Information Security 11

Web & EC Security

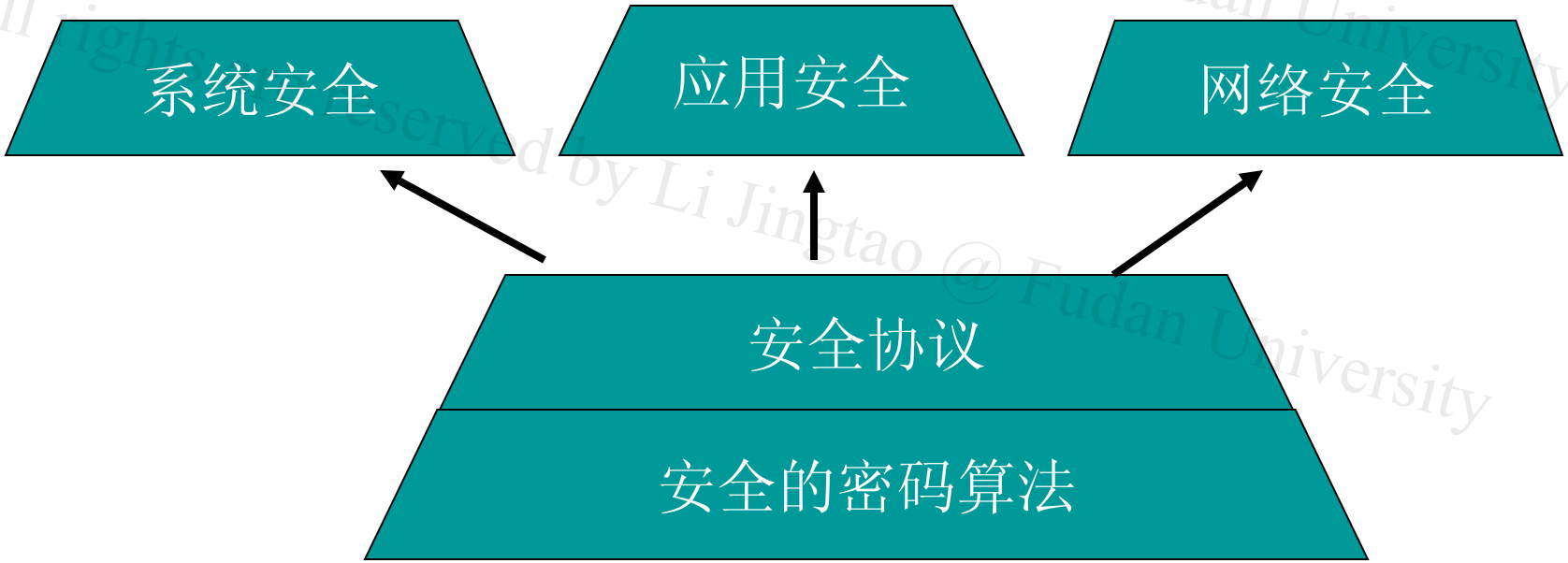
Chapter 17

Review

- Cryptography
- Authentication techniques
- PKI

Review

- Cryptography
- Authentication techniques
- PKI



Review

- **Security services**
  - Confidentiality
  - Integrity
  - Availability
  - Authentication
  - Non-repudiation

Outline

- **Web & EC Security Considerations**
  - **Definitions: web, EC**
  - **threats**
- **Secure Socket Layer (SSL) and Transport Layer Security (TLS)**
- **Secure Electronic Transaction (SET)**

Outline

- **Web & EC Security Considerations**
  - **Definitions: web, EC**
  - **threats**
- **Secure Socket Layer (SSL) and Transport Layer Security (TLS)**
- **Secure Electronic Transaction (SET)**

Web Security

- Web now widely used by business, government, individuals
- but Internet & Web are vulnerable

Web Security Considerations

- The WEB is very visible.
- Complex software hide many security flaws.
- Web servers are easy to configure and manage.
- Web server may be exploited as a launching pad into the intranet.
- Users are not aware of the risks.

Web Security

- So, have a variety of threats

  user *web server*

  – Confidentiality http, etc. plaintext
  – integrity
  – denial of service
  – Authentication

- need added security mechanisms

EC，Electronic Commerce

- Before Web
- electronic funds transfers (or: EFT, wire transfers)
- Electronic data interchange (EDI) occurs
- We mainly consider Internet Activities

从信息安全的发展来看

- 通信保密， 50s, 60s，
- 计算机安全， 70s, 80s
- 信息安全， 80s, 90s
- 信息保障

军用

↓

民用

安全技术 = 军火

出口限制

Web&EC, We Focus on

- **Security**
  - Confidentiality
  - integrity
  - denial of service
  - Authentication
- **Privacy**
- **Legal issues**

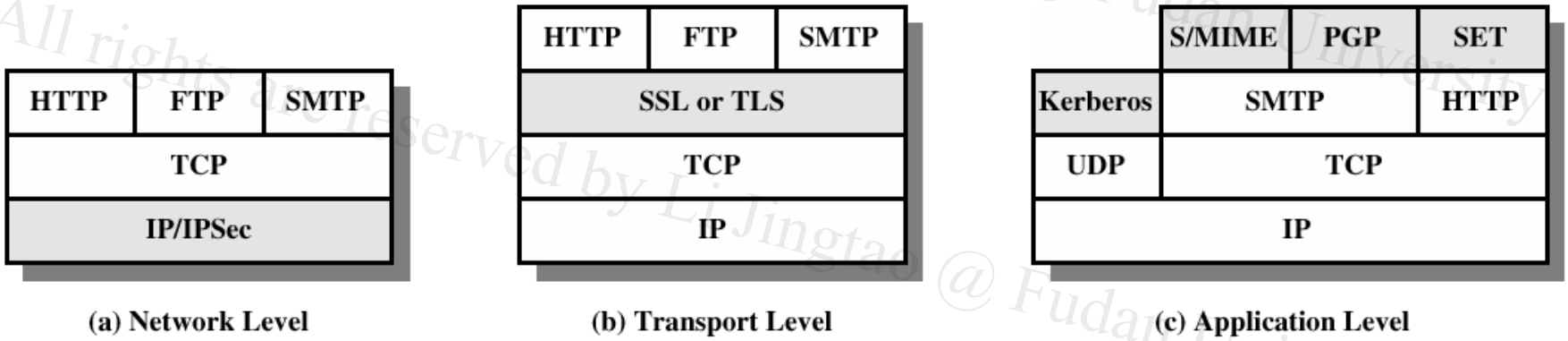
Outline

- Web & EC Security Considerations
  - Definitions: web, EC
  - threats
- **Secure Socket Layer (SSL) and Transport Layer Security (TLS)**
- Secure Electronic Transaction (SET)

Where to Secure

- *Q: If security mechanisms in application layer have been implemented. Security is needed in network level? Or vice versa?*
  - have a range of application specific security mechanisms
    - eg. S/MIME, PGP, Kerberos,
  - would like security implemented by the network for all applications
    - **SSL/HTTPS**
    - **IPSEC**

Security facilities in TCP/IP



(a) Network Level (b) Transport Level (c) Application Level

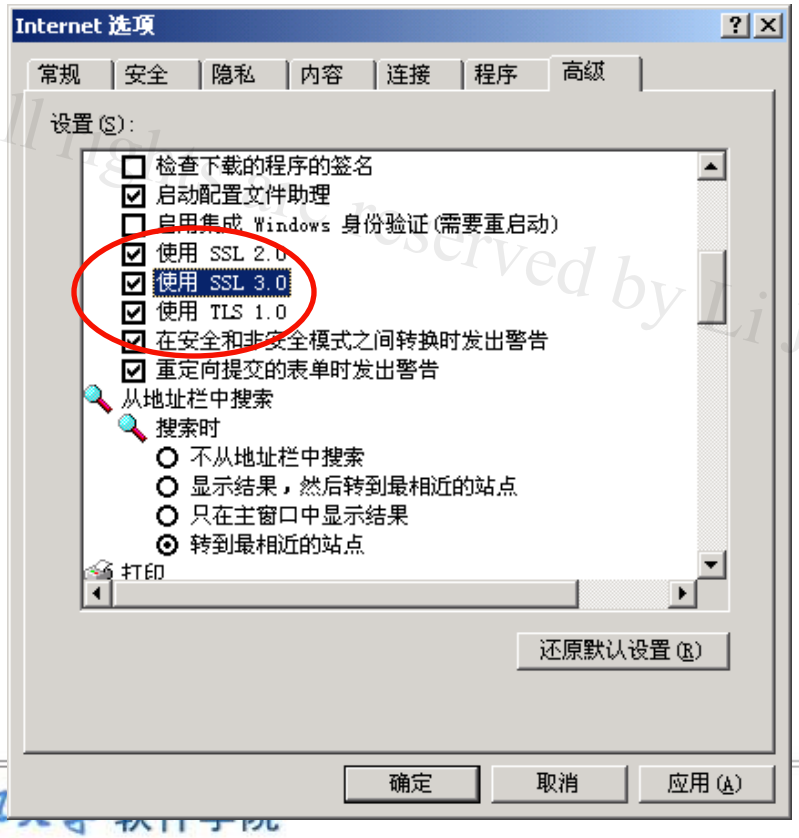
SSL and TLS

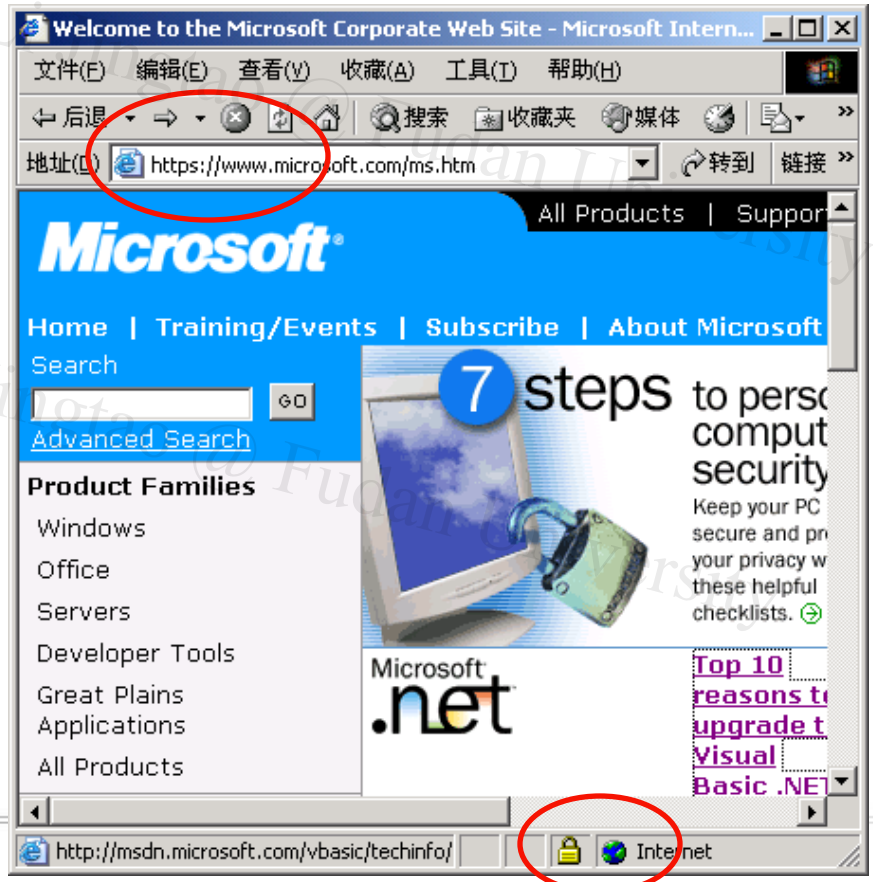
- originally developed by Netscape
- subsequently became Internet standard known as TLS (Transport Layer Security)
- TLS working group was formed within IETF

- SSL has two layers of protocols
- First version of TLS V1.0 (1999) can be viewed as an SSLv3.1

SSL/TLS协议

- 协议的设计目标
  - 为两个通讯个体之间提供保密性,数据完整性,身份认证
  - 互操作性、可扩展性、相对效率
- 协议的使用





An example

test

http://www.icbc.com.cn/index.jsp

SSL Architecture

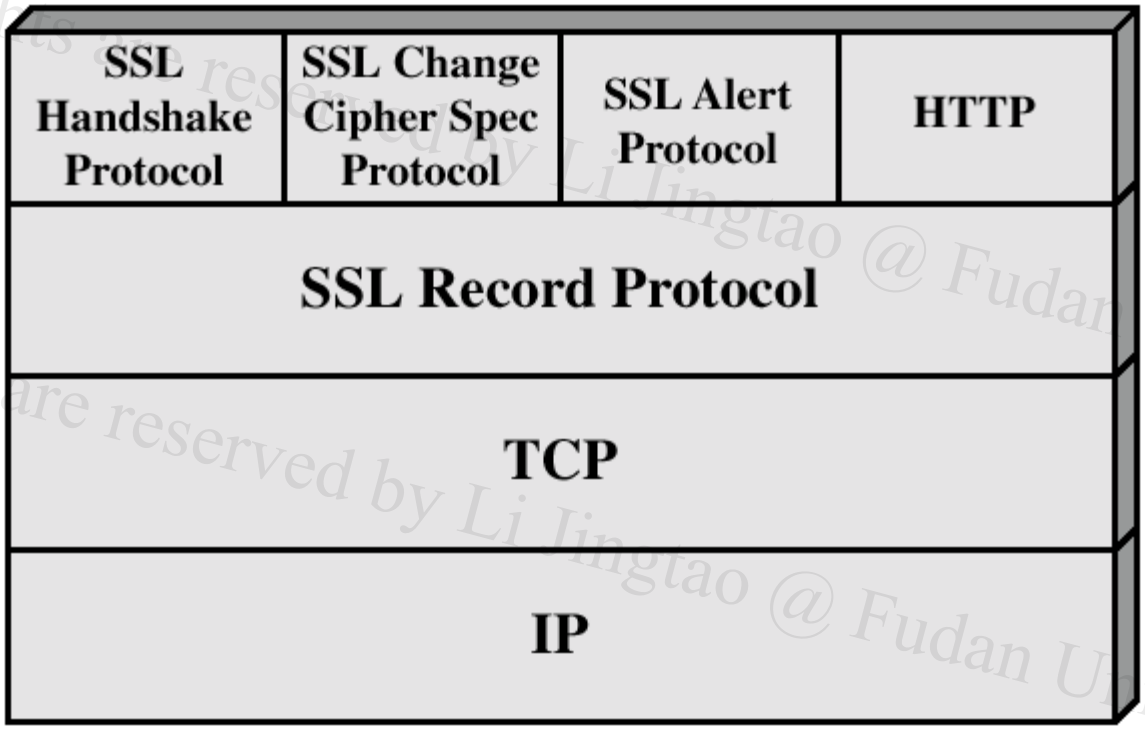


Figure 7.2 SSL Protocol Stack

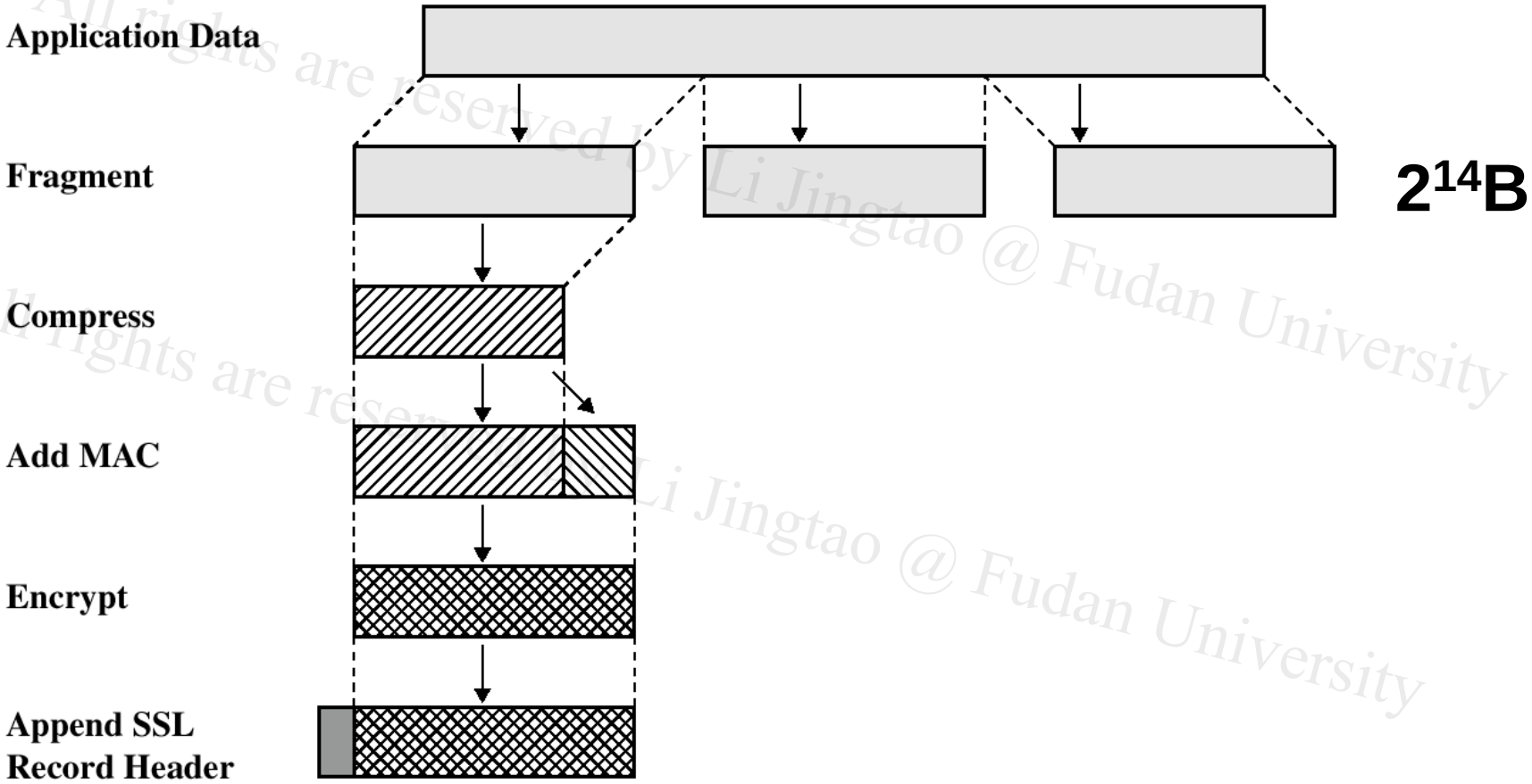
SSL/TLS概况

- 协议分为两层
  - 底层：ssl记录协议
  - 上层：ssl握手协议、ssl密码变化协议、ssl警告协议
- ssl记录协议
  - 建立在可靠的传输协议(如TCP)之上
  - 它提供连接安全性，有两个特点
    - 保密性，使用了对称加密算法
    - 完整性，使用MAC算法
  - 用来封装高层的协议
- ssl握手协议 -最复杂
  - 客户和服务器之间相互认证
  - 协商加密算法和密钥
  - 它提供连接安全性，有三个特点
    - 身份认证，至少对一方实现认证，也可以是双向认证
    - 协商得到的共享密钥是安全的，中间人不能够知道
    - 协商过程是可靠的

SSL 工作流程

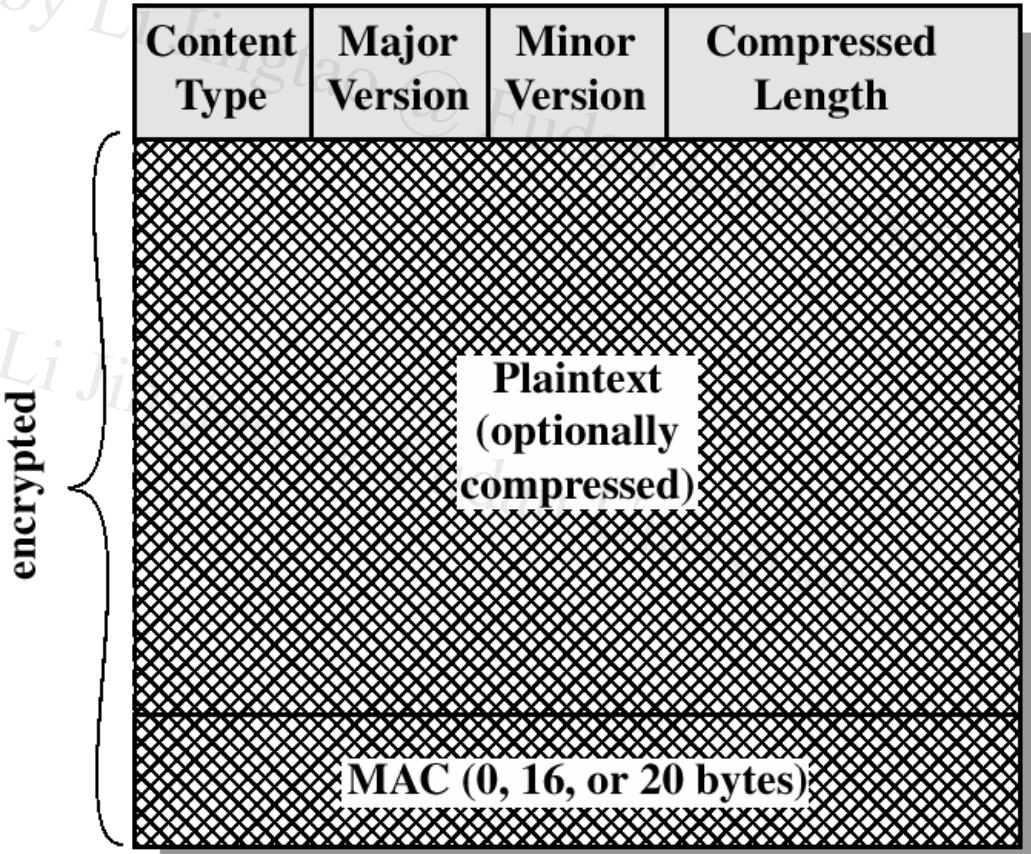
- 先握手
  - 单向身份认证，双向认证（可选）
  - 协商SSL会话的密钥等参数
- SSL记录协议
  - 加密会话数据
  - 提供完整性、保密性支持
- 什么是会话？
  - Session identifier、Peer certificate、
  - Compression method、……

SSL Record Protocol Operation



SSL Record Format

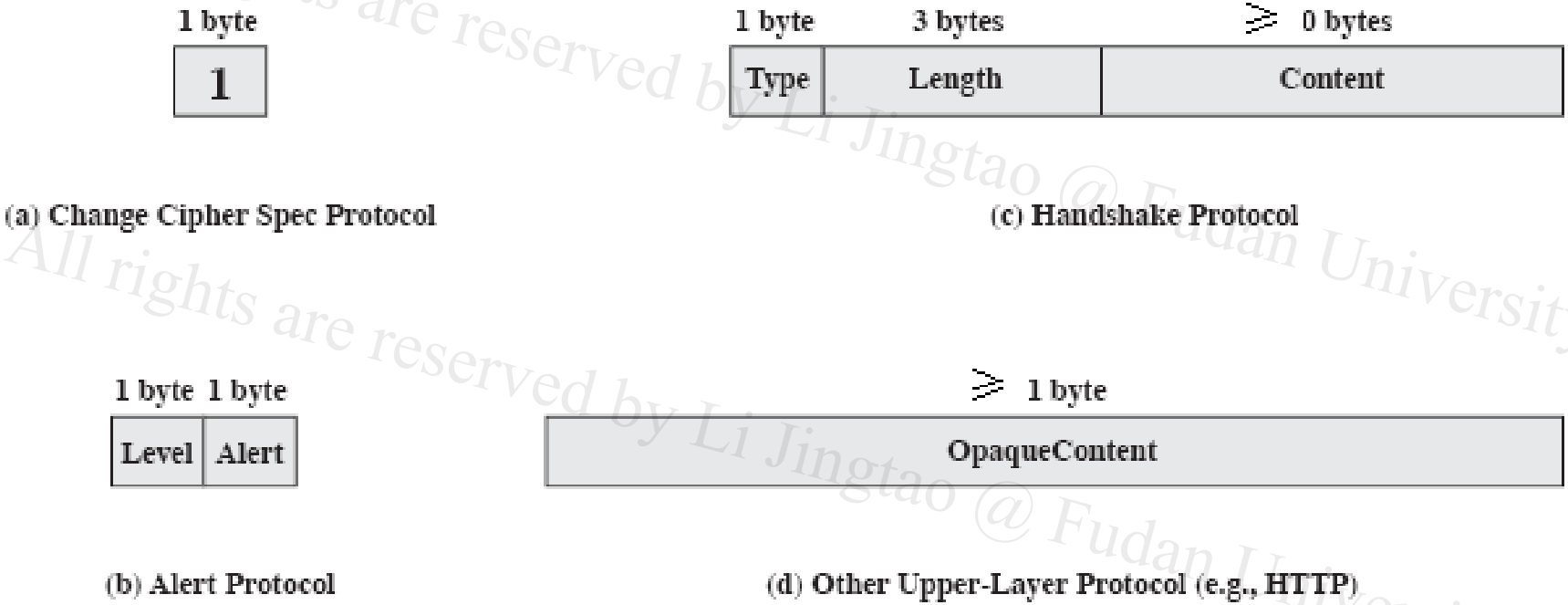
```
struct {
        ContentType type;          —— 8位，上层协议类型
        ProtocolVersion version;   —— 16位，主次版本
        uint16 length;             —— 加密后数据的长度，
                                      不超过2^14+2048字节
      EncryptedData fragment;      —— 密文数据
    } SSLCiphertext;
```



SSL Record Protocol Services

- **message integrity**
  - using a MAC with shared secret key
  - similar to HMAC but with different padding
- **confidentiality**
  - using symmetric encryption with a shared secret key defined by Handshake Protocol
  - AES, IDEA, RC2-40, DES-40, DES, 3DES, Fortezza, RC4-40, RC4-128
  - message is compressed before encryption

SSL Record Protocol Payload



Handshake Protocol

- The most complex part of SSL.
- Allows the server and client to authenticate each other.
- Negotiate encryption, MAC algorithm and cryptographic keys.
- Used before any application data are transmitted.

SSL握手协议的流程

- 交换Hello消息，对于算法、交换随机值等协商一致

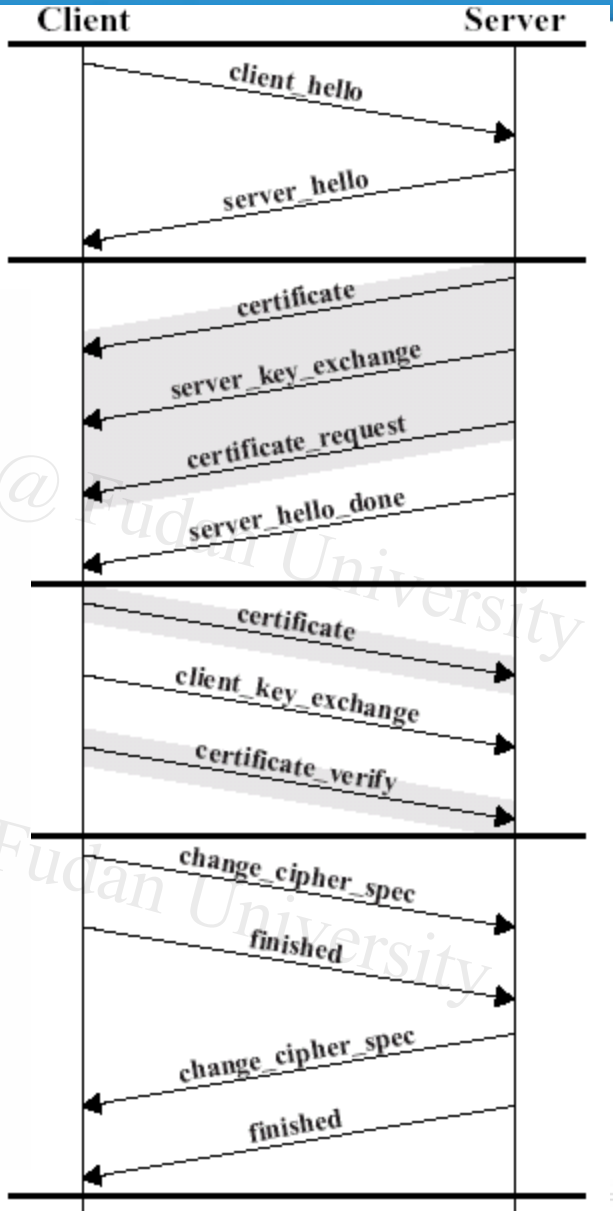
client_hello消息，包

版本、随机数(32位时
随机序列)、会话ID、
密码算法列表(Ciphe
支持的压缩方法列表

Phase 2
Server may send certificate, key exchange, and request certificate. Server signals end of hello message phase.

Phase 3
Client sends certificate if requested. Client sends key exchange. Client may send certificate verification.

Phase 4
Change cipher suite and finish handshake protocol.



TLS (Transport Layer Security)

- The same record format as the SSL record.
- IETF standard RFC 2246, similar to SSLv3
- with minor differences
  - in record format version number
  - uses HMAC for MAC
  - has additional alert codes
  - some changes in supported ciphers
  - changes in certificate types & negotiations
  - changes in crypto computations & padding

Outline

- Web & EC Security Considerations
  - Definitions: web, EC
  - threats
- Secure Socket Layer (SSL) and Transport Layer Security (TLS)
- **Secure Electronic Transaction (SET)**

Secure Electronic Transactions

- An open encryption and security specification.
- Protect credit card transaction on the Internet.
- developed in 1996 by Mastercard, Visa etc
- Companies involved:
  - MasterCard, Visa, IBM, Microsoft, Netscape, RSA, and Verisign
- Not a payment system.
- Set of security protocols and formats.

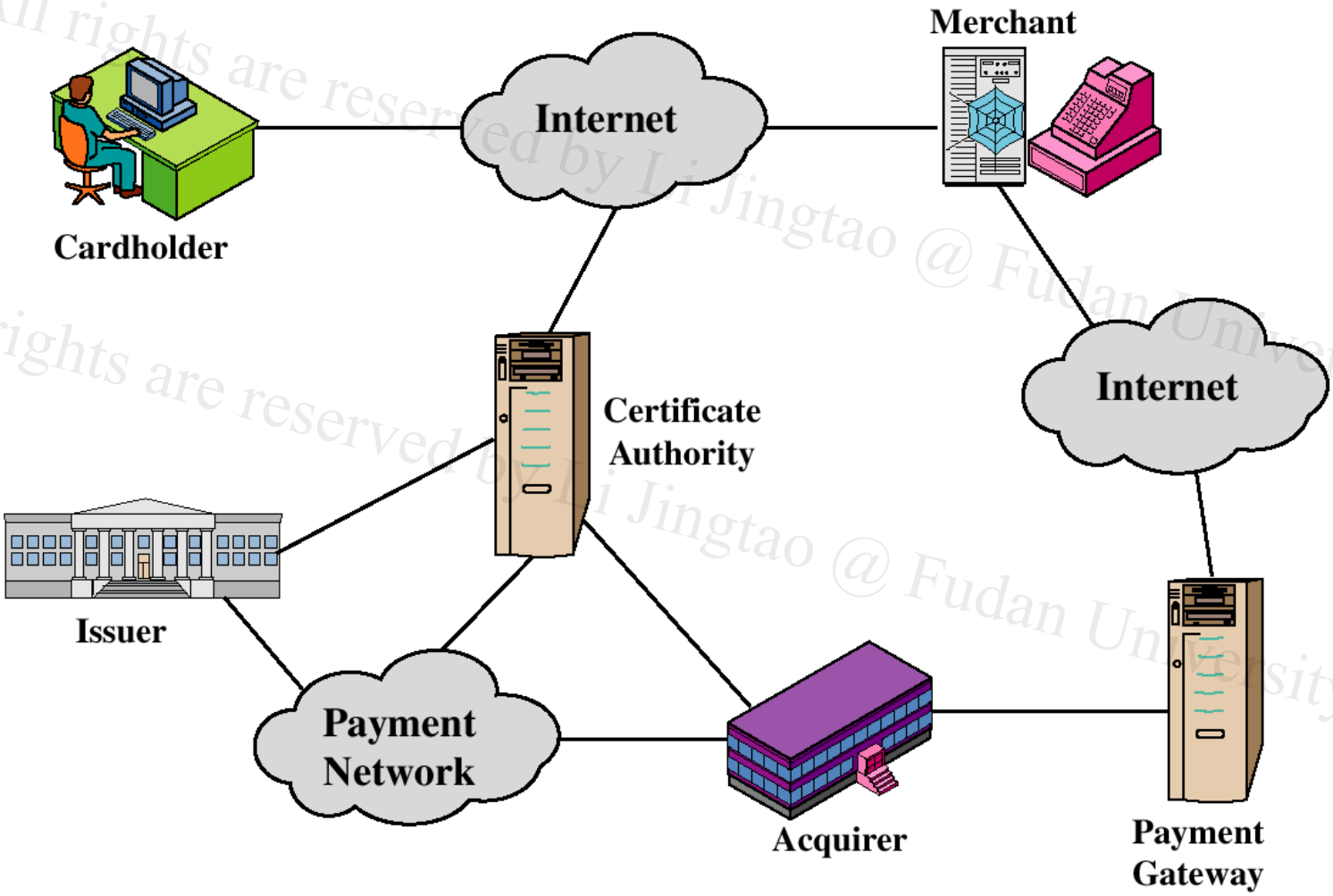
SET Services

- Provides a secure communication channel in a transaction.
- Provides tust by the use of X.509v3 digital certificates.
- Ensures privacy.
  - by restricted info to those who need it

SET Overview

- Key Features of SET:
  - Confidentiality of information
  - Integrity of data
  - Cardholder account authentication
  - Merchant authentication

SET Participants

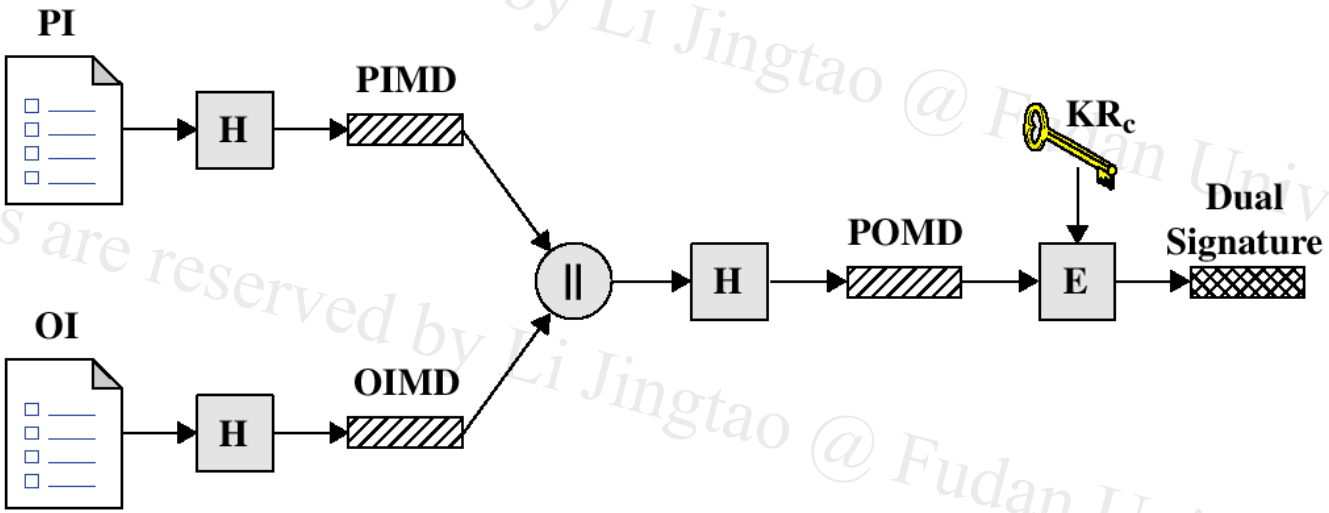


Sequence of events for

1. The customer opens an account.
2. The customer receives a certificate.
3. Merchants have their own certificates.
4. The customer places an order.
5. The merchant is verified.
6. The order and payment are sent.
7. The merchant request payment authorization.
8. The merchant confirm the order.
9. The merchant provides the goods or service.
10. The merchant requests payments.

Dual Signature

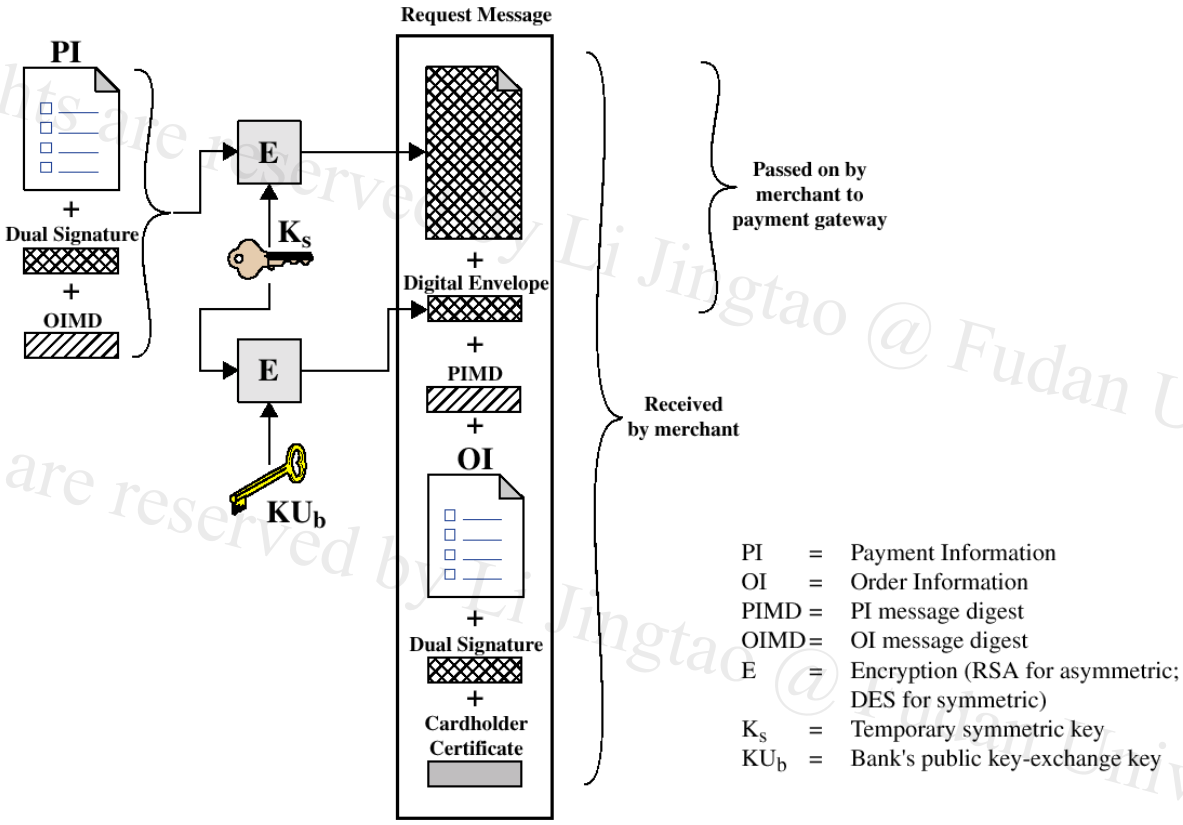
$$DS = E_{KR_c}[H(H(PI) \| \mathrm{H(OI)})]$$



PI = Payment Information
OI = Order Information
H = Hash function (SHA-1)
|| = Concatenation

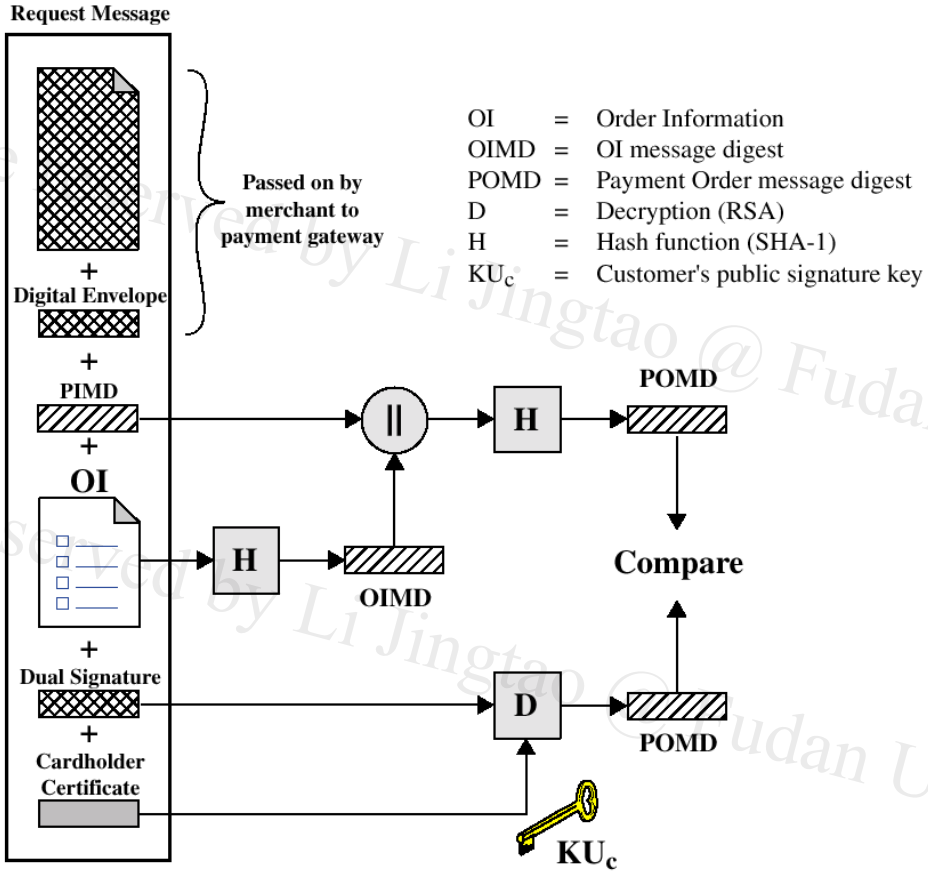
PIMD = PI message digest
OIMD = OI message digest
POMD = Payment Order message digest
E = Encryption (RSA)
KR_c = Customer's private signature key

Payment processing



Cardholder sends Purchase Request

Payment processing



Merchant Verifies Customer Purchase Request

Payment processing

- Payment Authorization:
  - Authorization Request
  - Authorization Response
- Payment Capture:
  - Capture Request
  - Capture Response

电子商务立法的背景

- 电子商务独特的运作方式
  - 向现有的商务规范模式提出了技术、财务和交易安全等方面的重大挑战；
  - 没有法律规范的电子商务将难以正常发展；
  - 及时制定并出台相应的法律法规，鼓励、引导维护电子商务沿着健康轨道发展，成为当前我国立法工作的一项重要任务。

世界电子商务立法基本情况

- 联合国贸易法委员会《电子商务示范法》和《电子签名统一规则》
- 美国《国际与国内商务电子签章法》，2000年
- 欧盟《电子签名统一框架指令》
- 新加坡《电子交易法》
- 中国台湾的《电子签章法》
- 韩国《电子商务基本法》
  - 具有借鉴意义的比较全面的法规
- 日本《电子签名与认证服务法》
- 澳大利亚《电子交易法》
- 马来西亚《数字签名法》

我国电子商务法律发展现状

- 电子商务交易安全的法律保护问题，涉及到两个基本方面:
  - 第一，电子商务交易首先是一种商品交易，其安全问题应当通过民商法加以保护；
  - 第二，电子商务交易是通过计算机及其网络而实现的，其安全与否依赖于计算机及其网络自身的安全程度。
- 电子签名法草案已经在2004年4月2日提请十届全国人大常委会第八次会议审议，有望获得与传统手写签名和盖章同等的法律效力

商用密码管理条例

- 目的：加强商用密码管理，保护信息安全，保护公民和组织的合法权益，维护国家的安全和利益。

- 管理机构：国家密码管理委员会及其办公室（国密办）主管全国的商用密码管理工作。自治区、直辖市负责密码管理的机构根据国密斑的委托，承担商用密码的有关管理工作

- 商用密码技术属于国家秘密，国家对商用密码产品的科研、生产、销售和使用实行专控管理。