网络安全协议及分析
传输层安全SSL和TLS

密码与网络安全系　刘虹

2025年春季学期

课程体系

第一章 概述

第二章 链路层扩展L2TP

第三章 IP层安全IPSec

第四章 传输层安全SSL和TLS

第五章 会话安全SSH

第六章 代理安全Socks

第七章 网管安全SNMPv3

第八章 认证协议Kerberos

第九章 应用安全

本章学习目标

- SSLv3的记录层
- TLS协议
- SSL应用

提纲

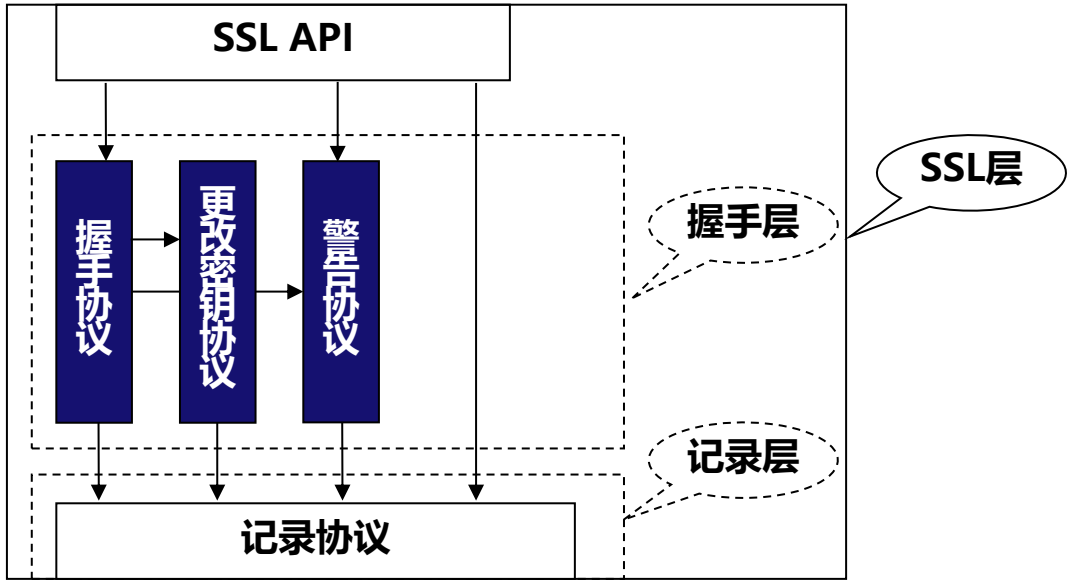
一、SSLv3的记录层

二、TLS协议

三、SSL应用及案例

SSL协议

- 从协议栈层次关系看，SSL位于应用层和传输层之间
- SSLv3是一个协议套件
  1. 握手协议
  2. 记录协议
  3. 更改密码规范协议
  4. 警告协议



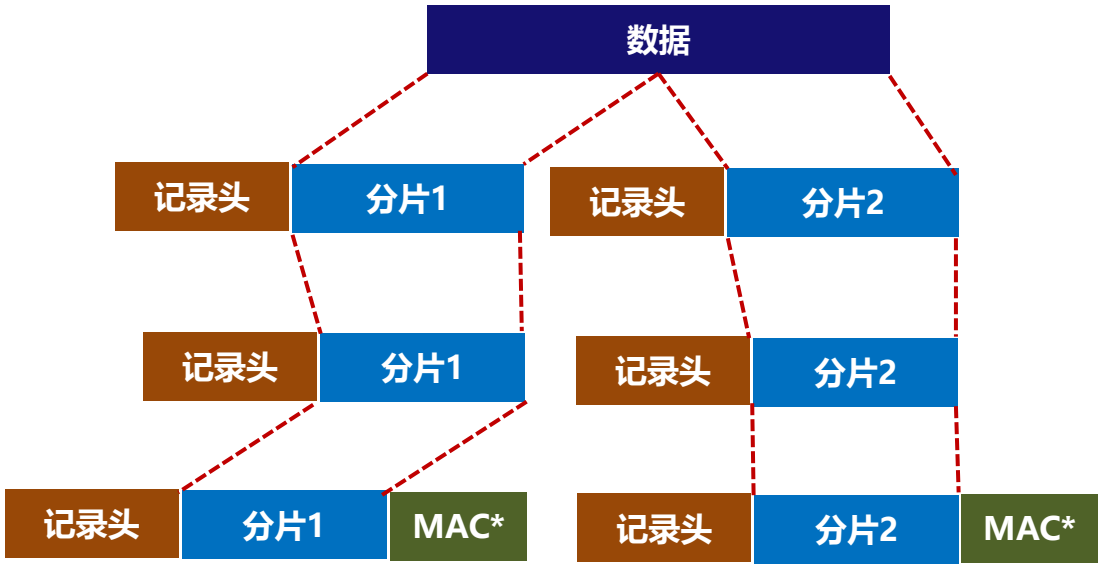
SSLv3记录

- 规范语言：
  - 杂项：/*...*/表述注释；[[ ]]表述可选项；opaque表述吴具体含义的单字节数据
  - 数字：uint8、uint16、uint24、uint32、 uint64
  - 向量：定长向量、变长向量
  - 枚举：某个变量的可能取值
  - 结构：某个变量由不同类型数据所组成
  - 变体：表示根据实际选择符的不同，可以选择不同的数据
  - 赋值：赋值即给一个变量赋予常量值

SSLv3记录

- 数据处理过程：分片→压缩→计算MAC→加密
  - 分片
  - 压缩
  - 计算MAC
  - 消息加密

- **序列密码算法**：密文包括数据和MAC两部分
- **分组密码算法**：除数据、MAC外，还包含“填充”和“填充长度”字段



提纲

一、SSLv3的记录层

二、TLS协议

三、SSL应用及案例

二 TLS协议

- 协议描述
  - 在协议框架描述方面，TLS包括记录层和握手层两个协议，握手、更改密码规范和警告作为记录层协议的子协议描述。
- MAC计算
  - SSLv3：MD5、SHA-1
  - TLSv1：HMAC

- MAC= Hash(Mcs | pad_2 |(Hash(Mcs | pad_1 | seq_num| SSLCompressed.type | SSLCompressed.length | SSLCompressed.fragment))
- MAC= HMAC_Hash(Mcs, seq_num | TLSCompressed.type | TLSCompressed.version | TLSCompressed.length | TLSCompressed.fragment)

二 TLS协议

- 密钥导出
  - PRF（Pseudo-Random Function，伪随机函数），在定义该函数之前，TLS首先定义**数据扩展函数**。

```
P_hash(secret, seed)=
                    HMAC_hash(secret, A(1) | seed) |
                    HMAC_hash(secret, A(2) | seed) |
                    HMAC_hash(secret, A(3) | seed) |...

A(0) = seed
A(1) = HMAC_hash (secret, A(i-1))
PRF(secret, label, seed) = P_<hash> (secret, label | seed)
```

二 TLS协议

- 散列函数输入
  - Certificate Verify和Finished消息中都需求计算散列值

Certificate Verify

- H_MD5 = MD5 (handshake_messages)
- H_SHA = SHA (handshake_messages)

- 填充长度
  - SSLv3的填充数据仅应填满一个分组长度
  - TLS的填充则允许在填满一个分组长度后，继续填充成任意个分组。

二 TLS协议与其子协议

- TLS 握手协议还能细分为 5 个子协议：
  - 1.change_cipher_spec (在 TLS 1.3 中这个协议已经删除，为了兼容 TLS 老版本，可能还会存在)
  - 2.alert
  - 3.handshake
  - 4.application_data
  - 5.heartbeat (TLS 1.3 新加的，TLS 1.3 之前的版本没有这个协议)
    - 这些协议之间的关系可以用SSL/TLS协议子关系图来表示：

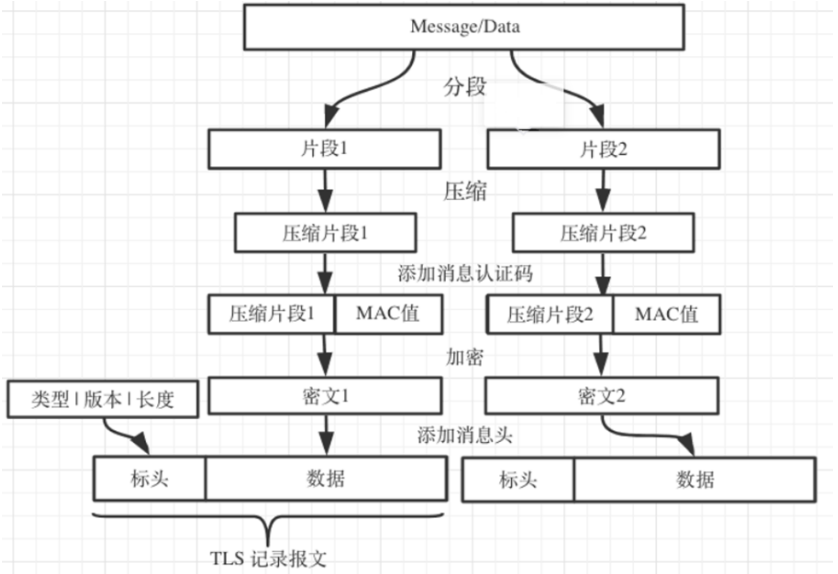
二 TLS1.2与TLS1.3在子协议上的区别

- **TLS 记录层在处理上层 5 个协议(密码切换协议，警告协议，握手协议，心跳协议，应用数据协议)的时候，TLS 不同版本对不同协议加密的情况不同，具体情况如下：**

协议版本	密码切换协议	警告协议	握手协议	心跳协议	应用数据协议
TLS1.3	无此协议	根据连接状态不同进行加密，即一部分会加密	一部分加密	不加密	加密
TLS1.2	不加密	不加密	不加密	无此协议	加密

二 TLS记录层协议

- 记录层
  - 将上层的信息块分段为TLSPlaintext记录，每一条TLS记录以一个短表头开始。原始消息经过分段 (或者合并)、压缩、添加认证码、加密转为 TLS 记录的数据部分。其中对上层应用数据协议进行密码保护，对其他的子协议只是简单封装(即不加密)。
    - 图片为记录层将不同的自握手协议进行封装处理的过程：（封装后加上消息头，打包往下给TCP处理)



二 TLS记录层协议

对握手层协议的枚举类型如图：

```
enum {
    invalid(0),
    change_cipher_spec(20),
    alert(21),
    handshake(22),
    application_data(23),
    heartbeat(24),  /* RFC 6520 */
    (255)
} ContentType;
```

ContentType 是对握手协议的封装，消息头类型和握手层子协议编号的对应关系如下：

消息头类型	ContentType
change_cipher_spec	0x014
alert	0x015
handshake	0x016
application_data	0x017
heartbeat (TLS 1.3 新增)	0x018

二 TLS记录层协议

- 记录层协议结构如下：
  - 其中length是TLSPlaintext.fragment 的长度。长度不得超过 2^14 字节。接收超过此长度的记录的端点必须使用 “record_overflow” alert 消息终止连接；fragment是正在传输的数据。此字段的值是透明的，它并被视为一个独立的块，由类型字段指定的更高级别协议处理。

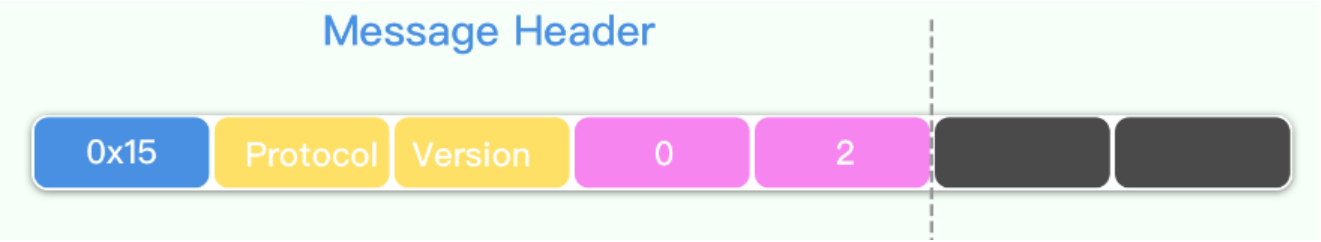
  - 当尚未使用密码保护时，TLSPlaintext 结构是直接写入传输线路中的。一旦记录保护开始，TLSPlaintext 记录将受到密码保护。

二 TLS密码切换协议

- 注意：该协议在 TLS 1.3 标准规范中已经删除，但是实际使用中为了兼容 TLS 老版本和一些消息中间件，所以实际传输中还可能用到这个协议。
  - 作用：该协议是TLS记录层对应用数据是否进行加密的分界线。客户端或者服务端一旦收到对端发送的密码切换协议，就表明接下来传输数据过程中可以对应用数据进行加密了。
  - 经过记录层包装后，结构如下：

二 TLS警告协议

- 作用：该协议用来表示关闭信息和错误
  - 经过TLS记录层包装后，结构如下：



二 TLS警告协议

- TLS 1.2 的所有警告描述信息如右图
  - 收到close_notify警告后，表明连接从一个
  - 方向开始有序的关闭，收到这个警报后，
  - TLS实现方应表明应用程序的数据结束。

```
enum {
      close_notify(0),
      unexpected_message(10),
      bad_record_mac(20),
      decryption_failed_RESERVED(21),
      record_overflow(22),
      decompression_failure(30),
      handshake_failure(40),
      no_certificate_RESERVED(41),
      bad_certificate(42),
      unsupported_certificate(43),
      certificate_revoked(44),
      certificate_expired(45),
      certificate_unknown(46),
      illegal_parameter(47),
      unknown_ca(48),
      access_denied(49),
      decode_error(50),
      decrypt_error(51),
      export_restriction_RESERVED(60),
      protocol_version(70),
      insufficient_security(71),
      internal_error(80),
      user_canceled(90),
      no_renegotiation(100),
      unsupported_extension(110),
      (255)
  } AlertDescription;
```

二 TLS握手协议

- 注意：该协议在TLS1.2和TLS1.3版本发生了很大变化，两个版本在密钥协商和密码套件选择上都有很大不同
  - 作用：双方将通过这个协议协商出密码块，这个密码块会交给 TLS 记录层进行密钥加密。也就是说握手协议达成的“共识”(密码块)是整个 TLS 和 HTTPS 安全的基础。
  - 经过 TLS 记录层包装以后，结构如下:

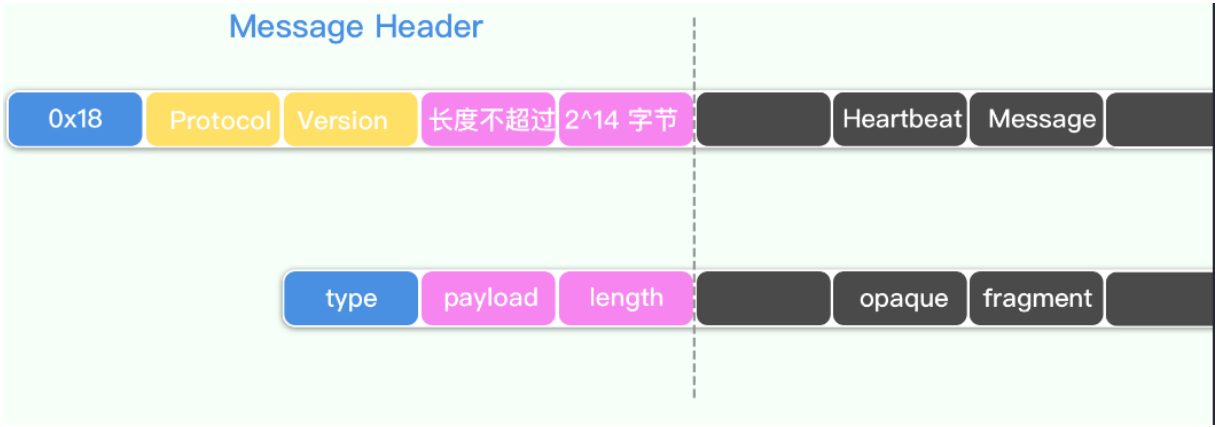
二 TLS应用数据协议

- 作用：该协议就是TLS上层的各种协议，TLS将主要保护的数据数据放在该协议里。
  - 经过 TLS 记录层包装以后，结构如下:

  - TLS记录层会根据加密模式的不同在应用数据末尾加上MAC检验数据

二 TLS心跳协议

- TLS1.3新加的协议
  - 作用：允许在不需要重协商的情况下，使用 keep-alive 功能。
  - 经过 TLS 记录层包装以后，结构如下:



提纲

一、SSLv3的记录层

二、TLS协议

三、SSL应用及案例

三 利用SSL保护高层应用安全

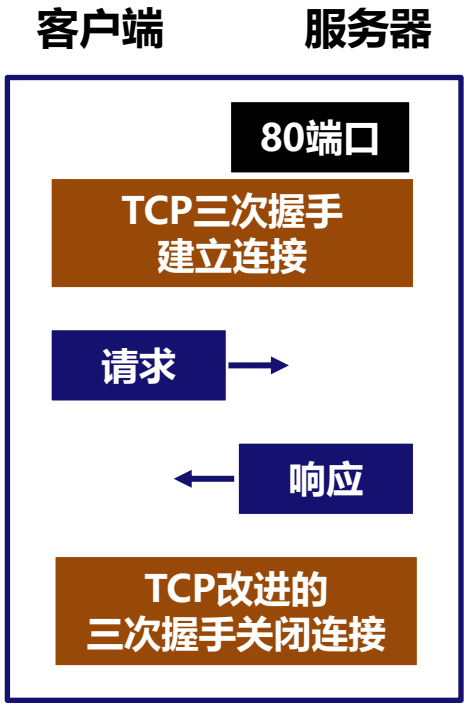
- 分设端口
  - 为不同的访问方式提供不同的监听端口。
  - HTTP客户端使用普通方式访问web服务器时，与80号端口建立连接，否则与443号端口建立连接，其他协议的使用方式类似。基于SSL的协议通常在协议后添加一个S作为标识。

http：//wwwexamplewebsite.cn/examplewebpage.html

https：//wwwexamplewebsite.cn/examplewebpage.html　443号端口

三 利用SSL保护高层应用安全

- 从协议时序的角度
  - SSL的引入对高层应用的协议时序没有影响，只是比普通访问增加了SSL握手及安全断连步骤；
- 从语法和语义的角度
  - 安全访问方式下的通信数据要经过安全处理和安全验证，应用层的数据不再是字节流，而是记录。



三 利用SSL保护高层应用安全

- 向上协商的策略需要修改应用层协议
  - 220：Ready to start TLS
  - 501：Syntax error
  - 504：TLS not available due to temporary reason

SSL VPN 技术在校园网中的应用

- 身份鉴别
- 访问策略
- 数据转发

三 SSL证书

- **SSL证书：**
  - **域名验证型证书**
    - **单域名证书就是只针对用户只有一个域名的情况，一个域名对应一个证书。通常用于比较简单的网站。**
    - **多域名证书则是一个证书可以保护多个不同的域名，根据证书发放机构的不同，证书支持的域名数也各不相同。**
    - **通配符证书则是涵盖根域名或主机名上的所有内容的类型，最重要的是它将包括所有子域名，所有这些域名都将被通配符SSL证书覆盖。**
  - **组织验证型证书**
  - **扩展验证型证书**

三

TLS的安全问题

- TLS 所采用的加密算法的漏洞
- TLS 版本兼容带来的漏洞
- TLS 实现的漏洞
- TLS 所使用的数字证书漏洞

三 TLS的安全问题

- Cipher Block Chaining (CBC) 加密模式
  - 如果攻击者获得了合法的密文，可以通过不断的向服务器发送篡改的信息，通过观察服务器返回的信息，即可知道构造内容是否正确。

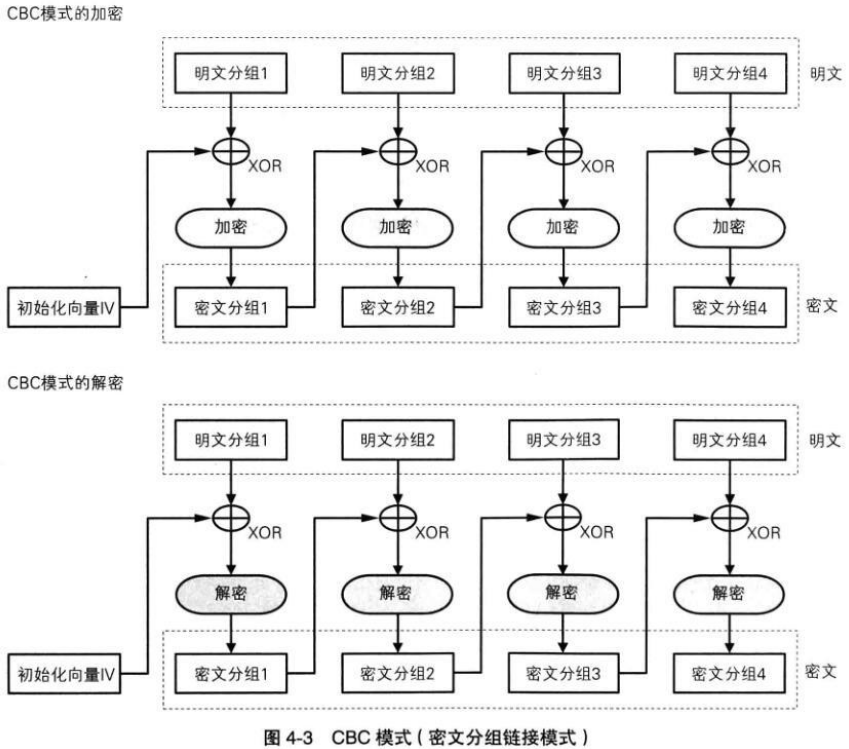


图 4-3 CBC 模式（密文分组链接模式）

三 TLS的安全问题

- Lucky Thirteen 攻击
  - 利用填充的不确定性，攻击者能够通过修改填充的内容来进行测试。
  - 引发攻击的最重要原因是填充，使用CBC 模式，并且利用TLS 完整性保护机制。攻击者可以通过修改填充字节并观察服务器做出的响应和响应时间，从而提取相关信息，判断修改的内容是否正确。

三 TLS的安全问题

- POODLE 攻击
  - 造成POODLE 攻击的根本原因也是CBC 模式在设计上的缺陷，CBC 只对明文进行了身份验证，而没有对填充字节部分进行完整性验证。
  - 在进行POODLE 攻击时，攻击者能够截获密文，正常情况下，直接修改填充字节的内容的方法是不可行的，因为如果改变了MAC 值时会引发错误，只有当最后整个块都是填充数据时，攻击者才能够可以进行自由的修改并且不会导致MAC 校验的失败。

三 TLS的安全问题

- BleichenBacher攻击
  - 攻击者能够通过修改ClientHello 信息，使SSL 3 版本看起来像SSL 2 版本的ClientHello 信息，强制服务器使用漏洞更多的SSL 2。
  - 为了应对Bleichenbacher 攻击，从RFC 2246（TLS 1.0）开始的所有TLS RFC 建议“以与正确格式化的RSA 块不可区分的方式处理错误格式化的消息”

三 TLS的安全问题

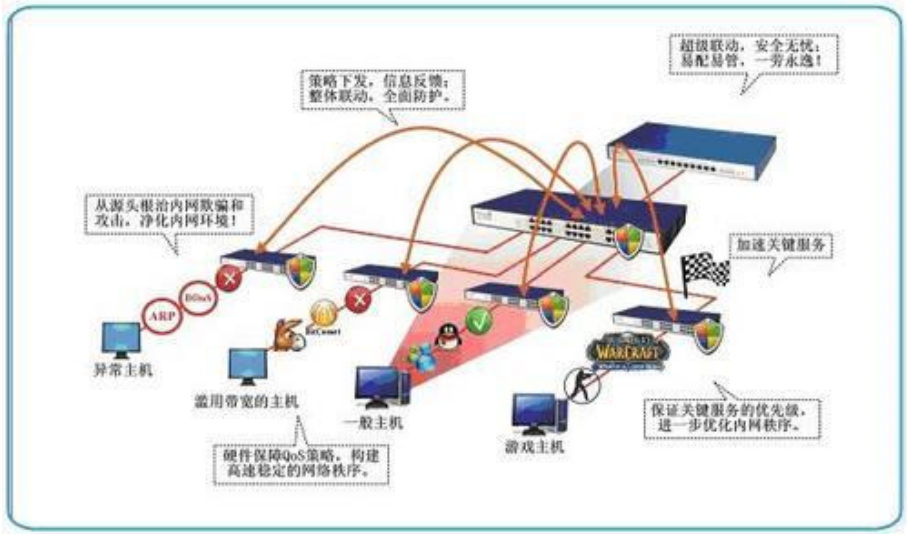
- DROWN 攻击
  - SSLv2 虽然是退役的协议，但是还有大量的服务器支持该协议，没有完全移出废弃协议，从而导致严重的后果。
  - 利用该漏洞，观察服务器的响应来解密的RSA 密文信息。并且利用这个这个漏洞，攻击者可以在没有RSA 密钥私钥的情况下，可以完成跨协议的攻击，来解密SSLv3 或者更高级的TLS 会话。
  - 就算服务器本身不支持SSLv2，但是与使用SSLv2 的服务器共享RSA密钥，也会受到DROWN 攻击的连锁反应。

三 TLS的安全问题

- 单字节（双字节）偏差攻击
  - 这种类型的偏差在密码学中是极其危险的，只要知道了RC4密钥流中的第二字节倾向于0，那么就能够知道经过加密的密文的第二字节。其他存在偏差的字节也是同样的。
  - 如果要在TLS 中进行攻击，需要建立多个连接，获取相同明文被多种不同密钥加密的密文数据。
  - 观察第二字节的值，如果出现频率较高，那么这个值很可能就是明文内容中的相同值。

二 TLS的安全问题

- 三次握手攻击
  - 三次握手攻击，利用的漏洞是协议的设计问题，主要是利用TLS 协议的RSA/DH 密钥交换缺陷和会话恢复的缺陷来绕过防护措施。



三 TLS的安全问题

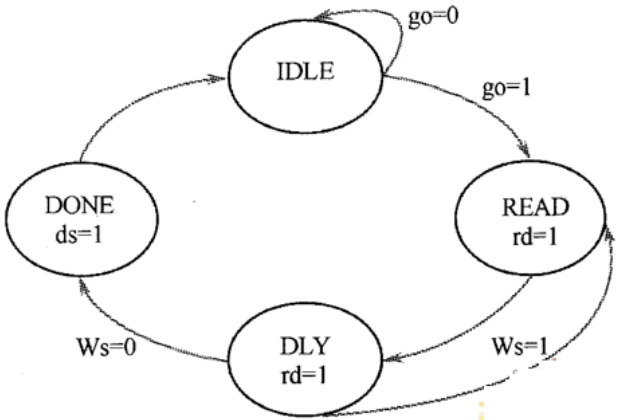
- SLOTH 攻击
  - 攻击者使用弱哈希算法，如客户端可以利用MD5 进行降级攻击。
  - 在握手的初期，客户端将ClientHello 数据包发生给服务器；数据包中声明了服务器可以使用的签名和加密算法。
  - TLS 被降级后，中间人攻击者就可以冒充服务器，解密所有加密的流量。

三 TLS的安全问题

- 降级攻击
  - 降级攻击是攻击者使用一些策略，让服务器和客户端采用比较弱的协议或者加密方式的一种攻击。
  - 在这种攻击中，主动网络攻击者干扰协商，导致诚实的对等方完成密钥交换，尽管使用的方式比自己使用的模式弱。
  - 为了防止对特定协议模式的攻击，关闭导致其协商的配置也是必要的

三 TLS的安全问题

- 利用状态机检测漏洞
  - 在TLS 协议的实现中，必须处理各种版本协议和相关的扩展，认证模式和密钥交换的方法，而不同的组合在客户端和服务器端之间又形成了不同的消息序列。



三 TLS的安全问题

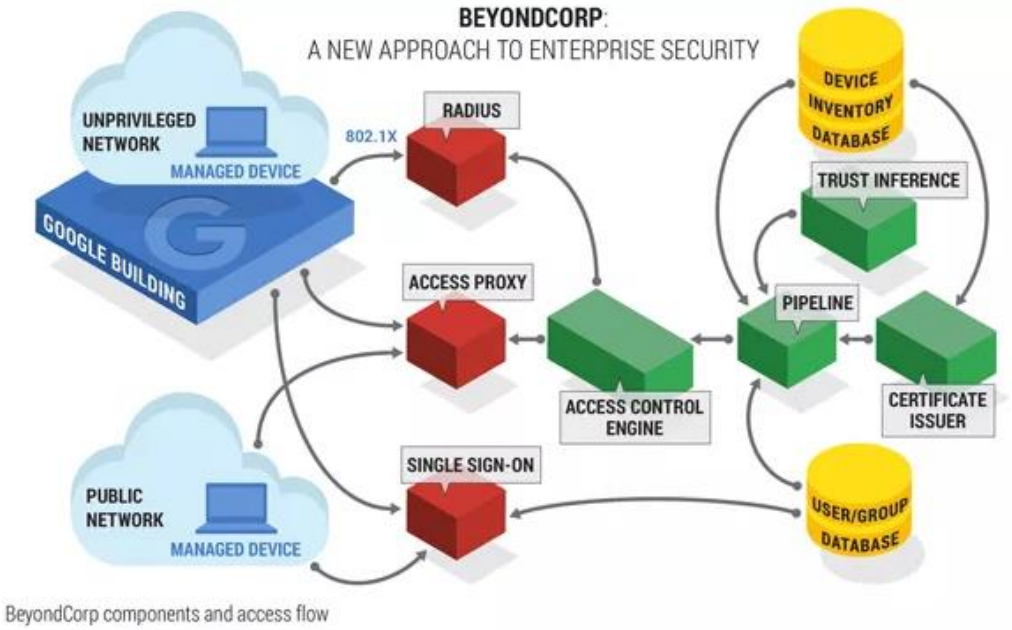
- 心脏出血
  - Heartbleed 是OpenSSL 实现上存在的漏洞，通过发送特殊信号Heartbeat 给服务器，来查看服务器是否在线，当服务器在线时，会发送回复信息给主机，然后允许进行安全地发送这个信号确保对方是否在线。

三 小结

- SSL增强传输层的安全性，为高层应用提供较为通用的安全方案。
- 提供机密性、完整性、服务器认证以及可选的客户端认证服务。
- SSL协议套件由握手、更改密码规范、警告和记录协议构成。
  - 握手协议实现算法协商、密钥生成和身份认证，支持会话恢复等握手方式。
  - 更改密码规范协议用以通告对等端使用新的安全参数来保护数据
  - 警告协议则同时具备安全断连和错误通告功能。
  - 记录协议是SSL数据承载层，高层应用及其他三个协议的数据都封装在记录中传递。

谷歌的零信任架构

- 零信任
  - 中心思想是不应自动信任内部或外部的任何人/事/物，应在授权前对任何试图接入企业系统的人/事/物进行验证。



BeyondCorp components and access flow

办公地点：理科大楼B1209

联系方式：17621203829

邮箱：liuhongler@foxmail.com