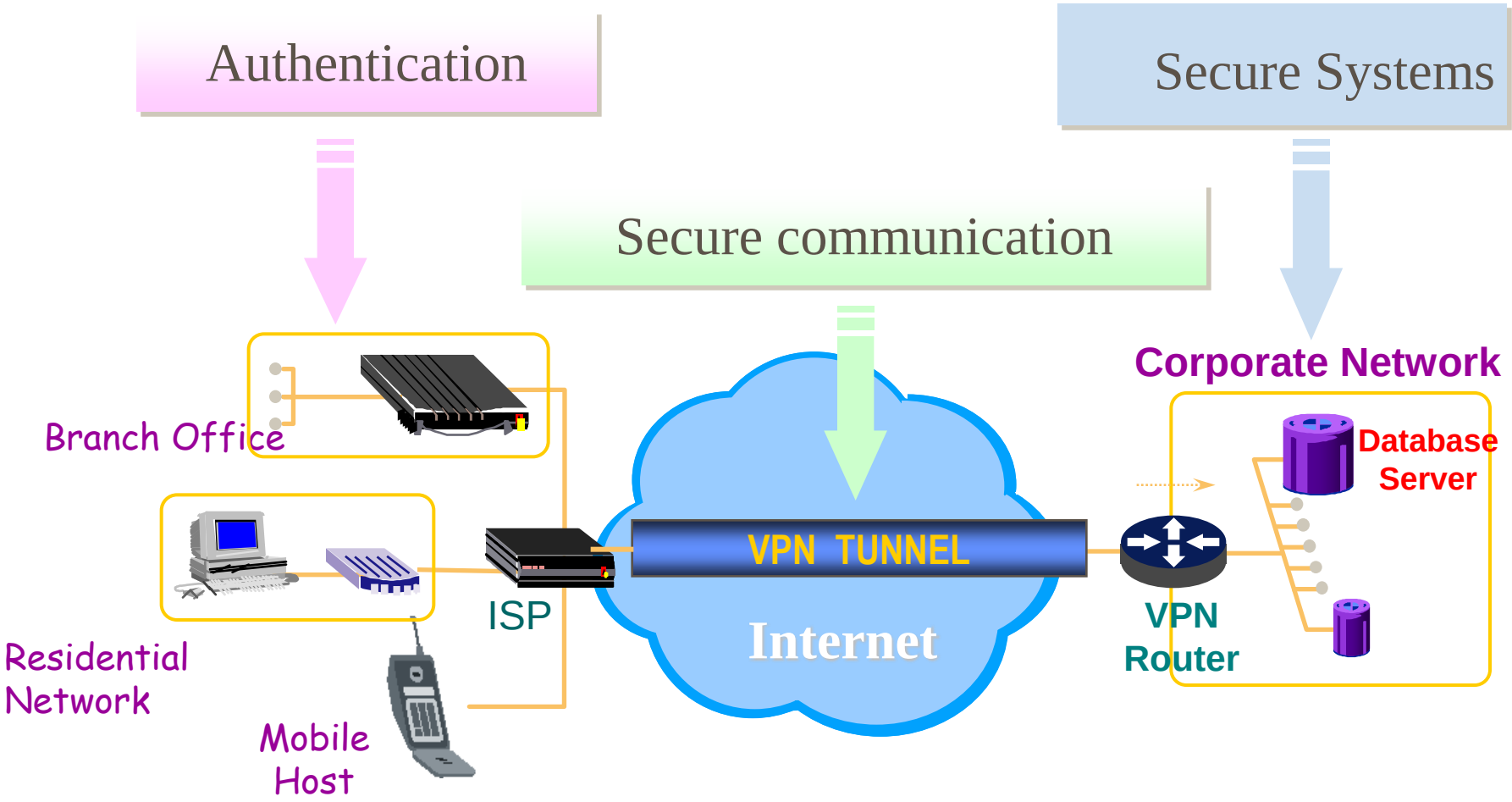
Information Management Department

National Taiwan University

Outline

- Introduction
- IP Security Architecture
- Security Association (SA)
- Security Protocols
  - Operation Modes – Transport, Tunnel
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)
- Internet Key Management (IKE)
  - Oakley key exchange protocol
  - ISAKMP key management protocol

IPSec - Introduction



Network Security - Authentication

- Goal：convenient、secure authentication methods and mechanisms
  - low-cost, easy to carry
  - secure
- 相關技術趨勢：
  - 帳密、通行碼、IC卡、自然人/工商憑證、手機、指紋、聲紋、視網膜....
  - 多種方法合併使用提高安全性
  - 整合 Public Key Infrastructure (PKI)，達成網路身分證的目的

Network Security : Secure Communication

- Goals
  - secrecy、integrity 、 origin verification
- Technologies：
  - IPsec（RFC-24xx ）、IPSP（IP Security Policy)、IKE（Internet Key Exchange）
  - Encryption: e.g., AES
  - Computational efficiency (speed): encryption chip、IPSec chip

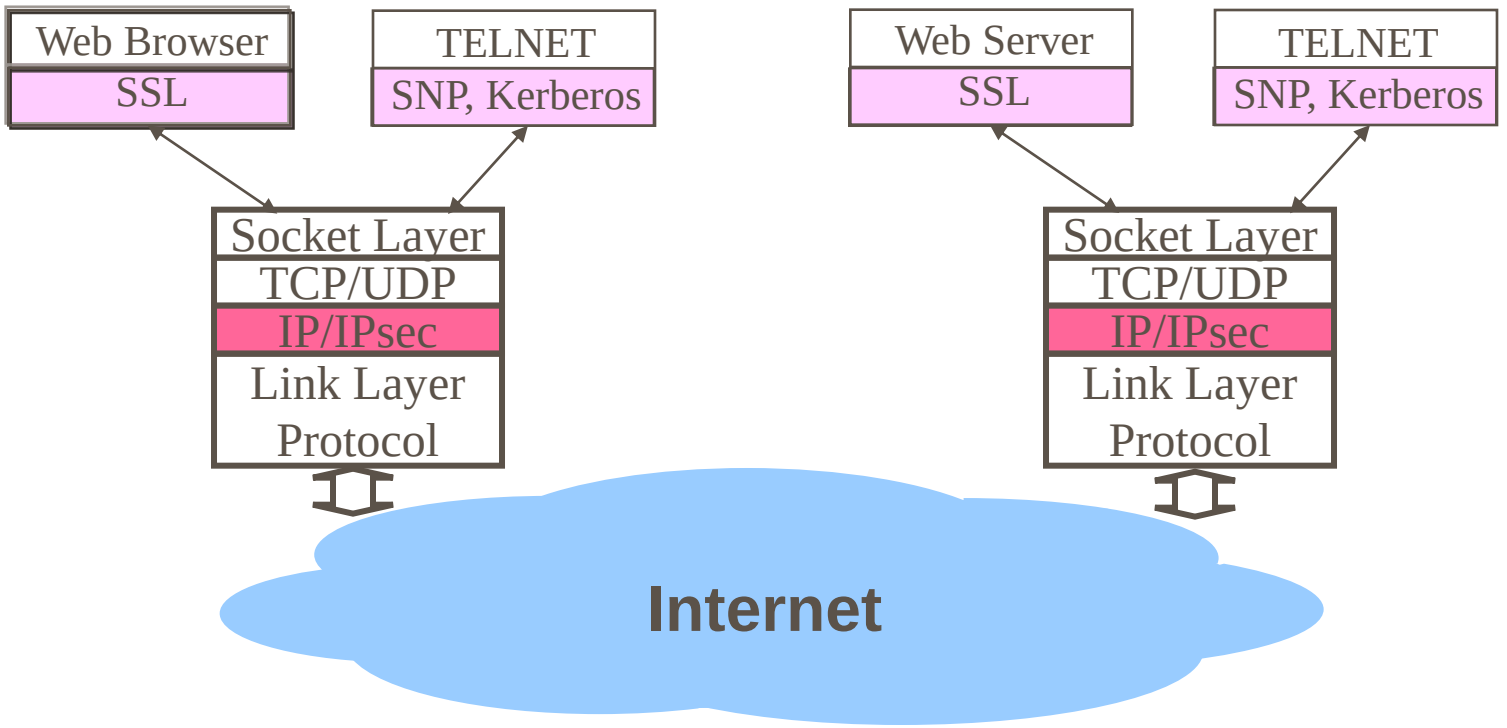
Network Security – Secure Systems

- Goals
  - Prevent hosts from malware attacks such as DoS, service disruption, data stealing and destruction and viruses.
- Technologies :
  - **Firewall**, **network security auditing**, monitoring, and vulnerability check, intrusion detection, anti-virus, etc.
  - Data backup, remote backup & disaster recovery, fault-tolerance
  - Information Security Management System (ISMS)
    - A systematic approach to managing *sensitive* company information so that it remains secure.
    - It encompasses people, processes and IT systems.
    - British Standards Institution (BSI) published a code of practice for these systems, which has now been adopted internationally as ISO/IEC 27001:2005.

Introduction

- In 1994, the Internet Architecture Board (IAB) initiated the work on IP security
- IPsec provides security service at the IP layer
- It allows a system to *select* required security protocols (authentication and/or encryption) and algorithm(s), and put in place any cryptographic keys necessary.
- Support of IPsec is mandatory for IPv6 and optional for IPv4.

Internet Security - Solutions



IPsec – History

- IETF
  - IP Security **Protocol** Working Group （IPSEC）
- In August, 1995 - basic IPsec kernel (RFC 1636 et. al)
  - To secure the network infrastructure from unauthorized monitoring (eavesdrop) and control (intercept and replay) of network traffic
  - To secure end-user-to-end-user traffic using authentication and encryption mechanisms

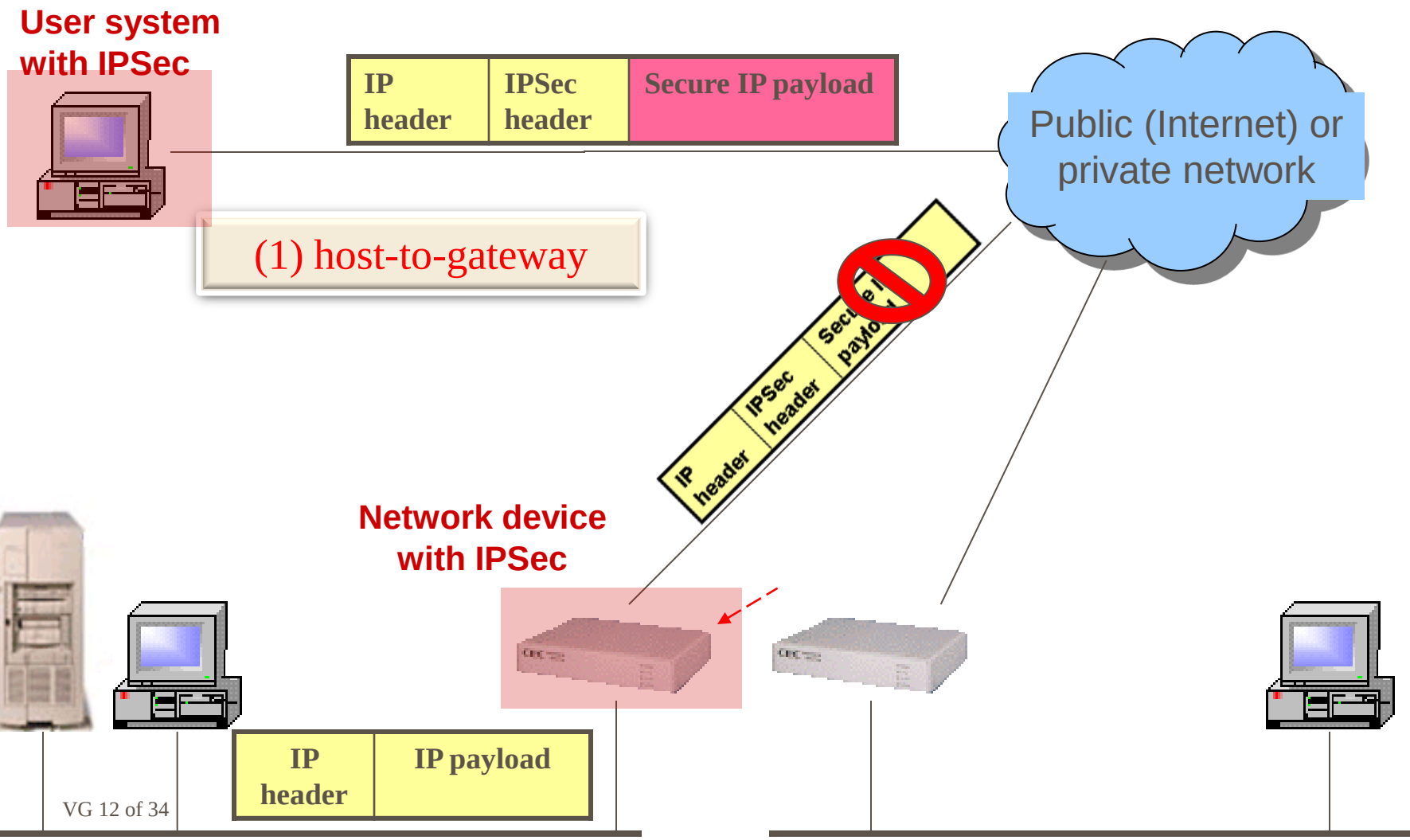
The most serious types of attacks in 1995 ...

- Computer Emergency Response Team (CERT) in USA
- IP spoofing
  - creates packets with false IP addresses and
  - exploits applications that use authentication based on IP
- Various forms of eavesdropping and packet sniffing
  - Attackers read transmitted information (including logon information and database contents)

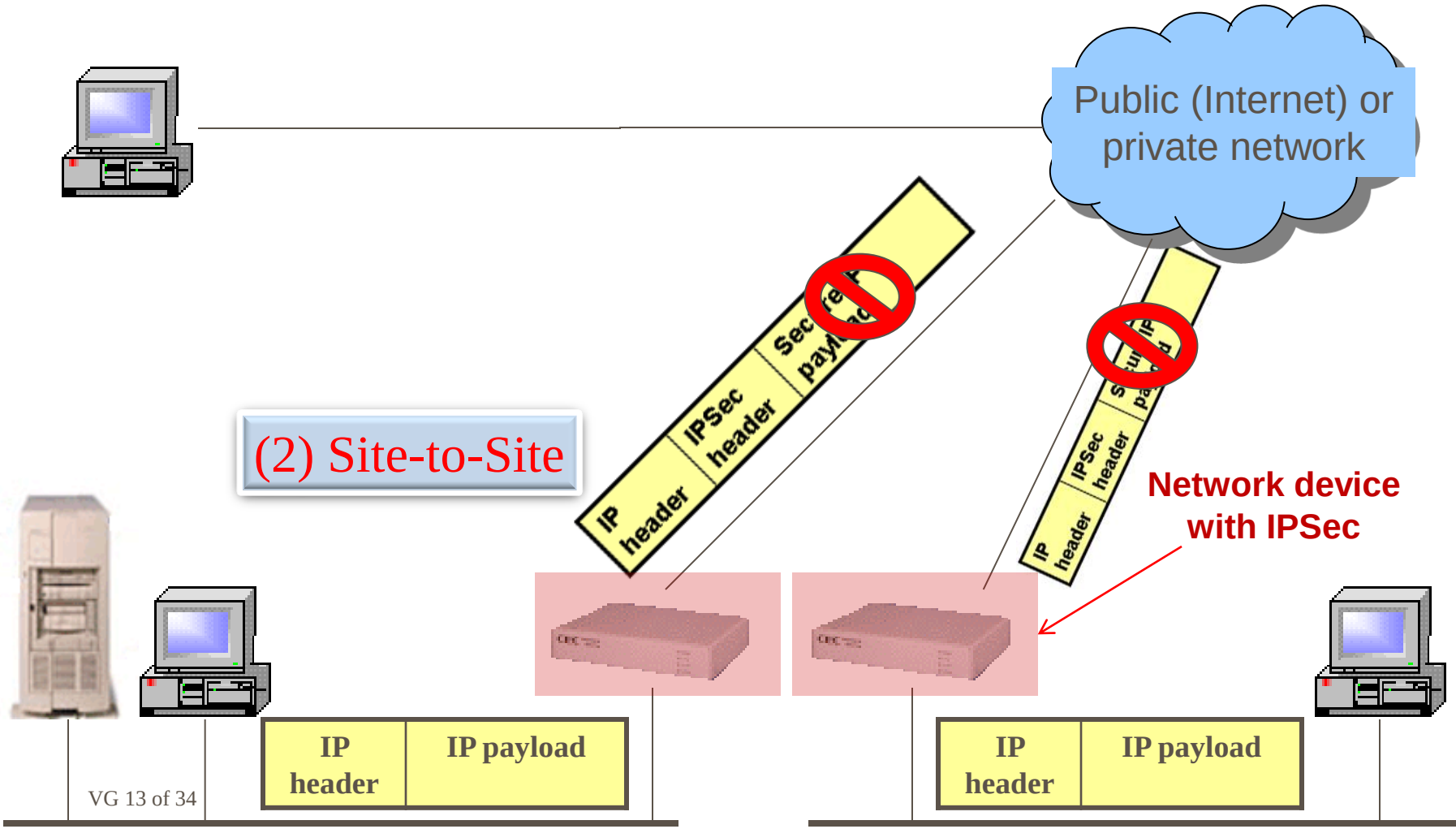
Application of IPSec

- Encrypt and/or authenticate ***all*** traffic *at the IP level*
- IPSec protocols operate in networking devices, e.g., routers and firewalls, connecting LANs to the Internet, or hosts (including mobile devices)
  - *Encrypt* traffic going into the WAN;
  - *Decrypt* traffic coming from the WAN
- Typical scenarios
- These operations are *transparent* to workstations, servers and users on the Intranet

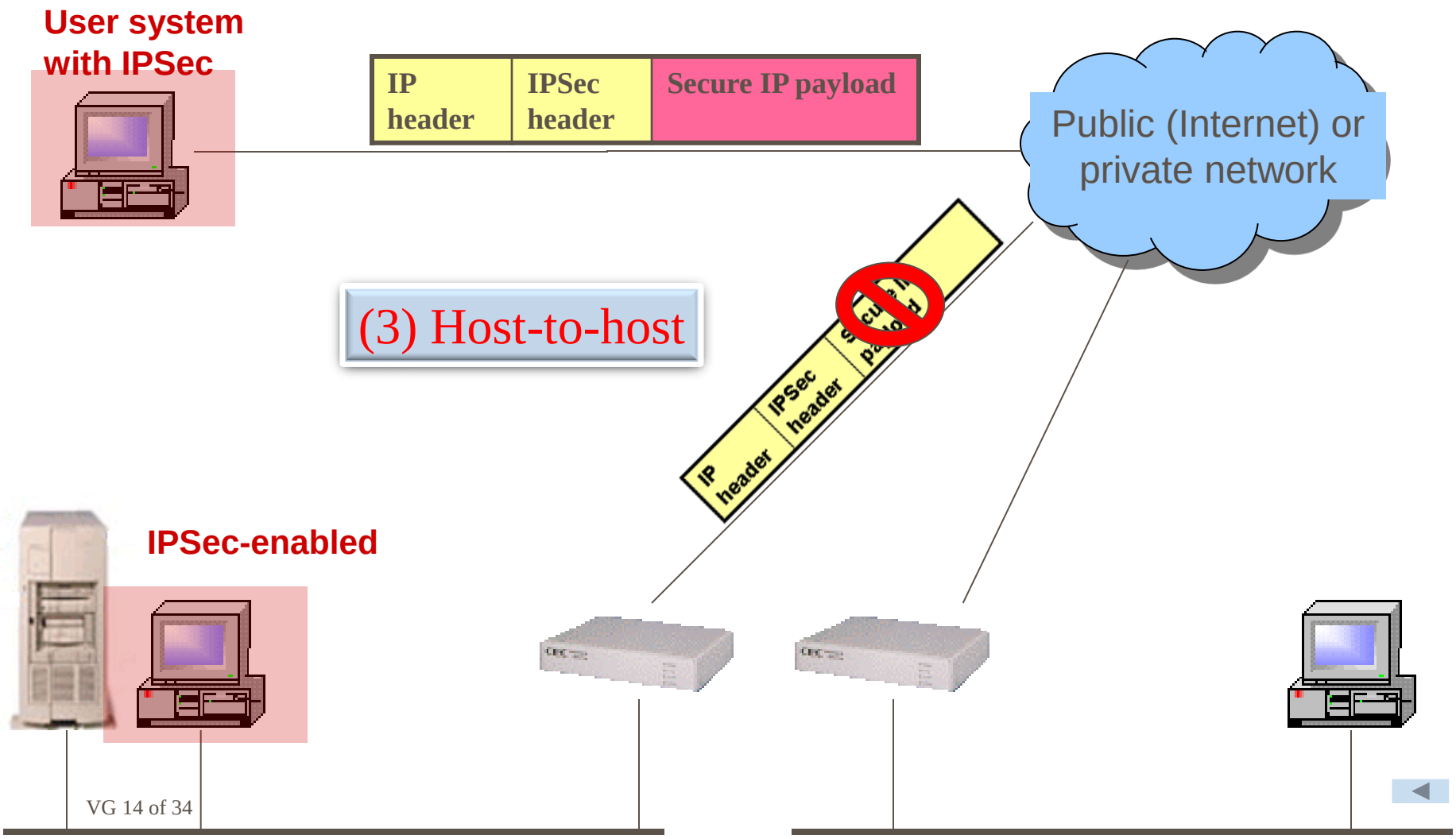
IP Security Scenario



IP Security Scenario



IP Security Scenario



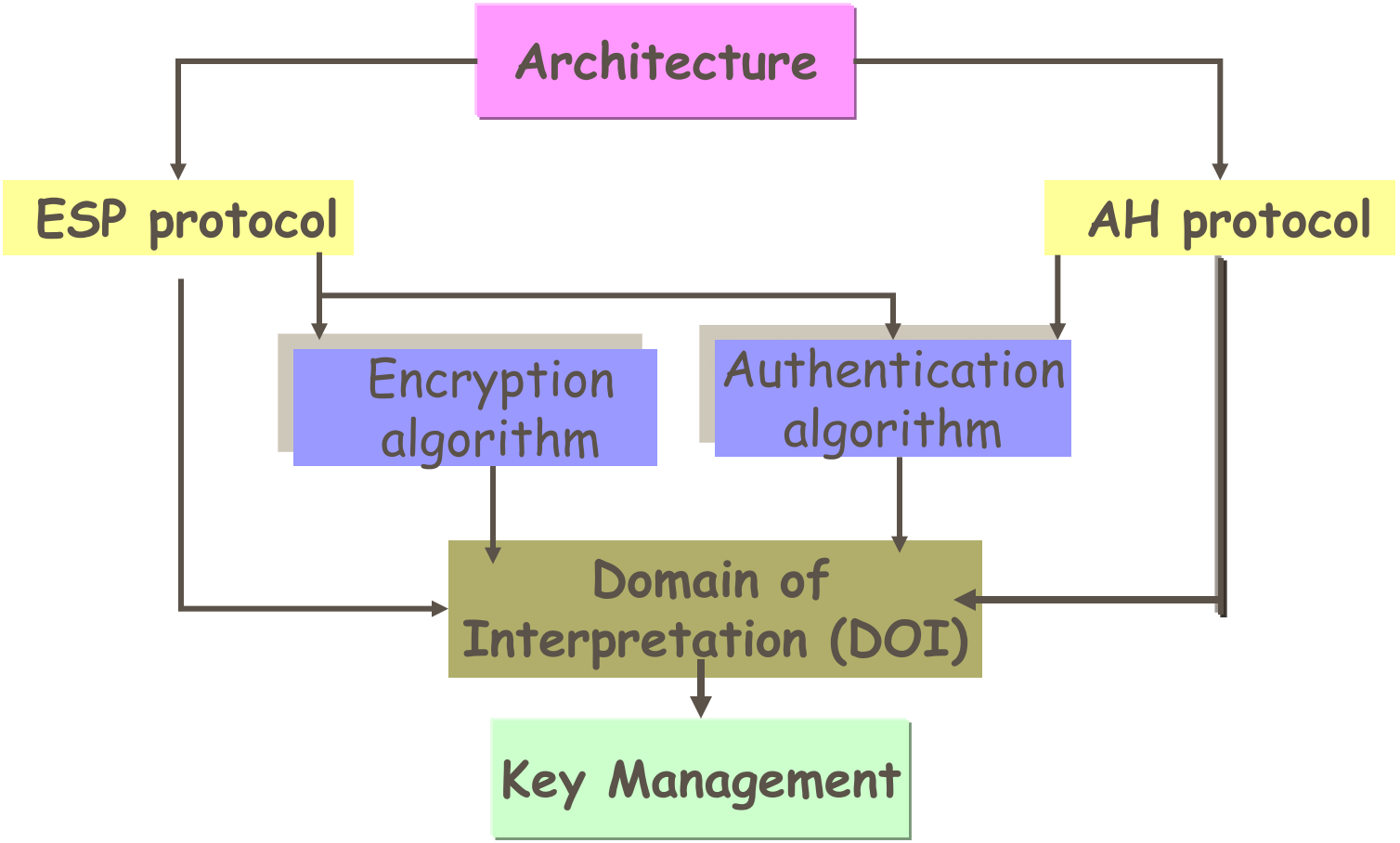
Benefits of IPsec

- All IP-based applications
- Routing Applications

IP Security Architecture

- Documents
- Services
- Concept of Service Association

IPSec Document Overview

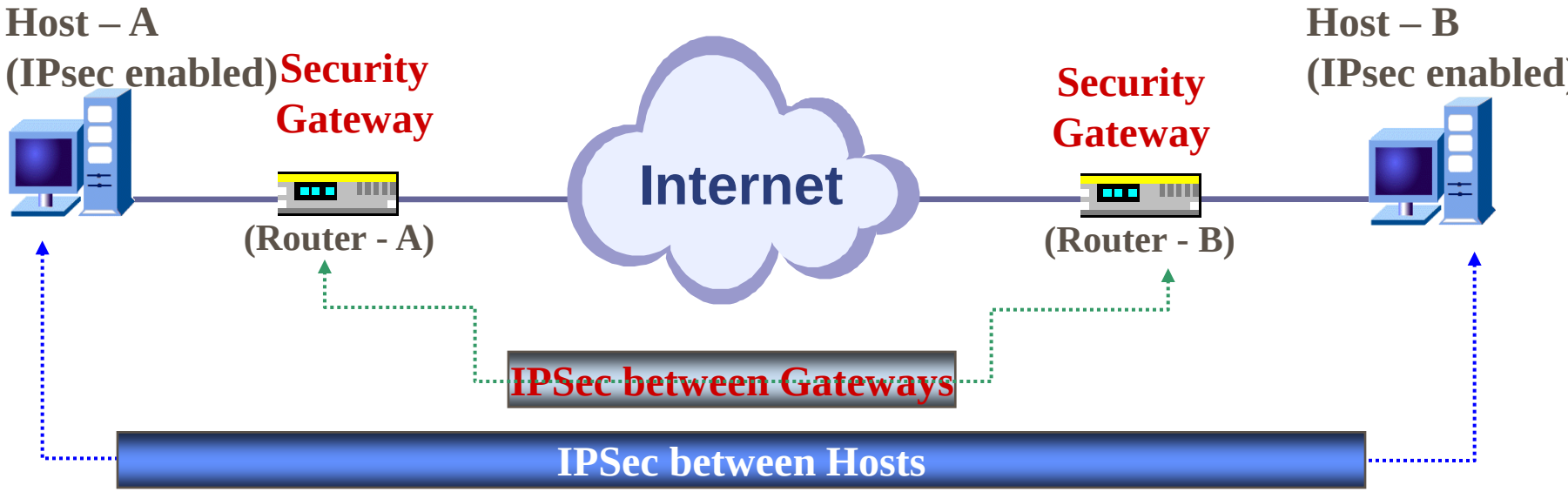


IPsec - Introduction

- Encapsulation Modes
  - To determine the security scope - Transport (layer 4^+) or Tunnel (layer 3^+) mode
- Security Protocols
  - Provide different levels of security

IPsec – Packet Encapsulation

- Transport mode : host-to-host
  - Tunnel mode : gateway-to-[host/gateway]



IPsec - Security Protocol

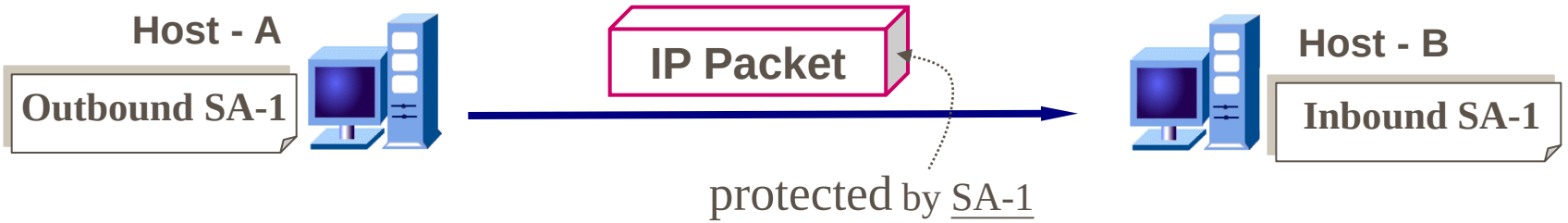
- Authentication Header (AH)
  - Data Origin Authentication
  - Connectionless Integrity
- Encapsulating Security Payload (ESP)
  - Confidentiality (Encryption)
  - Data Origin Authentication (option)
  - Connectionless Integrity (option)

IPsec Documents

- DOI (Domain of Interpretation)
  - Contains *values* needed for the other documents to relate to each other
    - e.g., *identifiers* for approved encryption and authentication algorithms, and *operational parameters* such as key lifetime.
  - RFC 2407 - The Internet IP Security Domain of Interpretation for ISAKMP

IPsec – Security Associations (SA)

- An SA is a one-way *relationship* between a sender and a receiver that provides security services to the traffic carried on it.
  - For two-way secure exchange – *two* SAs are needed



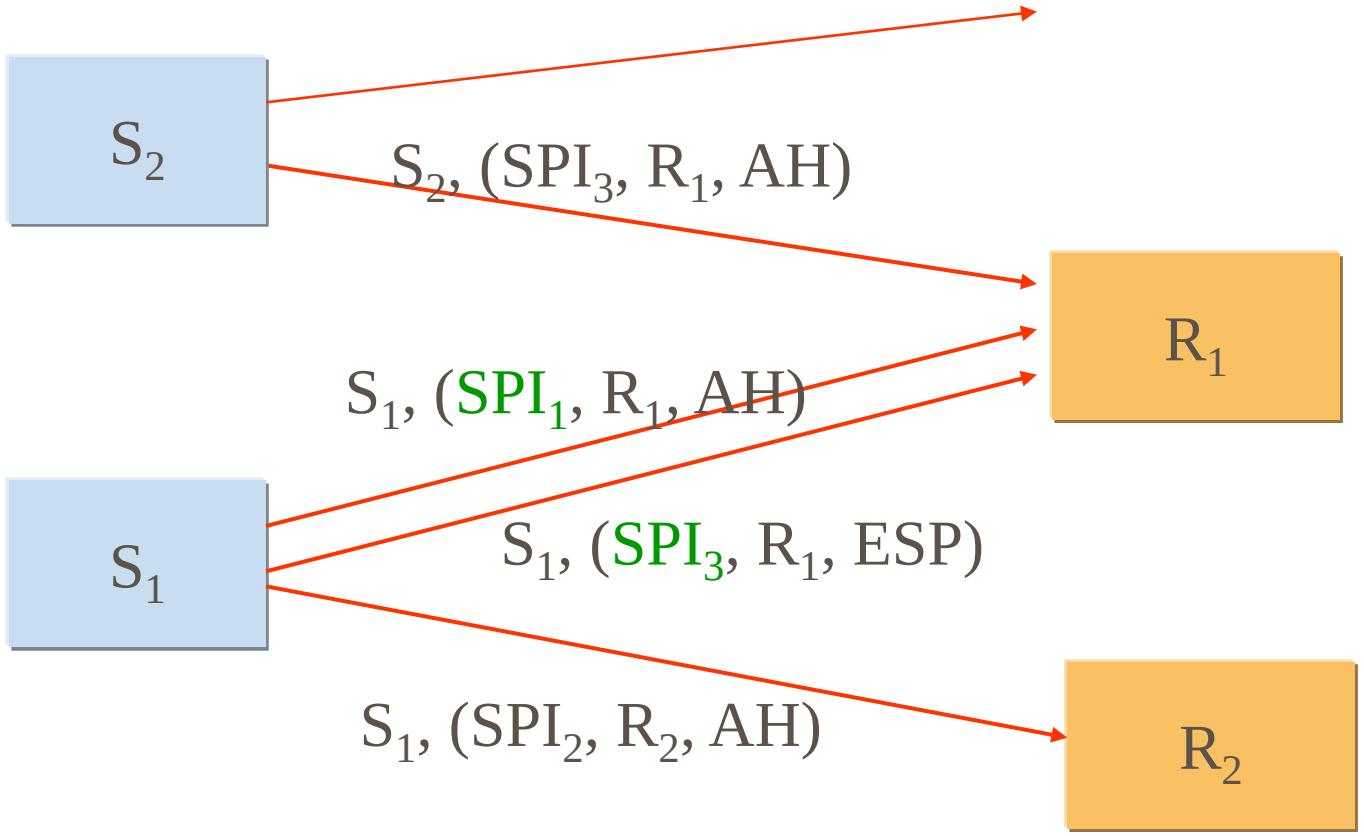
IPsec - Security Association (SA) (cont'd)

- An SA is uniquely identified by *three* parameters:
  - Security Parameter Index (SPI)
  - IP Destination Address
  - Security Protocol Identifier (e.g., AH or ESP)
- Key generation
  - manually keying
  - automated – IKE (Internet Key Exchange)

Security Association - Identity Parameters

- Security Parameter Index (SPI)
  - A bit string assigned to an SA
  - Only of local (w.r.t. *sender*) significance
  - Carried in AH and ESP headers to enable the receiver to select the SA under which a received packet will be processed.
- IP Destination Address
- Security Protocol Identifier
  - AH or ESP

SA: Many-to-many relationship



Security Association- other Operational Parameters (1/4)

- Sequence Number Counter
  - A 32-bit value used to generate the Sequence Number field in AH or ESP headers
- Sequence Number Overflow
  - A flag to indicate whether to generate an auditable event when overflow of sequence number counter occurs.
  - The goal is to prevent further transmission of packets on this SA.

Security Association- other Operational Parameters (2/4)

- Anti-Replay Window
  - Used to determine whether an inbound AH or ESP packet is a replay.
- AH Information
  - About authentication algorithm, keys, key lifetimes, and related parameters used with AH.

Security Association- other Operational Parameters (3/4)

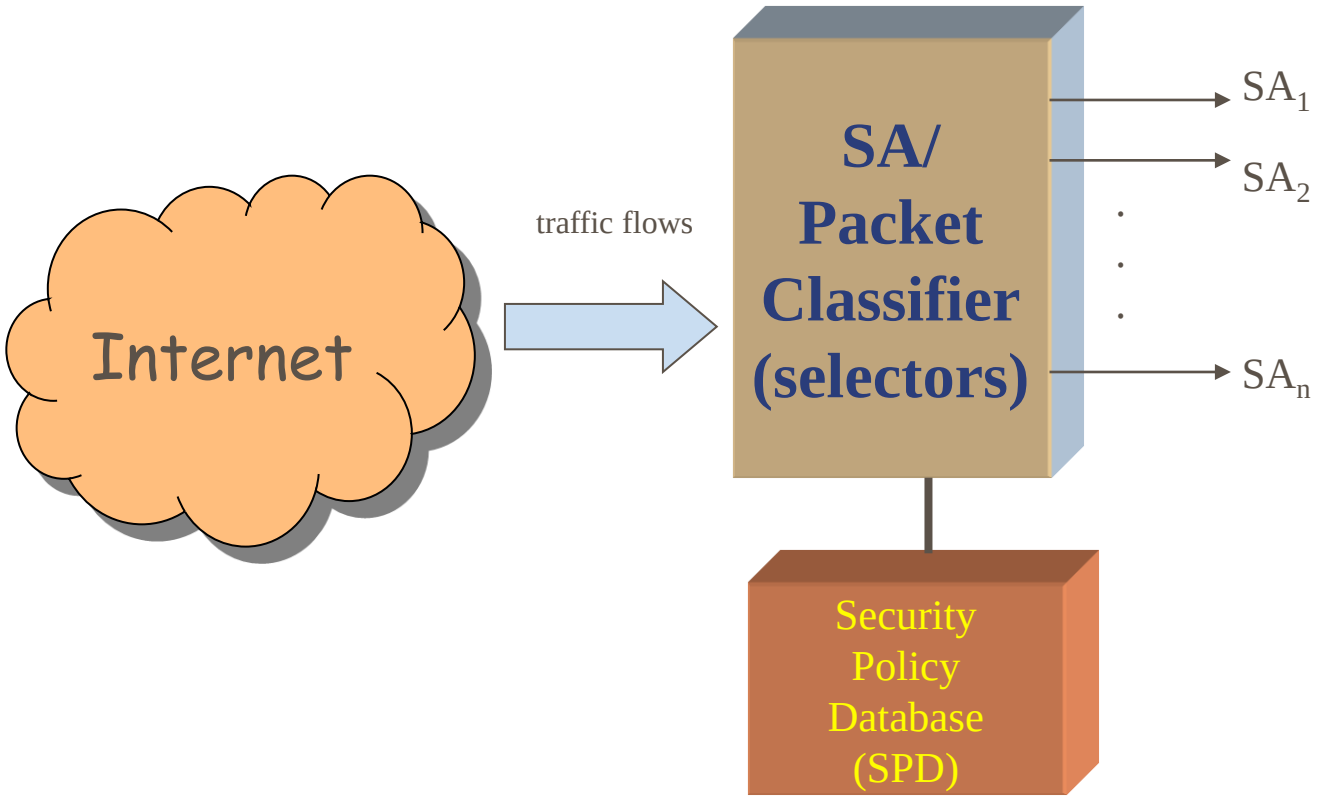
- ESP Information
  - About encryption and authentication algorithms, keys, initialization values, key lifetimes, and related parameters used with ESP
- Lifetime of an Security Association
  - A *time interval* or *byte count* after which an SA must be replaced with a ***new*** SA (and new SPI) or *terminated*
  - Must indicate which of these actions should occur.

SA Selectors (filters)

- Security Policy Database (SPD) contains entries.
- Each SPD entry contains a set of [illegible] layer protocol field values called selectors
- Selectors are used to filter incoming and outgoing traffic in order to map it into a particular SA.
- An entry may associate with one single SA or multiple SAs; or multiple entries may relate to a single SA

Packet classification

Packet Classification: SA filtering



- Compare the values of the *selector fields* against SPD to find a matching entry
- may point to zero or more SAs

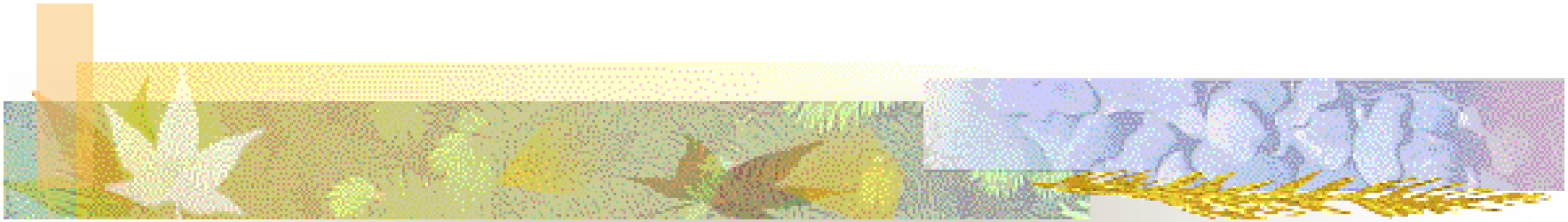
■ Determine the SA, if any, and its associated SPI.

■ Do the required IPsec processing (AH or ESP).

SPD - Selectors

- #1: Destination IP address
  - A single address, an enumerated list or range of addresses, subnet, or a wildcard
- #2: Source IP address
  - A single address, an enumerated list or range of addresses, subnet, or a wildcard
- #3: User ID
  - A user identifier from the operating system, available if IPsec is running on the *same operating system* as the user
- #4: Data Sensitivity Level
  - Used for systems providing information flow security (e.g., Secret or Unclassified)
- #5: Transport Layer Protocol
  - A single protocol number, a list of protocol number
- #6: Source and Destination Ports
  - Individual TCP/UDP port values, an enumerated list of ports or a wildcard
- #7: IPsec Protocol
  - AH or ESP or AH/ESP
  - IPv4 protocol or IPv6 Next Header field
- #8: IPv4 Type of Service (TOS)
  - A specific value or a wildcard

The end. ☺



Secure Sockets Layer (SSL) Protocol

What is SSL?

- It was originally developed by Netscape.
- SSL has been accepted on the World Wide Web for *authenticated* and *encrypted* communication between clients and servers.
- It is an *application* layer protocol
- The SSL protocol uses TCP/IP on behalf of the higher-level protocols such as HTTP.

SSL: Design Goals

- Provide authentication, privacy and data integrity between two communicating applications.
- Server authentication
  - Allows a user to confirm a server's identity.
- Client authentication
  - Allows a server to confirm a user's identity.
- An encrypted connection
  - Provides high degree of confidentiality for the communication between a client and a server.
- Extensibility
  - *New* public key and encryption methods can be incorporated as necessary.

Hypertext Transfer Protocol Secure (HTTPS)

- SSL encryption is *available* on major Web browsers.
- HTTPS is a combination of the HTTP with the SSL.
- It provides encryption and secure identification of the server.
- HTTPS connections are often used for e-commerce or web-based sensitive transactions, e.g., online access to financial accounts on Internet.
- **HTTPS** should not be confused with Secure HTTP (S-HTTP) specified in RFC 2660

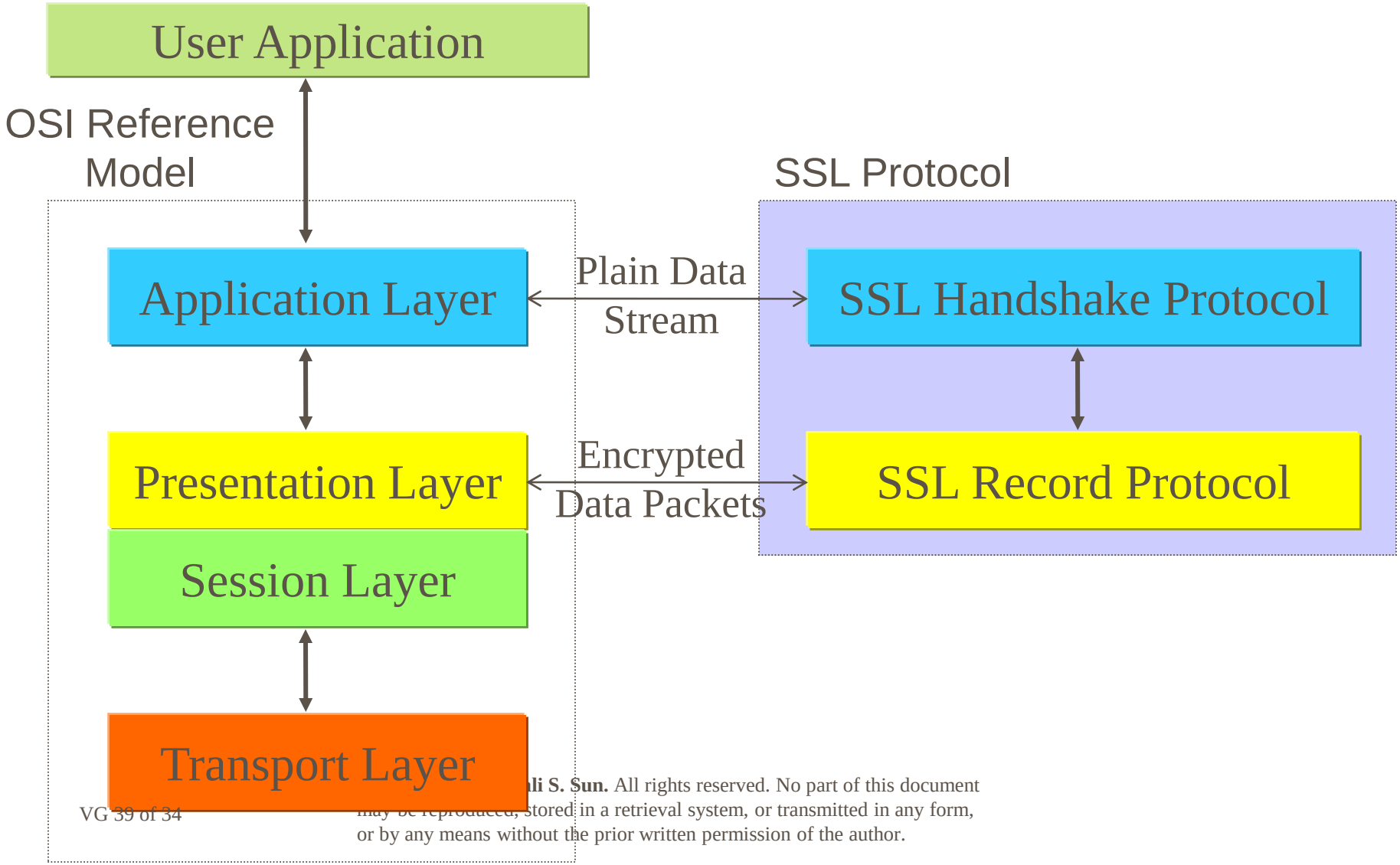
Secure Hypertext Transfer Protocol (S-HTTP)

- S-HTTP is a little-used alternative to the HTTPS for encrypting web communications carried over HTTP.
- HTTPS and S-HTTP were both defined in the mid-1990s to address Internet security need.
- Netscape and Microsoft supported HTTPS rather than S-HTTP, leading to HTTPS becoming the de facto standard mechanism for securing web communications.

Protocol Stack

- SSL *Handshake* Protocol (SSLHP)
  - negotiates cryptographic methods to be used
  - performs **mutual authentication** of server and client
- SSL *Record* Protocol (SSLRP)
  - packetizes data into *records*
  - performs the agreed encryption/decryption on records

Protocol Stack



SSL Record Protocol

- Properties
  - The connection is **private**.
    - Symmetric cryptography is used for data encryption.
  - The connection is **reliable**.
    - Message integrity is checked by using a keyed *MAC* (Message Authentication Code)

SSL Record Protocol