第五章 安全协议技术

- SSL中的握手协议

周世杰

信息与软件工程学院

EMail: sjzhou@uestc.edu.cn

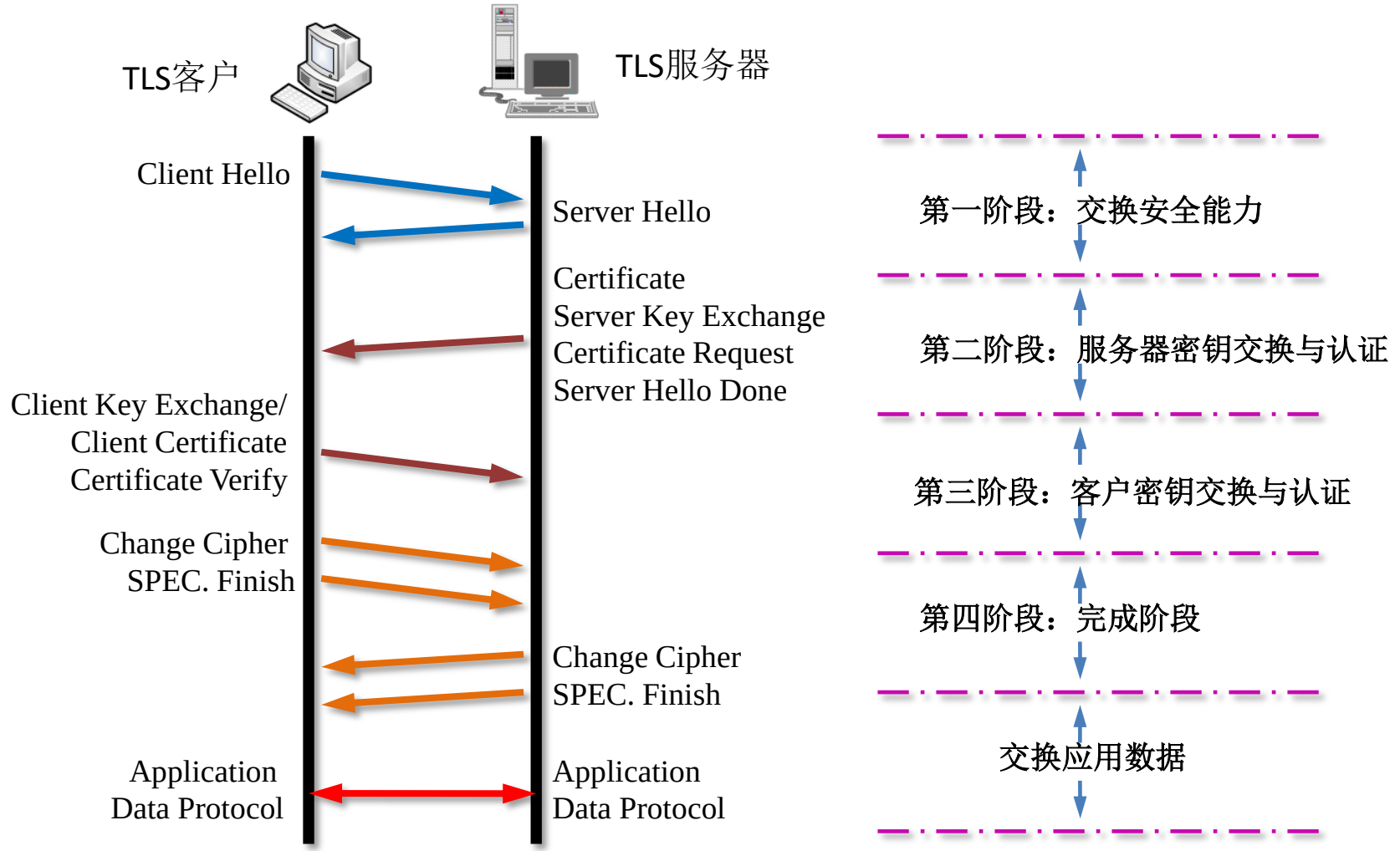
SSL的握手协议

- 握手协议本质上是一个密钥交换协议，但它也包含认证功能，因此可以视为认证和密钥交换协议
- 握手协议主要由四个过程组成
  - 交换安全能力
  - 服务器认证和密钥交换
  - 客户端认证和密钥交换
  - 完成：通知启用新的安全参数

为什么需要服务器密钥交换和客户端密钥交换两个过程？

因为SSL在同一个连接的两个方向采用不同的密钥

SSL的握手协议


TLS客户
TLS服务器
Client Hello
Server Hello
Certificate
Server Key Exchange
Certificate Request
Server Hello Done
Client Key Exchange/
Client Certificate
Certificate Verify
Change Cipher
SPEC. Finish
Change Cipher
SPEC. Finish
Application
Data Protocol
Application
Data Protocol
第一阶段：交换安全能力
第二阶段：服务器密钥交换与认证
第三阶段：客户密钥交换与认证
第四阶段：完成阶段
交换应用数据

握手协议第一阶段：交换安全能力

- 客户和服务器之间通过发送要求建立会话的消息（Client Hello 消息和 Server Hello 消息），交换彼此的要求和能力
  - 使二者在TLS版本、会话表示、将要使用的密码组（包括加密算法、压缩算法、密钥交换算法等）方面达成一致
  - 从而为下一步所需要的安全参数提供了具体的信息

握手协议第一阶段：交换安全能力

The Client Hello message &The Server Hello message

- SSL版本号（SSL Version ）：一般是客户所支持的最高版本号
- 随机数（ ClientHello.random & ServerHello.random ）：防重放攻击
- 会话标示（ Session Identifier）：用来唯一标示这个会话
  - 0： 新建一个会话和连接
  - 非0：在已有会话上建立连接（也叫做会话重用）
- 加密算法：客户支持的密码算法，包括：
  - 密钥交换算法（Key Exchange）
  - 加密算法（cihper Spec）:密码算法、MAC算法、MAC长度、密钥材料、IV大小
- 数据压缩算法：客户支持的压缩算法

SSL支持的密码算法

加密算法	密钥交换算法	数字摘要算法	压缩算法
• IDEA_CBC • RC2_CBC_40 • RC4_40 • RC4_128 • DES40_CBC • DES_CBC • 3DES_EDE_C • BC • NULL	• DHE_DSS • DHE_RSA • DH_anon • DH_DSS • DH_RSA • NULL • RSA	• NULL • MD5 • SHA	• NULL • PKZip • WinZip • gzip

握手协议第二阶段：服务器密钥交换与认证

服务器证书列表消息（Certificate）

- 通过服务器向客户发送自己的证书（和证书列表）来实现客户对服务器的身份认证。

服务器密钥交换消息（Server_Key_Exchange)

- 向客户端发送服务器自己的密钥信息。

客户端证书请求消息（Certificate_Request)

- 如果服务器需要对客户身份进行认证，则向客户发送客户证书请求（Certificate request）消息，要求客户在下一阶段返回自己合适的证书。
- 对于匿名密钥交换，如果客户收到服务器发送的Certificate request 消息，则通过报警消息发送致命错误后关闭连接。

服务器结束消息（Server_Hello_Done)

- 向客户发送服务器结束消息（Server Hello Done），通告客户可以执行密钥交换协议。

握手协议第二阶段：服务器密钥交换与认证

The Server Certificate message

(a) 服务器标示

(b) 服务器的证书（也可能是一组证书），包含服务器公钥

说明：

服务器证书消息是服务器向客户端传送自己的证书，使得客户端知道服务器的公钥以及其他信息。

握手协议第二阶段：服务器密钥交换与认证

Server Key exchange message

(a) 证书类型：用来指明服务器使用何种公钥体制

(b) 证书的认证权威：是一组服务器支持的证书权威（CA）

说明：

（1）服务器密钥交换消息用来向客户端发送服务器自己的密钥信息

（2）服务器密钥交换消息不是必须的

- 如果使用了固定Diffie-Hellman或者RSA密钥交换，则不需要。
- 反之，如果使用匿名Diffie-Hellman、瞬时Diffie-Hellman、Fortzza或者服务器在使用RSA时仅用了RSA签名密钥。
- **RSA**：在第一阶段包含了服务器的公钥
- 固定**DH**：由于在固定DH中，服务器在第一阶段发送的证书消息中包含了服务器自己的公钥

握手协议第二阶段：服务器密钥交换与认证

The Client Certificate Request message

- 证书类型：用来指明服务器支持公钥体制
- 证书的认证权威：是一组服务器支持的证书权威（CA）

说明：

如果服务器不使用匿名**Diffie-Hellman**，则客户端证书请求消息是必须的。它的目的是要求客户端向服务器发送证书等消息，以便对客户进行认证。

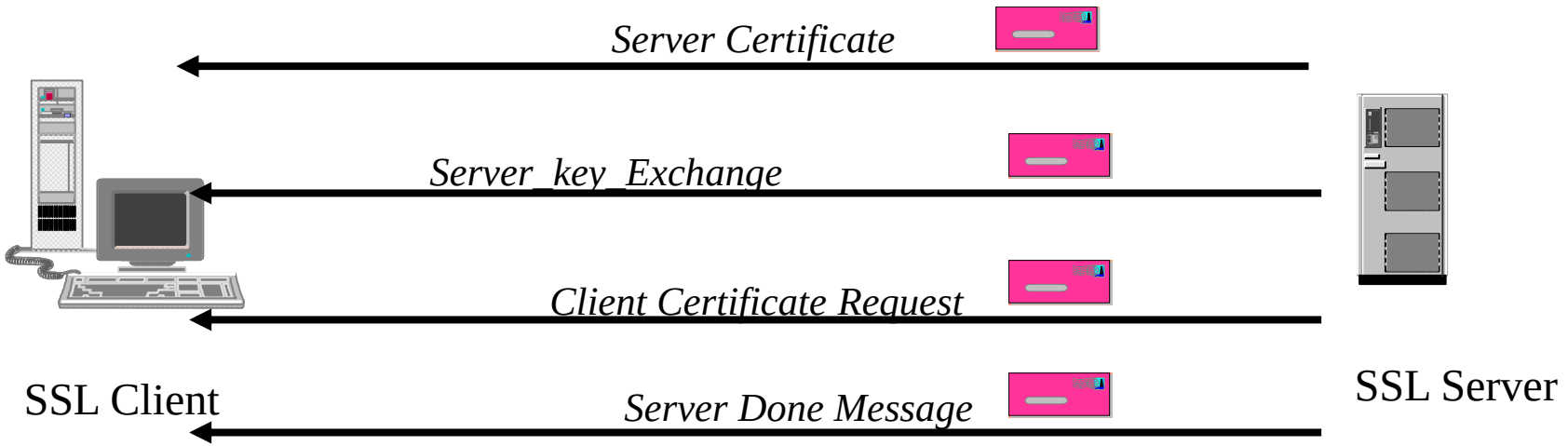
握手协议第二阶段：服务器密钥交换与认证

Server Done message

- 表明服务器的**hello**和相关信息结束
- 在此消息之后，服务器将等待客户端的应答

握手协议第二阶段：服务器密钥交换与认证

服务器到客户的消息交换小结



握手协议第三阶段：客户密钥交换与认证

- 在接收到服务器完成消息之后
  - 如果请求了证书，客户端需要验证服务器是否提供了合法的证书
  - 检查server_hello参数是否可以接受
  - 如果所有条件满足，则客户端向服务器发回一个或者多个消息：
    - （1）客户端证书消息（Certificate)：如果服务器请求了证书，必须有该消息
    - （2）客户端密钥交换消息(Client_Key_Exchange)：必须发送
    - （3）客户端证书校验消息（Ceritificate_Verify)：可以发送(便于服务器验证自己的证书）

握手协议第三阶段：客户密钥交换与认证

客户端证书消息（Certificate)

- 如果服务器请求了证书（即服务器发送了Certificate request 消息），且客户拥有合适的证书，客户端必须发送该消息来向服务器传递自己的证书。
- 如果客户没有合适的证书， 则通过向服务器发送一个零长度的证书列表结构，表明无法证明自己的身份。

客户端密钥交换消息(Client Key Exchange)

- 客户必须发送该消息用于完成与服务器之间的密钥交换。

客户端证书校验消息（Ceritificate Verify)

- 通过发送客户端的证书校验消息，允许服务器验证客户证书的有效性

握手协议第三阶段：客户密钥交换与认证

Client Certificate message

- 客户标示：客户的身份标示信息
- 客户的证书：客户证书的有关信息

说明：

如果服务器请求了证书，但是客户端没有合适的证书，则发送”无证书警报“消息

握手协议第三阶段：客户密钥交换与认证

Client Key Exchange message

- 密钥参数密钥：用服务器公钥加密的会话密钥或者是密钥交换消息

说明：

- 如果是RSA，该消息包含客户端生成的48字节的次密钥（ pre-master secret key ），并使用服务器证书中的公钥或者服务器密钥交换消息中的临时RSA密钥加密，它用于生成主密钥（ master secret key ）
- 如果是Diffie-Hellman，该消息包含客户端的Diffie-Hellman公钥参数

握手协议第三阶段：客户密钥交换与认证

Certificate Verify Message

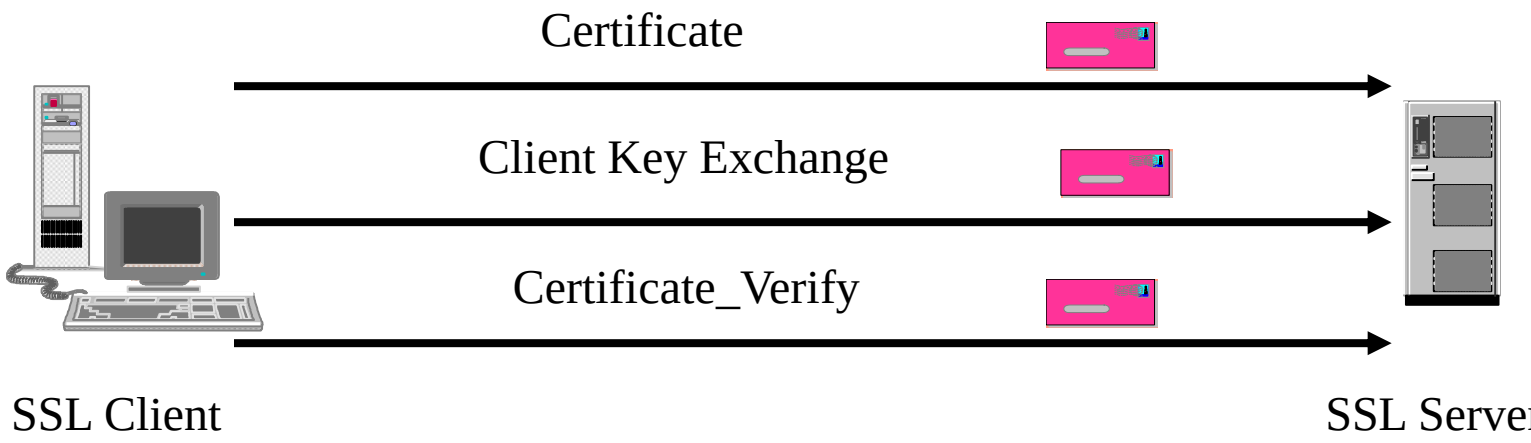
- 验证信息：客户证书的**Hash签名**验证信息

说明：

Hash签名很复杂，它对签名的所有消息即密钥信息等进行Hash运算，并用自己的私钥加密，从而即是有人盗用了客户端证书，也无法发送该证书验证消息

握手协议第三阶段：客户密钥交换与认证

客户到服务器的消息交换小结



握手协议第四阶段：结束阶段

- 此阶段完成安全连接的设置，主要包含以下消息：
  - 客户：
    - （1）客户端发送的修改密码规范消息（Change_Cipher_Spec)
    - （2）客户端发送的完成消息（Finished)
  - 服务器
    - （1）服务器发送的修改密码规范消息（Change_Cipher_Spec)
    - （2）服务器发送的完成消息（Finished)

握手协议第四阶段：结束阶段

客户的加密规范修改消息（Change Cipher Spec)

- 修改密码协议来通过服务器启用新的安全参数，且记录层协议对以后的所有数据均使用新的密码参数来加密。

客户的完成消息（Finished)

- 验证密钥交换和认证协议成功完成

服务器的修改密码规范消息（Change Cipher Spec)

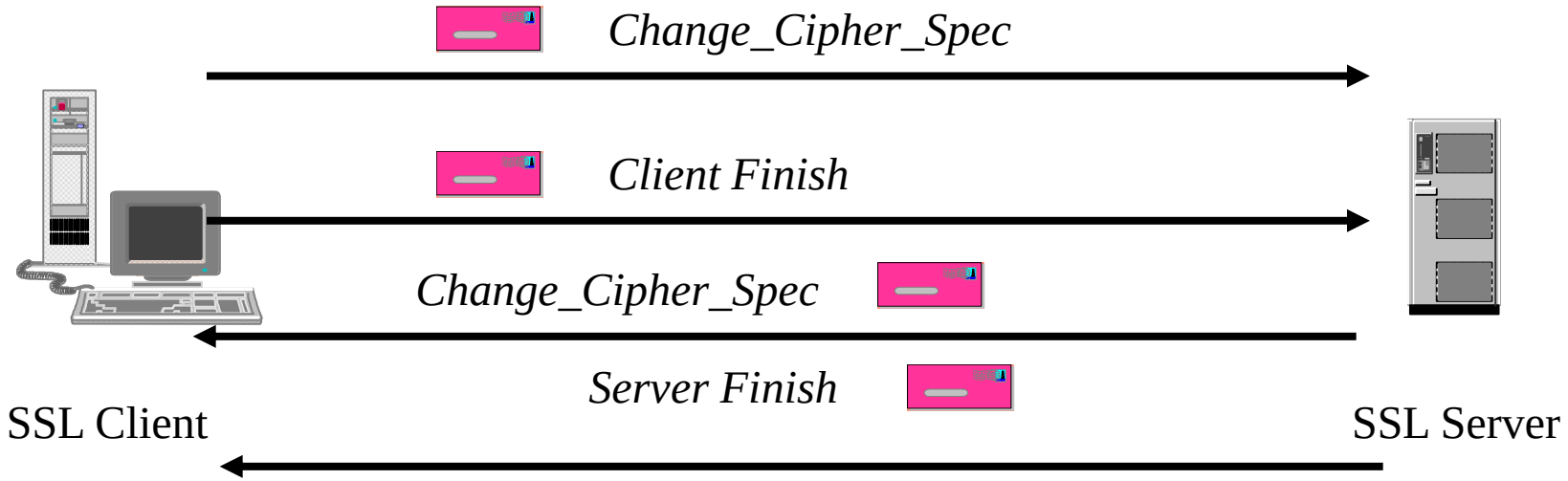
- 通告客户启用新的安全参数。

服务器的完成消息（Finished)

- 发送该消息后服务器将等待应用程序数据。

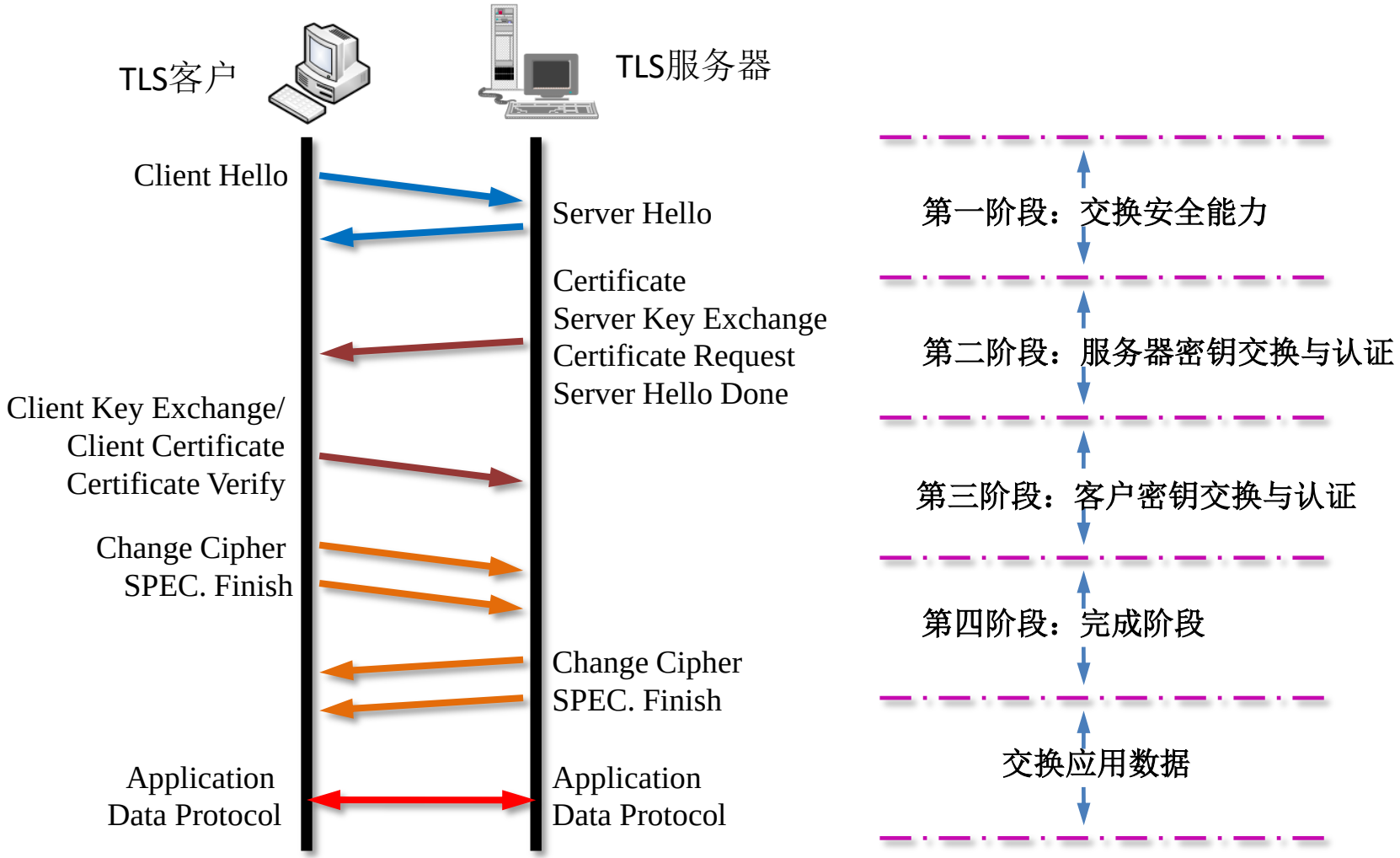
握手协议第四阶段：结束阶段

结束阶段的消息交换总结



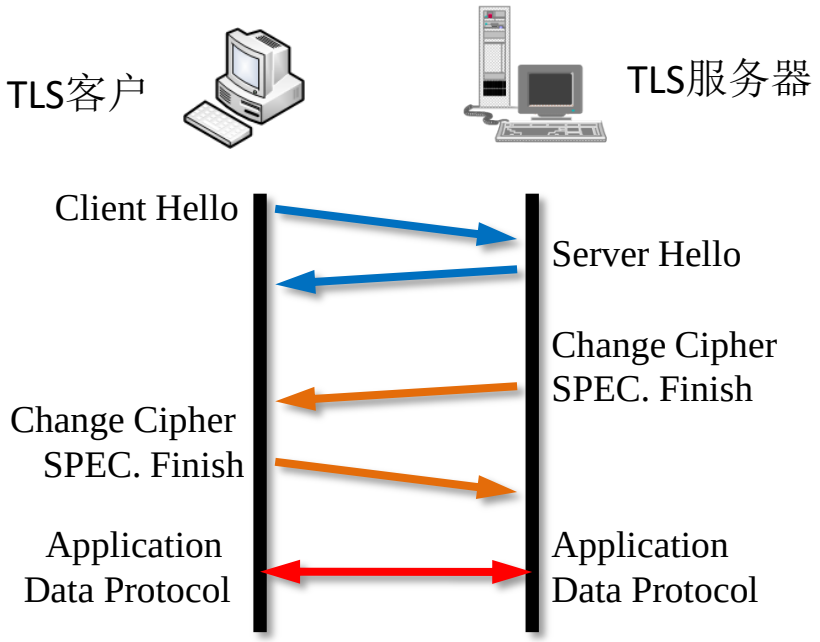
从此刻开始，客户端和服务器的记录层协议将启用新的密钥和算法进行数据加密

SSL的握手协议总结


TLS客户
TLS服务器
Client Hello
Server Hello
Certificate
Server Key Exchange
Certificate Request
Server Hello Done
Client Key Exchange/
Client Certificate
Certificate Verify
Change Cipher
SPEC. Finish
Change Cipher
SPEC. Finish
Application
Data Protocol
Application
Data Protocol
第一阶段：交换安全能力
第二阶段：服务器密钥交换与认证
第三阶段：客户密钥交换与认证
第四阶段：完成阶段
交换应用数据

会话重用

- 在SSL中，为了节约密码参数协商带来的开销，允许一个连接中的密码参数被多个会话重用
- 会话重用不需要经过完整的握手协议，只需要通知双方利用过去会话标示重用过去协商的密码参数即可。




谢谢！