



# 信息系统安全

## 网络安全

### 安全协议与WEB安全

陈春华 博士

chunhuachen@scut.edu.cn

2018 春季  
华南理工大学 软件学院

# 内容概要

---

- 密码系统回顾
  - 对称与非对称
- 密钥配送问题
- 混合密码系统
- 安全协议
  - 认证
  - 密钥协商协议
  - 认证及密钥协商协议
- 应用

# 安全协议

---

- 所谓协议，就是两个或者两个以上的参与者完成某项特定的任务而采取的一系列步骤。
- 安全协议是建立在某种体系（密码体制）基础上且提供安全服务的一种交互通信的协议，它运行在计算机网络或者分布式系统中，借助特定算法来达到身份认证、密钥分配等目的。
  - 参与实体可能是可以信任的，也可能是攻击者和完全不信任的实体

# 基本安全协议

---

- 认证协议

- 提供一个参与方关于其通信对方身份的一定确信度，比如**A**通过认证协议，确信参与协议的实体为身份**B**的拥有者

- 密钥交换协议

- 在参与协议的两个或者多个实体之间建立共享的秘密（又称为会话密钥）

- 认证及密钥交换协议

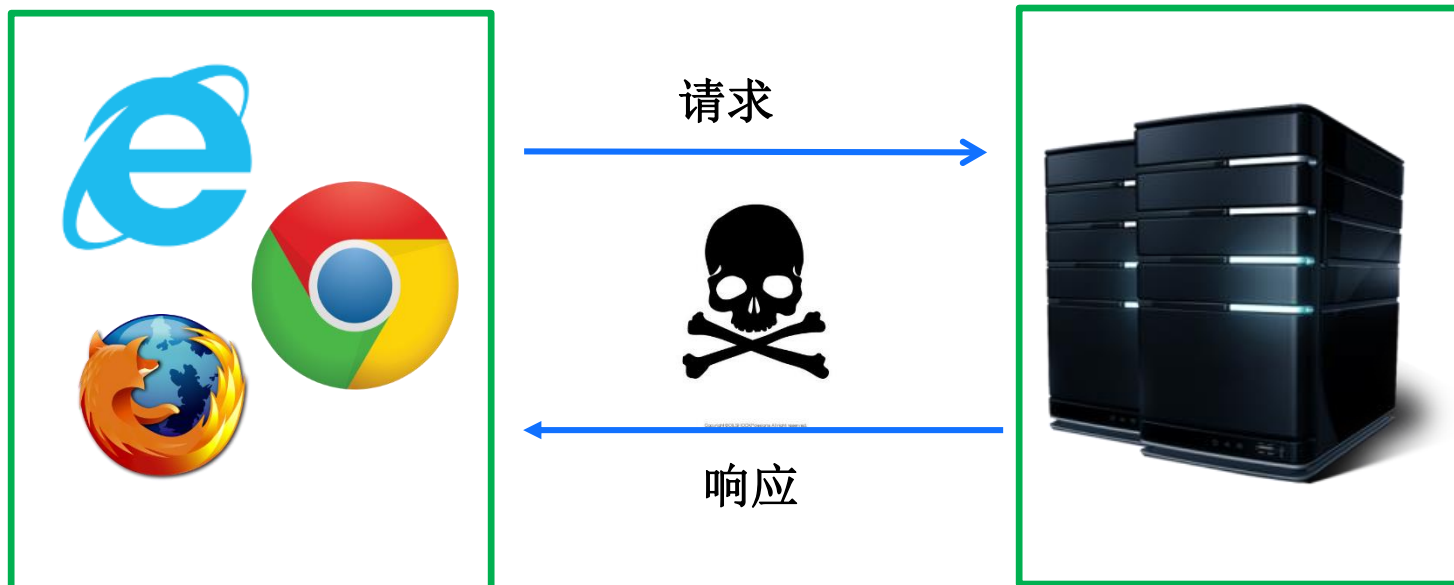
- 为身份已经确认的参与方建立一个共享秘密

# 认证协议及其他

---

- 参考：
  - 第7章@ 《基于案例的网络安全技术与实践》  
朱宏锋等著，清华大学出版社
  - 上课时使用板书！

# 网上购物-WEB通信安全模型



WEB/HTTP

# 网上购物-浏览商品



The screenshot shows the Taobao.com homepage. At the top is a navigation bar with links for '我的淘宝' (My Taobao), '购物车' (Shopping Cart), '收藏夹' (Favorites), '商品分类' (Product Categories), '卖家中心' (Seller Center), '联系客服' (Contact Customer Service), and '网站导航' (Site Navigation). Below this is the main header area featuring the '淘宝网' (Taobao.com) logo, a search bar with the text '愚人节，整的就是你!' (April Fool's Day, messing with you!), and a QR code for mobile access. The main content area is divided into several sections: '淘宝特色服务' (Taobao Special Services) on the left, a central banner for '淘宝买房省的!' (Taobao Buying Property is Cheaper!) with a '魅族 青年良品 699元 开售' (Meizu Youth Good Product 699 Yuan On Sale) advertisement, and a right sidebar with '公告' (Announcements), '规则' (Rules), '论坛' (Forum), '安全' (Security), and '公益' (Public Welfare) links. The bottom of the page features a '便民服务' (Convenient Services) section with links for '登录' (Login), '免费注册' (Free Registration), and '免费开店' (Free Store Opening).



# 网上购物-登录

https://login.taobao.com/member/login.jhtml?redirectURL=https%3A%2F%2Flist.taobao.com%2Fitemlist%2Fdefault.htm%3Fspm%3Da2106.2206569.0.0.QdUJVB%26cat%3D500

login.taobao.com

已验证身份

权限 连接

该网站的身份已通过VeriSign Class 3 Secure Server CA - G3的验证, 但没有公开审核记录。  
[证书信息](#)

与 login.taobao.com 的连接采用 128 位加密技术。但是, 此页中包含其他不安全的资源。他人能在传输过程中查看这些资源, 攻击者也可以进行修改, 从而改变网页的外观。

该连接使用 TLS 1.2。

该连接是使用 RC4\_128 进行加密的, 同时使用 SHA1 进行讯息身份验证并使用 RSA 作为密钥交换机制。

**网站信息**  
您以前从未访问过此网站。

证书

常规 详细信息 证书路径

**证书信息**

这个证书的目的如下:

- 保证远程计算机的身份
- 向远程计算机证明您的身份

\* 有关详细信息, 请参考证书颁发机构的说明。

颁发给: \*.taobao.com

颁发者: VeriSign Class 3 Secure Server CA - G3

有效期从 2013/ 3/ 30 到 2014/ 4/ 18

[了解证书的详细信息](#)

[颁发者说明\(S\)](#)

确定

https://login.taobao.com/.....

手机扫码, 快速登录  
请使用淘宝客户端扫描

刷新

登录名: 手机动态密码登录

手机号/会员名/邮箱

登录密码: [忘记登录密码?](#)

☐ 安全控件登录

登 录

微博登录 | 支付宝登录 免费注册



# 网上购物-继续浏览商品



The screenshot displays the Taobao.com homepage. At the top, the address bar shows the URL `www.taobao.com/?spm=a2106.m5058.1581860521.1.fXTUVz`. Below the address bar, the Taobao logo and navigation links are visible. The main navigation bar includes categories like 宝贝 (Items), 搜索 (Search), and 更多 (More). The left sidebar lists various product categories under '商品服务分类' (Product Service Classification). The main content area features a large banner for '戴玉堂' (Dai Yutang) with the text '指尖上的戴玉堂!' (Dai Yutang on the fingertips!). To the right of the banner, there is a section titled '斗小三神器' (Weapon for fighting off a mistress) with a book cover image. The bottom of the page shows a navigation bar with links to 天猫 (Tmall), 聚划算 (Juhuasuan), 超市 (Supermarket), 拍卖 (Auction), 一淘 (Yitao), 电器城 (Appliance City), Hitao妆扮 (Hitao Makeup), 旅行 (Travel), 云手机 (Cloud Phone), and 特色中国 (Special China).

## 网上购物-准备支付



buy.taobao.com/auction/buy\_now.jhtml

http://www.buy.taobao.com/auction/buy\_now.jhtml

tb3153445\_00 消息 手机逛淘宝 淘宝网首页 我的淘宝 购物车0 收藏夹 商品分类 卖家中心 联系客服 网站导航

**淘宝网**


1. 确认订单信息 2. 付款到支付宝 3. 确认收货 4. 双方互评

确认收货地址 [管理收货地址](#)

寄送至 广东省 广州市 番禺区 华工大学城校区B8-203 (陈春华 收) 15013153445 [修改本地址](#)

[使用新地址](#)

确认订单信息

店铺宝贝	单价(元)	数量	优惠方式(元)	小计(元)
店铺: 平墨斋国画店 卖家: 平墨斋真品画廊 <a href="#">和我联系</a> <a href="#">点击这里联系卖家!</a>  纯手绘兰花斗方国画山水画书画写意画花鸟画客厅... 卖家承诺7天内发货	40.00	<input type="text" value="1"/>	省30元:十元秒杀	10.00
给卖家留言: <input type="text" value="选填: 对本次交易的补充说明"/>	运送方式: 快递 8.00元		8.00	
发货时间: 卖家承诺订单在买家付款后, 7天内发货				
运费险: <input type="checkbox"/> 购买退货运费险, 退货可赔付9元 [?]		0.60		
店铺合计(含运费): ¥18.00				

☐ 找人代付 ☐ 匿名购买 ☐ 信用卡分期付款

实付款: ¥18.00

寄送至: 广东省 广州市 番禺区 华工大学城校区B8-203  
收货人: 陈春华 15013153445

**提交订单**

若价格变动, 请在提交订单后联系卖家改价, 并查看已买到的宝贝

# 网上购物-安全支付链接



淘宝网



正在创建支付宝安全链接...

正在创建支付宝安全链接??

https://cashier.alipay.com/standard/payment/cashier.htm?outBizNo=2014040111001001890049066581&timeStamp=12062321504478&bizId=...&trade=100018&orderId=040187...

cashier.alipay.com  
已验证身份

权限 连接

该网站的身份已通过VeriSign Class 3 Secure Server CA - G3的验证,但没有公开审核记录。  
[证书信息](#)

与 cashier.alipay.com 的连接采用 128 位加密技术。

该连接使用 TLS 1.0。

该连接是使用 RC4\_128 进行加密的,同时使用 SHA1 进行消息身份验证并使用 RSA 作为密钥交换机制。

网站信息  
您以前从未访问过此网站。  
[这分别意味着什么?](#)

https://cashier.alipay.com/...  
支付宝 | 我的收银台 中国大陆版

保 您正在使用支付宝担保交易

淘宝网 | 纯手绘兰花斗方国画山水画书画写意画花鸟... 卖家昵称: 平墨斋

余额宝支付立减, 订单满百即可参与, 免单金

支付宝账户( 15013153445 ) 可支付余额: 0.00 元 使用支付宝购物卡

余额宝可用金额 0元 立即转入 资金转入余额宝, 天天可赚收益, 还能随时支付

您的账户没有可支付余额, 请使用以下其他方式付款, 或充值后付款

付款方式: 储蓄卡 信用卡 扫码支付 现金或刷

快捷支付 72小时100%赔付 惠 每天都有银行优惠 积 银行积分当钱花 畅

中国农业银行 AGRICULTURAL BANK OF CHINA  
中国工商银行 INDUSTRIAL AND COMMERCIAL BANK OF CHINA  
中国建设银行 China Construction Bank  
中国邮政储蓄银行 POSTAL SAVINGS BANK OF CHINA  
中国银行 BANK OF CHINA  
招商银行 CHINA MERCHANTS BANK  
交通银行 BANK OF COMMUNICATIONS  
浦发银行 SPD BANK  
中国光大银行 CHINA EVERLIGHT BANK  
中信银行 CHINA CITIC BANK  
平安银行 PINGAN BANK  
中国民生银行 CHINA MINSHENG BANKING CORP., LTD.  
华夏银行 HUAXIA BANK  
广发银行 GGB  
兴业银行 INDUSTRIAL BANK CO., LTD.  
选择其他

下一步

证书  
常规 详细信息 证书路径

证书信息

这个证书的目的如下:

- 保证远程计算机的身份
- 向远程计算机证明您的身份

\* 有关详细信息, 请参考证书颁发机构的说明。

颁发给: \*.alipay.com

颁发者: VeriSign Class 3 Secure Server CA - G3

有效期从 2013/ 12/ 14 到 2015/ 2/ 13

[颁发者说明\(S\)](#)

了解证书的详细信息

确定



https://katongweb.alipay.com/express/expressTrade.htm?payAmount=248.00&useUnityLimit=true&channelType=DEBIT\_EXPRESS&orderDetailUrl=http%3A%2F%2Fcashier-pc

katongweb.alipay.com

已验证身份

权限 连接

该网站的身份已通过VeriSign Class 3 Secure Server CA - G3的验证, 但没有公开审核记录。  
[证书信息](#)

与 katongweb.alipay.com 的连接采用 128 位加密技术。  
  
该连接使用 TLS 1.0。  
  
该连接是使用 RC4\_128 进行加密的, 同时使用 SHA1 进行讯息身份验证并使用 RSA 作为密钥交换机制。

网站信息  
您以前从未访问过此网站。  
  
[这分别意味着什么?](#)

支付宝 | 收银台

保

您正在使用支付宝担保交易

淘宝网 | 和田青白玉一夜《叶》暴富貔貅手链, 买一送一 卖家昵称: letao9999

付款方式: 

中国工商银行

 储蓄卡 

快捷支付

安全设置检测成功! 付款环境安全可靠。

请填写以下信息用于实名认证。

姓名: 

付款银行卡的开户姓名

选择生僻字

证件: 

身份证

储蓄卡卡号:

手机号码: 

此卡在银行预留的手机号码

付款校验码: 

免费获取

☒ 开通快捷支付, 下次可凭银行卡信息快速付款。

☒ 开通余额宝, 同意《余额宝服务协议》《天弘基金管理有限公司网上交易...》

为保障支付宝账户安全, 请设置支付宝支付密码。

设置支付宝支付密码: 

6-20位英文字母、数字和字符的组合, 区分大小写。

确认密码:

同意协议并付款

《支付宝快捷支付服务协议》

证书

常规 详细信息 证书路径

证书信息

这个证书的目的如下:

- 保证远程计算机的身份
- 向远程计算机证明您的身份

\* 有关详细信息, 请参考证书颁发机构的说明。

颁发给: \*.alipay.com

颁发者: VeriSign Class 3 Secure Server CA - G3

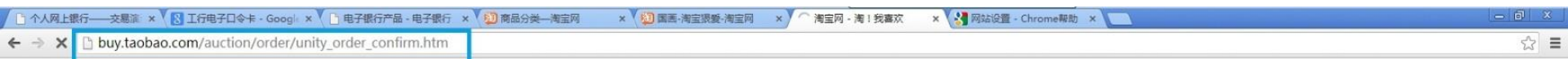
有效期从 2013/ 12/ 14 到 2015/ 2/ 13

颁发者说明(S)

了解证书的详细信息

确定

- 采用银行卡支付国际安全标准



淘宝网



正在创建支付宝安全链接...

<http://buy.taobao.com> --> <https://cashier.alipay.com> --> <https://katongweb.alipay.com>

1. confidentiality
2. authenticity

浏览器

SSL/TLS 安全通道

alipay.com  
服务器

[https](https://) = http + SSL/TLS

# 传输层安全通信协议

---

- 传输层：提供主机中两个进程之间的逻辑通信
- 网络层：提供主机与主机之间的逻辑通信
- 在传输层提供安全机制的优点在于：
  - 不需要强制为每一个应用做安全方面的改进
  - 可为不同的应用配置不同的安全策略
- 在传输层提供安全通信服务的机制主要有
  - 安全套接层协议（**Secure Socket Layer, SSL**）
  - 又称为传输层安全协议（**Transport Layer Secure, TLS**）



# SSL与TLS概述

---

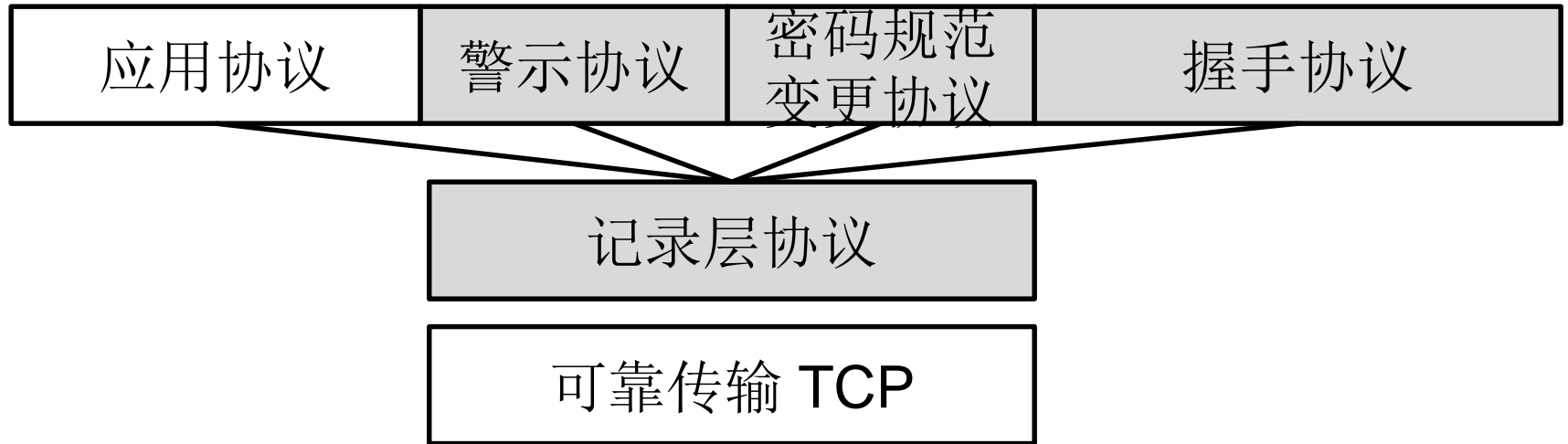
- 1995年, Netscape公司, SSL2.0
  - 在浏览器Netscape 1.1中加入SSL, 以保护浏览器和web服务器之间重要数据的传输。
- 1996年, Netscape公司, SSL3.0
  - 事实工业标准, 大多数浏览器和web服务器支持
- 1997年, IETF基于SSL3.0发布了TLS1.0规范
  - SSL3.0与TLS协议极其相似, 这里不做区别, 统称为SSL/TLS

# SSL与TLS概述

HTTP	FTP	SMTP	其他
SSL 或者 TLS			
TCP			

- **SSL/TLS**位于应用层与传输层之间，并建立在可靠连接（**TCP**）之上
- 其设计目标是为应用提供防止窃听，篡改，消息伪造等攻击
- 对用户/应用来说，**SSL/TLS**是可选层

# SSL/TSL分层模型



- 从结构上分：记录层以及记录层上承载的不同消息类型（来自不同的上层协议）
- 应用协议，指使用可靠数据传输服务**TCP**的网络应用协议，如**web/HTTP**

# SSL/TLS分层模型

---

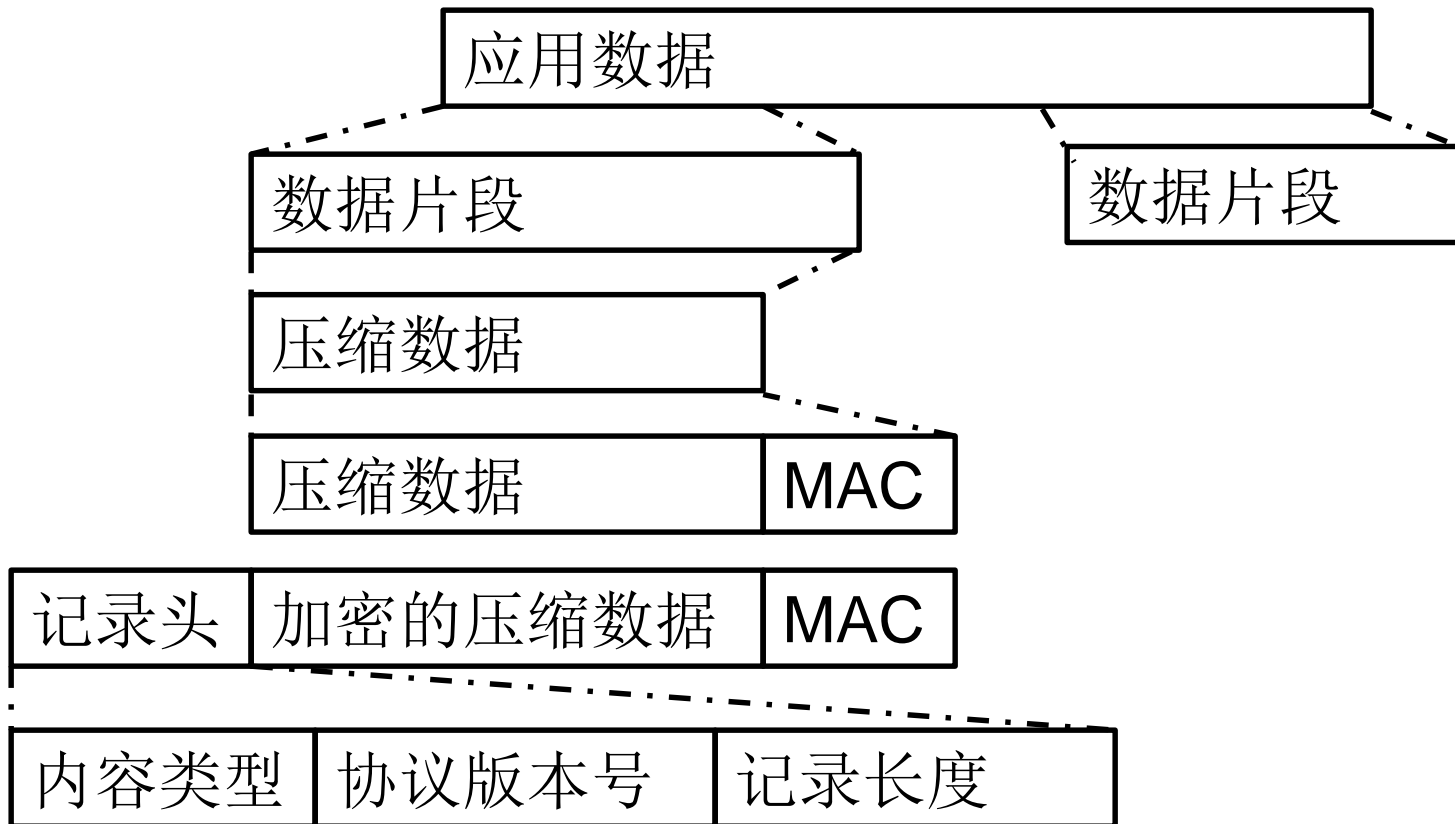
- SSL/TLS连接分为两个阶段，即握手与数据传输阶段
- 握手阶段：对服务器进行认证并确立用于保护数据传输的加密密钥，必须在传输任何应用数据之前完成握手（握手协议-认证及密钥交换）
- 数据传输阶段：一旦握手完成，数据就被分成一系列经过保护的记录（记录层封包）进行传输。

# 记录协议

---

- 在SSL/TLS中，实际的数据传输是使用记录层协议来实现的。
- 记录层协议将高层协议数据看做协议数据单元（载荷），为提供分片，压缩，计算MAC，加密和封装服务，形成记录，并将记录交给TCP
- 由此，记录层协议实际上是高层协议的载体，通信的保密性和完整性是有这一层来保证的。

# 记录层协议

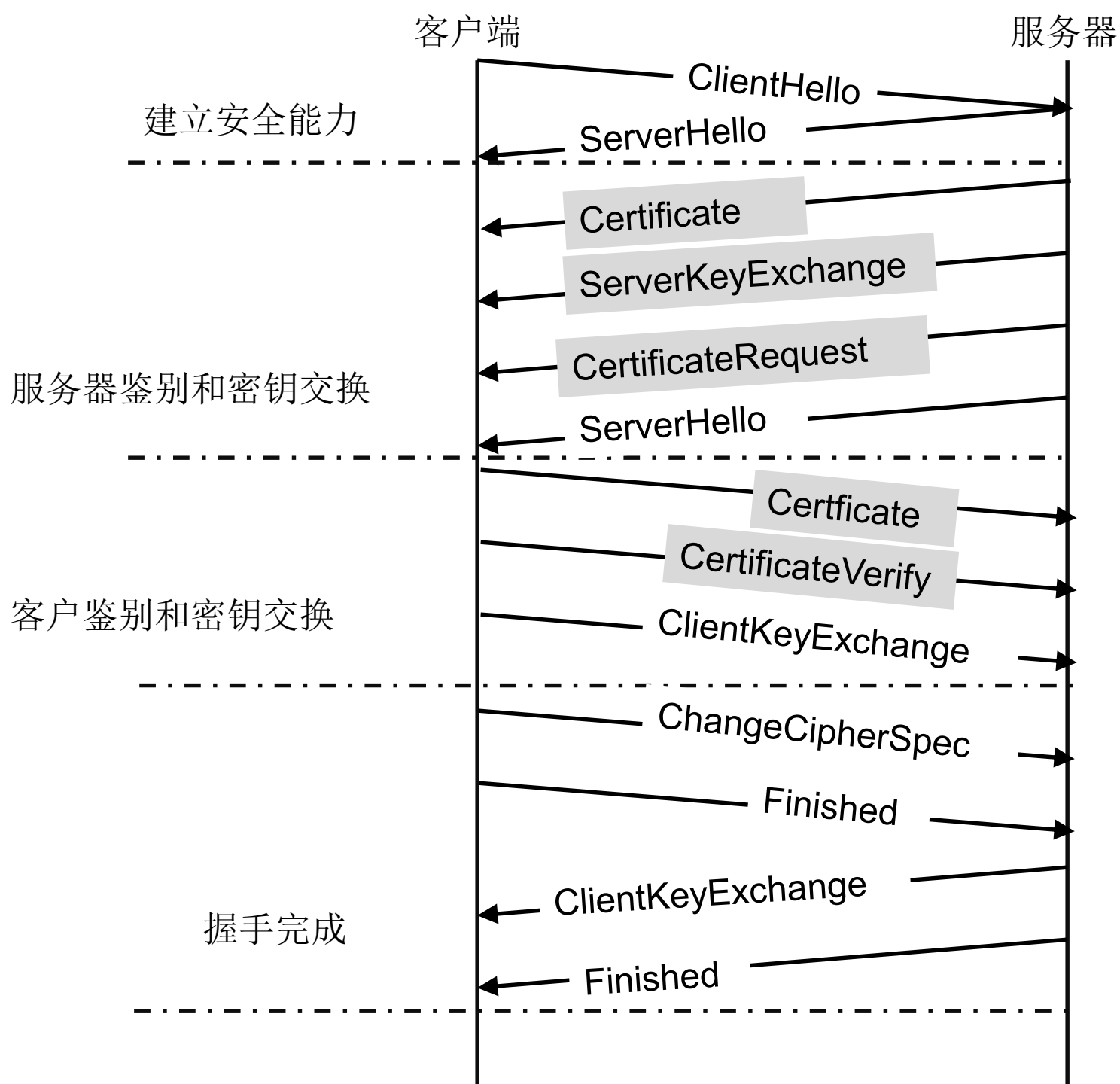


# 握手协议

---

- 在**SSL/TLS**客户端与服务器端之间鉴别双方身份，协商加密算法和密钥参数，为建立一条安全的通信连接做好准备。
- 在实际应用中（尤其是**HTTPS**），由于终端用户缺少数字证书，**SSL/TLS**仅实现服务器端的认证
  - 用户如何认证？在**SSL/TLS**安全通道中使用用户/密码认证机制





# ClientHello

---

- 请求建立连接，客户端发送**ClientHello**消息，该消息的目的是向服务器传输连接首先项：
  - **Client\_version**: 所能支持的SSL/TLS最高版本号
  - **Random**: 包含客户端生成一个32字节随机结构，其中4个字节为日期与时间戳。
  - **Session\_id**: 先前安全连接的id，用于重复使用对应连接的安全参数；或为null，表示希望建立新的安全参数
  - **Cipher\_suite**: 客户端支持的密码算法组合的列表，按优先选择次序排列；由服务器决定使用何种算法，如果服务器不支持，将返回握手失败警告并关闭连接
  - **Compression\_methods**: 支持的压缩算法

# ServerHello

---

- 如果接受客户的安全连接建立请求，返回ServerHello消息：
  - **Server\_version**: 服务器选择的SSL版本
  - **Random**: 服务器生成的随机结构
  - **Session\_id**: 先前安全连接的id或者长度为0，说明不想恢复先前的安全参数，将建立新的
  - **Cipher\_suite**: 服务器选择的密钥算法
  - **Compression\_methods**: 服务器选择的压缩算法

# Certificate (可选消息)

---

- 服务器证书
- 证书类型必须是由被选择的加密套件中密钥交换算法所支持的，通常是**X509v3**版本证书；
- 在实际使用中（尤其是**HTTPS**），该消息通常会发送，用户必须亲自检查该证书是否真实可信（在浏览器的帮助下）；
- 该证书通常支持**RSA**密钥交换

# ServerKeyExchange (可选消息)

---

- 服务端用于密钥交换的参数 (Diffie-Hellman)
- 如果服务器没有发送Certificate或者由于选择的密钥套件设定，服务器所发送的Certificate选用了没有密钥交换功能的非对称算法做数字签名是

# CertificateRequest (可选消息)

---

- 要求实现客户端认证时请求客户端证书

# ServerHello

---

- 服务器Hello过程结束的消息，开始等待并接受客户端的响应



# Certificate (可选消息)

---

- 客户端数字证书，用于认证客户端身份
- 如果客户端没有合适的证书，将返回一个握手失败的致命性的报警

# ClientKeyExchange

---

- 消息提供创建随机密钥串(`pre_master_secret`)时客户端所提供的信息
- 通常使用**RSA**密钥交换，此时，客户端产生一个**`pre_master_secret`**结构，并用服务器的公钥对器进行加密，然后将加密的结果传送给服务器

# CertificateVerify (可选消息)

---

- 在提供客户端认证时发送。
- 该消息在发送完有数字签名能力的客户端 **Certificate** 之后发送，用于验证证书的拥有者就是本次通信的对方
- 该消息包含一个用于客户端私钥进行签名的从第一消息以来的所有握手消息的哈希值

# ChangeCipherSpec 客户端/服务器

---

- 该消息将通知对方，切换使用新协商好的算法和密钥参数，而未来的消息将使用那些算法保护

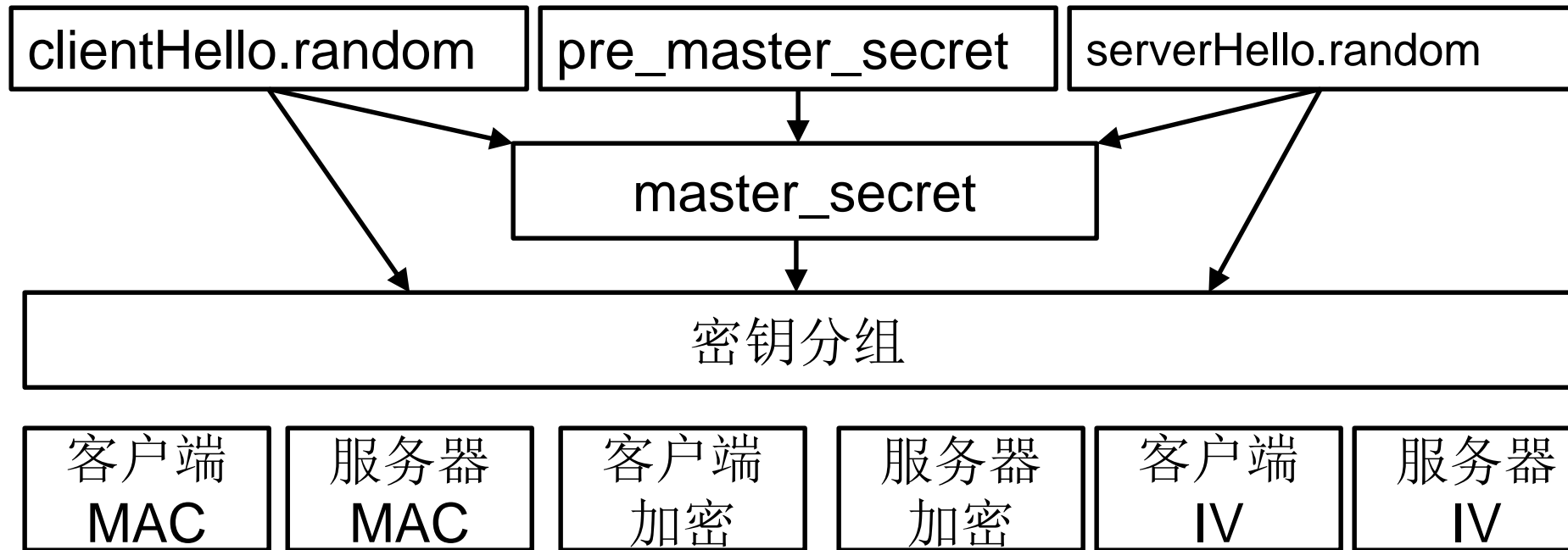
# Finished 客户端/服务器

---

- 握手阶段结束消息。
- 两个作用：
  - 表示握手已经结束，可以进行应用层数据的发送；
  - 验证握手过程的正确性；含有建立会话过程中所有消息的**MAC**值，使用新建立的算法和密钥参数计算。

# 密钥导出

- 一旦交换了 `pre_master_secret`, 需要将其扩展成独特的加密密钥, 用于完成加密、认证等任务。



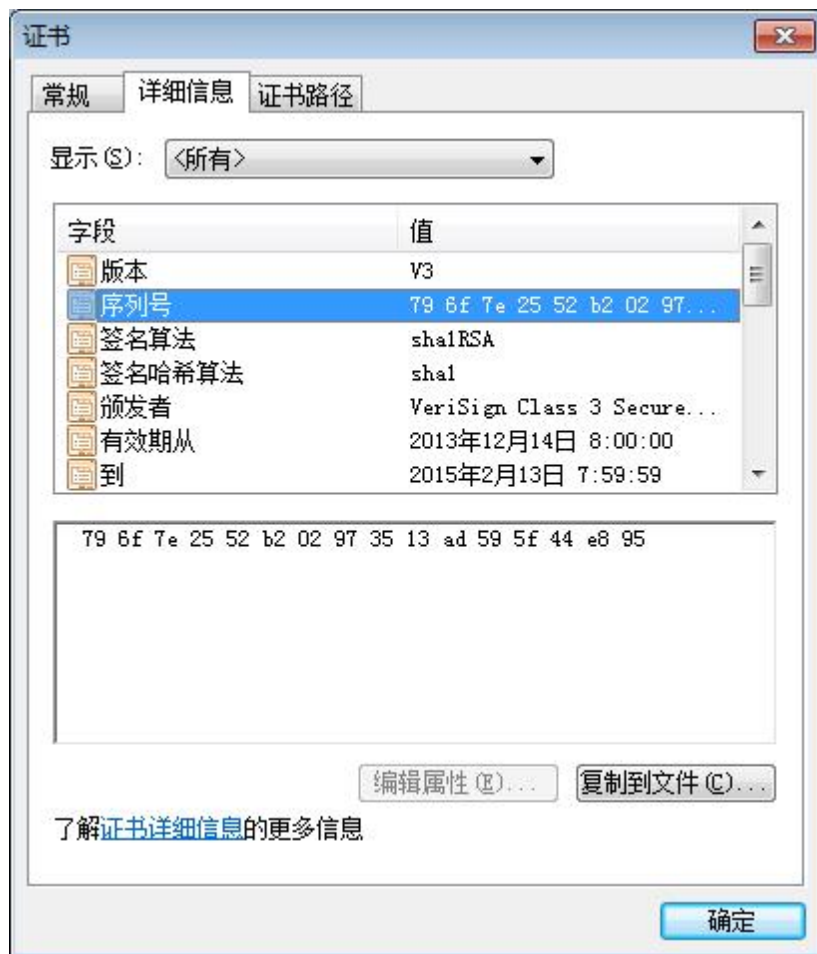
# 基于数字证书认证服务器



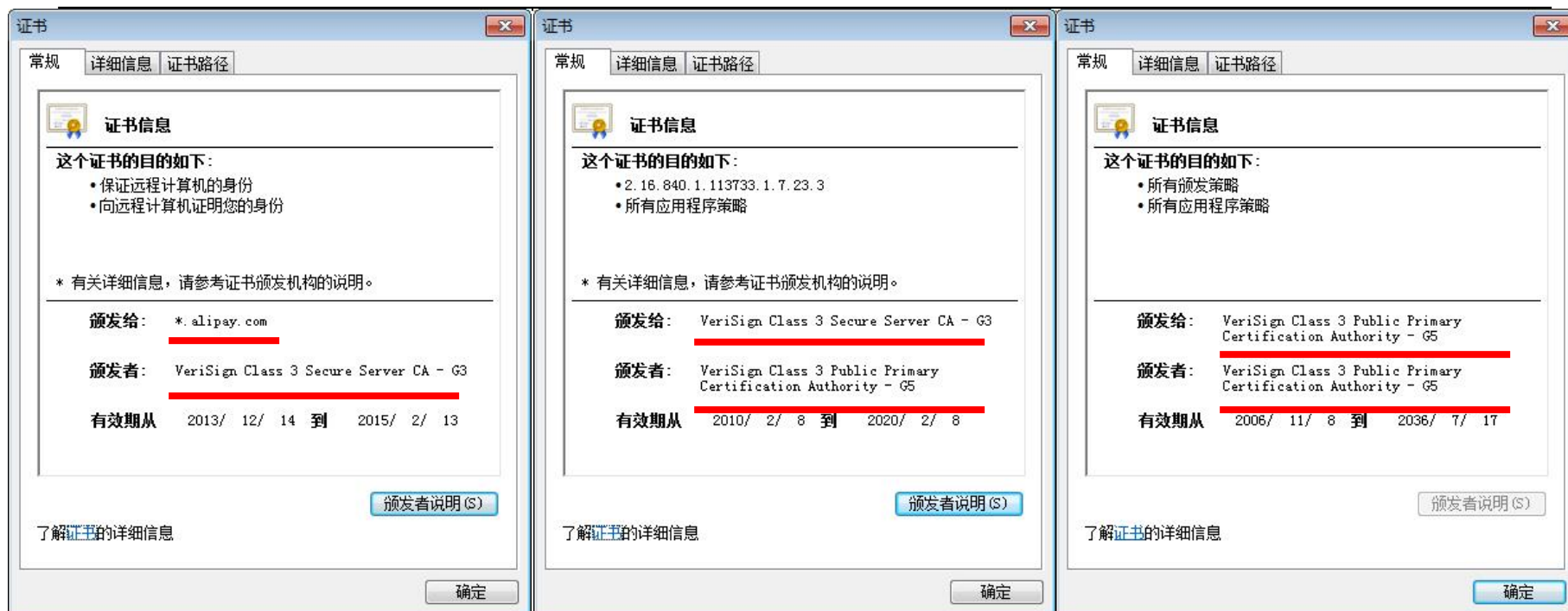
The image shows a screenshot of an Alipay payment page. A dialog box titled "证书" (Certificate) is overlaid on the left side of the browser window. The dialog box has tabs for "常规" (General), "详细信息" (Detailed Information), and "证书路径" (Certificate Path). The "常规" tab is selected, showing "证书信息" (Certificate Information). It states: "这个证书的目的如下:" (The purpose of this certificate is as follows:). Below this, it lists two points: "• 保证远程计算机的身份" (Guarantee the identity of the remote computer) and "• 向远程计算机证明您的身份" (Prove your identity to the remote computer). A note says: "\* 有关详细信息, 请参考证书颁发机构的说明。" (For more details, please refer to the certificate issuer's instructions). The certificate details are: "颁发给: \*.alipay.com" (Issued to: \*.alipay.com), "颁发者: VeriSign Class 3 Secure Server CA - G3" (Issuer: VeriSign Class 3 Secure Server CA - G3), and "有效期从 2013/ 12/ 14 到 2015/ 2/ 13" (Valid from 2013/ 12/ 14 to 2015/ 2/ 13). There is a button "颁发者说明(S)" (Issuer Information) and a link "了解证书的详细信息" (Learn more about the certificate). The background page is the Alipay "我的收银台" (My Checkout Counter) page, showing the user's account balance as 0.00 and various payment options like "扫码支付" (Scan to pay) and "信用卡" (Credit card).



# 服务器证书

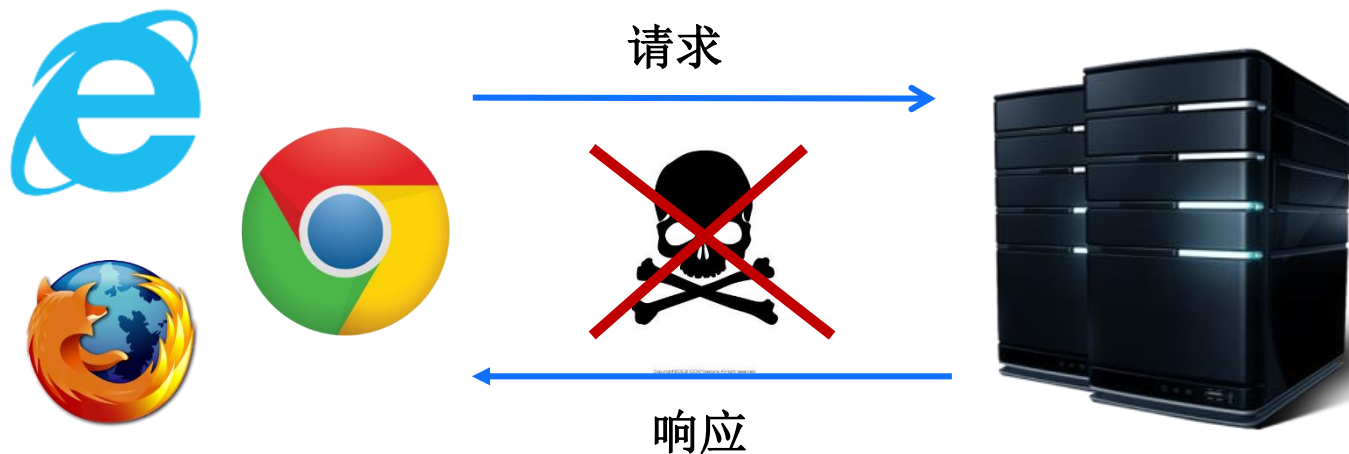


# 数字证书链



# 用户认证及后续通信安全

- 淘宝用户密码+支付宝密码



## WEB/HTTPS



## Further Reading: