2023-2024学年秋季学期

Web安全技术

Web Security

授课团队：刘奇旭、刘潮歌

学生助教：曹婉莹、孙承一

Web安全技术

Web Security

1.3 HTTP与Cookie

刘潮歌

liuchaoge@iie.ac.cn

2022年9月19日

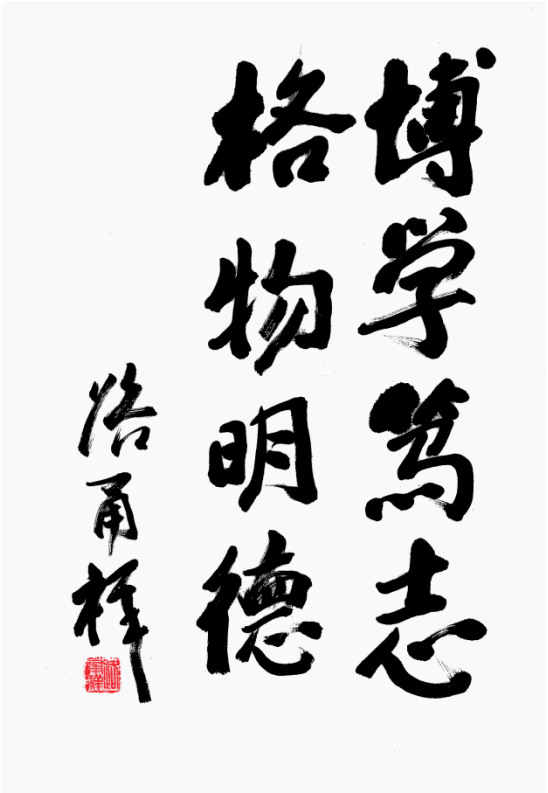
中国科学院大学
University of Chinese Academy of Sciences

一章一问

- HTTP协议和Cookie有哪些安全问题，现在有哪些解决办法？

本章大纲

- **HTTP及安全问题**
  - 基础知识回顾
  - HTTP安全问题
  - HTTPS协议
- **Cookie及安全问题**
  - 基础知识
  - 安全策略
  - 安全问题



基础知识回顾

- **概述**
- HTTP（Hyper Text Transfer Protocol），超文本传输协议
- 一个为分布式、合作式、多媒体信息系统服务的协议
- 功能是在客户端和服务器之间传输超文本数据
- 从协议栈上看，属应用层，基于TCP/IP层进行数据传输

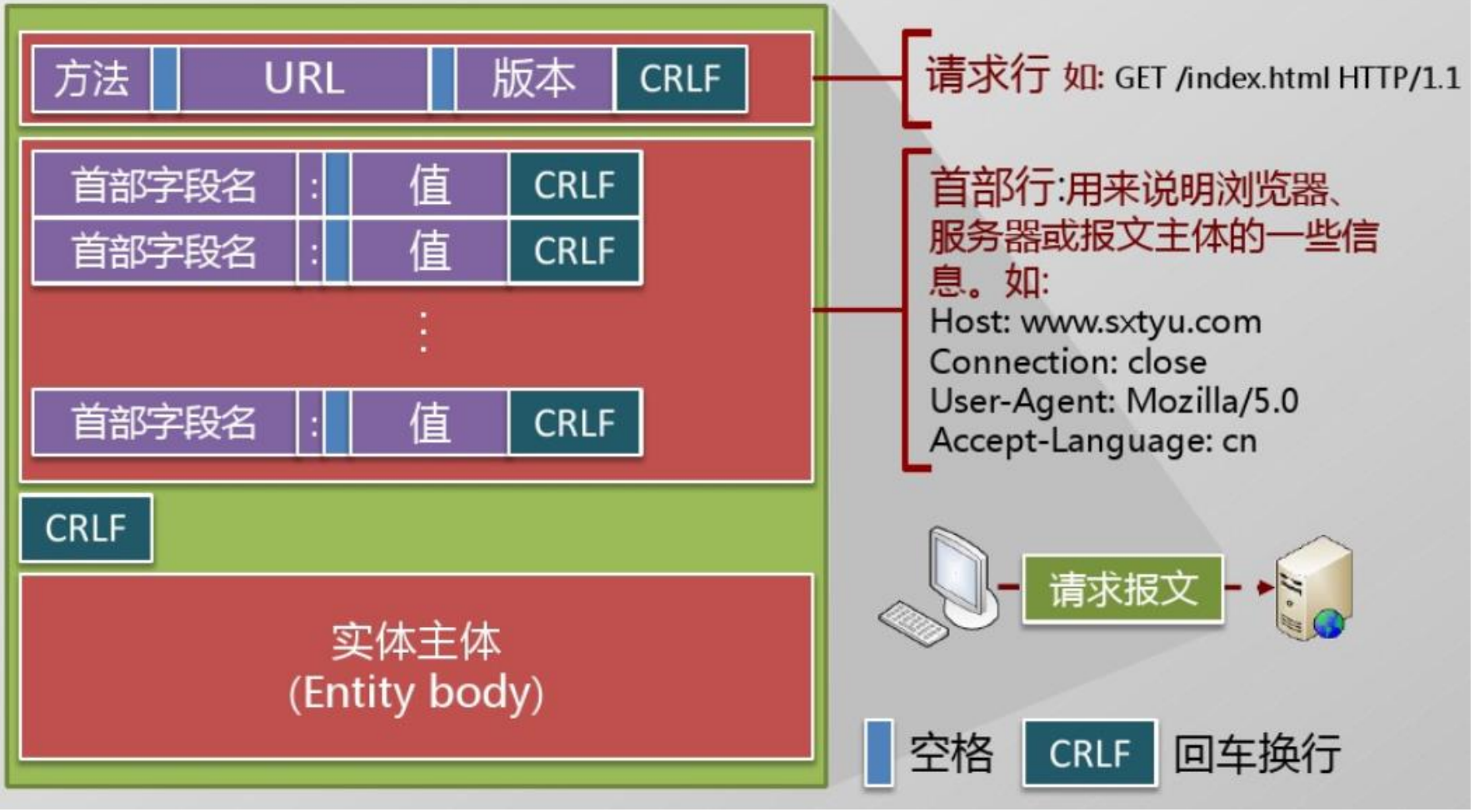
基础知识回顾

- 工作流程
- HTTP是位于TCP层上的应用层协议
- 基于<请求-响应>工作模式
- 典型流程：

1. 客户端与运行HTTP服务器的主机建立TCP连接（三次握手）；
2. 客户端通过与TCP连接发出HTTP请求消息（GET/POST…）；
3. 服务器接受到请求后，解析并处理请求，然后发出HTTP响应消息；
4. 重复步骤3~4（HTTP 1.1）；
5. 关闭TCP连接（四次挥手）。

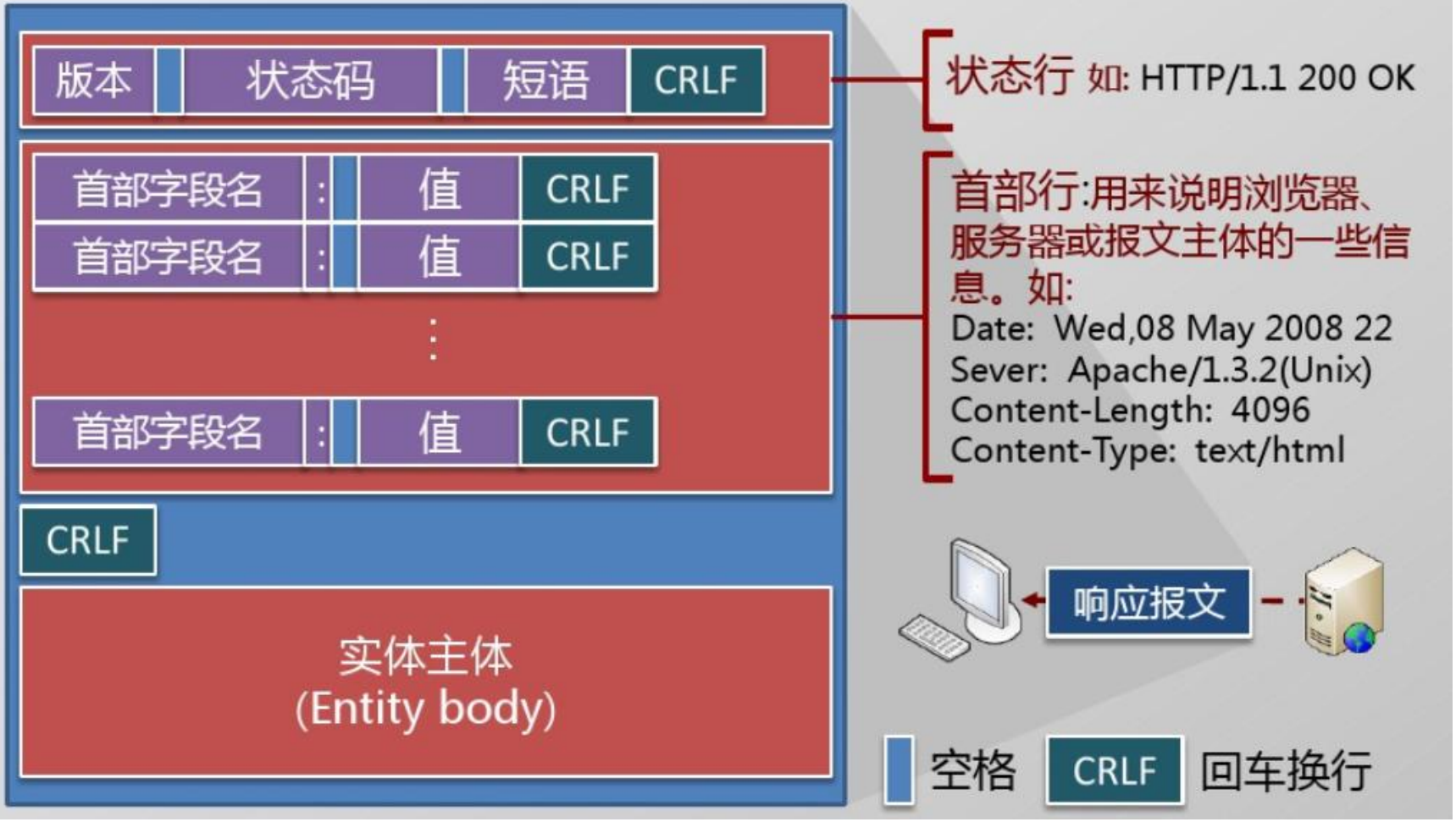
请求报文

即从客户端(浏览器)向Web服务器发送的请求报文。报文的所有字段都是ASCII码。



响应报文

即从Web服务器到客户机(浏览器)的应答。报文的所有字段都是ASCII码。



首部字段或消息头

头(header)	类型	说明
User- Agent	请求	关于浏览器和它平台的信息，如Mozilla5.0
Accept	请求	客户能处理的页面的类型，如text/html
Accept-Charset	请求	客户可以接受的字符集，如Unicode-1-1
Accept-Encoding	请求	客户能处理的页面编码方法，如gzip
Accept-Language	请求	客户能处理的自然语言，如en(英语)，zh-cn(简体中文）
Host	请求	服务器的DNS名称。从URL中提取出来，必需。
Authorization	请求	客户的信息凭据列表
Cookie	请求	将以前设置的Cookie送回服务器器，可用来作为会话信息
Date	双向	消息被发送时的日期和时间
Server	响应	关于服务器的信息，如Microsoft-IIS/6.0
Content-Encoding	响应	内容是如何被编码的（如gzip）
Content-Language	响应	页面所使用的自然语言
Content-Length	响应	以字节计算的页面长度
Content-Type	响应	页面的MIME类型
Last-Modified	响应	页面最后被修改的时间和日期，在页面缓存机制中意义重大
Location	响应	指示客户将请求发送给别处，即重定向到另一个URL
Set-Cookie	响应	服务器希望客户保存一个Cookie

抓包分析

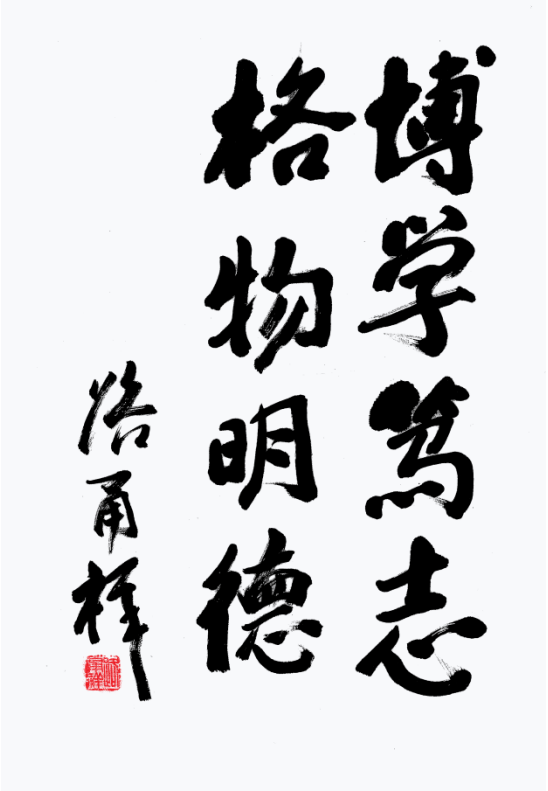
```
GET /jggk_101117/skjj/201501/t20150127_4305430.html HTTP/1.1
Host: www.iie.cas.cn
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.278
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, sdch
Accept-Language: zh-CN,zh;q=0.8
Cookie: _gscu_1321407670=7442817828th0p10; _gscs_1321407670=74428178qfwzh610|pv:3

HTTP/1.1 200 OK
Date: Wed, 21 Sep 2016 03:23:58 GMT
Server: Apache/2.4.23 (Unix)
Accept-Ranges: bytes
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html

873
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<META http-equiv=x-ua-compatible content="IE=7, IE=9">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>.....----.....</title>
<meta name="keywords"
content=".....
....."/>
<meta name="description"
```

本章大纲

- **HTTP及安全问题**
  - 基础知识回顾
  - HTTP安全问题
  - HTTPS协议
- **Cookie及安全问题**
  - 基础知识
  - 安全策略
  - 安全问题



HTTP安全问题

- **数据明文传输**
- HTTP协议是明文传输协议，消息内容不经过加密处理
- 如果攻击者控制受害者传输网络，即可轻易嗅探或篡改传输内容

- **身份认证缺乏校验**
- 客户端与服务器通讯过程没有身份认证环节
- 客户端无法确认通信对方是正确的服务器

HTTP安全问题

- **数据明文传输**
- 网络嗅探与监听

- **身份认证缺乏校验**
- 中间人攻击

HTTP安全问题

- 网络嗅探与监听（Network Sniffer， Network Listening）
- 可以捕获网络报文
- Wireshark：经典的抓包工具

```
GET /jggk_101117/skjj/201501/t20150127_4305430.html HTTP/1.1
Host: www.iie.cas.cn
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.116 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, sdch
Accept-Language: zh-CN,zh;q=0.8
Cookie: _gscu_1321407670=7442817828th0p10; _gscs_1321407670=74428178qfwzh610|pv:3

HTTP/1.1 200 OK
Date: Wed, 21 Sep 2016 03:23:58 GMT
Server: Apache/2.4.23 (Unix)
Accept-Ranges: bytes
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html

873
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<META http-equiv=x-ua-compatible content="IE=7, IE=9">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>.....----.....</title>
<meta name="keywords"
content="..........
....."/>
<meta name="description"
```

传输信息
一览无遗

HTTP安全问题

```
POST /member.php?mod=logging&action=login&loginsubmit=yes&infloat=yes&lssubmit=yes&inajax=1 HTTP/1.1
Host: www.discuz.net
Connection: keep-alive
Content-Length: 82
Cache-Control: max-age=0
Origin: http://www.discuz.net
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.116 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://www.discuz.net/forum-3913-1.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8
Cookie: t7asq_4ad6_saltkey=uKklDAxI; t7asq_4ad6_lastvisit=1474424790;
t7asq_4ad6_st_t=0%7C1474428390%7Ce34820e74c71f8dc9eaf2f6ee23ba897; t7asq_4ad6_forum_lastvisit=D_3913_1474428390;
t7asq_4ad6_sendmail=1; t7asq_4ad6_lastact=1474428391%09plugin.php%09; pgv_pvi=6450992444; pgv_info=ssi=s1256806880

fastloginfield=username&username=abc&password=123456&quickforward=yes&handlekey=lsHTTP/1.1 200 OK
Server: nginx
Date: Wed, 21 Sep 2016 03:26:46 GMT
Content-Type: text/xml; charset=gbk
Transfer-Encoding: chunked
Connection: keep-alive
Cache-Control: no-store, private, post-check=0, pre-check=0, max-age=0
Set-Cookie: t7asq_4ad6_lastact=1474428406%09member.php%09logging; expires=Thu, 22-Sep-2016 03:26:46 GMT; path=/; domain=.discuz.net
Expires: -1
Cache-Control: no-store, private, post-check=0, pre-check=0, max-age=0
Pragma: no-cache
comsenz_tag: 28d312ca960a0c75e4bd3707a49d8e90
Content-Encoding: gzip
```

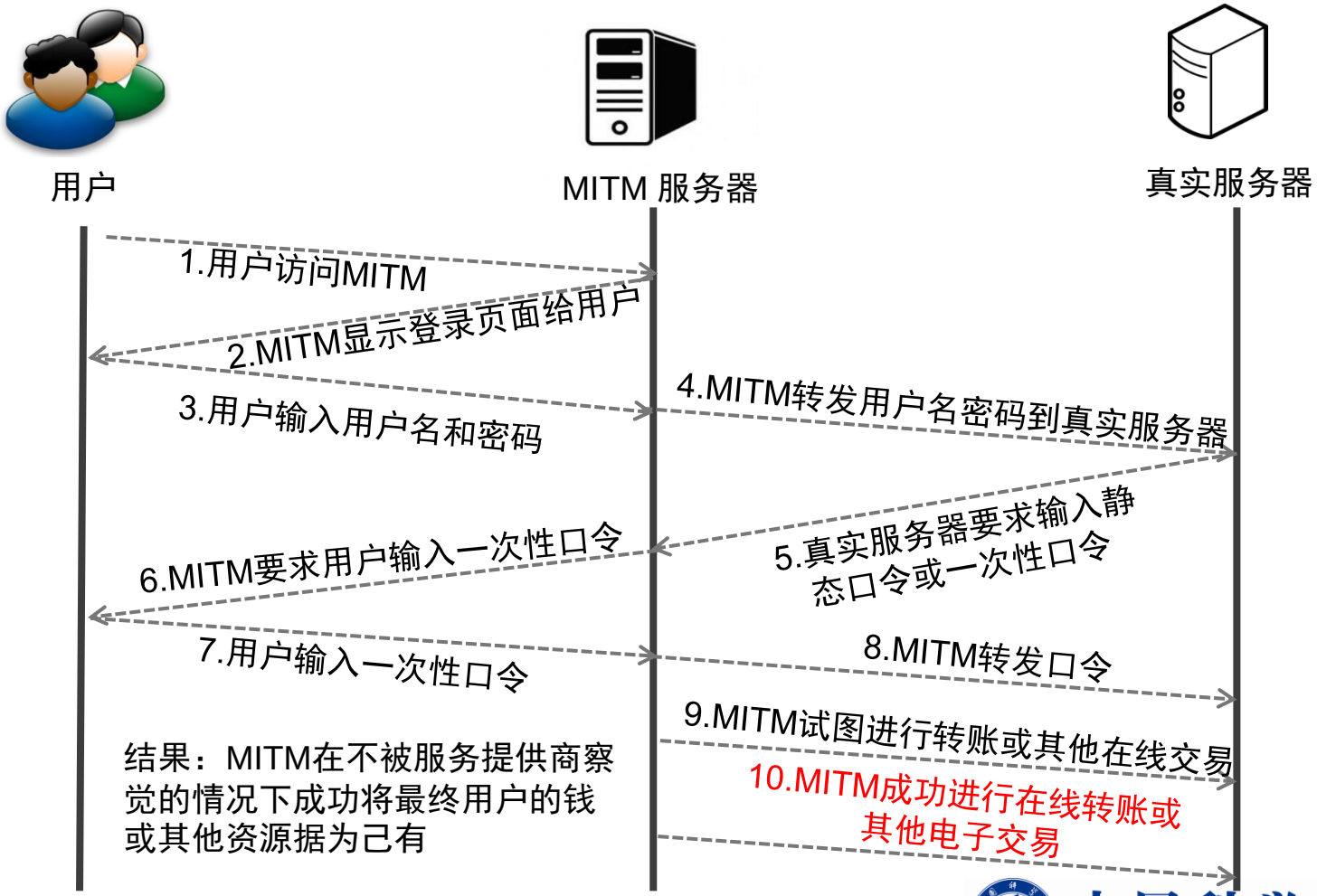
HTTP安全问题

- **中间人攻击（MITM，Man-in-the-middle attack）**
- 攻击者与通讯两端分别建立独立的联系，并交换其所收到的数据
- 通讯的两端认为他们正在直接与对方对话，但事际上整个会话都被攻击者完全控制
- 攻击成功的前提条件：攻击者能将自己伪装成全部参与会话的终端，并且不被识破

- 中间人攻击的重要原因是通信各端缺乏有效的认证

HTTP安全问题

- 中间人攻击（MITM，Man-in-the-middle attack）



HTTP安全问题

- **中间人攻击**
- 流量劫持和篡改
- 修改返回数据内容，如插入新的JavaScript脚本、iframe页面等
- 劫持网关设备、路由设备或者DNS，导致用户访问错误的网站
- 并非都是恶意的

HTTP安全问题

- 中间人攻击
- 流量劫持

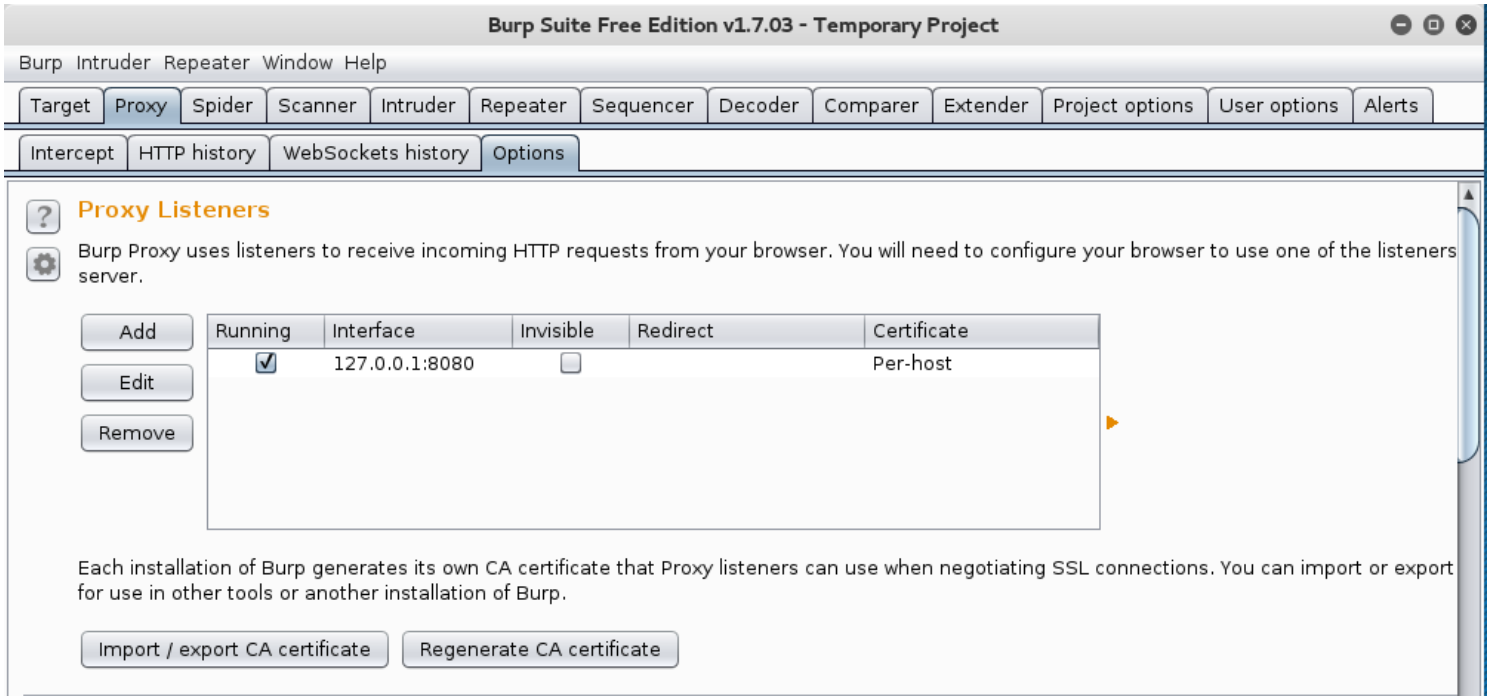
HTTP安全问题

- **中间人攻击**
- 典型工具——mitmproxy/mitmdump

- MITM神器：mitmproxy/mitmdump（交互版/非交互版）
- 开源托管在github，使用python开发，支持跨平台
- 能够捕获、分析、修改HTTP/HTTPS数据包

HTTP安全问题

- 中间人攻击
- 典型工具——Burp Suite



HTTP安全问题

- **典型攻击**
- 网络嗅探与监听，中间人
- **难点在于将恶意设备插入到通信链路中！**
- 无线网络监听
- 网络设备劫持：路由器、交换机、防火墙
- ARP欺骗
- 恶意钓鱼设备：Wifi
- DNS劫持

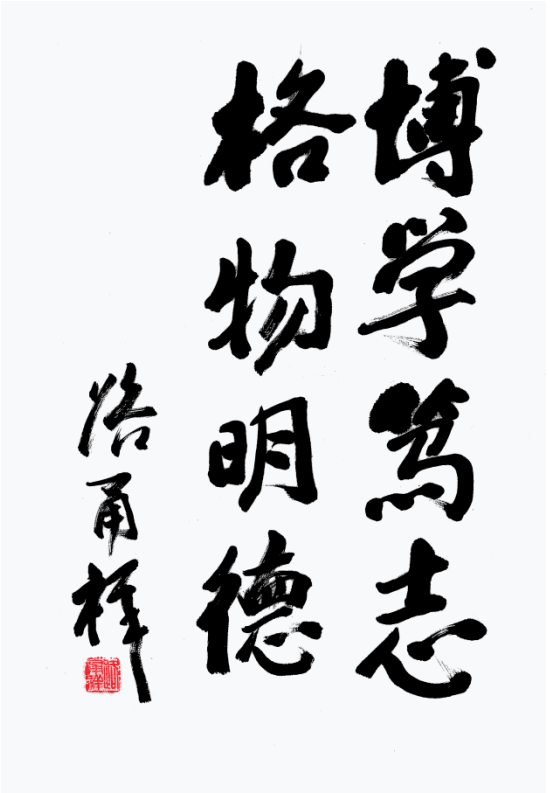
本章大纲

□ HTTP及安全问题

- 基础知识回顾
- HTTP安全问题
- HTTPS协议

□ Cookie及安全问题

- 基础知识
- 安全策略
- 安全问题



HTTPS协议

- **历史背景**
- Hyper Text Transfer Protocol over Security Socket Layer
- 1994年由Netscape创建，并在其Netscape Navigator浏览器中使用
- 初期HTTPS使用的是SSL协议，随着SSL协议逐渐演变成TLS协议，在2000年五月在RFC2818中正式确定了HTTPS标准

网络体系安全架构


OSI模型
TCP/IP模型
控制及应对措施
应用层
表示层
会话层
传输层
网络层
数据链路层
物理层
应用层
传输层
网络层
物理层
• 恶意程序扫描器
• PGP、S/MIME邮件加密器
• 安全的编码
• SSH、SET等安全协议
• Kerboeros协议
• TACACS等加密算法
SSL、TLS安全套接字技术
SOCKS代理技术
S/RPC
网络协议安全IPSEC
数据包过滤器
网络地址转换
NAT
点对点隧道协议（PPTP）
第二层隧道协议（L2TP）
询问握手认证协议（CHAP）
有线等效保密协议（WEP）
光纤

HTTPS协议

- 工作流程

- HTTPS同样也是应用层协议，相比HTTP多加入了SSL/TSL层
- 基于<请求-响应>工作模式
- 在正式传输数据前，先进行身份认证
- 认证成功后再协商传输的加密秘钥
- 后续的传输数据使用秘钥进行加密

HTTPS协议

- HTTPS通信中，客户端如何认证服务器身份？
- 通信密钥如何采用安全方式协商？

HTTPS协议

工作流程

1、客户端发起HTTPS请求

2、服务端准备公私钥和证书

3、服务端发送证书（含公钥）

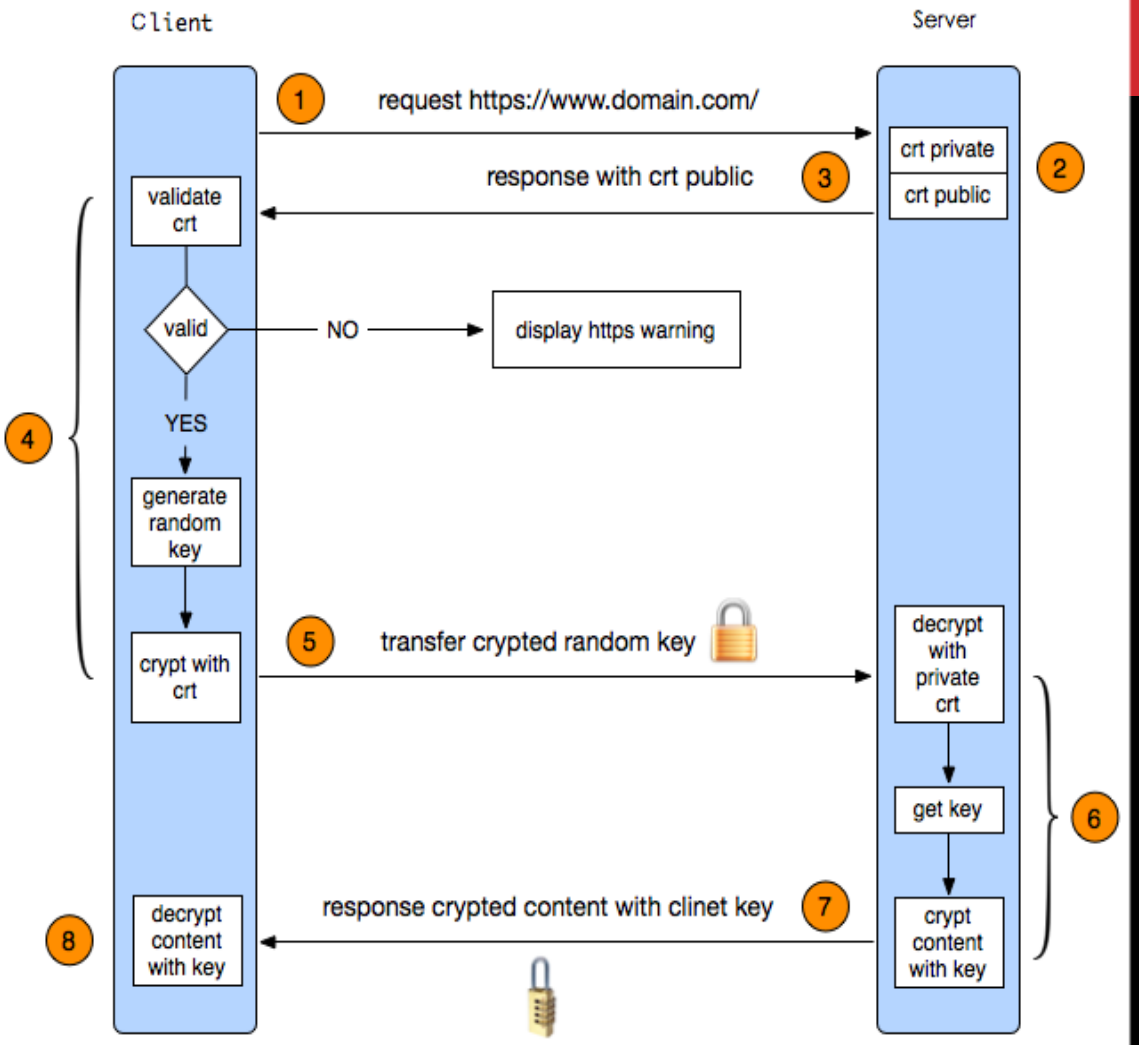
4、客户端解析证书

5、客户端生成对称密钥，并用公钥加密后，发送给服务端

6、服务端使用私钥解密，获得对称密钥

7、服务端使用对称密钥加密信息并发送

8、客户端使用对称密钥解密信息



HTTPS协议

- 要点
- 使用证书确认网站身份
  - 证书由专门的CA机构颁发，携带公钥信息，不可伪造或篡改
- 基于非对称密钥分发对称密钥
  - 客户端用公钥加密，服务器用私钥解密
  - 确保用于通信的对称密钥，不被攻击者监听获取
- 使用对称密钥通信
  - 加解密效率高

知识点1：数字证书

知识点2：非对称加密

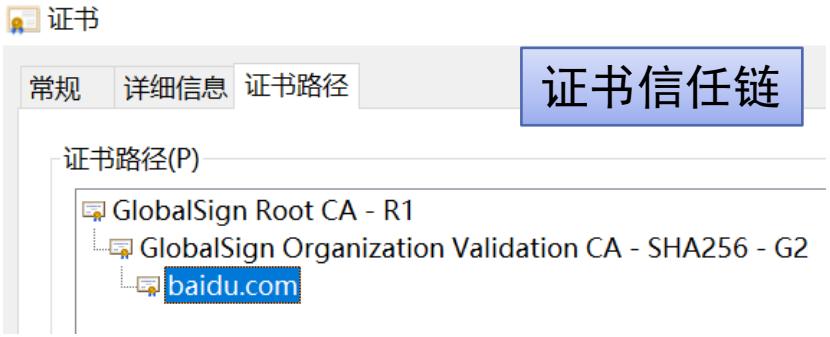
知识点3：对称加密

知识点1：数字证书

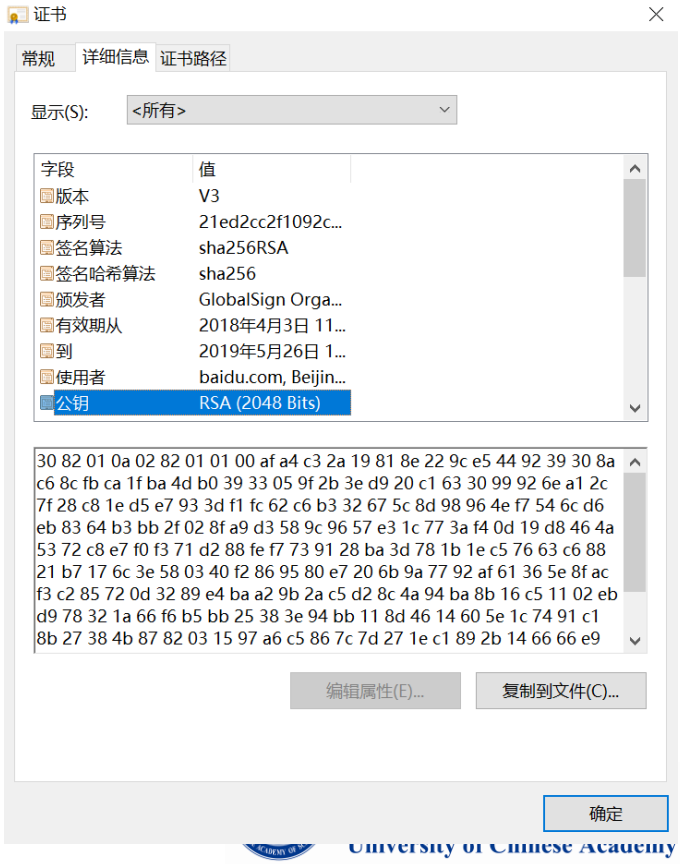
- 数字证书-验证公钥所属的用户身份
  - 网络世界里的“身份证”，信息不可篡改
- 证书管理机构（certificate authority，CA）
  - CA用其私钥对用户的身份信息（包括用户信息及其公钥等信息）进行签名，该签名和用户的身份信息一起就形成了证书。
  - 签名：对用户身份信息做哈希运算，对哈希值用私钥加密
- 证书信任链
  - 信任关系可传递，形成证书信任链

数字证书 举例


百度一下，你就知道
安全
https://www.baidu.com
连接是安全的
您发送给这个网站的信息（例如密码或信用卡号）不会外泄。 了解详情
证书（有效）
（目前使用了 23 个）Cookie
网站设置
新闻
Bai du 百度


证书
常规
详细信息
证书路径
证书信任链
证书路径(P)
GlobalSign Root CA - R1
GlobalSign Organization Validation CA - SHA256 - G2
baidu.com


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
• 向远程计算机证明你的身份
• 1.3.6.1.4.1.4146.1.20
• 2.23.140.1.2.2
* 有关详细信息，请参考证书颁发机构的说明。
颁发给: baidu.com
颁发者: GlobalSign Organization Validation CA - SHA256 - G2
有效期从 2018/4/3 到 2019/5/26
颁发者说明(S)
确定


证书
常规
详细信息
证书路径
显示(S): <所有>
字段
值
版本 V3
序列号 21ed2cc2f1092c...
签名算法 sha256RSA
签名哈希算法 sha256
颁发者 GlobalSign Orga...
有效期从 2018年4月3日 11...
到 2019年5月26日 1...
使用者 baidu.com, Beijin...
公钥 RSA (2048 Bits)
30 82 01 0a 02 82 01 01 00 af a4 c3 2a 19 81 8e 22 9c e5 44 92 39 30 8a
c6 8c fb ca 1f ba 4d b0 39 33 05 9f 2b 3e d9 20 c1 63 30 99 92 6e a1 2c
7f 28 c8 1e d5 e7 93 3d f1 fc 62 c6 b3 32 67 5c 8d 98 96 4e f7 54 6c d6
eb 83 64 b3 bb 2f 02 8f a9 d3 58 9c 96 57 e3 1c 77 3a f4 0d 19 d8 46 4a
53 72 c8 e7 f0 f3 71 d2 88 fe f7 73 91 28 ba 3d 78 1b 1e c5 76 63 c6 88
21 b7 17 6c 3e 58 03 40 f2 86 95 80 e7 20 6b 9a 77 92 af 61 36 5e 8f ac
f3 c2 85 72 0d 32 89 e4 ba a2 9b 2a c5 d2 8c 4a 94 ba 8b 16 c5 11 02 eb
d9 78 32 1a 66 f6 b5 bb 25 38 3e 94 bb 11 8d 46 14 60 5e 1c 74 91 c1
8b 27 38 4b 87 82 03 15 97 a6 c5 86 7c 7d 27 1e c1 89 2b 14 66 66 e9
编辑属性(E)...
复制到文件(C)...
确定

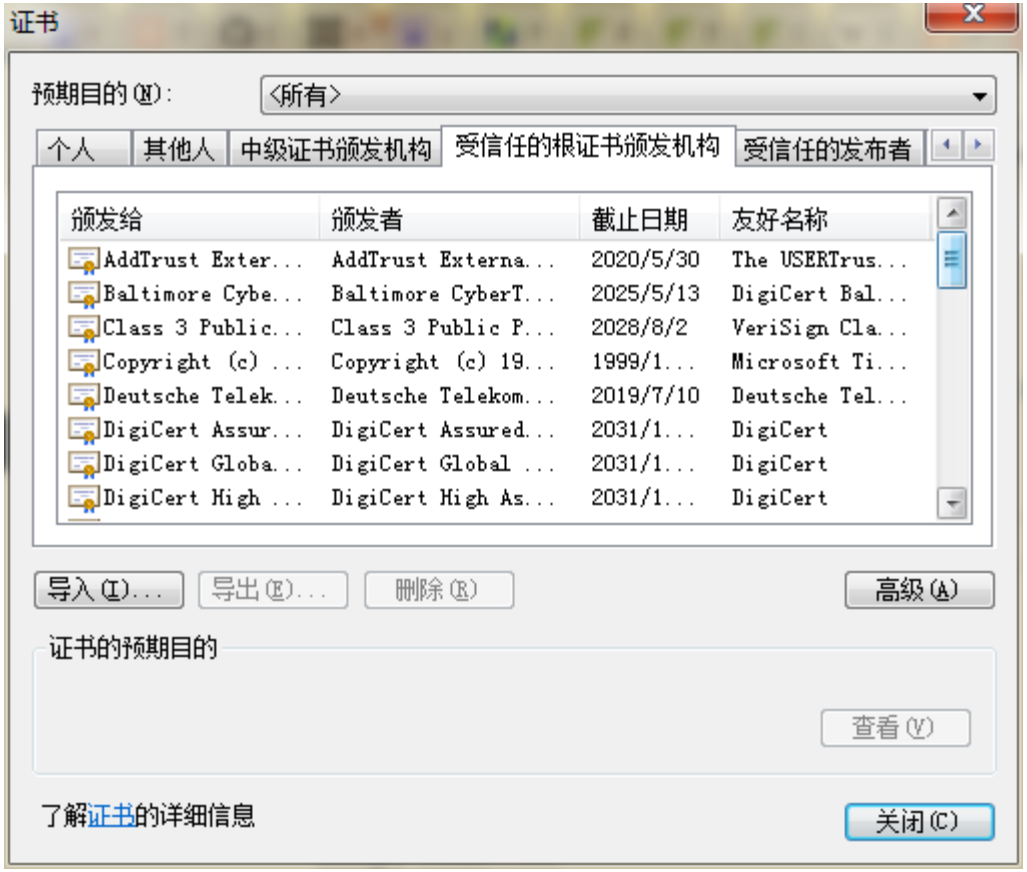
数字证书的格式

- 目前广泛采用的证书格式是国际电信联盟（ITU）提出的X. 509v3格式

内容	说明
版本V	X．509版本号
证书序列号	用于标识证书
算法标识符	签名证书的算法标识符
参数	算法规定的参数
颁发者	证书颁发者的名称及标识符(X.500)
起始时间	证书的有效期
终止时间	证书的有效期
持证者	证书持有者的姓名及标识符
算法	证书的公钥算法
参数	证书的公钥参数
持证书人公钥	证书的公钥
扩展部分	CA对该证书的附加信息，如密钥的用途
数字签名	证书所有数据经H运行后CA用私钥签名

浏览器根证书

- 各大浏览器厂商预置在浏览器内
- 直接接受浏览器信任的证书



HTTPS协议

- 数字证书是安全的
- 证书生成
- 网站管理员向CA(Certificate Authority, 认证中心)申请

UserInfo = {User, Domain, User_PubKey, HashAlgorithm…}

Hash = Hash_ Algorithm(UserInfo)

Signature = RSA_CA_Private(Hash, CA_PriKey)

Certificate = {UserInfo, Signature, HashAlgorithm…}

网站得到： Certificate， User_PubKey，User_PriKey

HTTPS协议

- 数字证书是安全的
- 证书校验
- 客户端操作

公开：CA_PubKey

Hash1 = Hash_ Algorithm(UserInfo)

Hash2 = RSA_CA_Public(Signature, CA_PubKey)

Compare(Hash1, Hash2)

- 比对成功则认为证书中的内容可信！

HTTPS协议

□ HTTPS是安全的

1、客户端发起HTTPS请求

2、服务端准备公私钥和证书

3、服务端发送证书（含公钥）

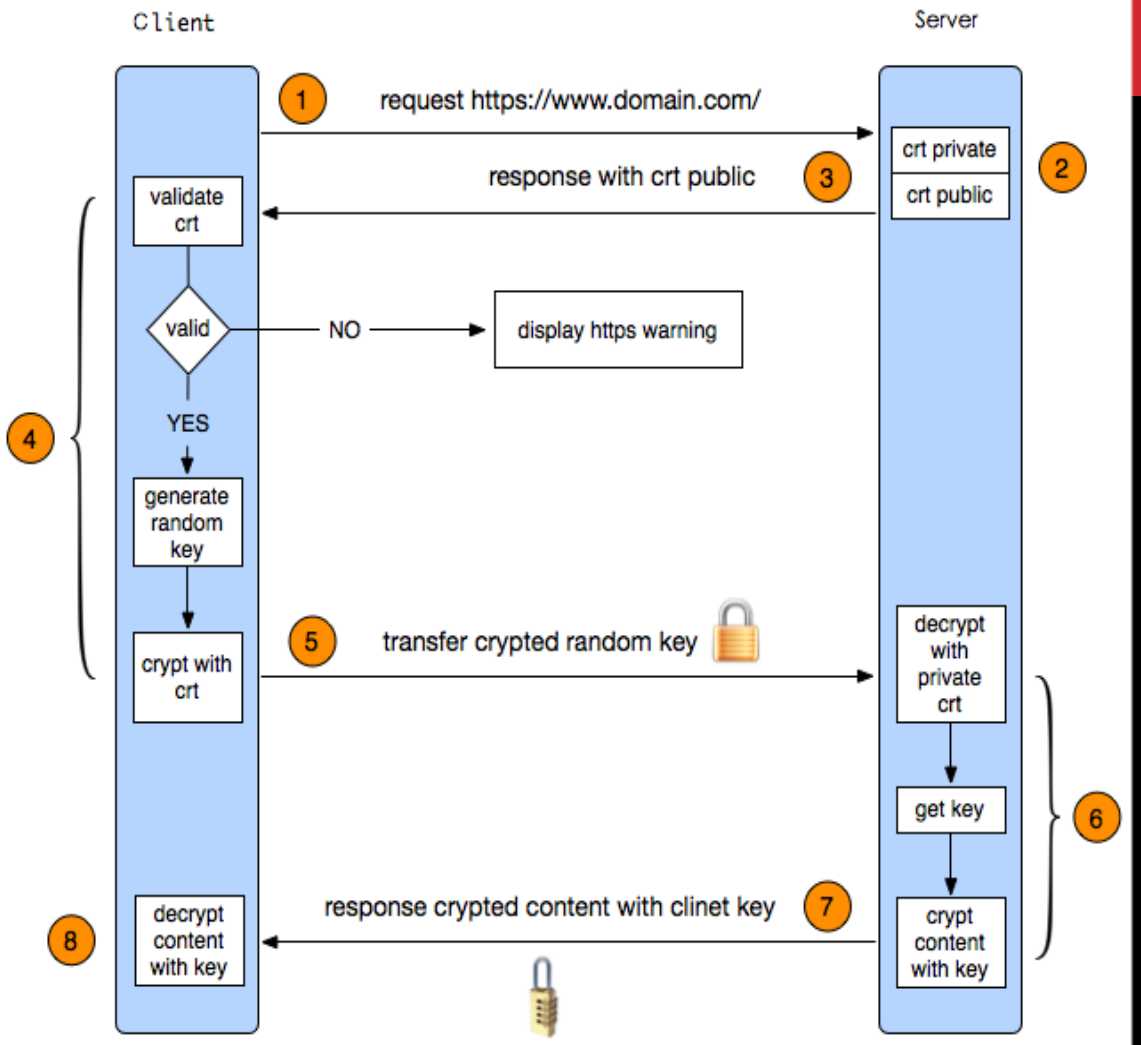
4、客户端解析证书

5、客户端生成对称密钥，并用公钥加密后，发送给服务端

6、服务端使用私钥解密，获得对称密钥

7、服务端使用对称密钥加密信息并发送

8、客户端使用对称密钥解密信息



知识点2、3：对称密码体制和非对称密码体制

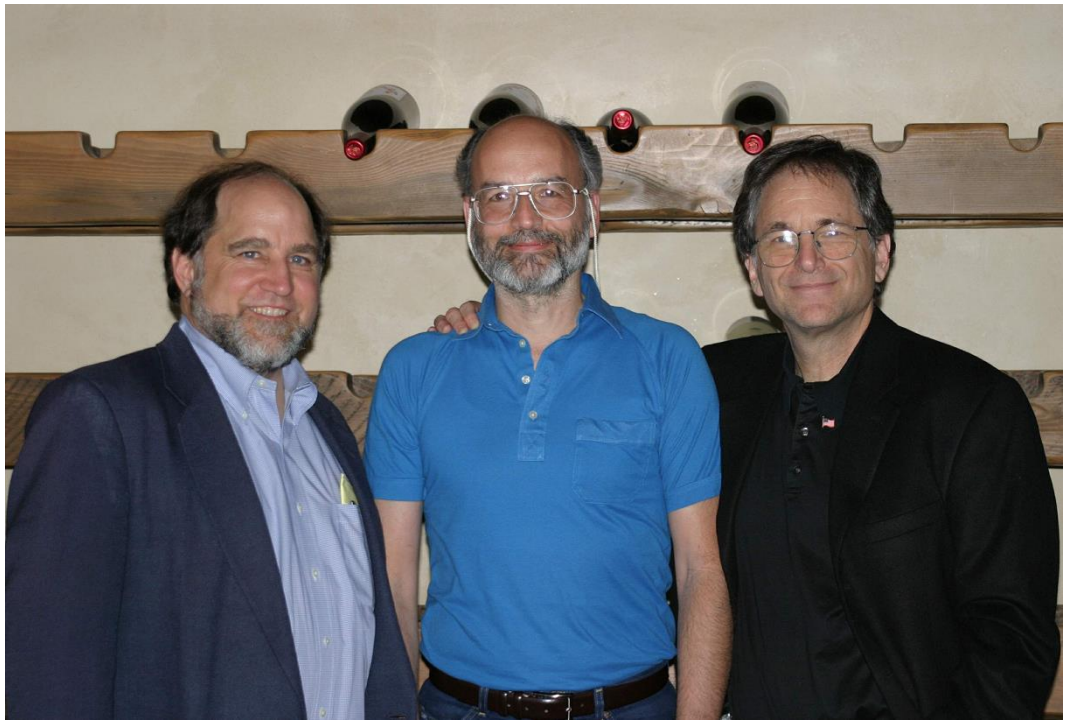
- **对称密码体制(Symmetric System, One-key System, Private-key System)**
  - 加密密钥和解密密钥相同，或者一个密钥可以从另一个导出，能加密就能解密，加密能力和解密能力是结合在一起的，开放性差。
- **非对称密码体制(Asymmetric System, Two-key System, Public-key System)**
  - 加密密钥和解密密钥不相同，从一个密钥导出另一个密钥是计算上不可行的，加密能力和解密能力是分开的，开放性好。

如何设计一个非对称加密算法

- **公钥和私钥必须相关，而且从公钥到私钥不可推断**
  - 必须要找到一个难题，从一个方向走是容易的，从另一个方向走是困难的
  - 如何把这个难题跟加解密结合起来

现代非对称密码学——RSA

- 1978年，MIT三位数学家R.L.Rivest，A.Shamir和L.Adleman 发明了一种用数论构造双钥体制的方法，即RSA算法
- RSA算法基于一个简单的数论事实：将两个大素数相乘十分容易，但那时想要对其乘积进行因式分解却极其困难



小结HTTPS协议

- 使用HTTPS协议可认证用户和服务器，确保数据发送到正确的客户机和服务器。
- HTTPS协议是由SSL+HTTP协议构建的可进行加密传输、身份认证的网络协议，要比http协议安全，可防止数据在传输过程中不被窃取、改变，确保数据的完整性。
- 浏览嗅探与监听、中间人
- 但是没有绝对安全！

HTTPS安全问题

- 协议设计不足
- 协议实现漏洞
- 证书相关问题

第 3 卷 第 2 期 信 息 安 全 学 报 Vol. 3 No. 2
2018 年 3 月 Journal of Cyber Security March, 2018

HTTPS/TLS 协议设计和实现中的安全缺陷综述

韦俊琳[1], 段海新[1], 万 涛[2]

[1]清华大学, 网络科学与网络空间研究院 北京 中国 100084
[2]华为公司渥太华研究中心 渥太华 加拿大

摘要 SSL/TLS 协议是目前广泛使用的 HTTPS 的核心, 实现端到端通信的认证、保密性和完整性保护, 也被大量应用到非 web 应用的其他协议(如 SMTP)。因为 SSL/TLS 如此重要, 它的安全问题也引起了研究者们的兴趣, 近几年对于 SSL/TLS 协议的研究非常火热。本文总结了近几年四大安全顶级学术会议(Oakland, CCS, USENIX Secuity 和 NDSS)发表的相关论文, 分析该协议设计的设计问题、实现缺陷以及证书方面的相关研究, 希望对 SSL/TLS 协议的改进和其他协议的安全性设计有参考价值。

关键词 SSL, TLS, 网络安全, 证书
中图法分类号 TP309.2 DOI 号 10.19363/j.cnki.cn10-1380/tn.2018.03.01

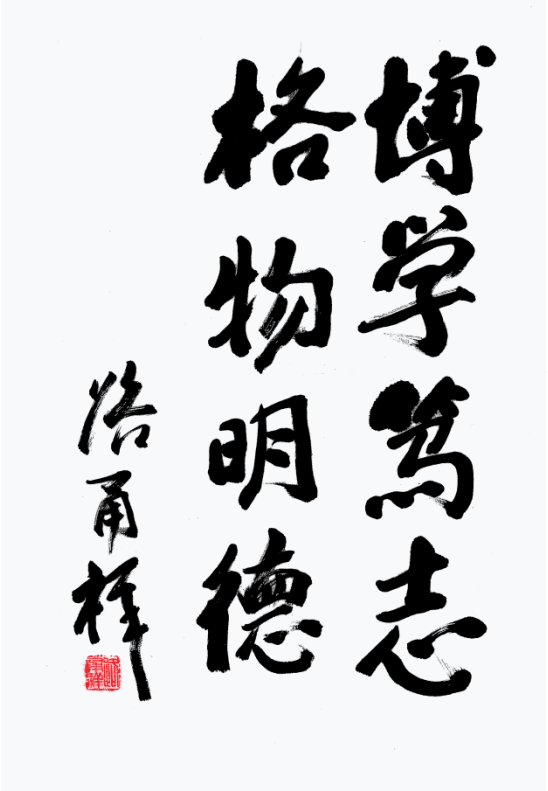
本章大纲

□ HTTP及安全问题

- 基础知识回顾
- HTTP安全问题
- HTTPS协议

□ Cookie及安全问题

- 基础知识
- 安全策略
- 安全问题



基础知识

- **设计目的**

- HTTP协议是无状态的协议，导致服务器无法判断是谁在浏览网页；
- 网上商城的购物车、用户的登录状态、用户曾经点过的按钮，访问过的页面等等均无法保存；
- 维持状态是很有必要，否则将严重影响交互性以及用户体验；
- cookie和session应运而生，二者的设计初衷都是为了维持状态；
- 简单来区分，session存于服务器，cookie存在客户端；

基础知识

工作过程

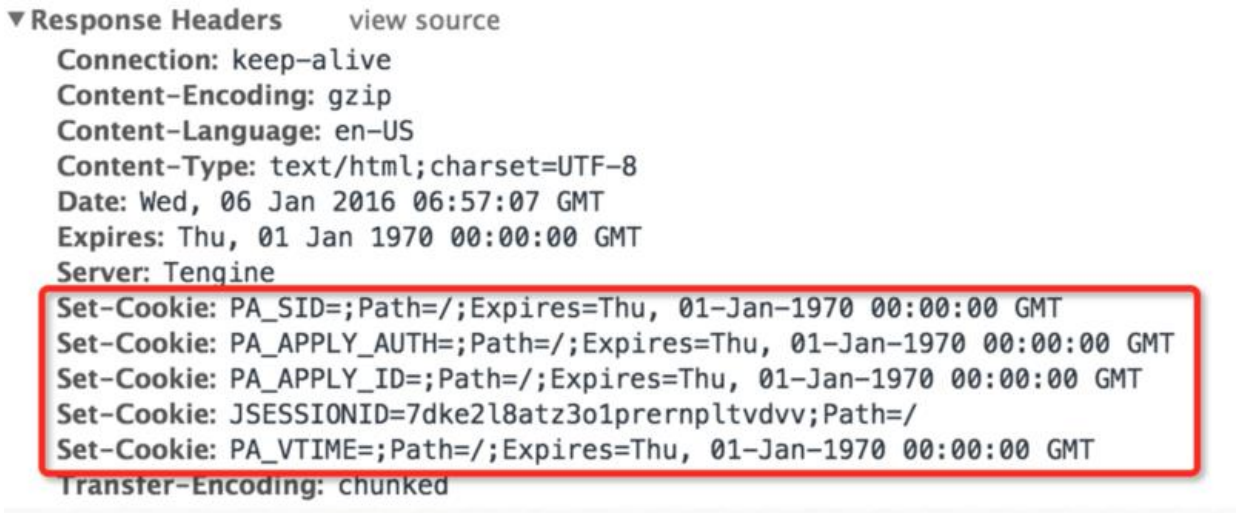
- 根据Expire（或max-age, 失效时间）属性值，将cookie区分为内存cookie和持久cookie
  - 内存cookie，只在本次会话中有效，会话结束后立即删除cookie；
  - 持久cookie，在客户端硬盘中存储，直至过了失效期；
- 后续的请求中，Cookie连同请求一起发送至服务器；
- 服务器根据cookie区分状态

基础知识

- **工作过程**
- 生成阶段：服务端（或本地JS脚本）根据不同的状态，生成特定的cookie，用以标示不同的身份或状态
- 设置阶段：服务端（或本地JS脚本）进行SetCookie，将生成的cookie设置与客户端中
  - 服务端：在响应头中以Set-Cookie字段返回cookie值，告知客户端保存
  - JS：调用document.cookie=“key=value”设置
- 使用阶段：
  - 客户端发送请求时，携带cookie，以维护会话状态

基础知识

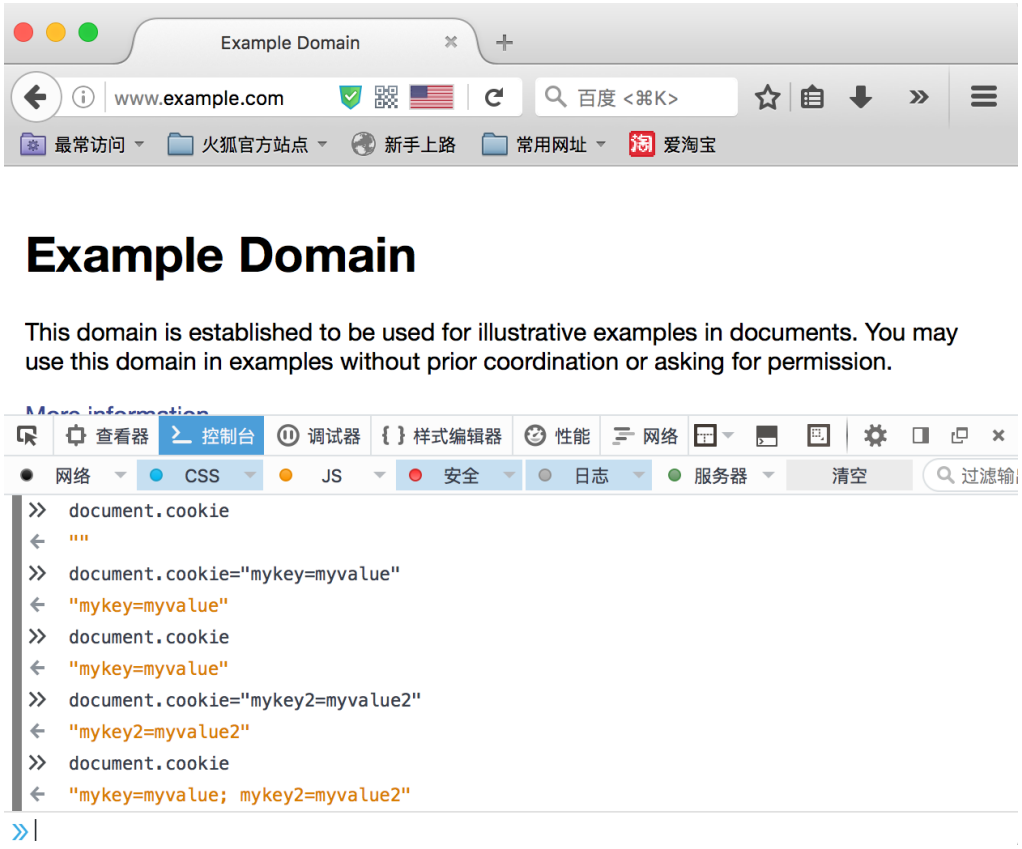
- **服务端设置**
- 以PHP为例
- setcookie(name,value,expire,path,domain,secure)



基础知识

本地JS设置

操作document.cookie对象

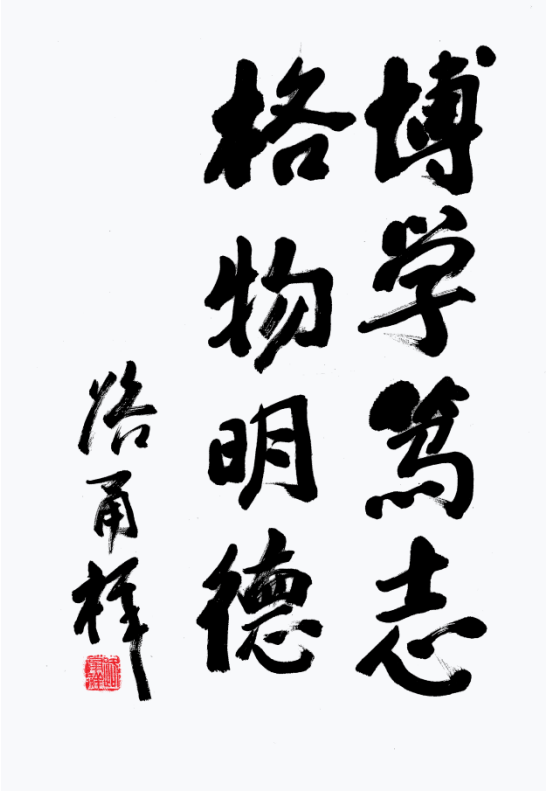


基础知识

- **cookie属性**
- Domain，指定cookie被绑定到哪台主机上，如：domain=.example.org，这是cookie会发送到*.example.org上；
- Path，控制那些访问能够触发cookie的发送。如不指定path，cookie对全站生效。如path=/test，则只在访问/test的网页时才会被发送；
- Expire（max-age），指明了cookie失效的时间，进一步将cookie划分为内存cookie和持久cookie；
- Secure，如指定则该cookie只能通过安全通道传输（即SSL通道）；
- Httponly，JS无法读取和修改标记为HttpOnly的Cookie，这样Cookkie可免受脚本的攻击（如XSS）；

本章大纲

- **HTTP及安全问题**
  - 基础知识回顾
  - HTTP安全问题
  - HTTPS协议
- **Cookie及安全问题**
  - 基础知识
  - 安全策略
  - 安全问题



安全策略

- **Cookie与同源**
- Cookie不应该被无关页面篡改
- Cookie的domain属性设计初衷是限制Cookie的有效范围，但实际上并不精准

安全策略

- **Cookie与同源**
- Cookie的domain参数设置的表现举例

foo.example.com的Cookie domain参数设置为：	实际的cookie范围	
	非IE浏览器	IE浏览器
完全未设置	foo.example.com(精确匹配）	*.foo.example.com
bar.foo.example.com	Cookie 未能设置成功：因为domain值比当前主机名范围更窄	
foo.example.com	*.foo.example.com	
baz.example.com	Cookie 未能设置成功：因为域名不匹配	
example.com	*.example.com	
ample.com	Cookie 未能设置成功：因为域名不匹配	
.com	Cookie 未能设置成功：因为域名太宽泛，会带来安全风险	

安全策略

- **安全的cookie设计**
- 一个相对安全的cookie登录状态设计方案：

1、用户登录根据信息组合生成token，存储在数据库中

2、生成token的信息包括用户名、IP、UA、expiration、salt等

3、信息组合再进行可逆加密算法进行加密

4、用户发送的token，解密得出用户名、IP等，并与数据库中对应的token比对

5、如果相同则视为登录状态，继续操作；否则下线操作，要求重新登录

安全策略

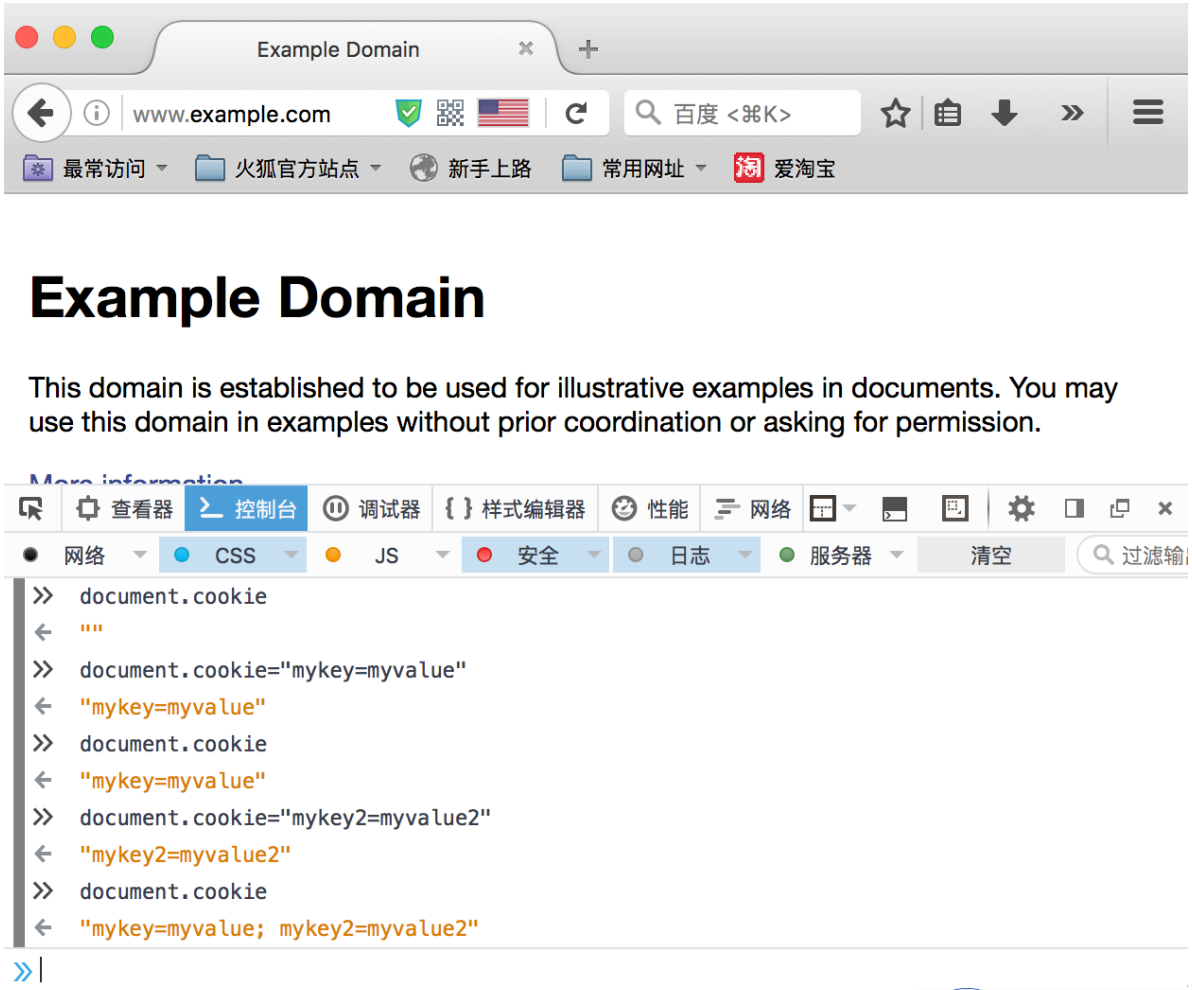
- **安全的cookie设计**
- Salt(属于随机值)字段属于用户不可知字段，防止直接伪造
- 加密算法，salt的使用，使猜解cookie的难度剧增
- IP，UA的限制，一定程度防止直接窃取cookie在其他终端登录

安全策略

- **HttpOnly保护**
- HttpOnly最早由微软提出，并在IE6中实现，至今已经逐渐成为一个浏览器标准。
- 浏览器将禁止页面的JavaScript访问带有HttpOnly属性的Cookie

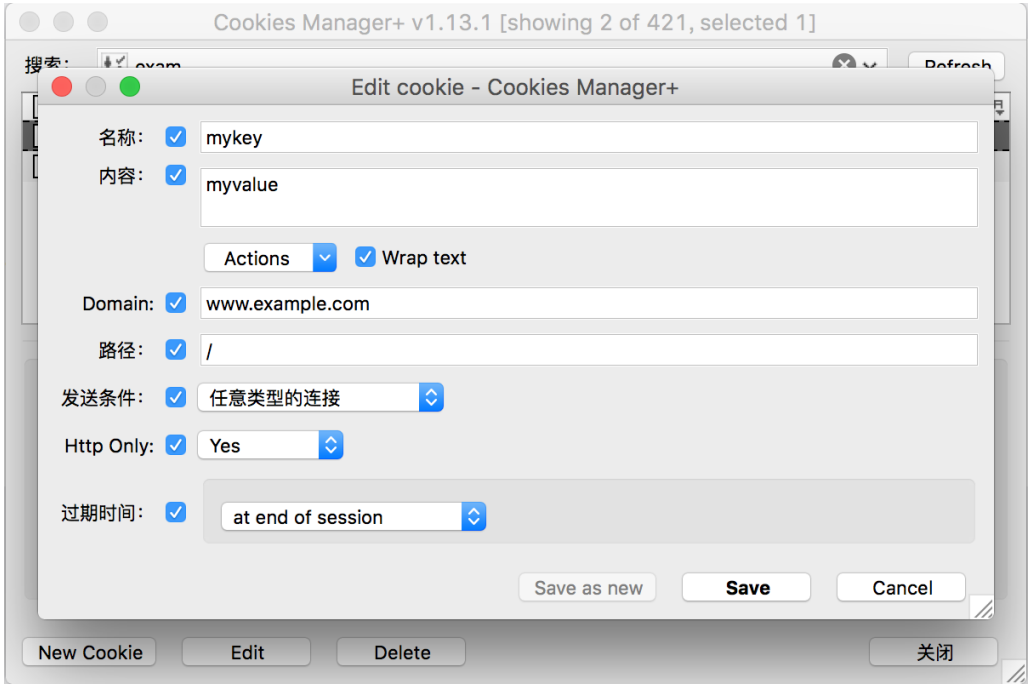
安全策略

□ HttpOnly保护

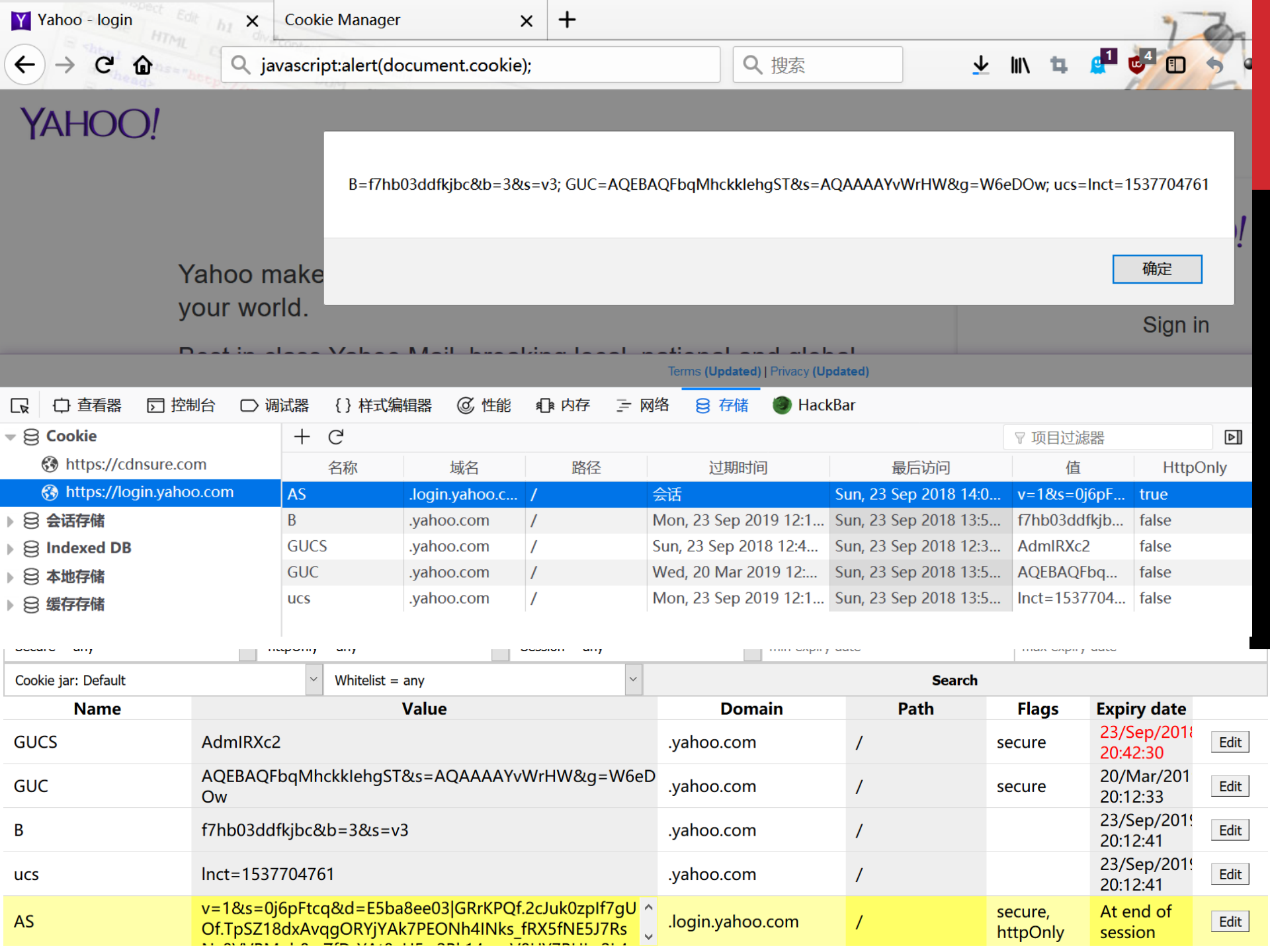


安全策略

□ HttpOnly保护

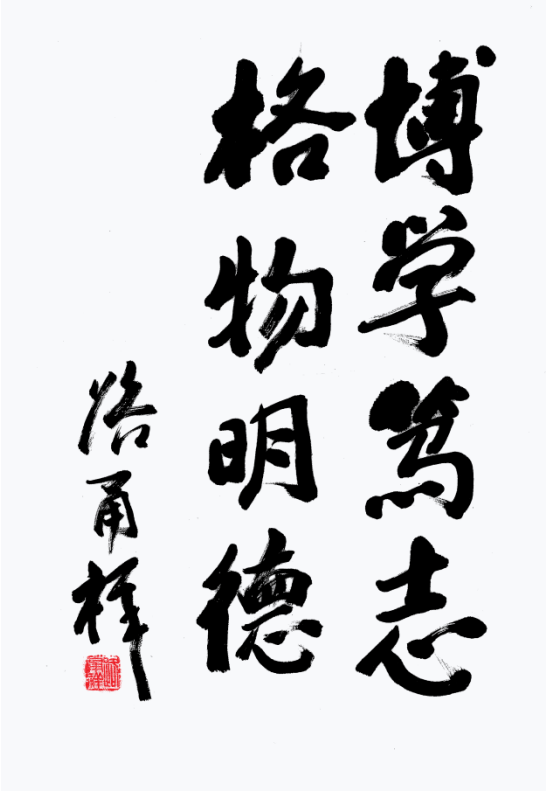


中国科学院大学 University of Chinese Academy of Sciences


Yahoo - login
Cookie Manager
javascript:alert(document.cookie);
搜索
YAHOO!
B=f7hb03ddfkjbc&b=3&s=v3; GUC=AQEBAQFbqMhckklehgST&s=AQAAAAYvWrHW&g=W6eDOw; ucs=lnct=1537704761
确定
Yahoo make
your world.
Sign in
Terms (Updated) | Privacy (Updated)
查看器
控制台
调试器
样式编辑器
性能
内存
网络
存储
HackBar
Cookie
https://cdnsure.com
https://login.yahoo.com
会话存储
Indexed DB
本地存储
缓存存储
项目过滤器
名称 域名 路径 过期时间 最后访问 值 HttpOnly
AS .login.yahoo.c... / 会话 Sun, 23 Sep 2018 14:0... v=1&s=0j6pF... true
B .yahoo.com / Mon, 23 Sep 2019 12:1... Sun, 23 Sep 2018 13:5... f7hb03ddfkjb... false
GUCS .yahoo.com / Sun, 23 Sep 2018 12:4... Sun, 23 Sep 2018 12:3... AdmIRXc2 false
GUC .yahoo.com / Wed, 20 Mar 2019 12:... Sun, 23 Sep 2018 13:5... AQEBAQFbq... false
ucs .yahoo.com / Mon, 23 Sep 2019 12:1... Sun, 23 Sep 2018 13:5... lnct=1537704... false
Cookie jar: Default
Whitelist = any
Search
Name Value Domain Path Flags Expiry date
GUCS AdmIRXc2 .yahoo.com / secure 23/Sep/2018 20:42:30 Edit
GUC AQEBAQFbqMhckklehgST&s=AQAAAAYvWrHW&g=W6eDOw .yahoo.com / secure 20/Mar/2019 20:12:33 Edit
B f7hb03ddfkjbc&b=3&s=v3 .yahoo.com / 23/Sep/2019 20:12:41 Edit
ucs lnct=1537704761 .yahoo.com / 23/Sep/2019 20:12:41 Edit
AS v=1&s=0j6pFtcq&d=E5ba8ee03|GRrKPQf.2cJuk0zpIf7gUOf.TpSZ18dxAvqgORYjYAk7PEONh4INks_fRX5fNE5J7Rs .login.yahoo.com / secure, httpOnly At end of session Edit

本章大纲

- **HTTP及安全问题**
  - 基础知识回顾
  - HTTP安全问题
  - HTTPS协议
- **Cookie及安全问题**
  - 基础知识
  - 安全策略
  - 安全问题



安全问题

- **cookie窃取**
- 窃取到cookie并原样发送，同样可以进行身份欺骗
- 典型手段
  - ✓基于HTTP明文，可在传输过程窃取；
  - ✓通过XSS利用脚本窃取；

安全问题

- **cookie猜解**

- 通过暴力破解或计算分析的办法，猜解cookie

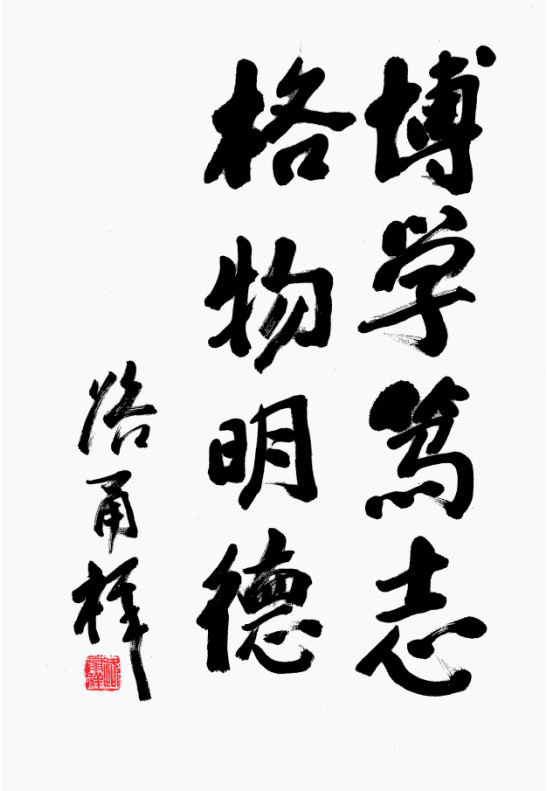
- 假设教务系统网站使用setcookie：account=studentnum+timestamp来标识学生登录状态，其中timestamp为登录时的时间戳;
- 在已经学号和大致登录时间（选课时间、期末查分）情况下，通过暴力枚举，即可实现身份欺骗；

安全问题

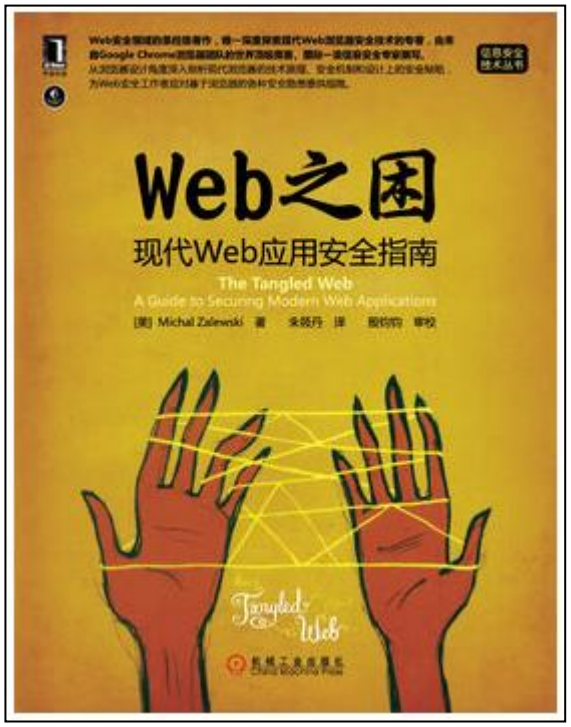
- **隐私信息泄露**
- 网站使用cookie来保存用户的活动轨迹
  - 看过某个商品，将某商品加入购物车
- 对数据进一步分析，甚至可以得到用户的生活习惯，兴趣爱好，从而产生商业的利益

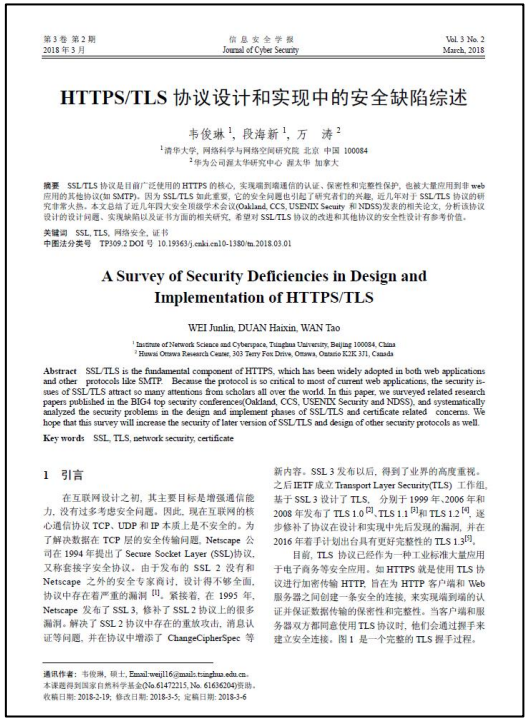
本章大纲

- **HTTP及安全问题**
  - 基础知识回顾
  - HTTP安全问题
  - HTTPS协议
- **Cookie及安全问题**
  - 基础知识
  - 安全策略
  - 安全问题



参考文献





第 3 卷 第 2 期 信 息 安 全 学 报 Vol. 3 No. 2
2018 年 3 月 Journal of Cyber Security March, 2018

HTTPS/TLS 协议设计和实现中的安全缺陷综述

韦俊琳[1], 段海新[1], 万 涛[2]
[1]清华大学, 网络科学与网络空间研究院 北京 中国 100084
[2]华为公司源太华研究中心 源太华 加拿大

摘要 SSL/TLS 协议是目前广泛使用的 HTTPS 的核心, 实现端到端通信的认证、保密性和完整性保护, 也被大量应用到非 web 应用的其他协议(如 SMTP)。因为 SSL/TLS 如此重要, 它的安全问题也引起了研究者们的兴趣, 近几年对于 SSL/TLS 协议的研究非常火热。本文总结了近几年四大安全顶级学术会议(Oakland, CCS, USENIX Security 和 NDSS)发表的相关论文, 分析该协议设计的设计问题、实现缺陷以及证书方面的相关研究, 希望对 SSL/TLS 协议的改进和其他协议的安全性设计有参考价值。

关键词 SSL, TLS, 网络安全, 证书
中图法分类号 TP309.2 **DOI 号** 10.19363/j.cnki.cn10-1380/tn.2018.03.01

A Survey of Security Deficiencies in Design and Implementation of HTTPS/TLS

WEI Junlin, DUAN Haixin, WAN Tao
[1] Institute of Network Science and Cyberspace, Tsinghua University, Beijing 100084, China
[2] Huawei Ottawa Research Center, 303 Terry Fox Drive, Ottawa, Ontario K2K 3J1, Canada

Abstract SSL/TLS is the fundamental component of HTTPS, which has been widely adopted in both web applications and other protocols like SMTP. Because the protocol is so critical to most of current web applications, the security issues of SSL/TLS attract so many attentions from scholars all over the world. In this paper, we surveyed related research papers published in the BIG4 top security conferences(Oakland, CCS, USENIX Security and NDSS), and systematically analyzed the security problems in the design and implement phases of SSL/TLS and certificate related concerns. We hope that this survey will increase the security of later version of SSL/TLS and design of other security protocols as well.

Key words SSL, TLS, network security, certificate

1 引言

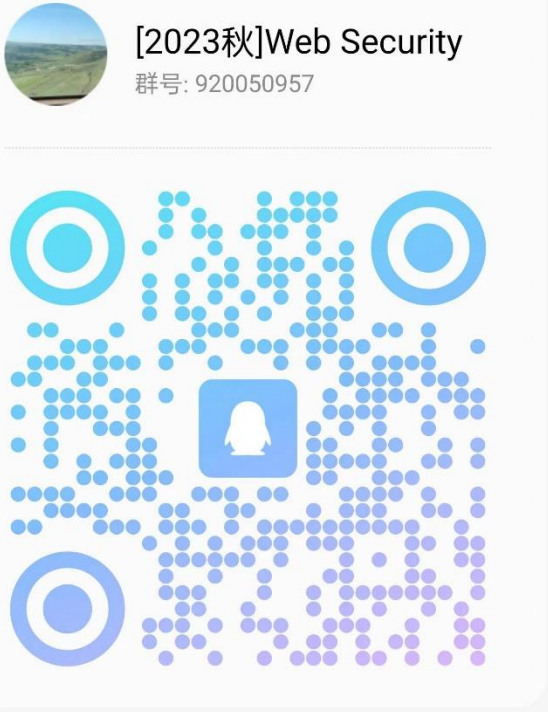
在互联网设计之初, 其主要目标是增强通信能力, 没有过多考虑安全问题。因此, 现在互联网的核心通信协议 TCP、UDP 和 IP 本质上是不安全的。为了解决数据在 TCP 层的安全传输问题, Netscape 公司在 1994 年提出了 Secure Socket Layer (SSL)协议, 又称套接字安全协议。由于发布的 SSL 2 没有和 Netscape 之外的安全专家商讨, 设计得不够全面, 协议中存在着严重的漏洞[1]。紧接着, 在 1995 年, Netscape 发布了 SSL 3, 修补了 SSL 2 协议上的很多漏洞。解决了 SSL 2 协议中存在的重放攻击, 消息认证等问题, 并在协议中增添了 ChangeCipherSpec 等新内容。SSL 3 发布以后, 得到了业界的高度重视。之后 IETF 成立 Transport Layer Security(TLS) 工作组, 基于 SSL 3 设计了 TLS, 分别于 1999 年、2006 年和 2008 年发布了 TLS 1.0[2], TLS 1.1[3]和 TLS 1.2[4]。逐步修补了协议在设计和实现中先后发现的漏洞, 并在 2016 年着手计划出台具有更好完整性的 TLS 1.3[5]。

目前, TLS 协议已经作为一种工业标准大量应用于电子商务等安全应用。如 HTTPS 就是使用 TLS 协议进行加密传输 HTTP, 旨在为 HTTP 客户端和 Web 服务器之间创建一条安全的连接, 来实现端到端的认证并保证数据传输的保密性和完整性。当客户端和服务器双方都同意使用 TLS 协议时, 他们会通过握手来建立安全连接, 图 1 是一个完整的 TLS 握手过程。

通讯作者: 韦俊琳, 硕士, Email:weijl16@mails.tsinghua.edu.cn.
本课题得到国家自然科学基金(No.61472215, No. 61636204)资助。
收稿日期: 2018-2-19; 修改日期: 2018-3-5; 定稿日期: 2018-3-6

后续课程内容

- **第一部分：基础知识**
- **介绍Web安全定义与内涵，国内外现状与趋势、近年来重大网络安全事件等，以及本课程可参考的书籍和网络资源；介绍本课程所需掌握的基础知识，包括HTTP/HTTPS协议、Web前后端编程语言、浏览器安全特性等。**
- 1.1 绪论
- 1.2 Web的简明历史
- 1.3 HTTP与Cookie
- 1.4同源策略



谢谢大家

刘潮歌

liuchaoge@iie.ac.cn

中科院信工所 第六研究室

中国科学院大学
University of Chinese Academy of Sciences