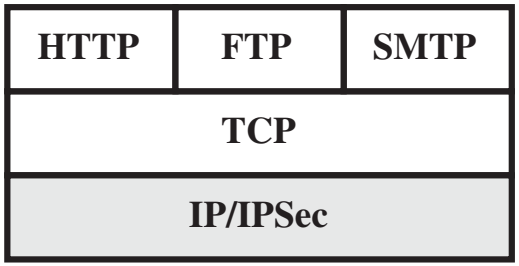
Secure Network Protocols

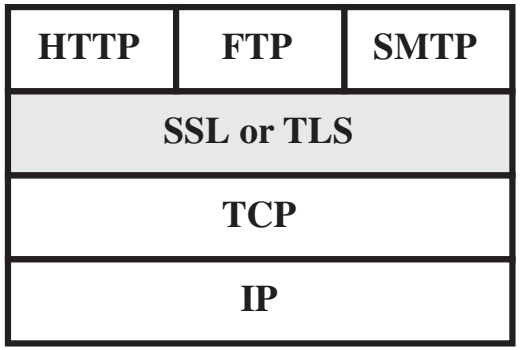
Kehuan Zhang

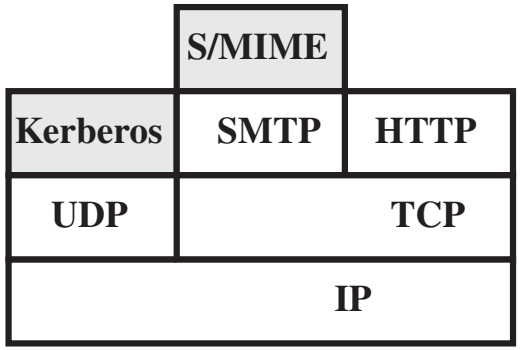
IERG4130 2022

Topics to Be Covered

- Application Layer: Secure E-mail and S/MIME - Application specific
- Transport Layer: SSL/TLS - Provide end-to-end security (secure connections)
- Network Layer: IPSec and VPN - Provide point-to-point security (between two hosts)







Correlations and Differences Among The Protocols

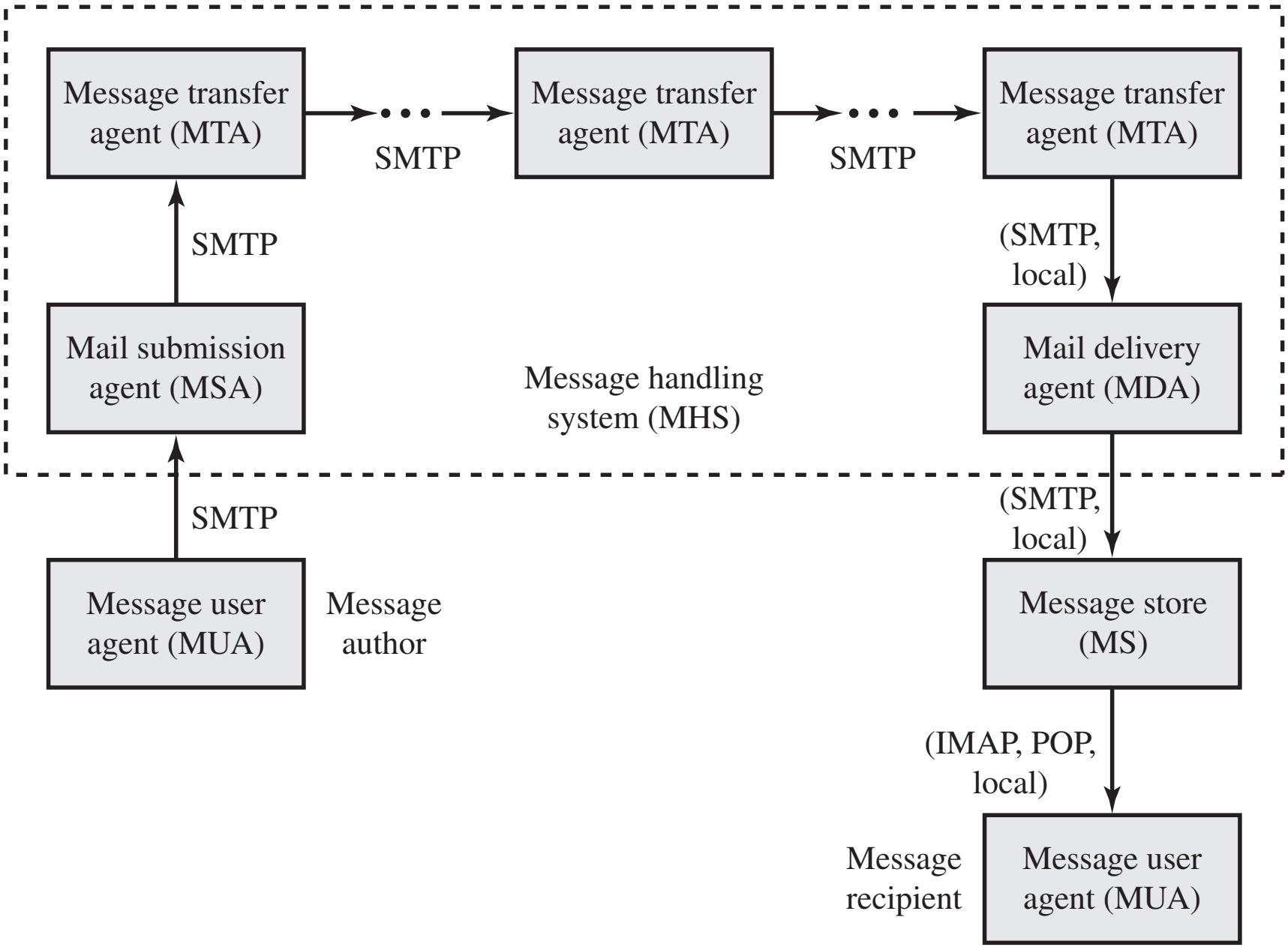
- Protocols may provide overlapped functionalities
  - E.g., IPSec can also protect data confidentiality, just like transport layer and application layer secure protocols
- But Each protocol may have some unique features
  - E.g., SSL/TLS and IPSec can only provide in-transmission security, while S/MIME can protect data after transmission
  - S/MIME also can provide non-repudiation, but IPSec and TLS generally could not
- **When learning those protocols, pay attention that**:
  - As long as two parties used the same protocols, they can talk to each other, no matter how complex the protocol could be
  - Understand the purpose of each protocol
  - Focus on how a protocol uses various crypto tools we have learned, like symmetric key encryption, asymmetric key encryption, MAC, etc.

Secure E-Mail and S/MIME

Why Do We Need S/MIME?

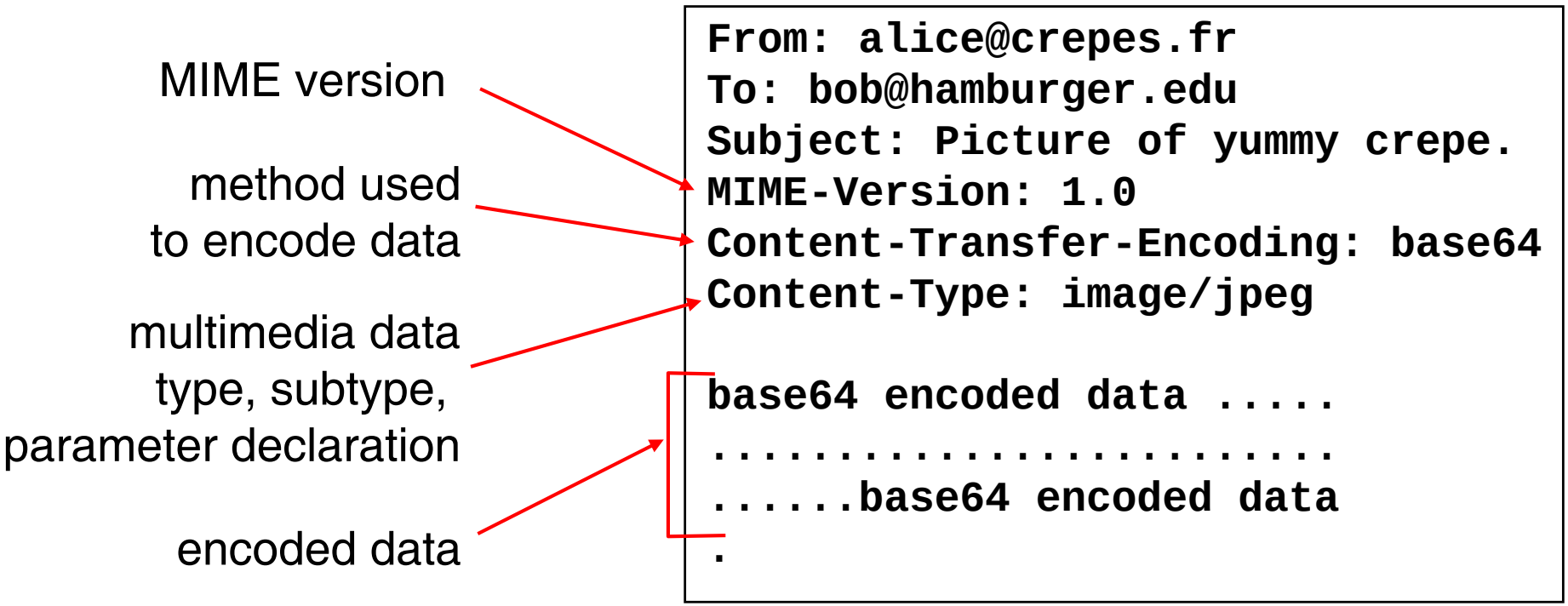
- What is S/MIME?
  - A security enhancement to the MIME Internet e-mail format standard
- What is MIME then?
  - Multipurpose Internet Mail Extension (RFC 2045, RFC 2046)
  - Extending the original SMTP (Simple Mail Transfer Protocol, RFC 822) - SMTP only support simple ASCII contents - SMTP may have problems when sending emails with binary files, Unicode texts, large sizes, etc.
    - ★ MIME introduced new headers and content formats as well as encodings to support multimedia e-mail other than simple ASCII messages
- So the evolving route is:
  - From SMTP $\rightarrow$ MIME: improvement on data format
  - From MIME *rightarrow* S/MIME: enhancement on data security

How E-mails Were Delivered?



E-mail Message Format: MIME

- Introduced new headers to declare MIME content type



MIME Types

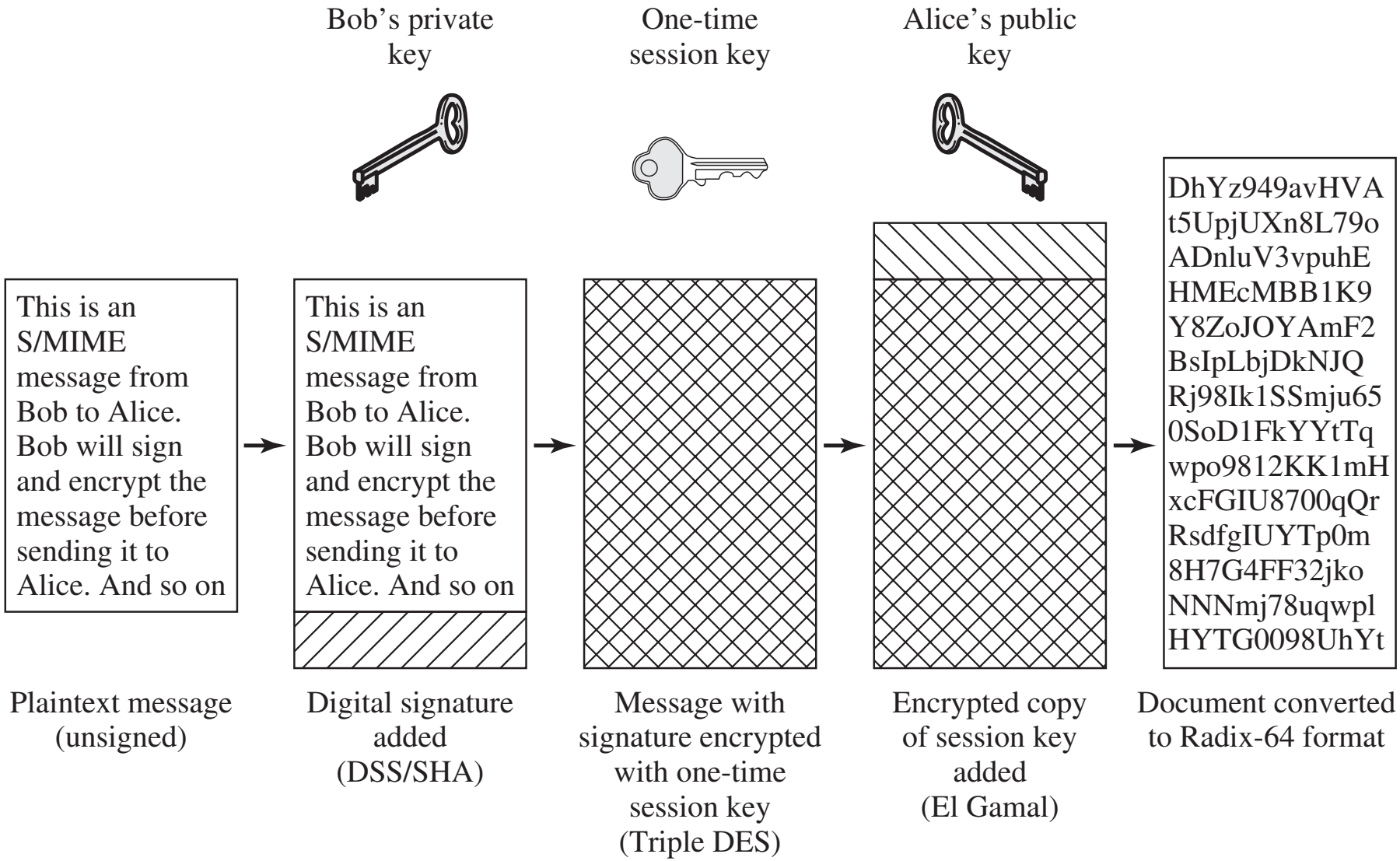
- Specification with *type/subtype*
  - E.g., image/jpeg in previous example
  - Sometimes may use compound subtype, like: *application/epub+zip*
- Text
  - Example subtypes: **plain**, **html**, like *text/plain*
- Image
  - Example subtypes: **jpeg**, **gif**, like *image/gif*
- Audio
  - Example subtypes: **mpeg** (for mp3), **wav**, like *audio/mepg*
- Video
  - Example subtypes: **mpeg**, **webm**
- Application:
  - Example subtypes: **pdf**, **zip**, like *application/pdf*
- Binary stream without specific format: *application/octet-stream*

S/MIME Functionalities

- Defined a new set of MIME content types to achieve confidentiality and/or integrity

Type	Subtype	S/MIME Parameter	Description
Multipart	Signed		A clear-signed message in two parts: one is the message and the other is the signature.
Application	pkcs7-mime	signedData	A signed S/MIME entity.
	pkcs7-mime	envelopedData	An encrypted S/MIME entity.
	pkcs7-mime	degenerate signedData	An entity containing only public-key certificates.
	pkcs7-mime	CompressedData	A compressed S/MIME entity.
	pkcs7-signature	signedData	The content type of the signature subpart of a multipart/signed message.

A Typical S/MIME Working Flow



- Algorithms can be changed to others, like SHA256 + AES + RSA
- Finally the document will be converted into base-64 format

Base-64 Encoding

- Also known as Radix-64 format
- The purpose of Base-64 encoding is to encode binary data to ASCII code so that binary data could be transmitted via ASCII-only protocols

Source	M			a			n			
ASCII	77 (0x4d)			97 (0x61)			110 (0x6e)			
Bit pattern	0 1 0 0 1 1 0 1			0 1 1 0 0 0 0 1			0 1 1 0 1 1 1 0			
Index	19			22			5		46	
Encoded	T			W			f		u	
Base64 Char	84 (0x54)			87 (0x57)			70 (0x46)		117 (0x75)	

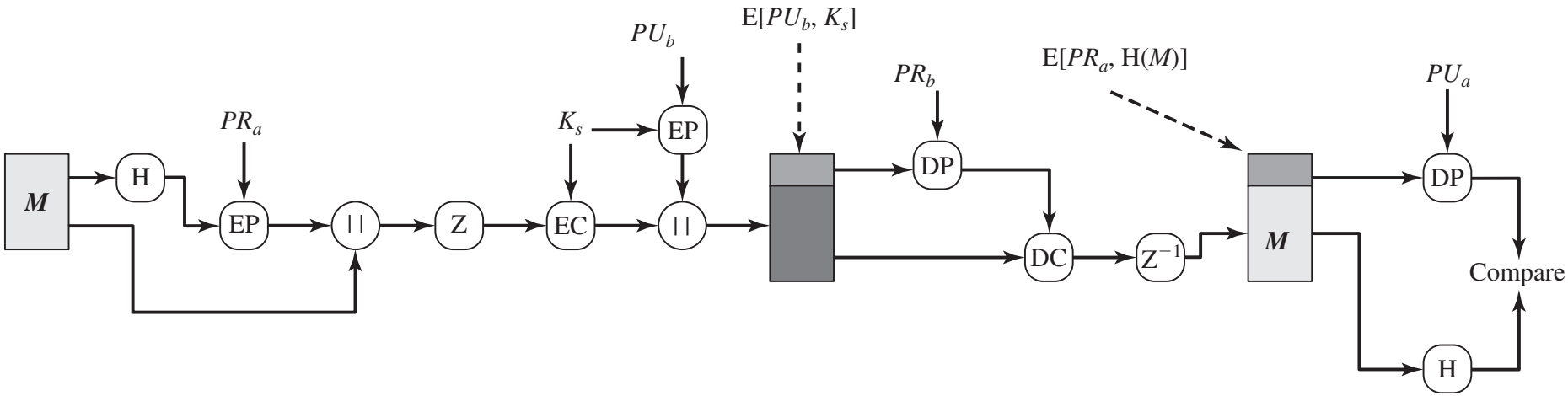
PGP (Pretty Good Privacy)

- 1991 – Creation of a single person, Phil Zimmermann
- Provides confidentiality and authentication services for electronic mail and file storage applications
- Selected best available cryptographic algorithms
- Integrated these algorithms into a general purpose application
- Source code and doc freely available on the net
- Agreement with company (Viacrypt) for low cost commercial version

Summary of PGP Services

Function	Algorithms Used	Description
Digital signature	DSS/SHA or RSA/SHA	A hash code of a message is created using SHA-1. This message digest is encrypted using DSS or RSA with the sender's private key and included with the message.
Message encryption	CAST or IDEA or Three-key Triple DES with Diffie-Hellman or RSA	A message is encrypted using CAST-128 or IDEA or 3DES with a one-time session key generated by the sender. The session key is encrypted using Diffie-Hellman or RSA with the recipient's public key and included with the message.
Compression	ZIP	A message may be compressed for storage or transmission using ZIP.
E-mail compatibility	Radix-64 conversion	To provide transparency for e-mail applications, an encrypted message may be converted to an ASCII string using radix-64 conversion.

Example of PGP Working Flow: From Alice to Bob

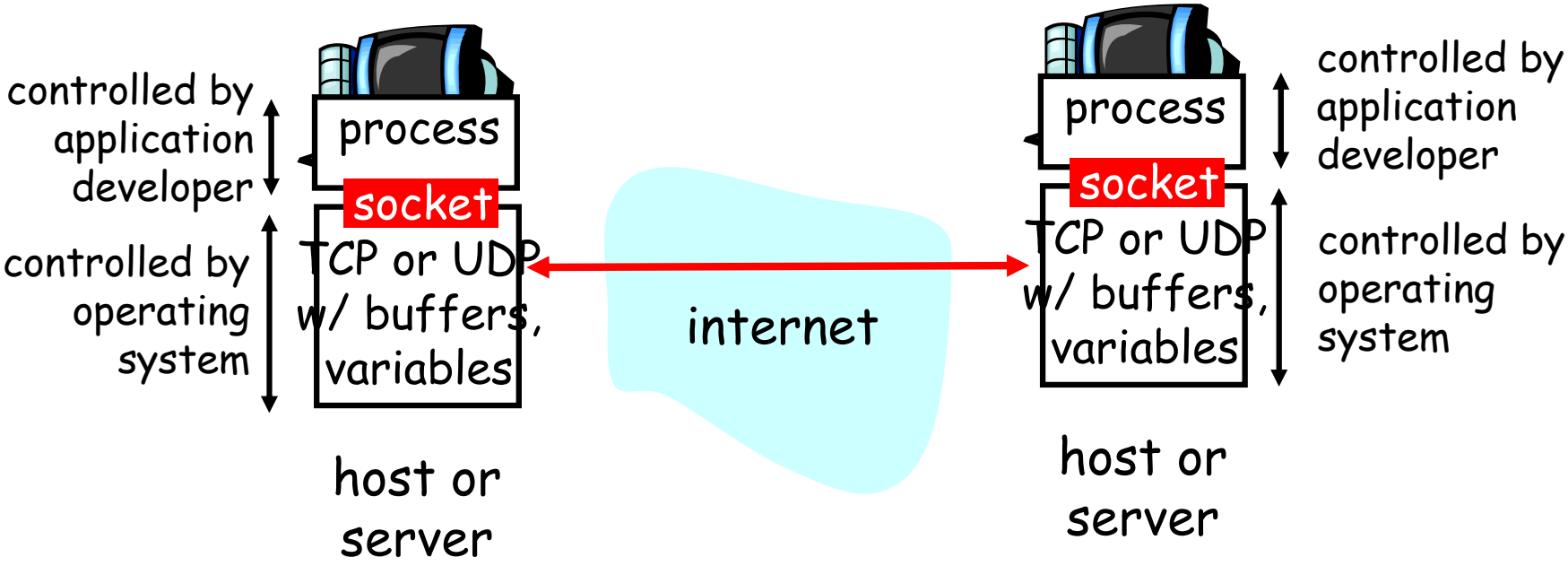


- Keys:
  - K_s: session key, PR_a: Alice's Private Key, PU_a: Alice's Public Key, PR_b: Bob's Private Key, PU_b: Bob's Public Key
- Encryption Algorithms:
  - EP: encryption with public-key, EC: encryption with symmetric key
  - DP: decryption with public-key, DC: decryption with symmetric key
- Messages Processing:
  - M: original message, H: Hash, $||$: message concatenate, Z: compress, Z^{-1}: decompress,

Secure Socket Layer (SSL) and Transport Layer Security (TLS)

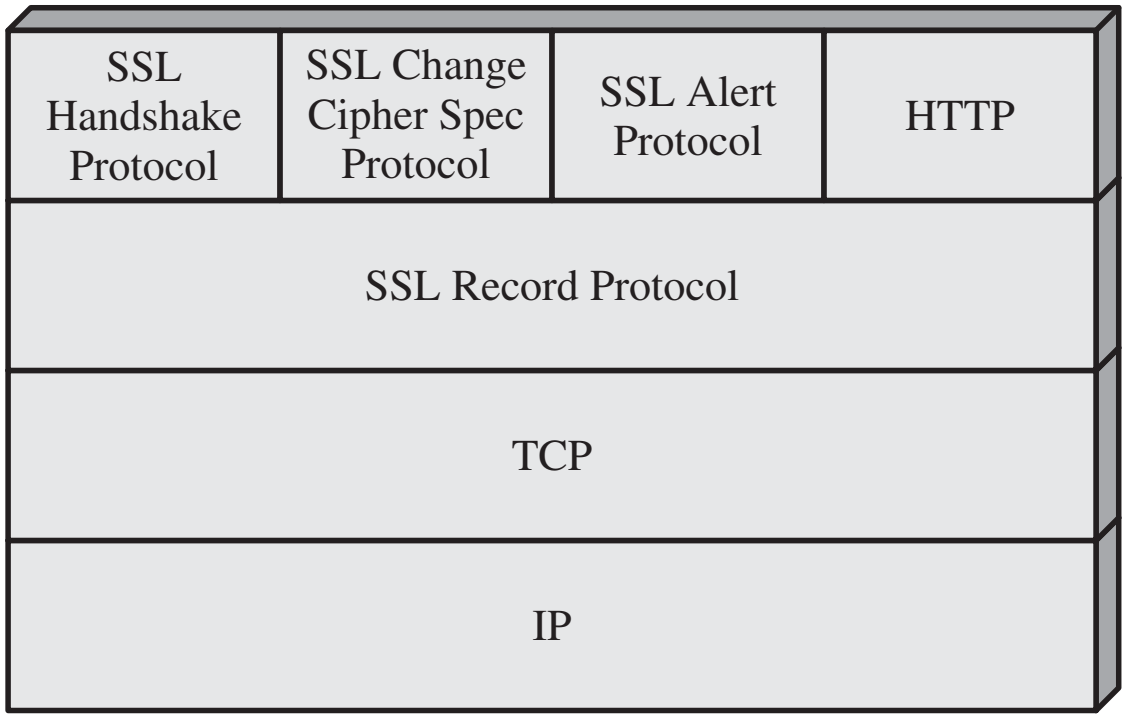
What Does Secure Socket Mean?

- Regular Socket Programming in TCP/IP

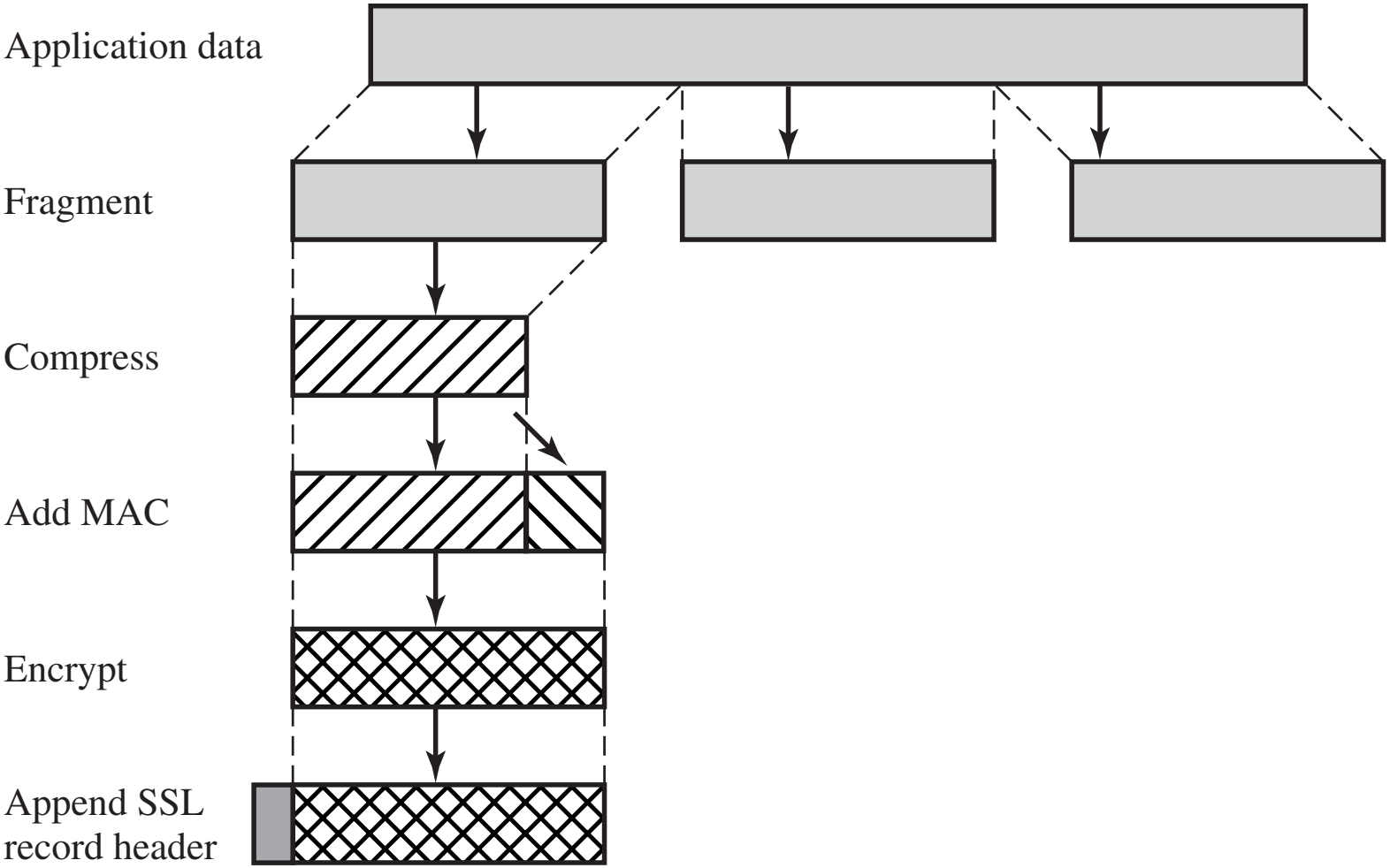


  - But above socket is insecure (e.g., no encryption)
- SSL/TLS aims to add security features
  - Through data encapsulation
  - Works above Transport layer but below Application Layer
  - SSL was originated by Netscape, but has been largely supplanted later by TLS

SSL/TLS Architecture

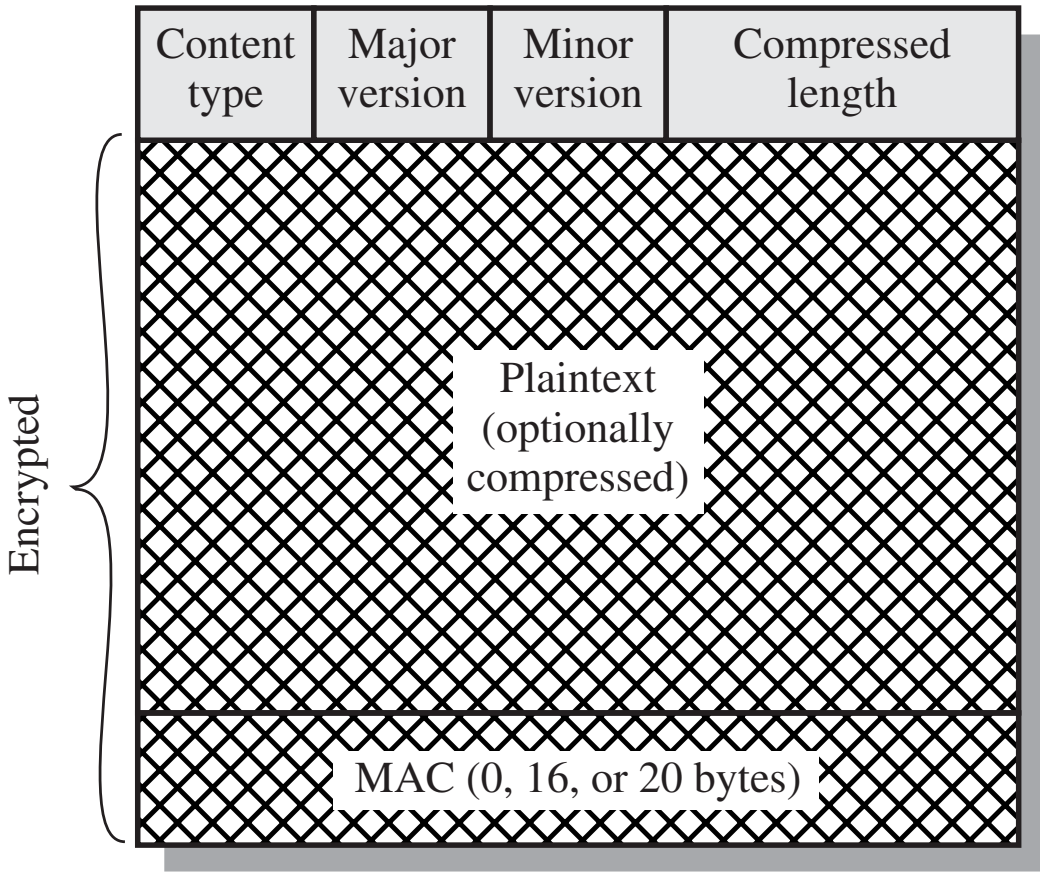


SSL/TLS Record Protocol Operations

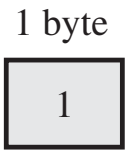


- Application data could come from HTTP (*HTTPS* RFC2818), FTP (FTP over TLS, RFC4217), SMTP (SMTP over TLS, RFC 3207), etc.
- The final Record data will become the TCP payload

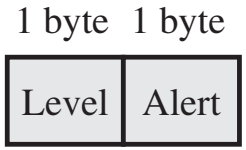
SSL/TLS Record Format



SSL/TLS Record Protocol Payload

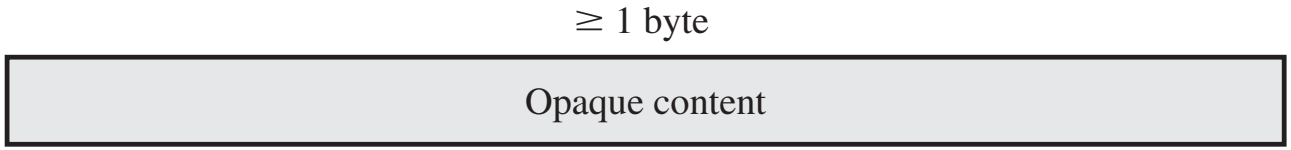


(a) Change Cipher Spec Protocol



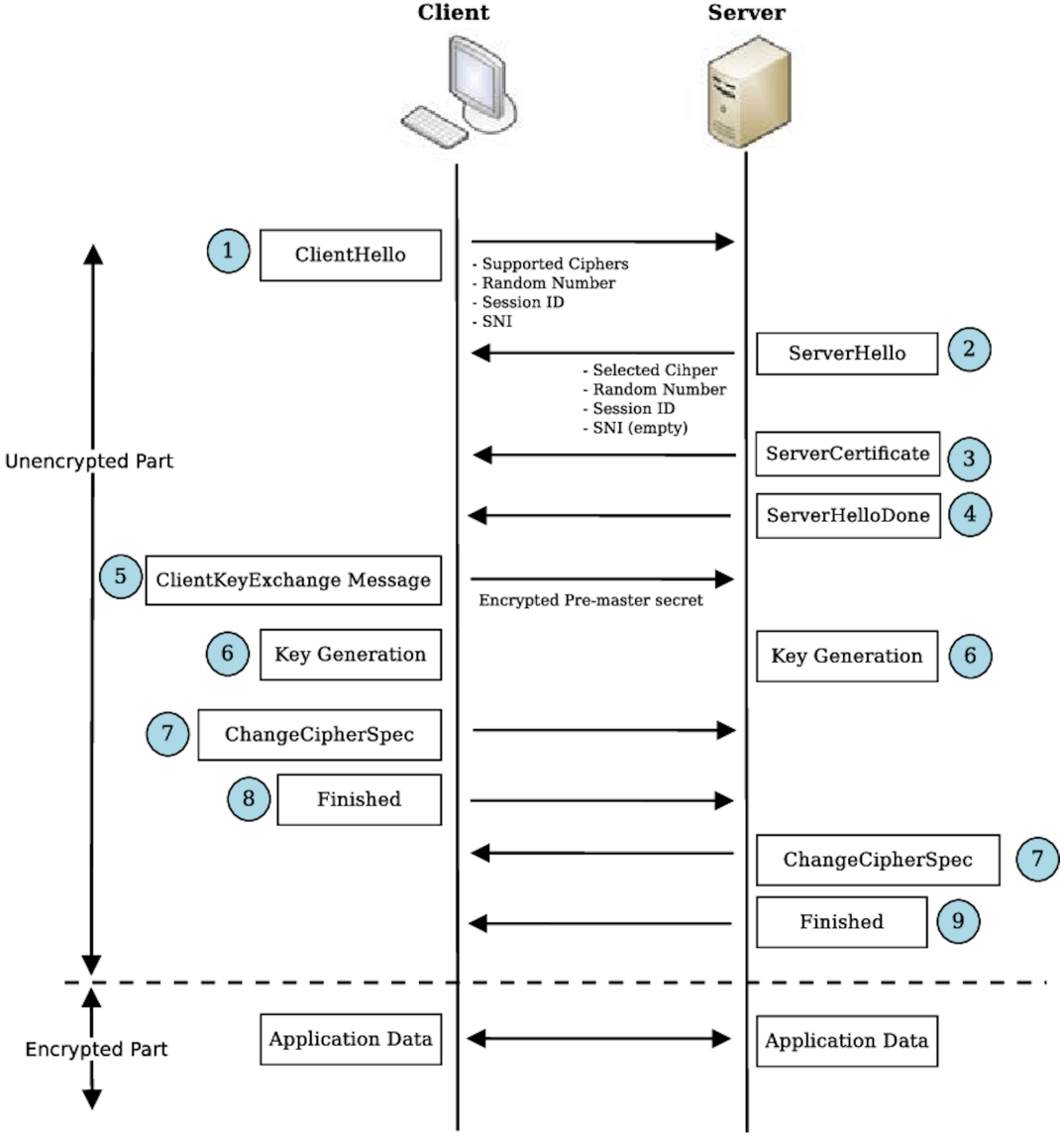
(b) Alert Protocol

(c) Handshake Protocol



(d) Other Upper-Layer Protocol (e.g., HTTP)

SSL/TLS Handshake Example



- Reading Material: key generation `https://www.acunetix.com/blog/articles/establishing-tls-ssl-connection-part-5/`

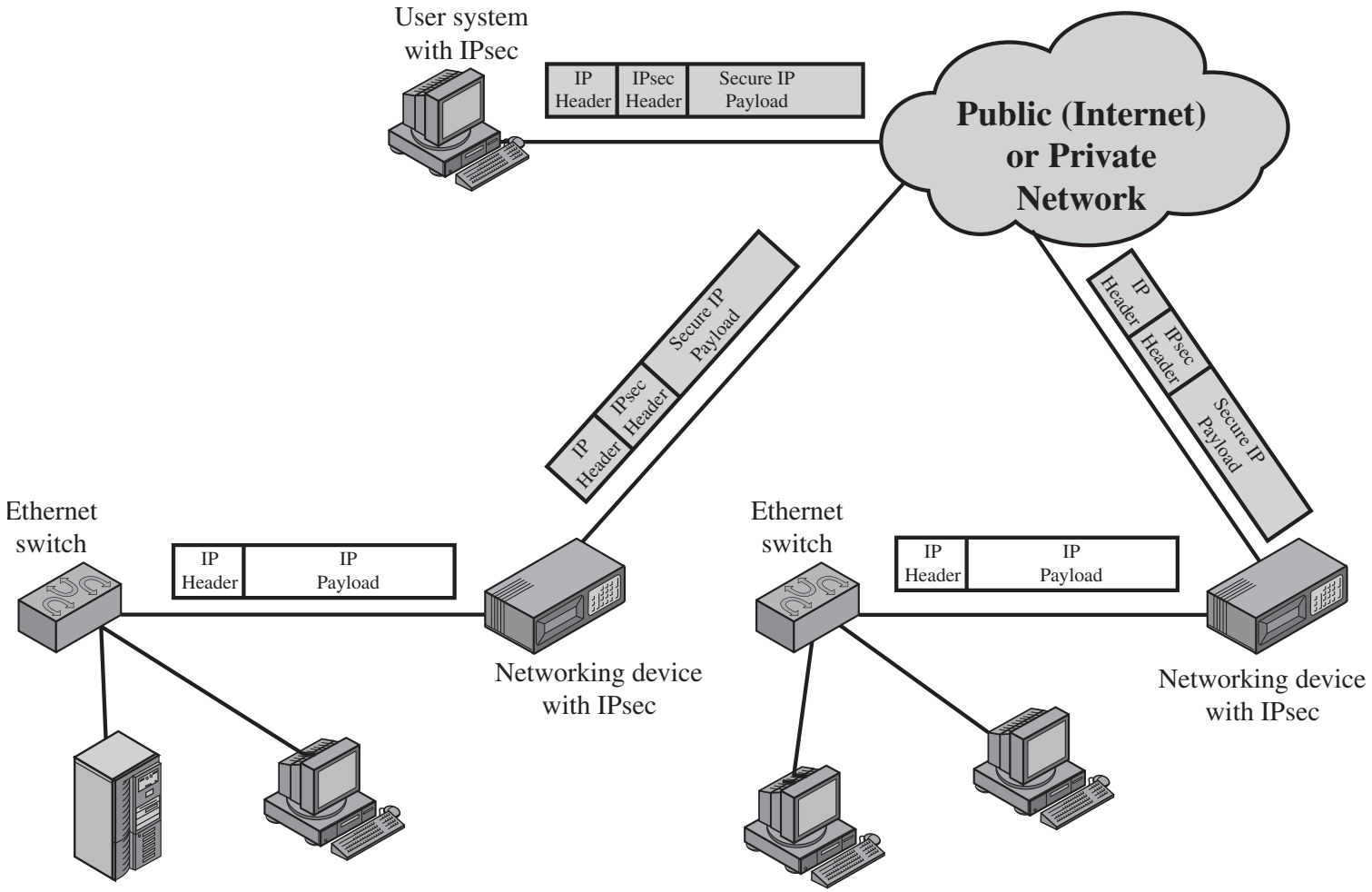
IPSec and VPN

IP Security Overview

- RFC2401(1998), RFC4301(2005): Security in the Internet Architecture
- Identified key needs:
  - secure network infrastructure from unauthorized monitoring
  - control network traffic
  - secure end-to-end user traffic using encryption and authentication
- According to CERT:
  - The most serious attacks are IP spoofing and eavesdropping/packet sniffing
- Next generation IP includes authentication and encryption
  - IPv6: IPSec "supposed to be" a mandatory part of IPv6
    - ★ Not true in real world
  - Available with IPv4

Applications of IPSec

- Secure branch office connectivity over the Internet
- Secure remote access over the Internet
- Establishing extranet and intranet connectivity with partners
- Enhancing electronic commerce security



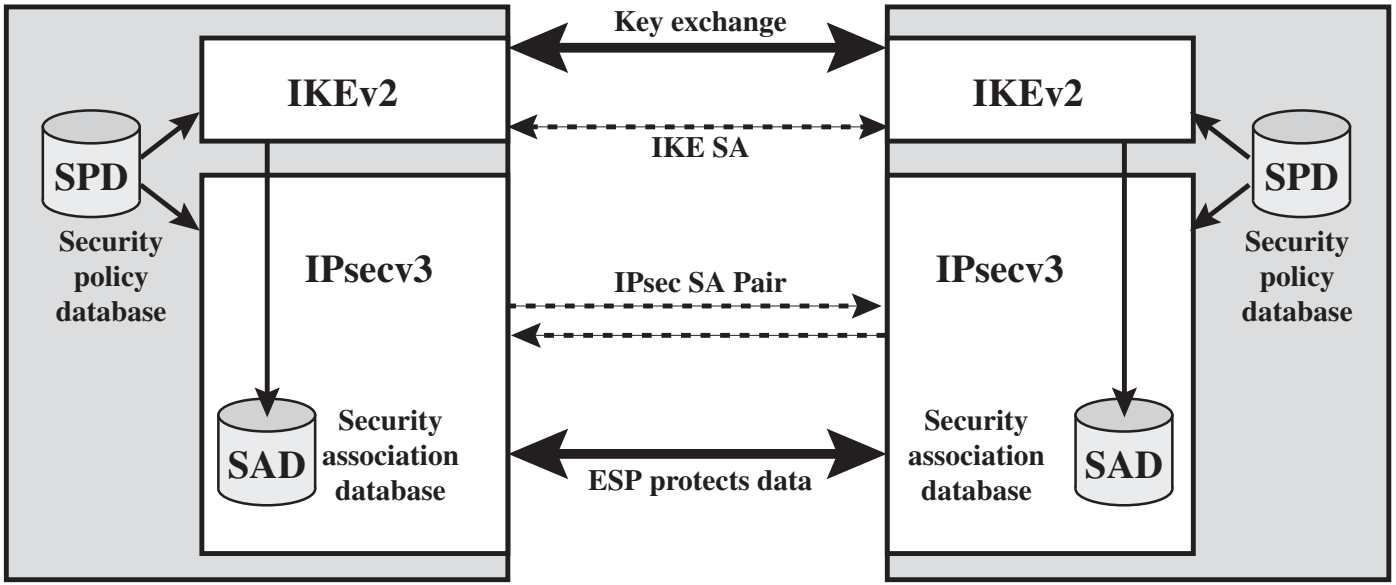
Pros and Cons of IPSec

- Benefits:
  - Strong security for all traffic when crossing the perimeter (assuming it is implemented in a firewall or router)
  - Below the transport layer (TCP, UDP) and transparent to applications
  - Transparent to the end users
  - Provides security for individual users – offsite workers, VPN
- Drawbacks:
  - Require Operating System changes
  - Not interwork with some existing/deployed networking technologies, esp. those muddle with Layer 4 and higher protocol elements, e.g.
    - ★ Network Address Translation (NAT) boxes (some solutions do exist)
    - ★ Load-balancers

IPSec Services

- Provides security services at the IP layer
  - Access control, data origin authentication, defense replay attack, confidentiality, etc.
- Enables a system to:
  - select required security protocols
  - determine algorithms to use
  - setup needed keys
- Two Protocols:
  - Authentication protocol – designated by the authentication header (AH)
    - ★ Decrecated, since ESP can provide message authentication
  - Encryption/Authentication protocol
    - ★ designated by the format of the packet, Encapsulating Security Payload (ESP); it is a mechanism for providing integrity and confidentiality to IP datagrams
- Two modes: Transport mode vs. Tunnel mode

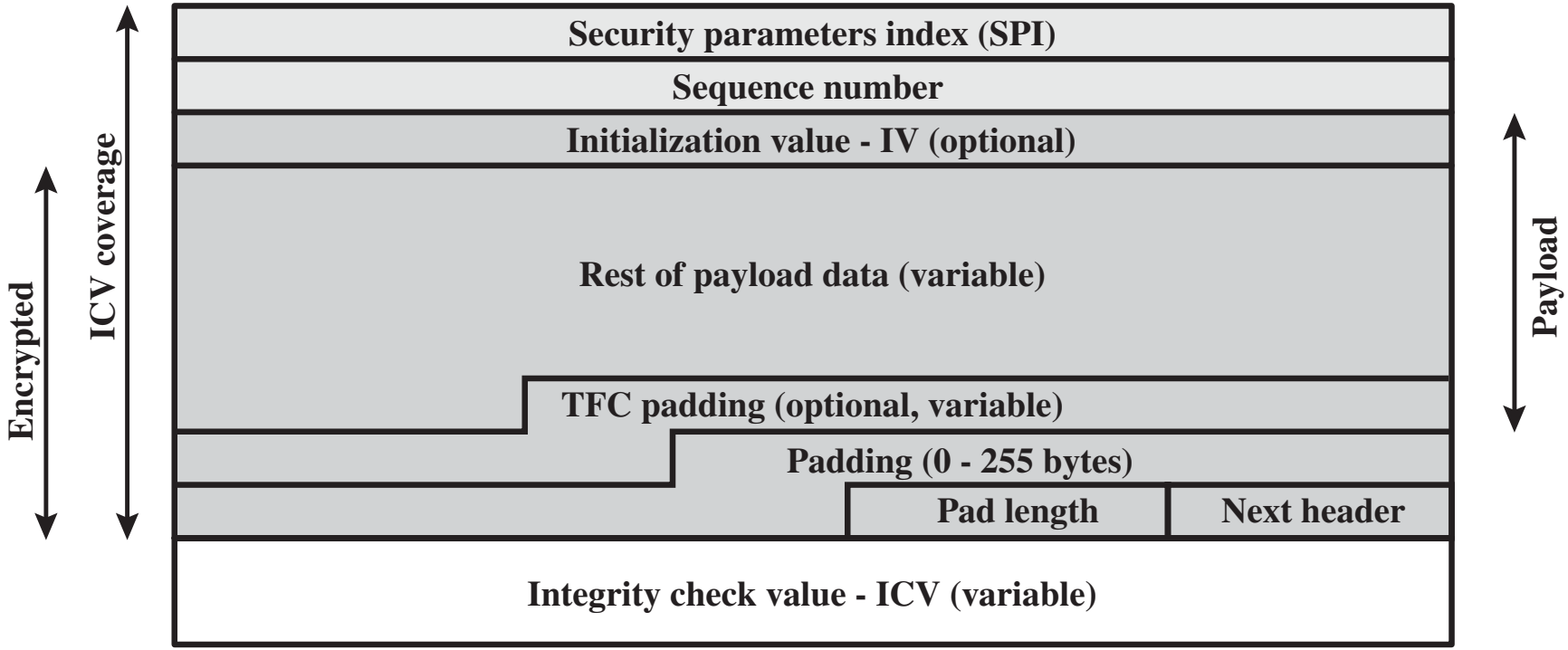
IPSec Architecture



- Terms
  - IKEv2: Internet Key Exchange (RFC 4306)
  - SA (Security Association): a one-way logical connection between sender and receiver that affords security services to the traffic carried on it.
  - SPD (Security Policy Database): mapping IP traffic to specific security policy
  - SAD (Security Association Database): mapping traffic to certain configuration - Working mode (tunnel/transport), encryption and/or authentication, etc.

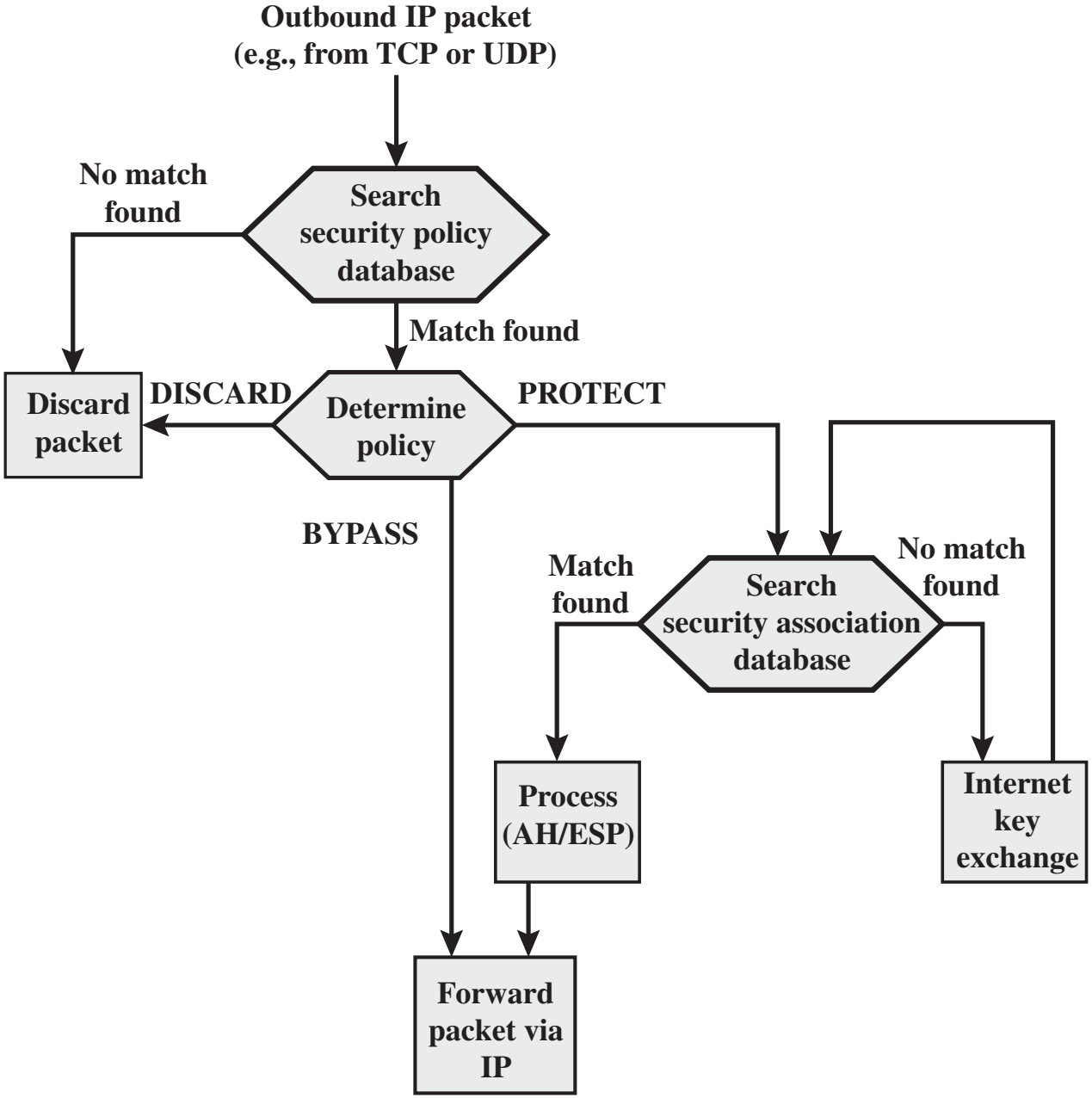
ESP (Encapsulating Security Payload)

- Can provides services like confidentiality data origin, anti-replay, and authentication

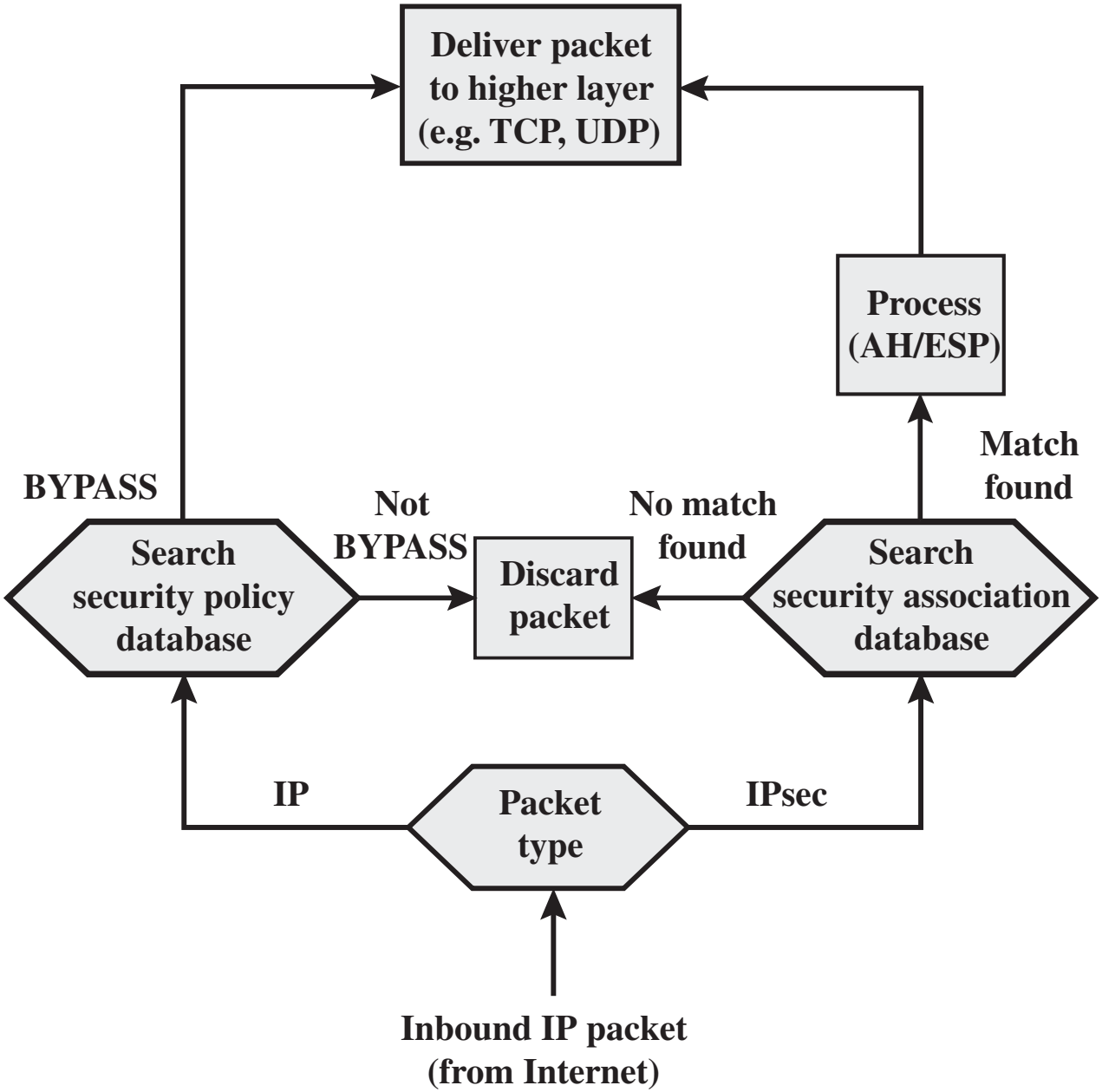


  - SPI: identify a security association in SAD
  - ICV: integrity check value
  - Initialization Value (IV): only needed by CBC- or other encryption mode
  - Optional Traffic Flow Confidentiality (TFC) padding
    - ★ Extra padding (besides 256 bytes) to hide traffic characteristics

Processing Flow for Outgoing Traffic



Processing Flow for Incoming Traffic



Transport vs. Tunnel Mode

- Transport mode (Figure on Left)
  - Protect IP packet payload, primarily for upper-protocols like TCP, UDP
  - Mostly used for end-to-end communication
- Tunnel mode (Figure on Right)
  - Protection for the entire packet
  - Add new outer IP packet with a new outer header
  - Packet travels through a tunnel from point to point in the network