黑客攻防

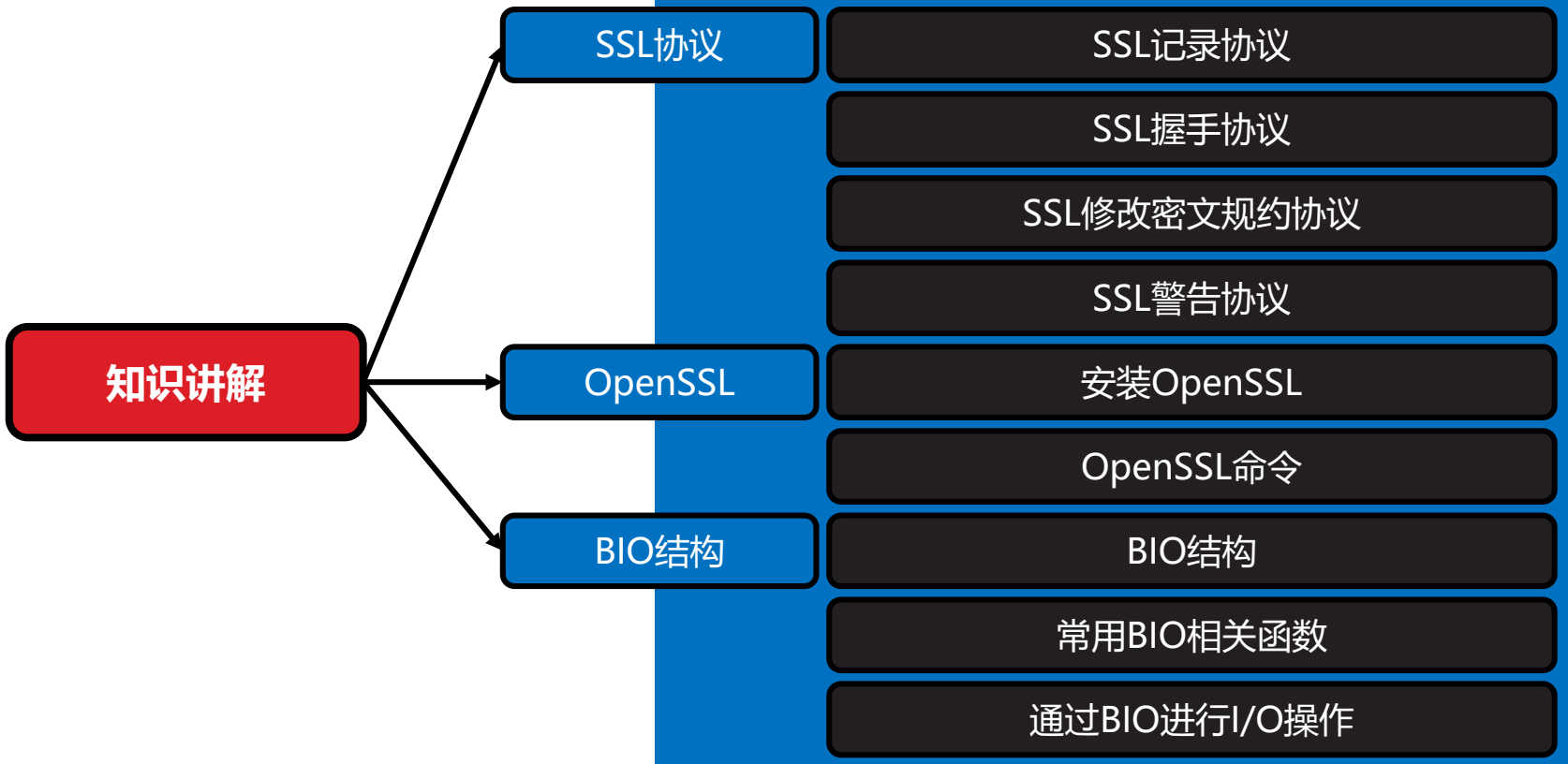
安全Web服务器

Unit07

内容

上午	09:00 ~ 09:30	作业讲解和回顾
	09:30 ~ 10:20	知识讲解
	10:30 ~ 11:20	
	11:30 ~ 12:00	
下午	14:00 ~ 14:50	实训案例
	15:00 ~ 15:50	
	16:00 ~ 16:50	扩展提高
	17:00 ~ 17:30	总结和答疑

知识讲解


知识讲解
SSL协议
SSL记录协议
SSL握手协议
SSL修改密文规约协议
SSL警告协议
OpenSSL
安装OpenSSL
OpenSSL命令
BIO结构
BIO结构
常用BIO相关函数
通过BIO进行I/O操作

SSL协议

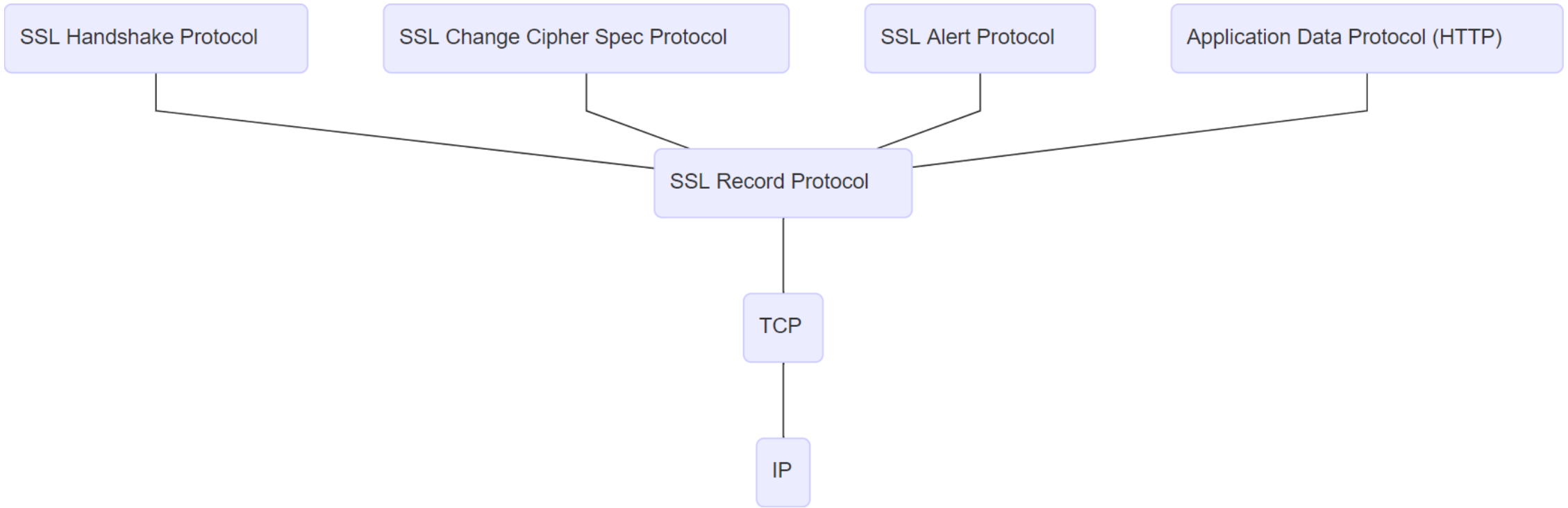
SSL协议

- 安全套接字层(Security Socket Layer, SSL)协议是网景(Netscape)公司于1996年提出的安全通信协议。它为网络应用层的通信提供了身份认证、数据保密和数据完整性校验等安全服务。设计该协议的主要目的是在网络环境中两个相互通信的进程之间，建立一个安全的数据通道
- SSL并非一个单独协议，而是包含两层结构的协议族。上层由SSL握手协议(SSL Handshake Protocol)、SSL修改密文规约协议(SSL Change Cipher Spec Protocol)和SSL警告协议(SSL Alert Protocol)组成，下层则是SSL记录协议(SSL Record Protocol)。SSL协议栈的结构如下图所示：

知识讲解

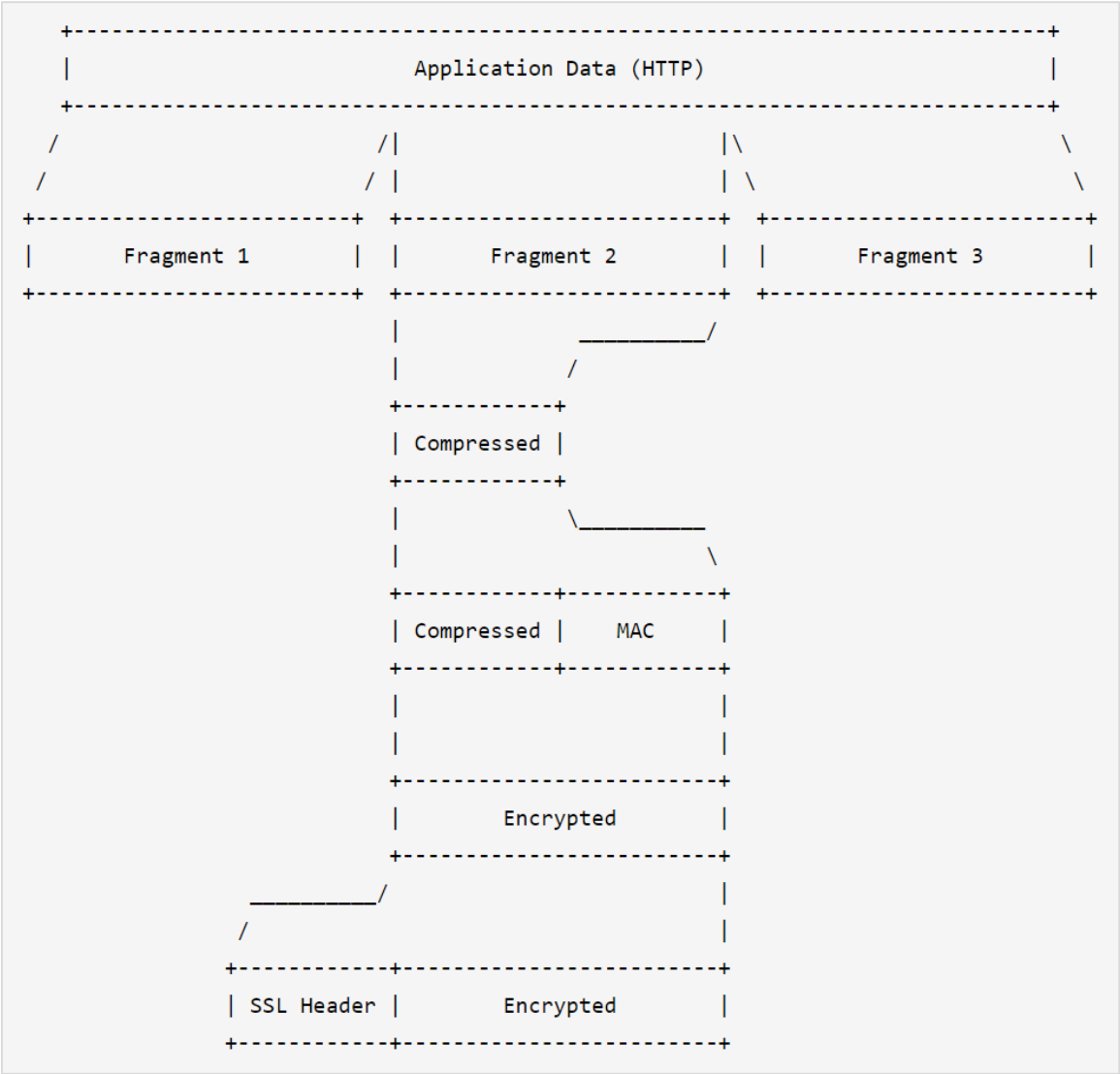
SSL协议

知识讲解


SSL Handshake Protocol
SSL Change Cipher Spec Protocol
SSL Alert Protocol
Application Data Protocol (HTTP)
SSL Record Protocol
TCP
IP

SSL记录协议

- SSL记录协议为通信提供机密性和完整性保护，其工作流程如下图所示：
  - 接收到应用层数据后，SSL记录协议首先对其进行分组，分组后每个数据块的大小不超过2^{14}=16384个字节
  - 然后，SSL记录协议对分组产生的每个数据块进行压缩，期间不能出现任何信息损失
  - SSL记录协议为每个压缩后的数据块计算消息认证码(Message Authetication Code, MAC)，即一种带密钥的消息摘要，并将该消息认证码附加在压缩数据块之后
  - SSL记录协议将压缩数据块和消息认证码作为一个整体进行加密
  - 最后，SSL记录协议在加密形成的密文之前添加SSL头部



知识讲解

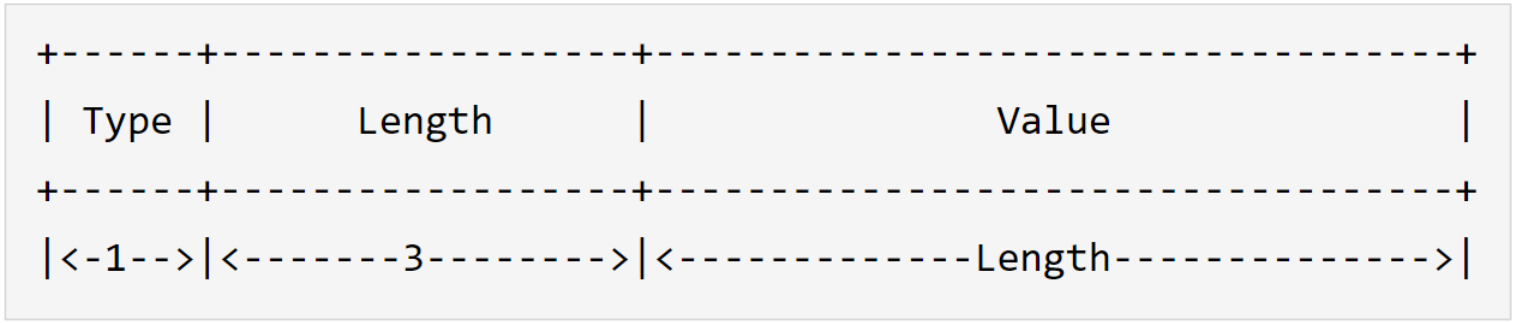
SSL握手协议

- 当SSL客户端和服务器首次通信时，双方通过SSL握手协议就一系列安全事宜达成共识，具体包括：
  - 密钥交换算法
  - 加密认证算法
  - 数据压缩算法
  - 双方数字证书
  - 与算法相关的各种参数

知识讲解

SSL握手协议

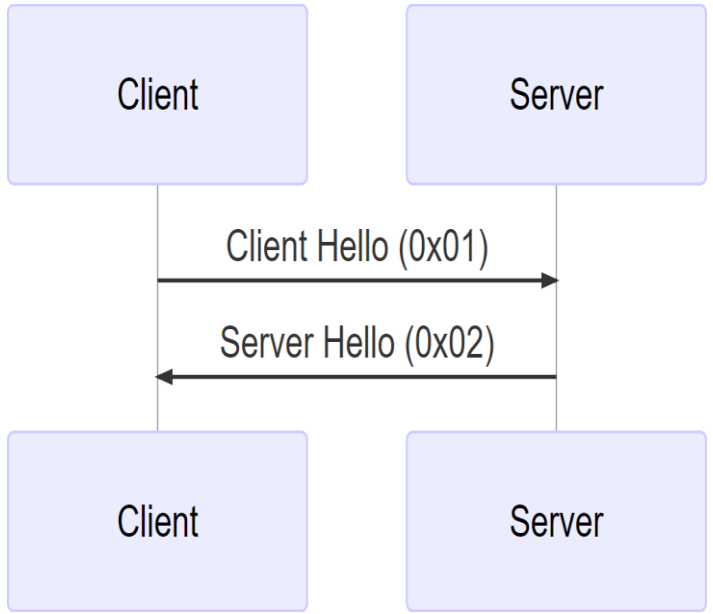
- SSL握手在应用层数据传输之前进行，包含一系列客户端与服务器之间的消息交换，其中每条消息均由三个字段组成：
  - 消息类型(T)，一个字节
  - 消息长度(L)，三个字节
  - 消息内容(V)，至少一个字节
- SSL握手消息的结构如下图所示：



知识讲解

SSL握手协议

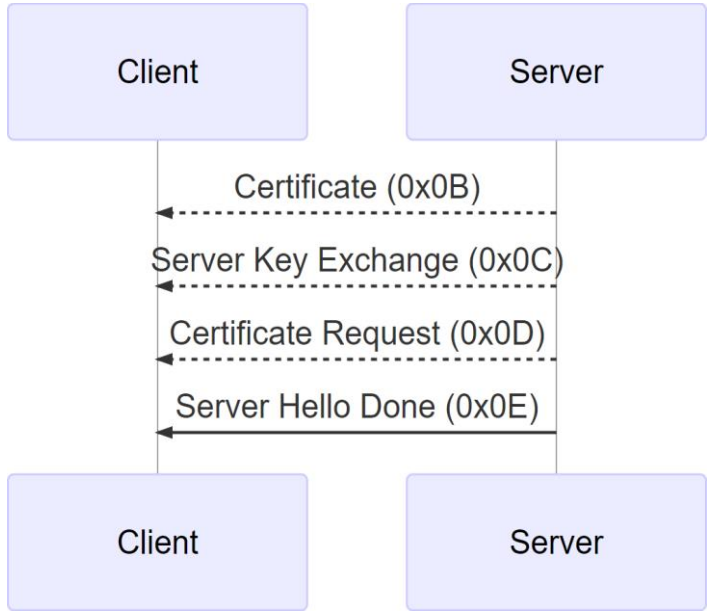
- SSL握手的发起阶段如下图所示：
  - 客户端向服务器发送Client Hello类型消息，内容包括：
    - 客户端所支持SSL协议的最高版本号
    - 随机码
    - 会话ID
    - 密码套件(Cipher Suite)，具体包括：
      - 密钥交换算法
      - 加密认证算法
      - 数据压缩算法
  - 服务器从客户端所提供的密码套件中确定后面使用的密钥交换算法、加密认证算法和数据压缩算法，并向客户端返回Server Hello类型消息，内容包括：
    - 客户端和服务器都支持的SSL协议最高版本号
    - 与客户端独立的随机码



知识讲解

SSL握手协议

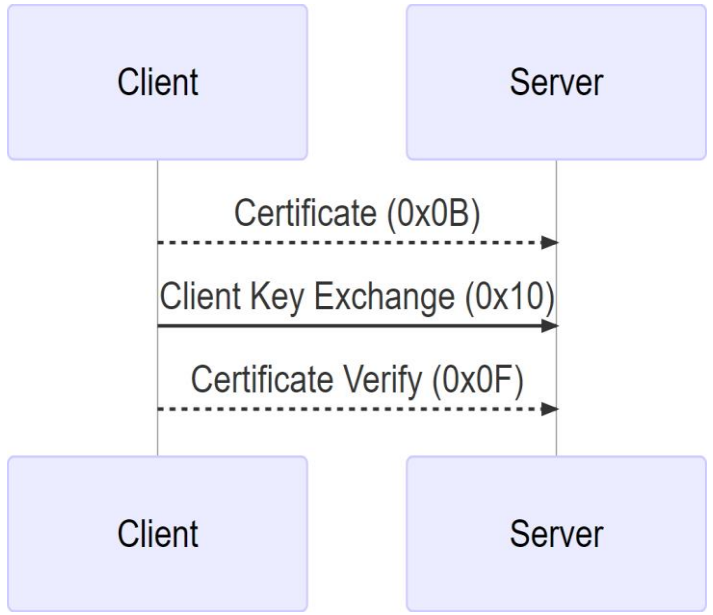
- SSL握手的服务器认证和密钥交换如下图所示：
  - 服务器向客户端发送Certificate类型的消息，向其出示自己的数字证书
  - 服务器向客户端发送Server Key Exchange类型的消息，告知其与密钥交换算法有关的参数
  - 服务器向客户端发送Certificate Request类型的消息，要求客户端出示其数字证书
  - 服务器向客户端发送Server Hello Done类型的消息，表明消息发送完毕，等待对方回应



知识讲解

SSL握手协议

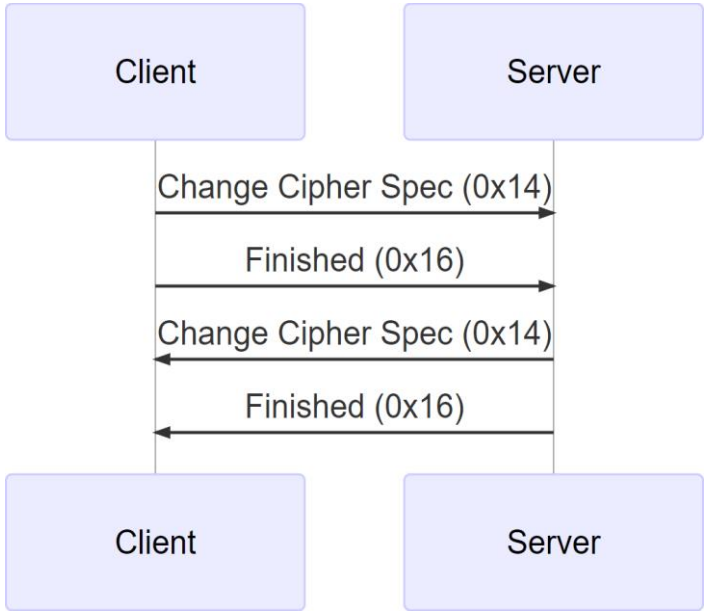
- SSL握手的客户端认证和秘钥交换如下图所示：
  - 收到服务器Server Hello Done类型的消息后，客户端首先验证服务器的数字证书是否合法，与密钥交换算法有关的参数是否可行。如果服务器要求出示数字证书，客户端还要向服务器发送Certificate类型的消息，向其出示自己的数字证书
  - 客户端向服务器发送Client Key Exchange类型的消息，告知其与密钥交换算法有关的参数
  - 客户端向服务器发送Certificate Verify类型的消息，该消息使用与客户端数字证书中的公钥相对应的私钥做了数字签名



知识讲解

SSL握手协议

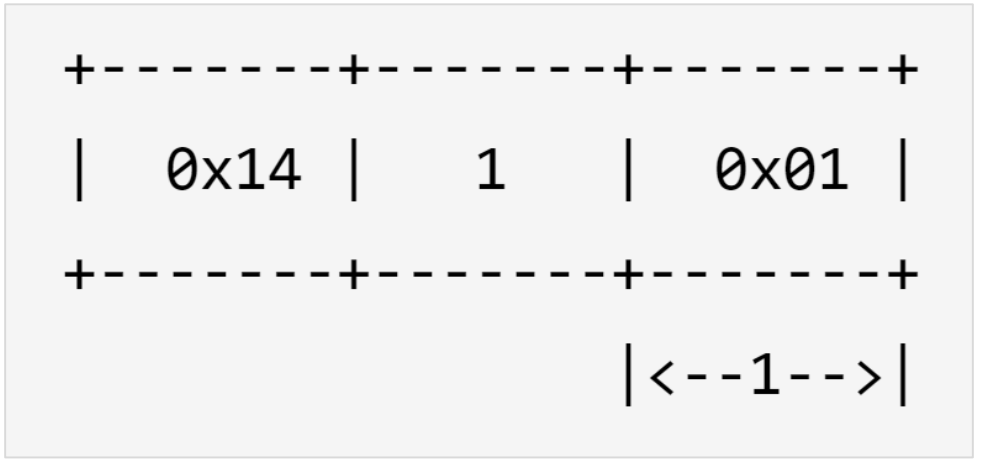
- SSL握手的结束阶段如下图所示：
  - 客户端和服务器分别向对方发送Change Cipher Spec和Finished类型的消息，告知对方SSL握手已经完成，双方的后续通信全部按照协商好的加密认证算法、数据压缩算法和密钥进行处理



知识讲解

SSL修改密文规约协议

- SSL修改密文规约协议只包含一种消息格式，消息类型为Change Cipher Spec (0x14)，消息内容只有一个字节——0x01。如下图所示：



- 该消息用于通知对方后续通信全部按照协商好的加密认证算法、数据压缩算法和密钥进行处理

知识讲解

SSL警告协议

- SSL警告协议用于在通信过程中出现错误或异常情况时给出警告或关闭连接。根据错误的严重程度分为：
  - Warning：一般错误
  - Fatal：致命错误，立即关闭连接

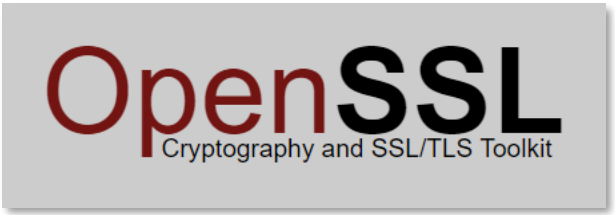
知识讲解

OpenSSL

安装OpenSSL

- OpenSSL最早发布于1998年，其前身是Eric Young和Tim Hudson共同开发的SSLeay，目前已更新至1.0.2g版本。OpenSSL提供了完全的、免费的和开源的SSL协议实现，支持SSL2.0、SSL3.0以及TSL1.0等协议版本，并且能工作于大部分主流操作系统上，如UNIX、Linux和Windows等。OpenSSL支持最常用的对称和公钥加密算法、消息摘要算法等，在提供命令行工具的同时也提供了应用编程接口(API)支持二次开发
- 在Ubuntu上安装OpenSSL非常简单：
  - sudo apt-get install libssl-dev

知识讲解



OpenSSL命令

- genrsa子命令用于生成RSA私钥

```
openssl genrsa [-out filename][-passout arg][-des][-des3]
               [-idea][-f4][-3][-rand file(s)][numbits]
```

选项	含义
-out filename	输出私钥到指定文件，默认为标准输出
-passout arg	输出文件口令
-des/-des3/-idea	针对私钥的加密算法，不指定则不加密
-f4/-3	选择公共组件
-rand file(s)	随机种子文件
numbits	模位数，缺省2048位

知识讲解

OpenSSL命令

- req子命令用于创建和处理数字证书申请(Cerificate Signing Request, CSR)

```
openssl req [-in filename][-inform DER|PEM][-out filename][-outform DER|PEM]
            [-text][-noout][-verify][-modulus][-new][-config filename]
            [-rand file(s)][-newkey rsa:bits][-newkey dsa:file][-keyout filename]
            [-key filename][-keyform DER|PEM][-x509][-days n]
```

选项	含义
-in filename	输入数字证书申请文件，仅当未使用-new和-newkey选项时有效
-inform DER|PEM	输入数字证书申请格式，DER采用ANSI的DER标准格式，PEM则为Base64编码格式
-out filename	输出数字证书申请文件
-outform DER|PEM	输出数字证书申请格式
-text	以文本方式打印数字证书申请
-noout	不打印数字证书申请编码版本
-verify	验证数字证书申请的数字签名

知识讲解

OpenSSL命令

- req子命令用于创建和处理数字证书申请(Cerificate Signing Request, CSR)

-modulus	打印数字证书申请的公钥模数
-new	生成数字证书申请
-config filename	数字证书申请模板文件
-rand file(s)	随机种子文件
-newkey rsa:bits	同时生成数字证书申请和RSA私钥，其参数指明私钥长度
-newkey dsa:file	同时生成数字证书申请和DSA私钥，其参数指明参数文件
-keyout filename	输出私钥文件
-key filename	输入私钥文件
-keyform DER|PEM	输入私钥格式
-x509	输出x509结构
-days n	如果使用了-x509选项，指定CA给第三方签证书的有效期天数，默认30天

知识讲解

OpenSSL命令

- x509子命令用于显示数字证书的内容、转换数字证书的格式、给CSR签名等

```
openssl x509 [-in filename][-inform DER|PEM|NET][-out filename][-outform DER|PEM|NET]
             [-md2/-md5/-sha1/-mdc2][-text][-noout][-modulus][-serial][-issuer]
             [-subject][-hash][-nameopt option][-email][-startdate][-enddate][-dates]
             [-fingerprint][-C][-trustout][-setalias arg][-alias][-clrtrust][-purpose]
```

选项	含义
-in filename	输入数字证书文件
-inform DER|PEM|NET	输入数字证书格式
-out filename	输出数字证书文件
-outform DER|PEM|NET	输出数字证书格式
-md2/-md5/-sha1/-mdc2	哈希算法，默认MD5
-text	以文本方式打印数字证书

知识讲解

OpenSSL命令

- x509子命令用于显示数字证书的内容、转换数字证书的格式、给CSR签名等

-noout	不打印数字证书编码版本
-modulus	打印数字证书的公钥模数
-serial	打印数字证书的序列号
-issuer	打印数字证书颁发者名
-subject	打印数字证书持有者名
-hash	打印数字证书持有者名的哈希值
-nameopt option	各种证书名称选项
-email	打印证书申请者的电子邮箱
-startdate	打印数字证书生效时间

知识讲解

OpenSSL命令

- x509子命令用于显示数字证书的内容、转换数字证书的格式、给CSR签名等

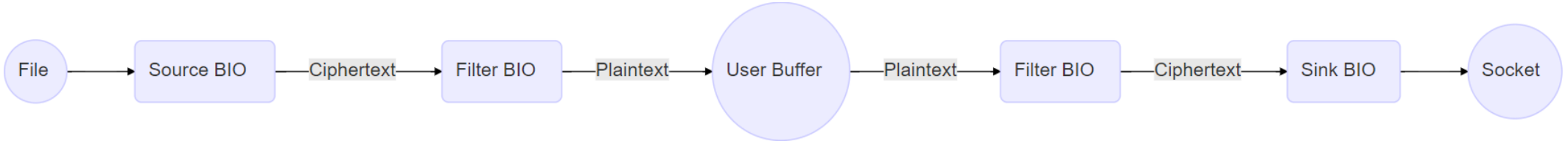
-enddate	打印数字证书到期时间
-dates	打印数字证书生效和到期时间
-fingerprint	打印DER格式数字证书的DER版本
-C	以C语言代码的格式打印结果
-trustout	打印可信数字证书
-setalias arg	设置数字证书别名
-alias	打印数字证书别名
-clrtrust	清除数字证书附加项中所有关于用途允许的内容
-purpose	打印数字证书附加项中所有关于用途允许和禁止的内容

知识讲解

BIO结构

BIO结构

- BIO是OpenSSL中重要的数据结构，其作用是封装并隐藏底层I/O操作的细节，无论是针对文件的读取和写入，还是基于套接字的接收和发送，都可以通过BIO类型的对象来完成。借助BIO结构，应用程序可以完全透明地实现SSL连接、加密通信以及文件读写等功能
- BIO分为两种：
  - Source/Sink型BIO：代表数据源/目的，如文件BIO和套接字BIO
  - Filter型BIO：把数据从一个BIO传递到另一个BIO，在传递过程中完成加解密
- 如下图所示：



知识讲解

BIO结构

知识讲解

```
typedef struct bio_st {
    BIO_METHOD      * method;               // 方法结构
    long           (* callback)(            // 回调函数
                      struct bio_st * bio,
                      int             mode,
                      const char    * argp,
                      int             argi,
                      long            argl,
                      long            ret);
    char            * cb_arg;              // 回调参数
    int               init;                // 初始化标志，1表示已初始化
    int               shutdown;            // 已关闭标志，1表示已被关闭
    int               flags;
    int               retry_reason;
    int               num;
    void            * ptr;
    struct bio_st   * next_bio;            // Filter型BIO的下一个节点
    struct bio_st   * prev_bio;            // Filter型BIO的上一个节点
    int               references;
    unsigned long     num_read;            // 读取字节数
    unsigned long     num_write;           // 写入字节数
    CRYPTO_EX_DATA    ex_data;
}   BIO;
```

常用BIO相关函数

- 通过BIO_new函数可以创建BIO对象：

```
BIO* BIO_new(BIO_METHOD* type);
```

- 在BIO结构的所有字段中，method可以说是最关键的一个字段，它决定了BIO对象的功能，而该字段的值则来自创建BIO对象时所提供的type参数。一般情况下，传递给type参数的值是通过某个具体的生成函数获得的，例如执行下面的代码，即可创建一个用于读写内存的BIO对象：

```
BIO* membio = BIO_new(BIO_s_mem());
```

知识讲解

常用BIO相关函数

- Source/Sink型BIO的生成函数

函数	功能
BIO_s_mem	封装内存操作，读写内存
BIO_s_fd	封装一个文件描述符，读写该文件
BIO_s_file	封装标准输入、标准输出和标准错误
BIO_s_accept	封装Socket API的accept函数，等待并接受来自远程主机的连接请求
BIO_s_connect	封装Socket API的connect函数，向远程主机发起连接请求
BIO_s_socket	封装Socket API，实现网络通信
BIO_s_bio	封装一个BIO对，向其中一个写入，从另外一个读出
BIO_s_null	封装空设备，写入数据被丢弃，读取得到EOF

知识讲解

常用BIO相关函数

- Filter型BIO的生成函数

函数	功能
BIO_f_ssl	封装SSL协议，按照协议的要求对数据进行加工
BIO_f_base64	封装Base64编解码，写入时编码，读取时解码
BIO_f_cipher	封装加解密，写入时加密，读取时解密
BIO_f_md	封装摘要计算，通过的消息被计算摘要
BIO_f_buffer	封装缓冲区操作，写入的数据被传递给下一个BIO， 读取的数据则来自前一个BIO
BIO_f_null	封装空操作，相当于不存在

知识讲解

通过BIO进行I/O操作

- BIO_read函数

```
int BIO_read(BIO* bio, void* buf, int len);
```

  - 从bio读取len字节数据到buf中。成功返回实际读取的字节数，失败返回0或-1，若该bio没有实现此功能的方法，则返回-2

- BIO_write函数

```
int BIO_write(BIO* bio, const void* buf, int len);
```

  - 将buf中的len字节数据写入bio。成功返回实际写入的字节数，失败返回0或-1，若该bio没有实现此功能的方法，则返回-2

知识讲解

通过BIO进行I/O操作

- BIO_gets函数

```
int BIO_gets(BIO* bio, char* buf, int size);
```

  - 从bio读取最多包含size-1个字符的字符串到buf中，该字符串以空字符结尾。成功返回实际读取的字符数(不含结尾空字符)，失败返回0或-1，若该bio没有实现此功能的方法，则返回-2
  - 对消息摘要型BIO调用此函数，会返回整个摘要字符串，而不受size参数的限制

知识讲解

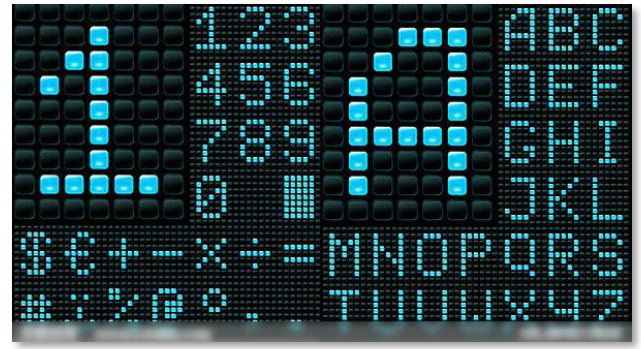
通过BIO进行I/O操作

- BIO_puts函数

```
int BIO_puts(BIO* bio, const char* buf);
```

  - 将buf中以空字符结尾的字符串写入bio。成功返回实际写入的字符数(不含结尾空字符)，失败返回0或-1，若该bio没有实现此功能的方法，则返回-2

知识讲解



通过BIO进行I/O操作

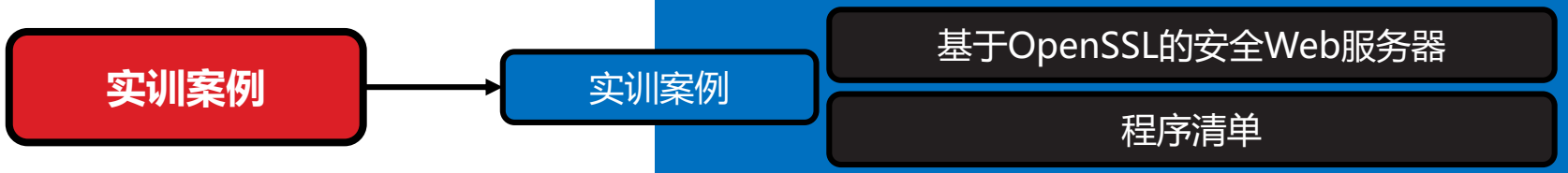
- BIO_flush函数(宏)

```
#define BIO_flush(bio) (int)BIO_ctrl(bio, BIO_CTRL_FLUSH, 0, NULL)
```

  - 将bio内部缓冲区中的数据一次性全部写出。有时也用于设置EOF标志，表示无数据可写。成功返回1，失败返回0或-1
  - 所有针对非阻塞Source/Sink型BIO的读写操作返回失败(0或-1)，并不意味着一定发生了错误，也可能仅仅是目前暂时不可读取或写入，此时若BIO_should_retry(bio)的值为1，可于稍后重试

知识讲解

实训案例



实训案例

基于OpenSSL的安全Web服务器

- 在理解HTTPS和SSL工作原理的基础上，实现安全的Web服务器
  - 服务器能够并发处理多个请求，要求至少能支持GET命令
  - 进一步扩展Web服务器的功能，增加对HEAD、POST和DELETE命令的支持
- 编写必要的客户端测试程序，用于发送HTTPS请求并显示服务器返回的响应，也可以使用一般的Web浏览器测试服务器

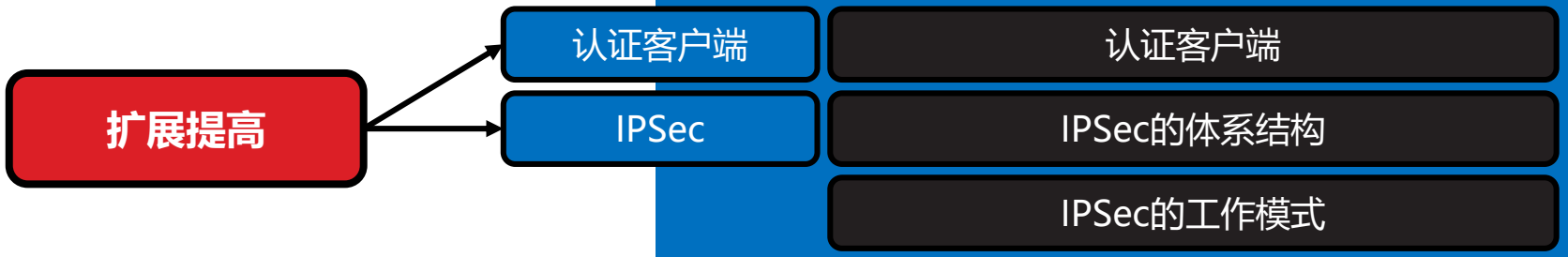
代码实践

程序清单

代码实践

- 声明Thread类
  - thread.h
- 实现Thread类
  - thread.cpp
- 声明ClientThread类
  - clientthread.h
- 实现ClientThread类
  - clientthread.cpp
- 声明SecWebServer类
  - secwebserver.h
- 实现SecWebServer类
  - secwebserver.cpp
- 测试SecWebServer类
  - secwebserver_test.cpp
- 测试SecWebServer类构建脚本
  - secwebserver_test.mak

扩展提高



认证客户端

认证客户端

- 建立SSL连接时，客户端通常会要求服务器提供认证证书，认证通过后才能继续建立连接。相反服务器一般不会要求客户端提供认证证书
- 所谓双向认证，即在客户端认证服务器的同时，服务器也认证客户端，双方都要向对方提供自己的认证证书，任一方未通过认证，都不能建立SSL连接
- 在OpenSSL中实现双向认证，只需在单向认证的基础上，设置客户端的可信任CA证书和要求客户端提供认证证书的属性即可

知识讲解

认证客户端

- 设置对客户端的可信任CA证书

```
int SSL_CTX_load_verify_locations(SSL_CTX* ctx, const char* cafile, const char* cadir);
```

  - 例如：

```
SSL_CTX_load_verify_locations(ctx, "../pems/client_root_cer.pem", NULL);
```

知识讲解

认证客户端

- 设置对客户端的可信任证书链深度

```
int SSL_CTX_set_verify_depth(SSL_CTX* ctx, int depth);
```

  - 例如：

```
SSL_CTX_set_verify_depth(ctx, 1);
```

知识讲解

认证客户端

- 设置要求客户端提供认证证书的属性

```
int SSL_CTX_set_verify(SSL_CTX* ctx, int mode, int (*verify_callback)(int, X509_STORE_CTX*));
```

  - 例如：

```
SSL_CTX_set_verify(ctx, SSL_VERIFY_PEER | SSL_VERIFY_FAIL_IF_NO_PEER_CERT, NULL);
```

知识讲解

基于IPSec的安全通信

基于IPSec的安全通信

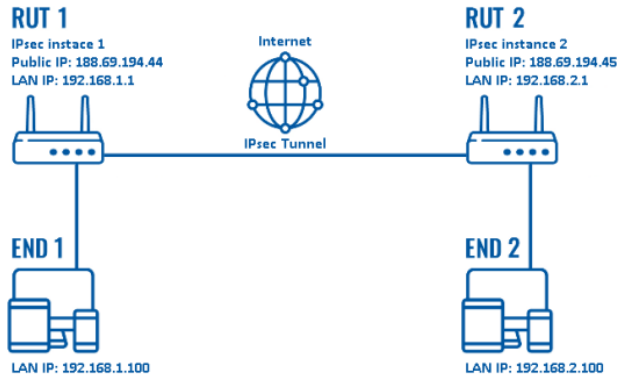
- SSL可以保证Web浏览器和Web服务器之间的安全通信，PGP和S/MIME可以实现安全的邮件传递，但所有这些安全技术都只能用于局部业务，并不能保证TCP/IP整体上的安全通信。为此，互联网工程任务组(The Internet Engineering Task Force, IETF)于1998年11月发布了IP安全标准IPSec，作为一种工作在开放互联网上的通用安全协议
- IPSec对IPv4是可选的，对IPv6则是强制的。IPSec是截至目前唯一一种可为任何形式的互联网通信提供安全保障的安全协议。同时，IPSec也是一套完整且易于扩展的基础网络安全解决方案

知识讲解

IPSec的体系结构

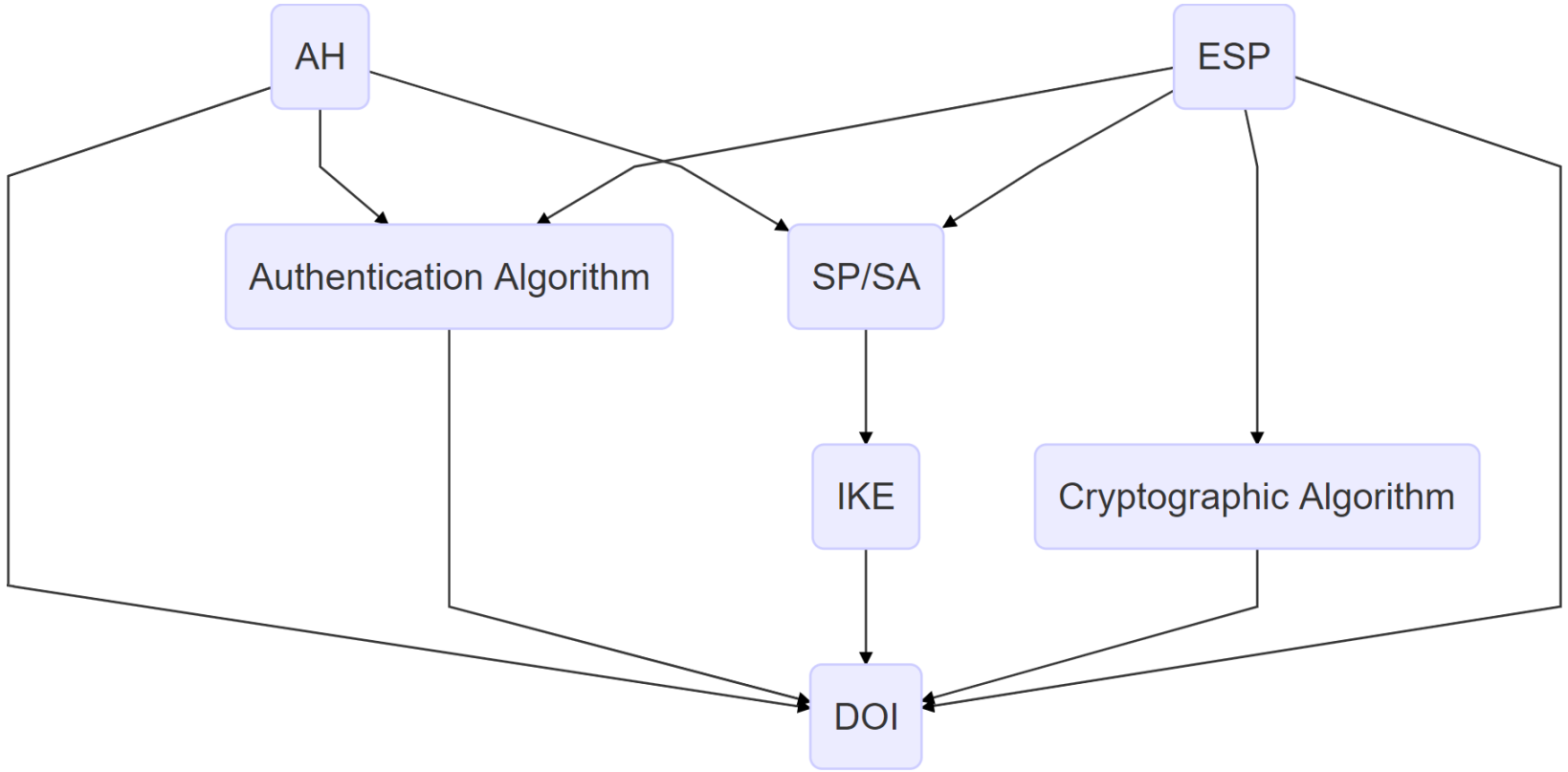
- IPSec协议是一个协议族，具体包括：
  - 认证头(Authentication Header, AH)协议
  - 封装安全载荷(Encapsulation Security Payload, ESP)协议
  - 互联网密钥交换(Internet Key Exchange, IKE)协议
  - 安全策略(Security Policy, SP)和安全联盟(Security Association, SA)
  - 解释域(Domain of Interpretation, DOI)

知识讲解



IPSec的体系结构

- IPSec的体系结构如下图所示：



知识讲解

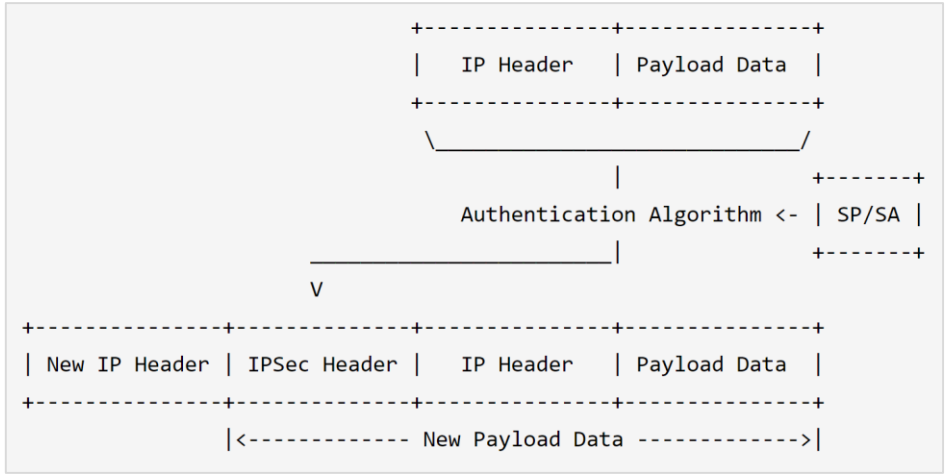
IPSec的体系结构

- IPSec的体系结构如下图所示：
  - 认证头(AH)和封装安全载荷(ESP)都是插入IP包数据载荷部分的协议头，为IP通信提供数据源认证、抗重播、数据完整性校验等安全服务。此外，封装安全载荷(ESP)还负责提供机密性服务
  - 安全策略(SP)决定两个实体之间能否通信以及如何通信。所有的安全策略(SP)都存放在安全策略库(Security Policy Database, SPD)中。针对库中的每条安全策略均可定义丢弃、绕过或应用IPSec三种行为中的一种
  - 那些被定义为应用IPSec的安全策略条目，均会指向一个或一串安全联盟(SA)。安全联盟(SA)包含针对IP包的各种安全参数，如安全协议、加密和认证算法、密钥及其生存周期、抗重播窗口大小等
  - 安全联盟(SA)既可以手动地静态创建也可以自动地动态创建，互联网密钥交换(IKE)会参与到动态创建安全联盟(SA)的过程中，以提供有关密钥协商的细节

知识讲解

IPSec的体系结构

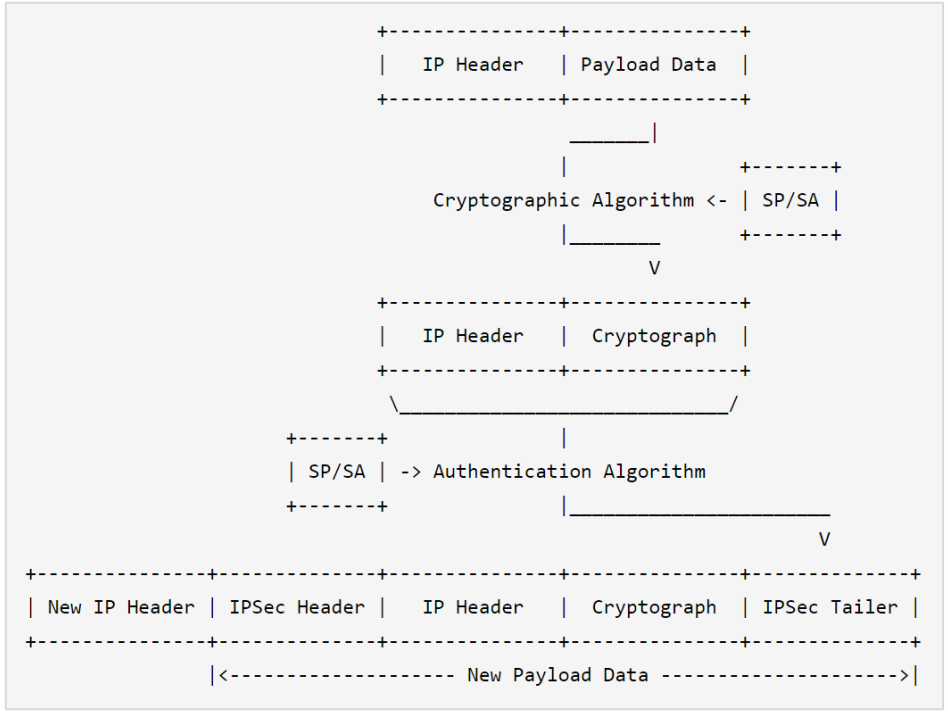
- AH
  - AH的工作机制就是根据SP/SA中的认证算法，对整个包括上层协议在内的IP包计算消息摘要并签名，以形成包含认证数据在内的IPSec头，作为数据载荷的一部分放入IP包
  - 接收时，重新计算原始IP包的消息摘要，并验证IPSec头中的数字签名，验证失败者一律丢弃，以此实现针对数据源的身份鉴别和数据本身的完整性保护



知识讲解

IPSec的体系结构

- ESP
  - ESP的工作机制是先根据SP/SA中的加密算法，对包括上层协议在内的IP包数据载荷进行加密，然后根据SP/SA中的认证算法，对加密得到的密文连同IP包头计算消息摘要并签名，以形成包含认证数据在内的IPSec尾，连同包含加密信息在内的IPSec头一起作为数据载荷的一部分放入IP包
  - 接收时，重新计算密文连同IP包头的消息摘要，并验证IPSec尾中的数字签名，验签通过后再根据IPSec头中的加密信息对密文部分做解密，以此实现针对数据源的身份鉴别和数据本身的完整性与机密性保护



知识讲解

IPSec的体系结构

- IKE
  - IKE的主要任务就是在动态创建SA的过程中为其提供被称为“保护套件”的安全参数，其中包括：
    - 加密算法
    - 摘要算法
    - 验证算法
    - Diffie-Hellman组
      - Diffie-Hellman (DH)算法是一种公共密钥算法，通信双方在不传送密钥的情况下通过交换一些数据，计算出共享的密钥
  - IKE是一个用户态进程，系统启动后即以守护进程的方式运行于后台，可通过以下两种方式请求IKE服务：
    - SP要求动态创建SA
    - 远程IKE需要协商SA

知识讲解

IPSec的体系结构

- IKE
  - IKE协商分为两个阶段：
    - 第一阶段：通过协商创建一个经过认证的安全信道，为双方的后续通信提供机密性、完整性和源认证服务
    - 第二阶段：在第一阶段所建SA的保护下完成IPSec的具体协商
  - IKE协商包括三对消息：
    - SA交换消息：协商确认有关SP的细节
    - 密钥交换消息：交换Diffie-Hellman公共值和辅助数据(随机数)
    - 身份ID和认证数据交换消息：对身份和整个SA交换过程的认证

知识讲解

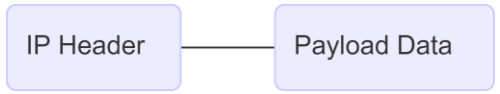
IPSec的体系结构

- SP和SA
  - 每个SP由选择符和策略项两部分组成：
    - 选择符来自网络层和传输层，如源地址及端口、目的地址及端口、传输层协议等
    - 策略项为丢弃、绕过或应用IPSec三种行为之一
  - 每个以应用IPSec作为策略项的SP均有一个SA与之对应，其中包含一系列经协商产生的安全约定：
    - 用于保护数据安全的IPSec协议，AH或者ESP
    - 转码方式
    - 密钥及其有效期
  - SA是单向的：
    - 如果主机A和B通过ESP进行安全通信，那么主机A的SA (out)和主机B的SA (in)必须共享完全相同的安全参数
    - 同理主机A的SA (in)和主机B的SA (out)也必须共享完全相同的安全参数

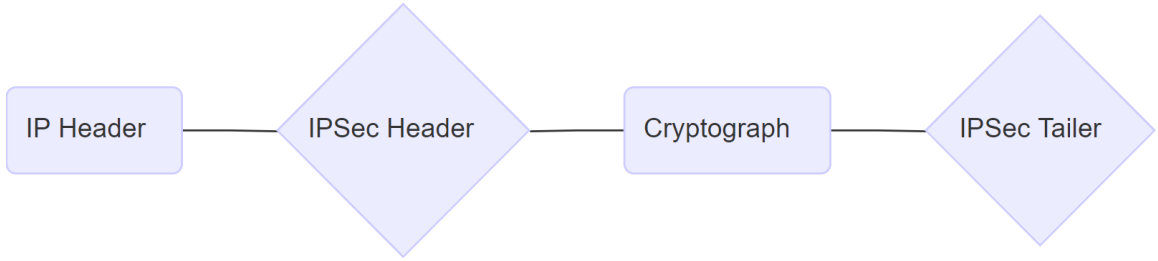
知识讲解

IPSec的工作模式

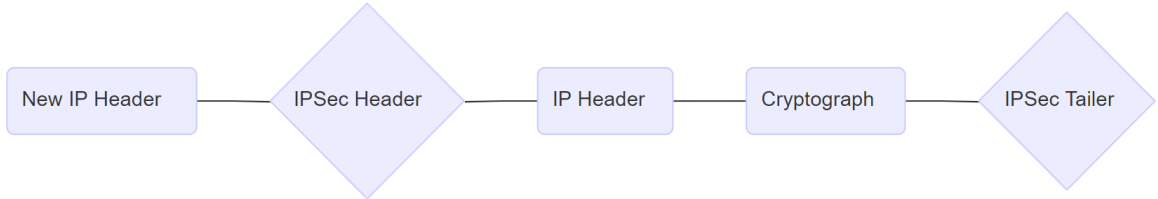
- 针对原始形态的IP包：



- IPSec有两种工作模式：
  - 传输模式：只保护传输层协议数据



  - 隧道模式：保护整个IP层协议数据



知识讲解

总结和答疑