百度HTTPS实践

----安全，快速，可靠

Az | 百度运维部
chenxiyang@baidu.com

个人介绍

陈曦洋(Az)
百度资深运维工程师，08年加入百度运维部。

承担网页搜索在线系统运维工作。
之后专门负责流量接入方向，面临过秒杀活动，
大型攻击和重大故障的考验。
近3年作为网页搜索接入运维方向的技术负责人，
主要承担
访问速度，
可达性，
安全搜索等方向事务。

@Az的majia

引言

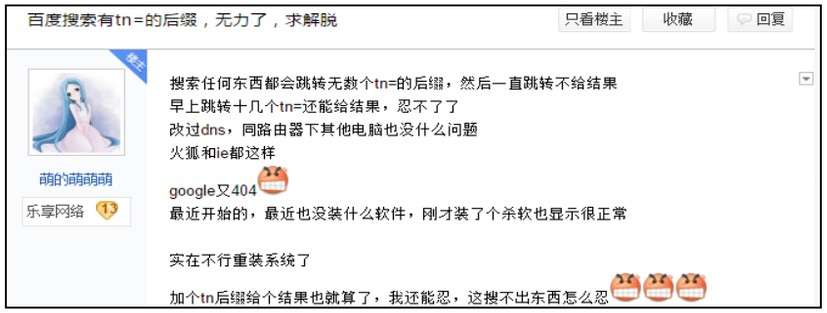
- 2015年3月，**百度搜索**成为国内首家完成全站https改造的大型站点
- **全站HTTPS**已经成为百度产品的标准
- **统一接入平台**大幅提升HTTPS的接入效率和性能

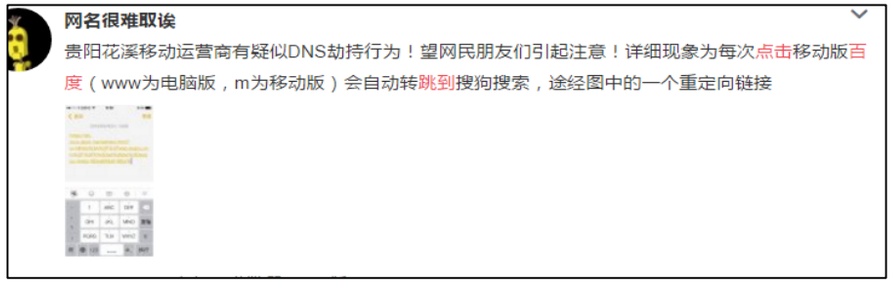
章节

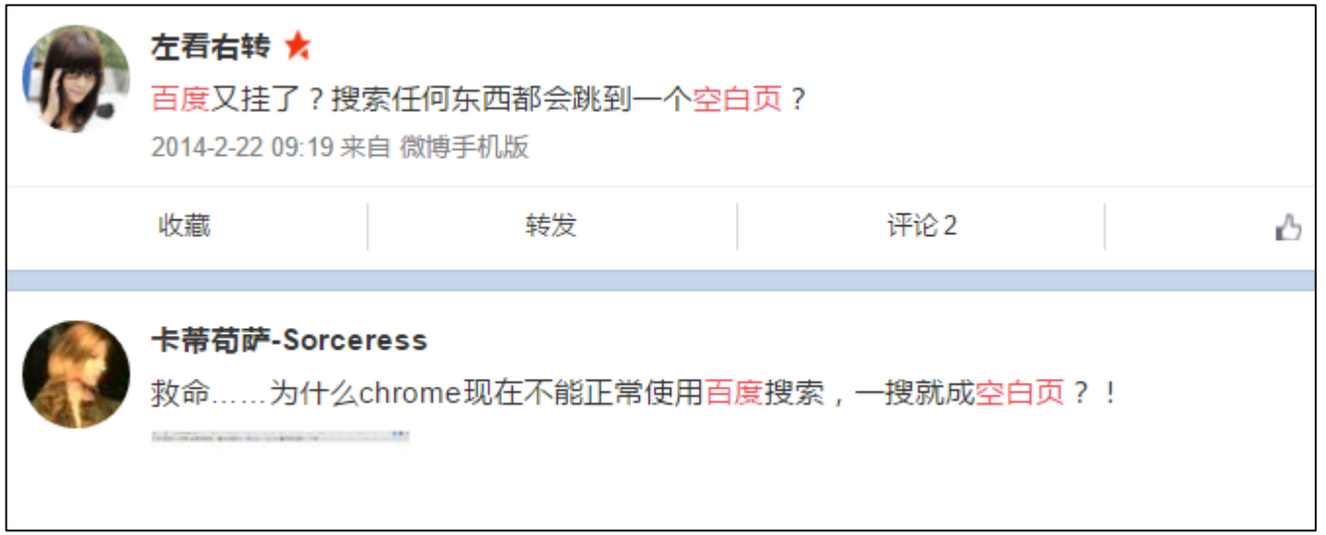
- 全站HTTPS的原因
- 协议原理
- 改造成本
- 优化方案
- 其他问题
- 参考文献

全站HTTPS的原因

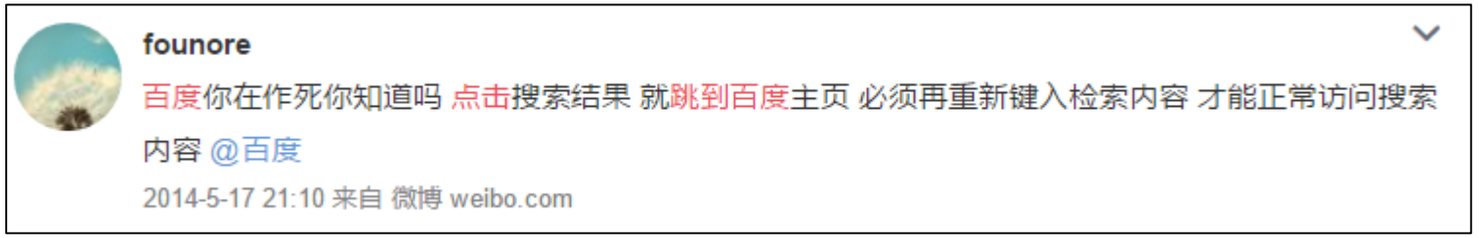
用户反馈问题 | 缺乏有效的技术解决方案







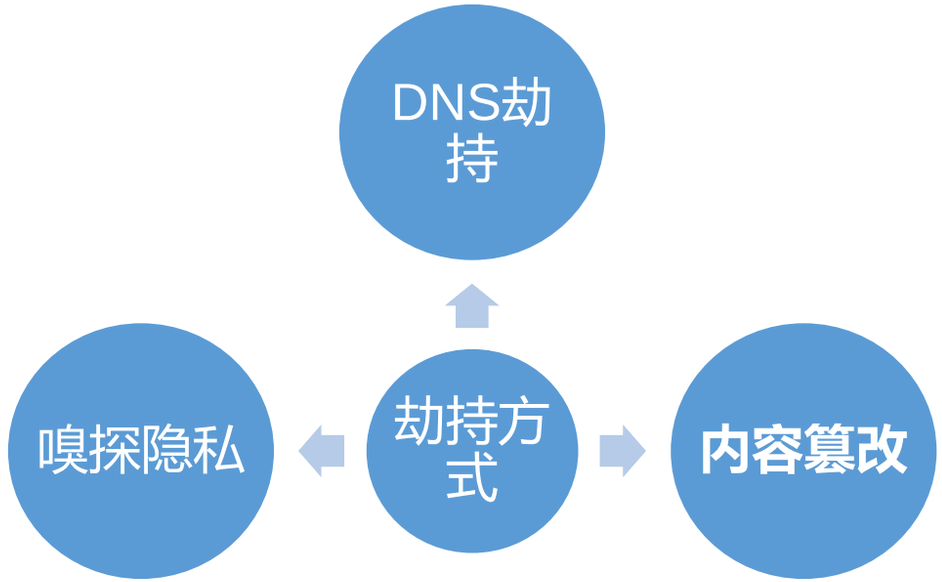
- 加上url参数,302跳转,不停刷新
- 手机号泄露
- DNS劫持到其他网站
- 搜索功能异常
- 白页



用户：你们出问题了，赶紧修好
我们：臣妾做不到啊
投诉能解决一些问题。。

劫持的分析 | 使用HTTPS来解决传输安全的问题

劫持方式



https-support

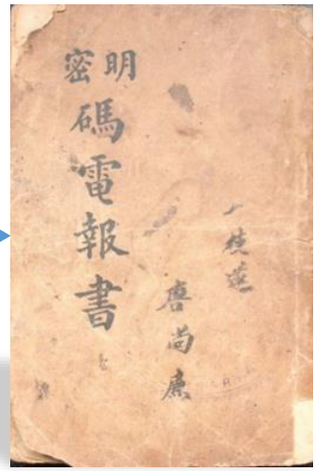
搜索　运维

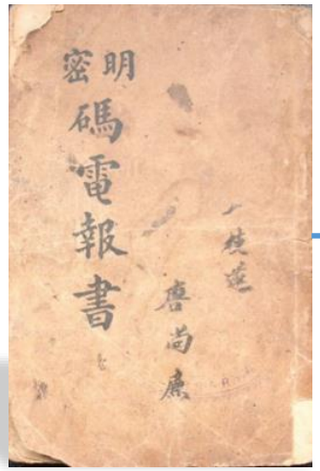
劫持阶段

域名解析 → **传输过程** → 浏览器/客户端

协议原理简介

协议原理介绍 | 对称加密(一)





协议原理简介 | 对称加密(二)

密钥更换

密钥泄露

密码破解

非安全信道的窃听

身份和数据伪造

ENIGMA

AF

协议原理简介 |如何解决对称加密问题 非对称！

密钥更换

密钥泄露

密码破解

非安全信道的窃听

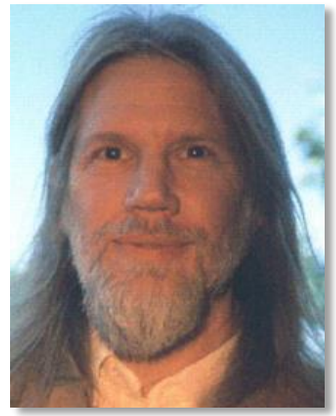
身份和数据伪造

加密解密分离

计算难度

完整性验证

逆向验证身份



DH(Diffie-Hellman)

RSA

协议原理简介 | DH 和 RSA

DH

离散对数

非安全信道密钥协商
不是加密算法

通信双方共同参与协商

有中间人攻击的风险

计算量大

RSA

欧拉定理，**费马**小定理，中国剩余定理
破解难度在于**大数的因式分解**

可作为密钥协商
也是加密算法

密钥协商时
由接受请求方提供公钥

计算量大

协议原理简介 | tls/ssl

计算量大

非对称做密钥交换

对称做数据传输加密

密钥协商(非对称)-对称加密-散列算法

ECDHE-RSA-AES128-GCM-SHA256

中间人攻击

PKI体系(主要依赖证书和CA构建信任链)

对称加密密钥+前向加密

三个随机数

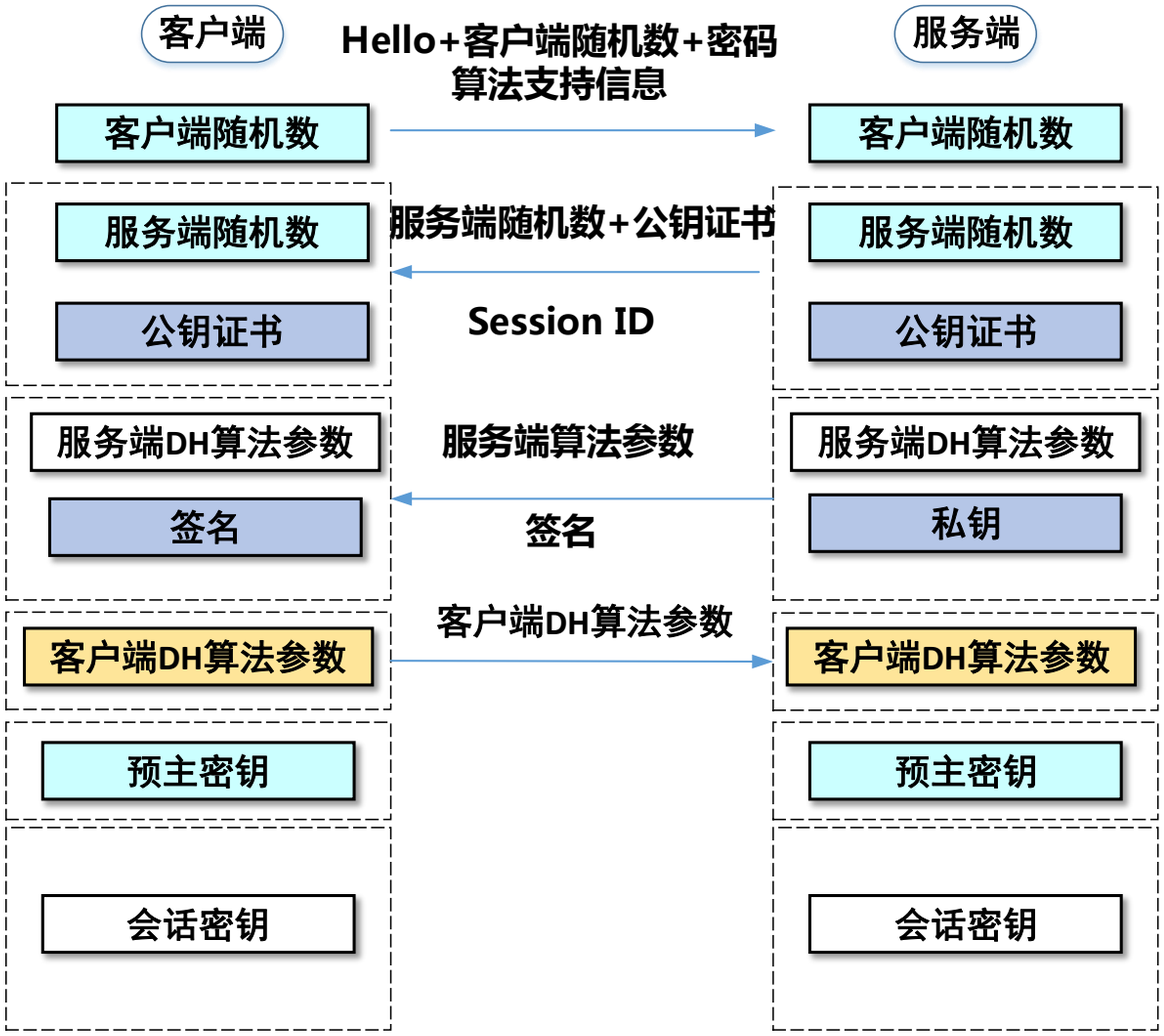
premaster secret

用RSA和DH协商的区别

私钥泄露也无法解密

客户端记录信息就可以解密

协议原理简介 | 总结



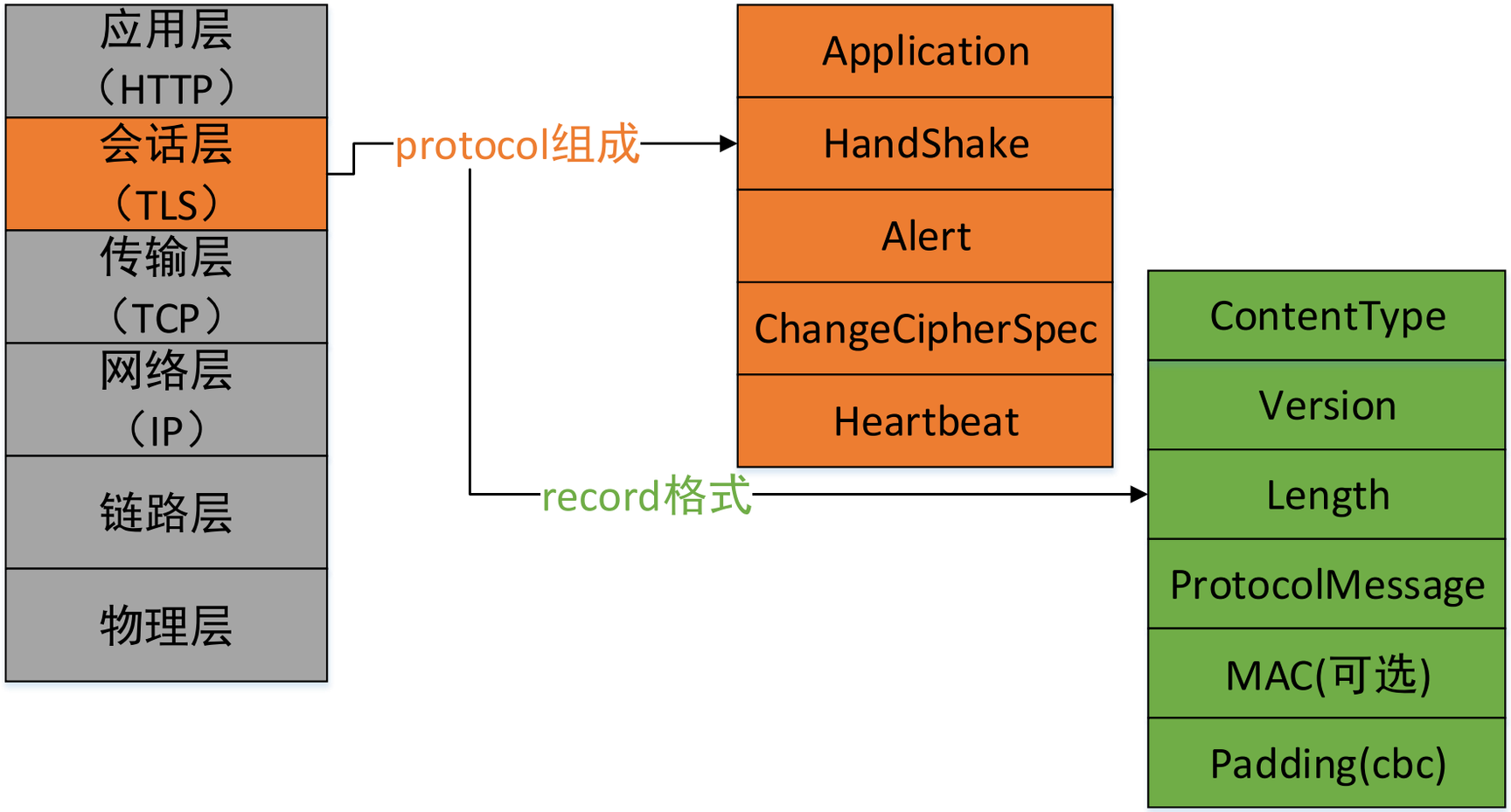
非对称做密钥交换

对称做数据传输加密

PKI体系进行身份认证

三个随机数
(需要保密的是premaster secret)

协议原理简介 | 层次



改造成本

改造成本 | 各种担忧

计算性能

访问速度

架构成本

产品成本

改造成本 | 计算性能

计算性能

1024位证书

2048位证书

访问速度

架构成本

产品成本

1024位

单核性能: 1500 cps (from google)

1% of the CPU load

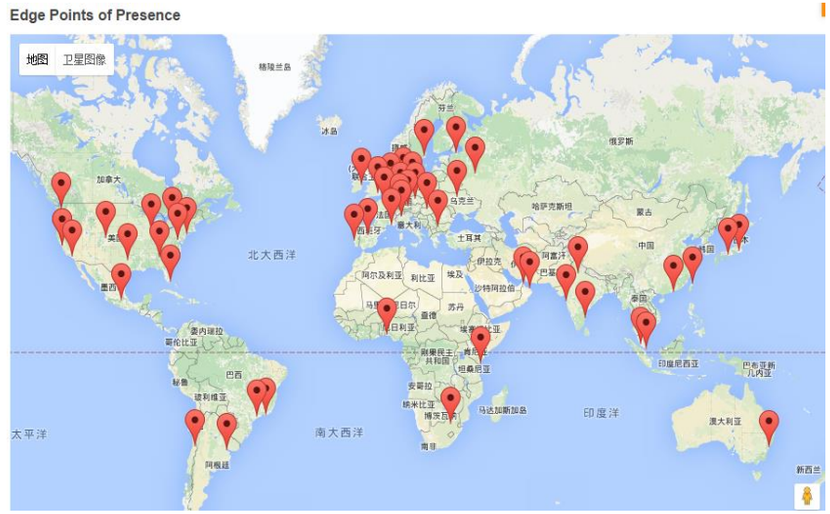
2048位

单核性能: 300-800 cps

相对HTTP下降 6-8倍 1个数量级

HTTP cps 2W+

HTTPS cps 2000-3000



改造成本 | 访问速度

计算性能

1024位证书

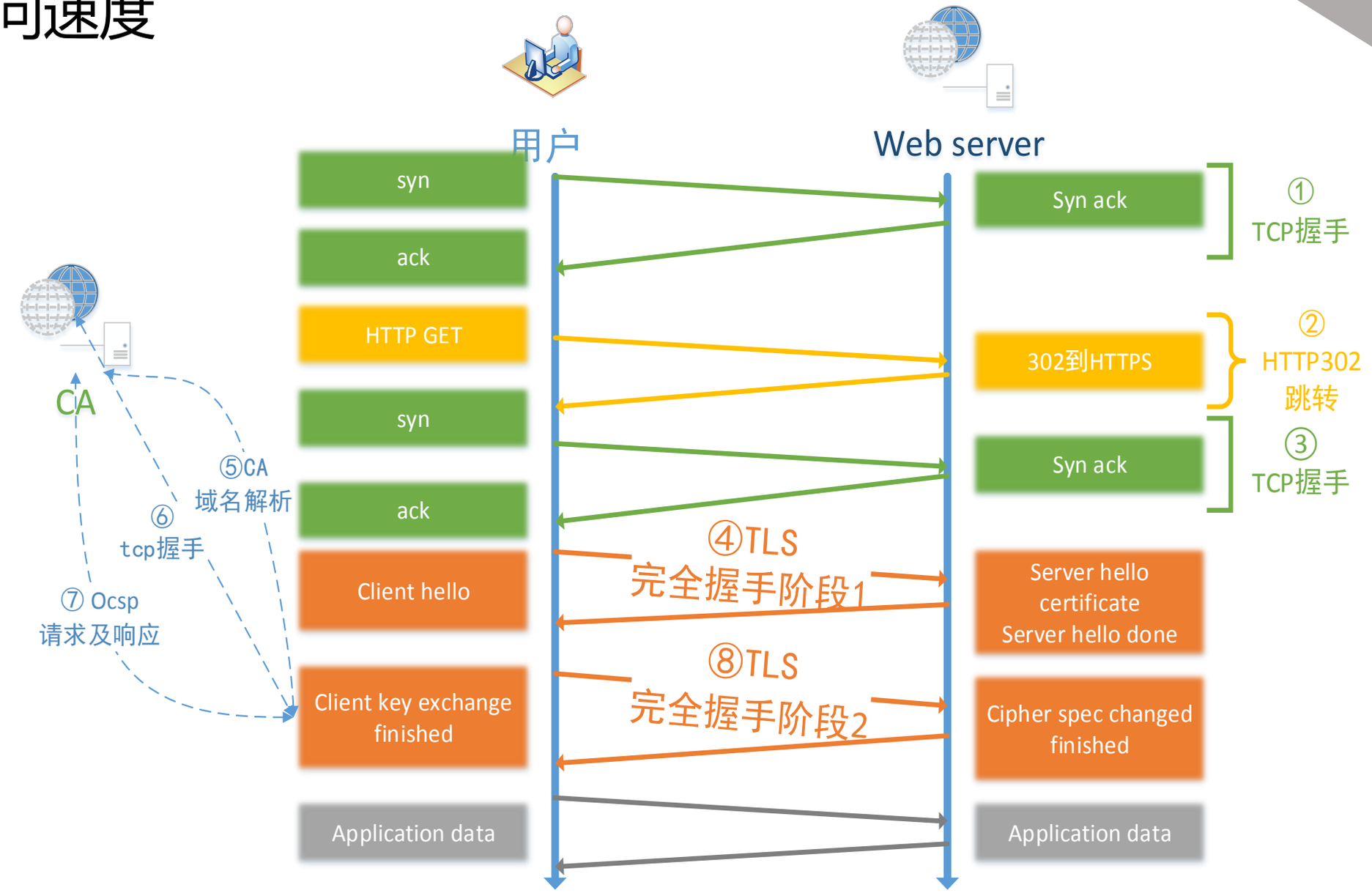
访问速度

250-500ms

500-1500ms

架构成本

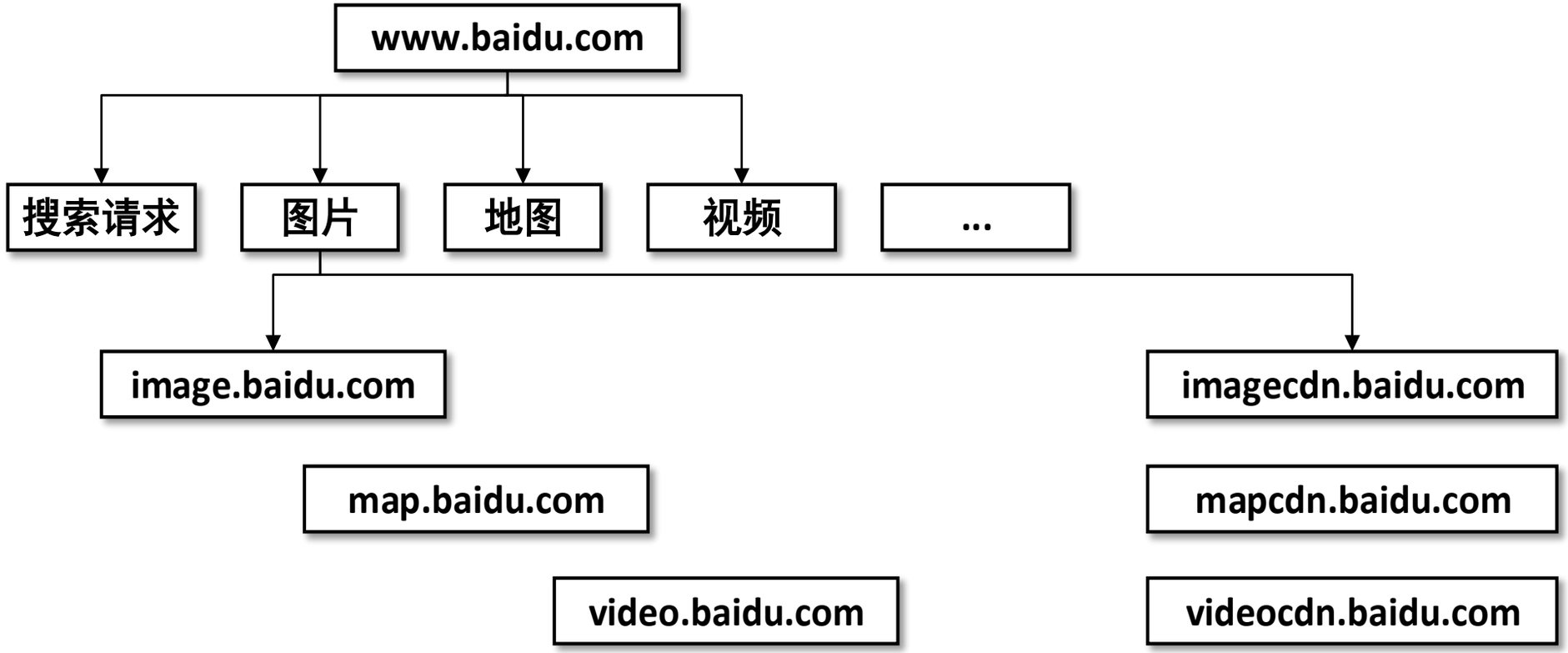
产品成本



改造成本 | 架构和产品

计算性能

访问速度



架构成本

整体接入架构

业务线+域名

产品成本

渲染层

富媒体

各种坑

优化方案

优化方案 | 计算性能

优先使用ECC

使用最新版的openssl

硬件加速方案

TLS远程代理计算

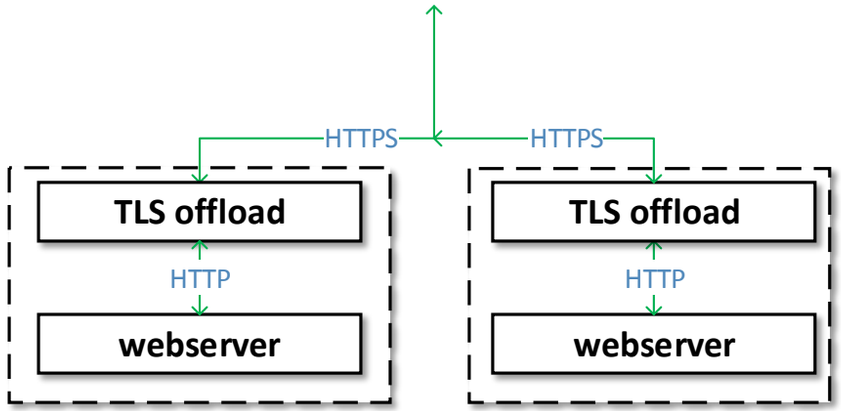
对称密钥大小	RSA和DH密钥大小	ECC密钥大小
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

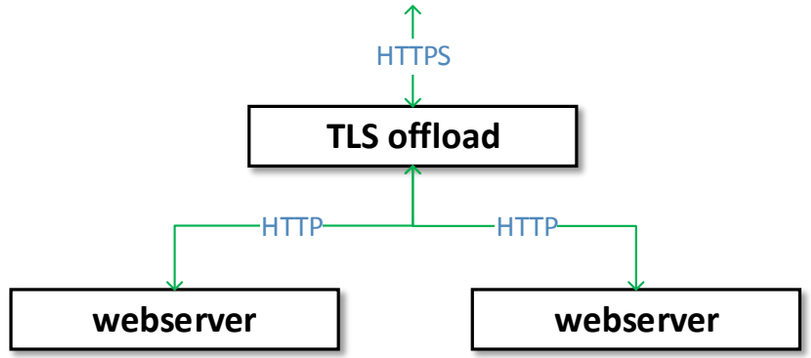
优化方案 | 计算性能

优先使用ECC

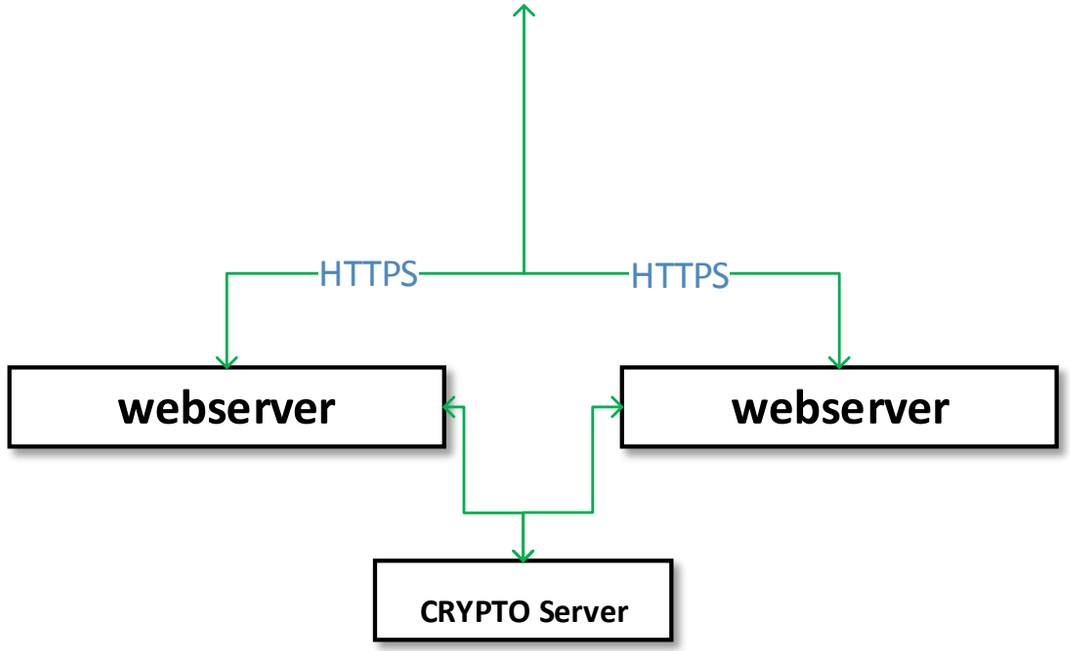
使用最新版的openssl

硬件加速方案





TLS远程代理计算



优化方案 | 访问速度

Session resume

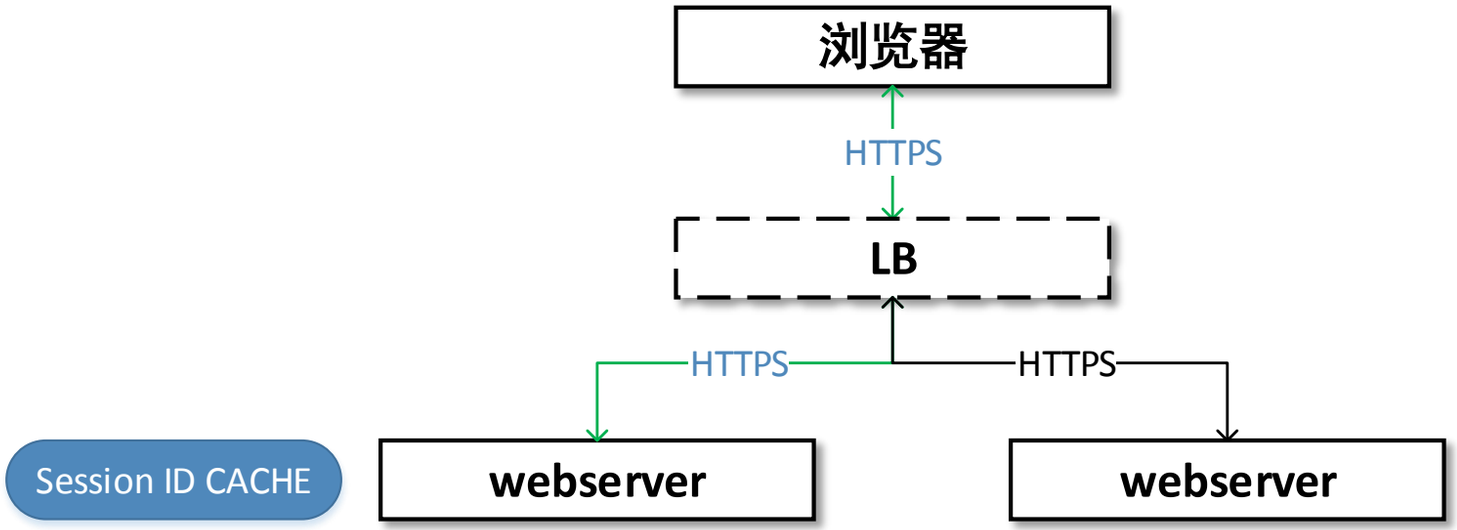
- Session cache
- Session ticket

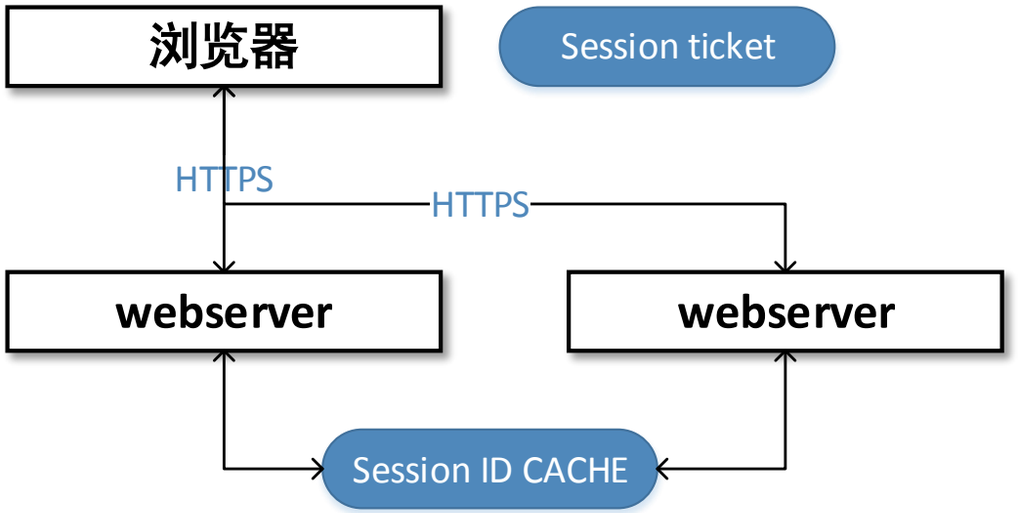
HSTS

Ocsp stapling

False start

SPDY/HTTP2





优化方案 | 访问速度

Session resume

Session cache

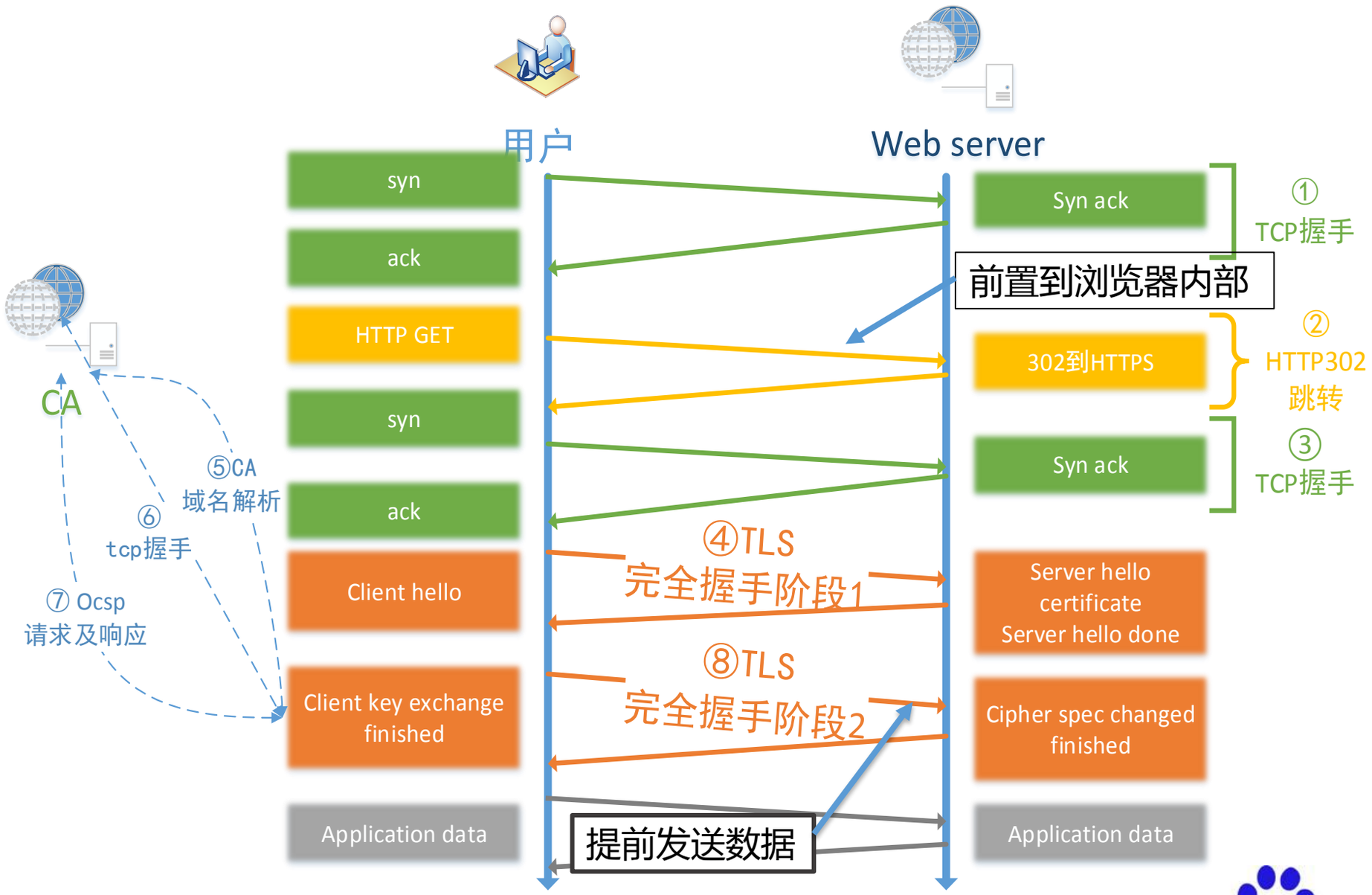
Session ticket

HSTS

Ocsp stapling

False start

SPDY/HTTP2



优化方案 | 访问速度

Session resume

Session cache

Session ticket

HSTS

Ocsp stapling

False start

SPDY/HTTP2

TLS record size

单TCP连接与支持优先级的多路复用

Header压缩

Server Push

HTTP head-of-line block

CWND+SLOW START

优化方案 | 访问速度

极限

False Start + Session Resumption + OCSP stapling + HSTS + RecordSize + CWND = 1 RTT

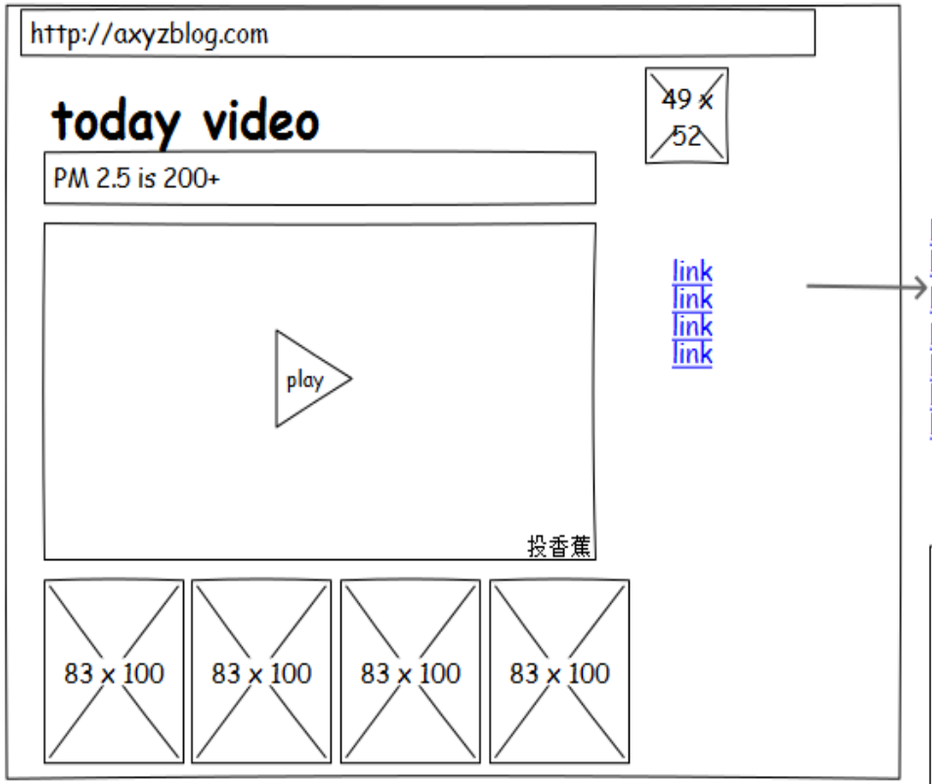
0 RTT? Quic

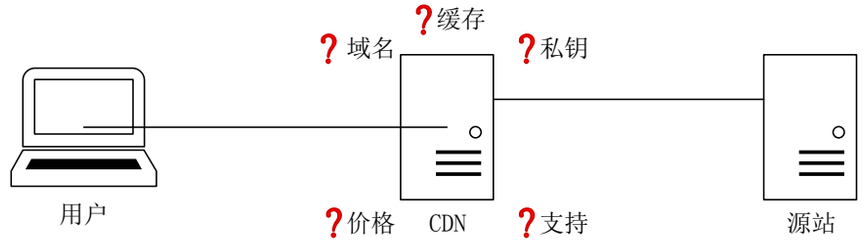
预连接

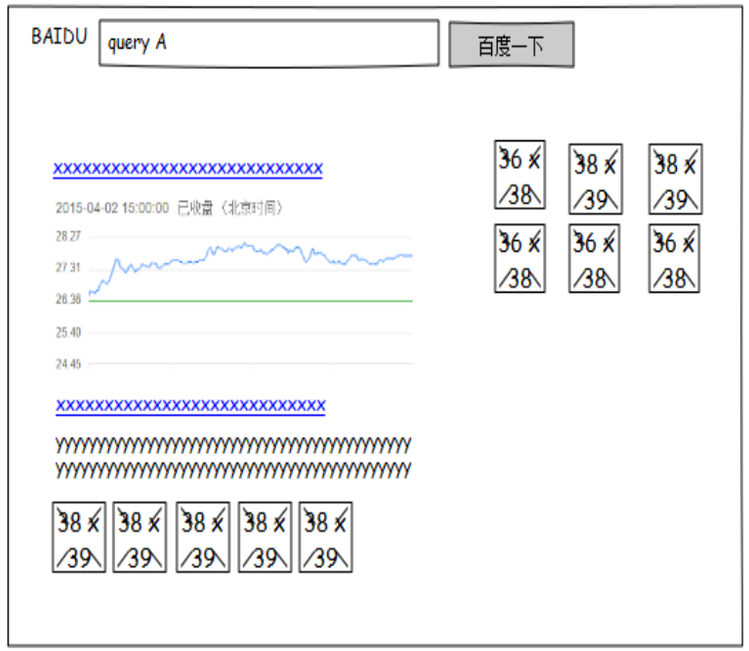
网页端　　客户端　　APP端

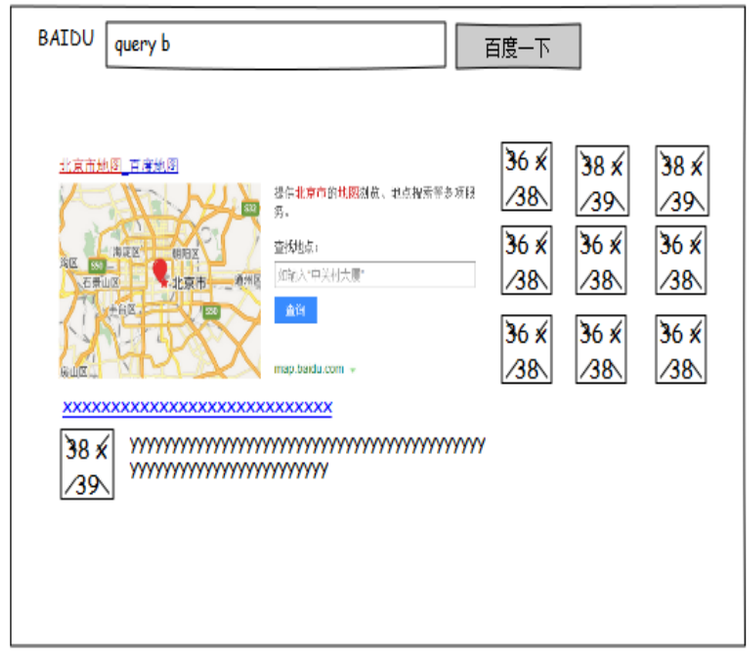
架构相关

优化方案 | 网站复杂程度对架构规划的影响

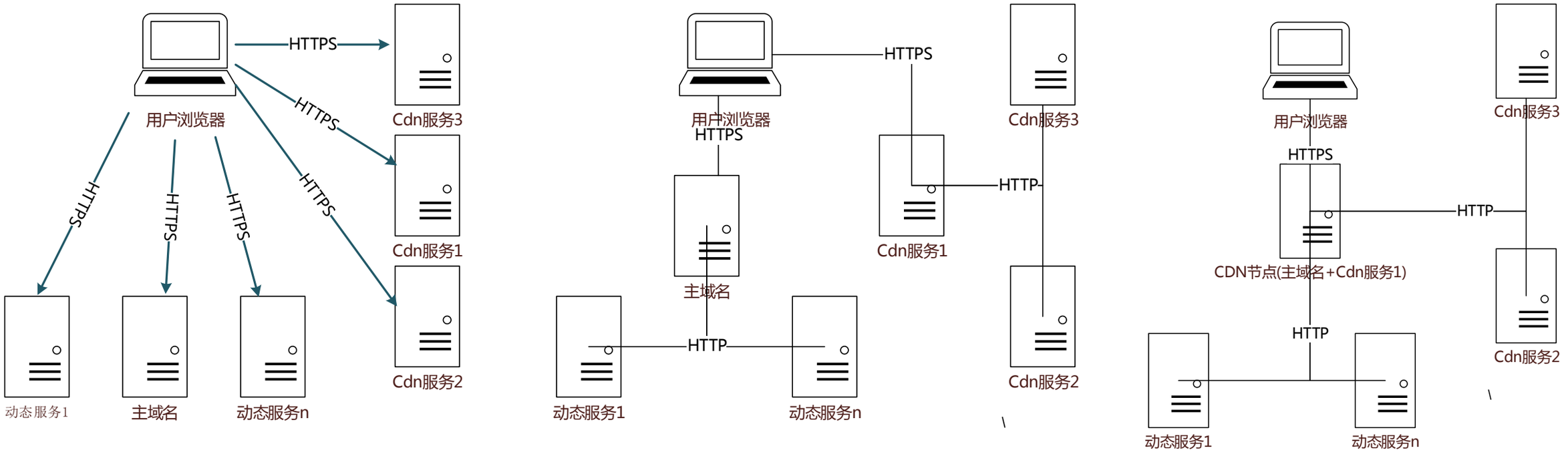








优化方案 | 网站复杂程度对架构规划的影响



优化方案 | 网站复杂程度对架构规划的影响

成本和速度最优

个人建议站点发展到一定规模时考虑如下问题:

域名规划/控制域名数量

统一接入/共享IP

图片等静态资源CDN等做成公共服务，制定严格使用规范和架构

限制第三方内容

优化方案 | 产品改造过程中的问题

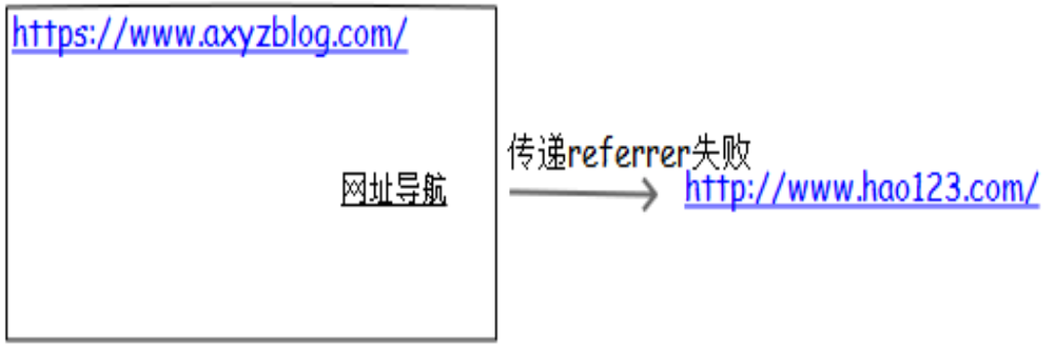
传递Referrer

```
<meta content="always" name="referrer">
```

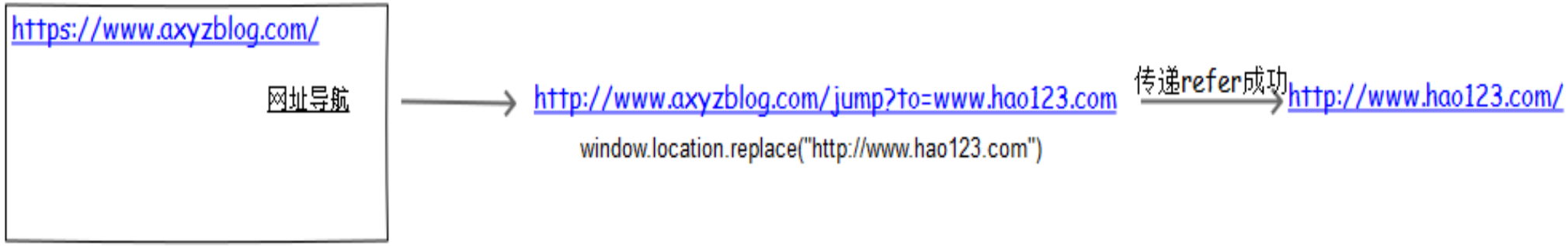
form提交

视频播放

用户异常



混合内容

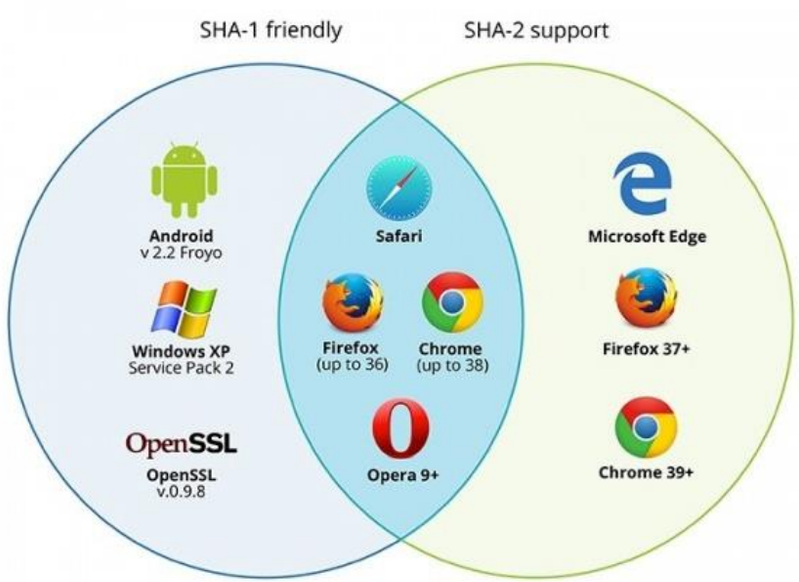


其他问题

其他问题

SHA256的问题

<Android 2.3 XP SP3



Certificate Expiration Date	Chromium 39 Nov 18, 2014	Chromium 40 Dec 30, 2014	Chromium 41 Feb 10, 2015
After January 01, 2017			https://
After June 06, 2016	https://		
After January 1, 2016	https://	https://	

SPDY的问题

HTTPS绝对安全吗

其他问题

SHA256的问题

15年底之后

无法申请SHA1证书了

16年底之前

基于协议特征的SHA1 SHA256双证书适配
精确到浏览器的小版本 用户影响 0.1%-1%

SPDY的问题

16年底之后

SHA256

HTTPS绝对安全吗

搜索/电商/银行(招行 工行 中行)

告知/帮助用户升级(希望可以合作)

其他问题

SHA256的问题

TCP head-of-line block

SPDY的问题

编码问题

HTTPS绝对安全吗

其他问题

没有绝对的安全

SHA256的问题

实现和依赖的系统

SPDY的问题

OpenSSL Heartblood

iOS 7.0.6修复的漏洞

私钥的保管

CDN的回源

HTTPS绝对安全吗

浏览器的漏洞

302

手机号的泄露

阴谋论-随机数和椭圆曲线加密

其他问题

SHA256的问题

清华 段海新教授

SPDY的问题

HTTPS绝对安全吗

参考文献

百度运维部的系列文章 http://op.baidu.com/2015/04/https-index/

Ilya Grigorik http://www.igvita.com/

High-Performance Browser Networking

Is TLS Fast Yet?

其他相关介绍

https://blog.helong.info/blog/2015/09/06/tls-protocol-analysis-and-crypto-protocol-design/
http://www.ruanyifeng.com/blog/2014/09/illustration-ssl.html
http://8btc.com/thread-1240-1-1.html
http://www.cocoachina.com/ios/20150918/13488.html?utm_source=tuicool
http://segmentfault.com/a/1190000002554673
http://rrsongzi-gmail-com.iteye.com/blog/603015
http://blog.jobbole.com/79617/

谢谢

Baidu 百度