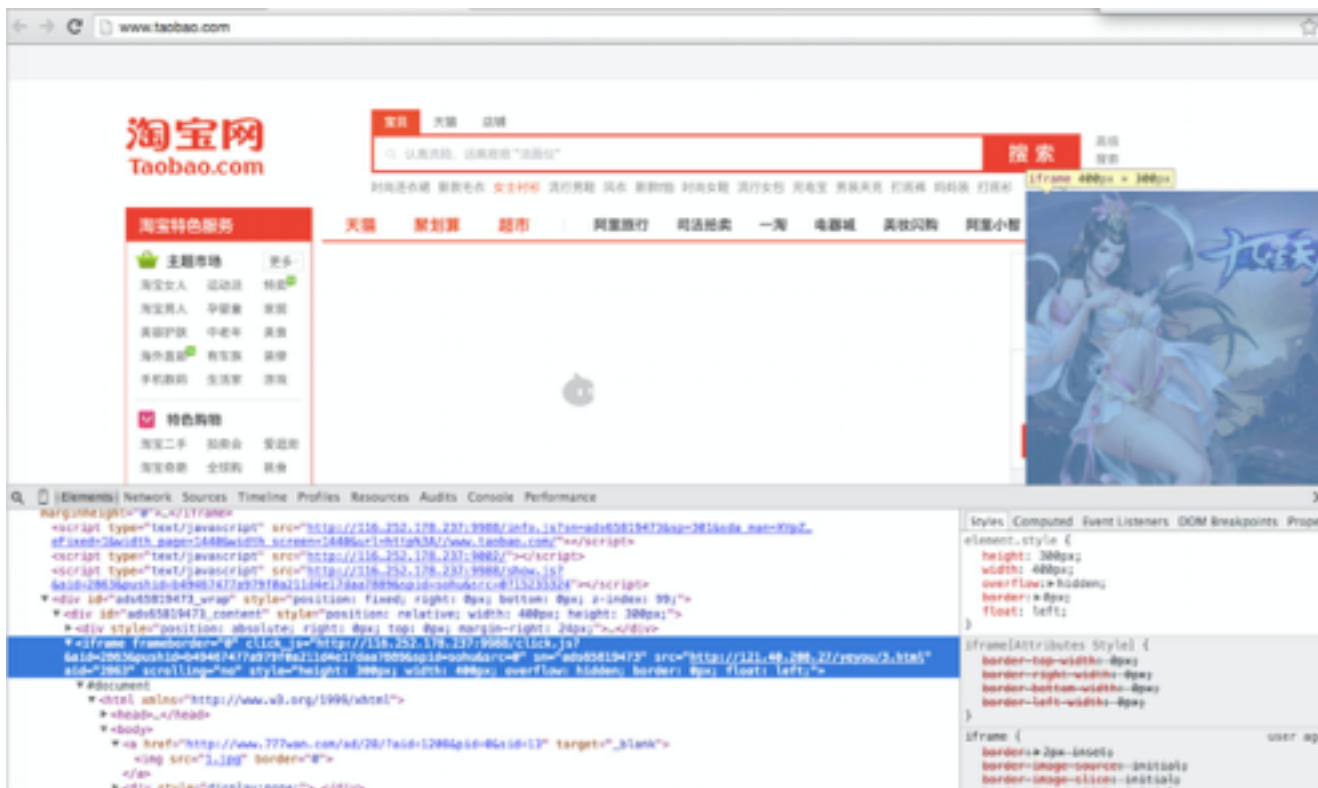


淘宝HTTPS探索

阿里巴巴集团

李振宇（震羽）

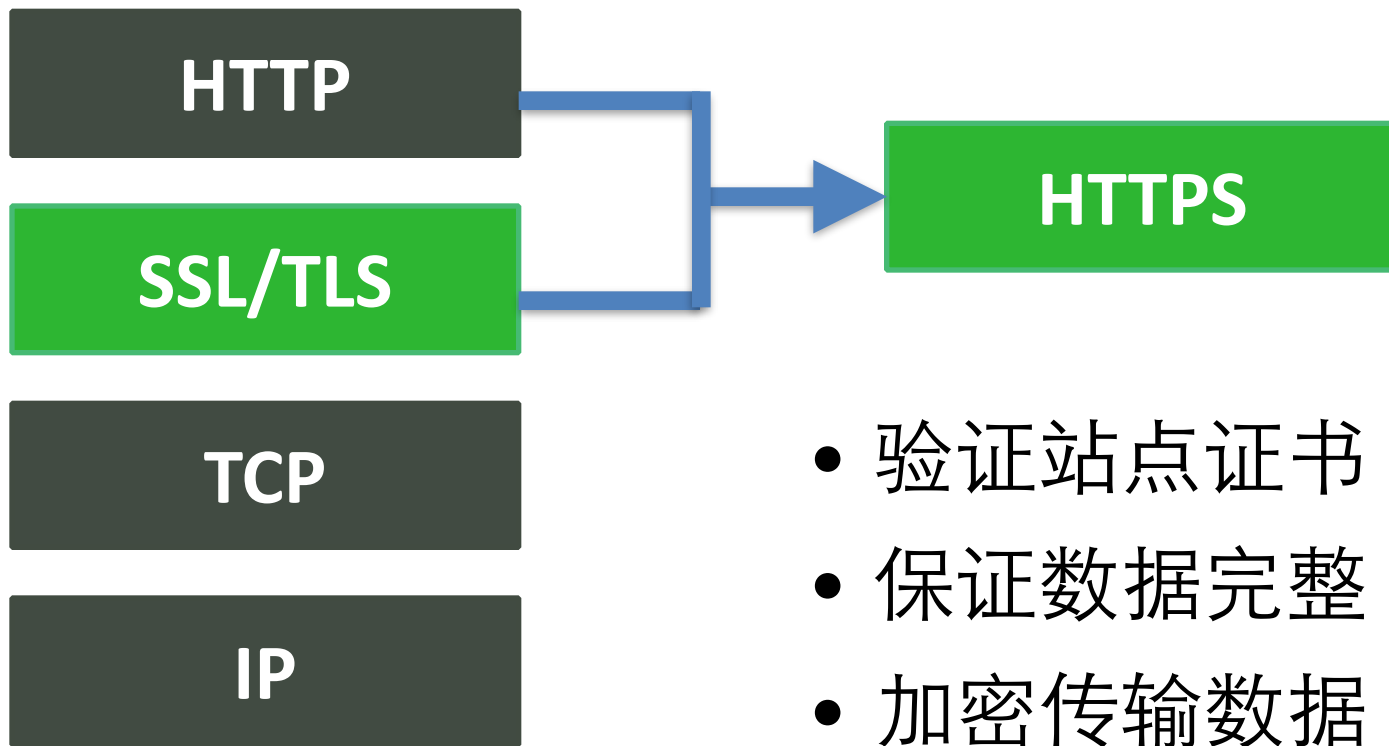




我们的用户
之前遇到的
问题

HTTPS能解决这些问题





服务器性能

HTTPS耗费CPU的元凶是什么？



用户体验

HTTPS一定比HTTP慢吗？



如何选择证书

证书是个什么玩意？我该如何选择？



安全和兼容性

上了HTTPS就安全了吗？还要注意什么？

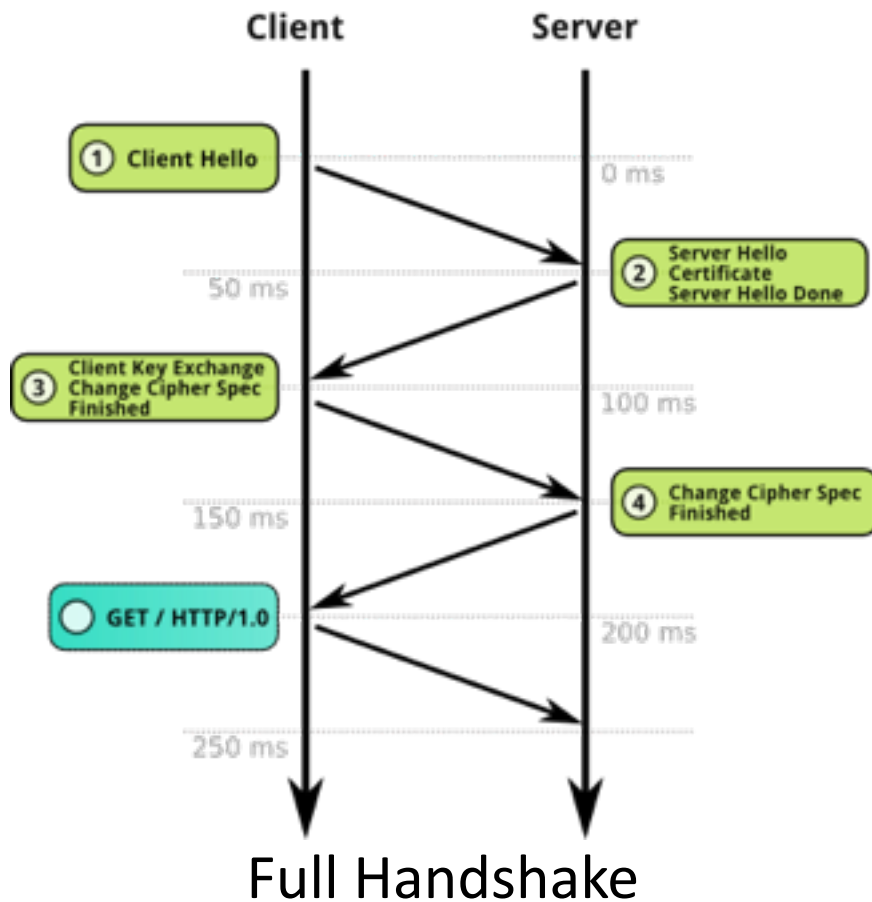
代码改造

怎么改造代码最简单？





服务器性能



非对称加密

- TLS握手

对称加密

- 数据加解密

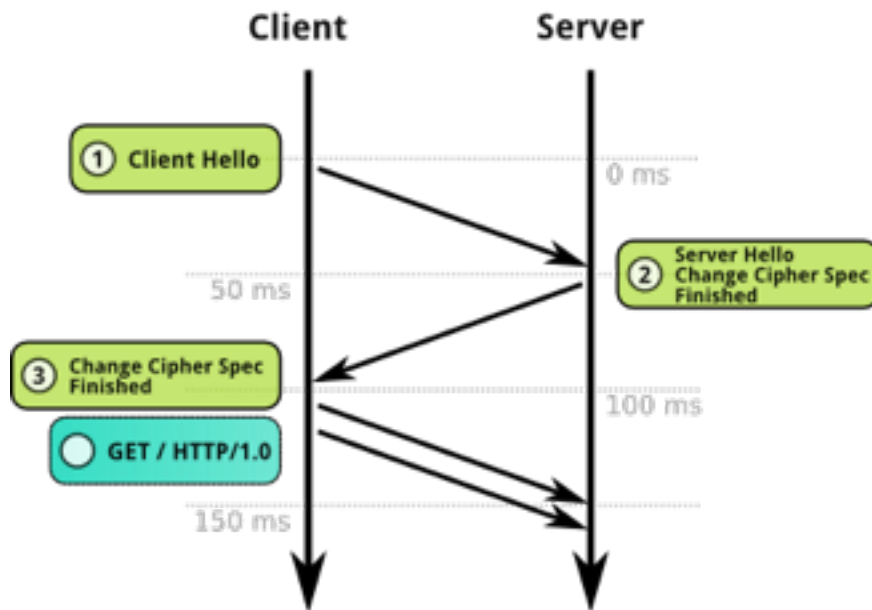
openssl benchmarks

```
$ > openssl speed aes rsa2048
```

webserver benchmark

```
$ > ab (-k) , 1:30
```

尽可能的减少TLS握手



Abbreviated handshake

SessionID:

服务端存储session、兼容性高，合理设置cache大小

SessionTicket:

50%支持，客户端存储session，支持集群模式，nginx默认开启，优先级高，有过期时间设置

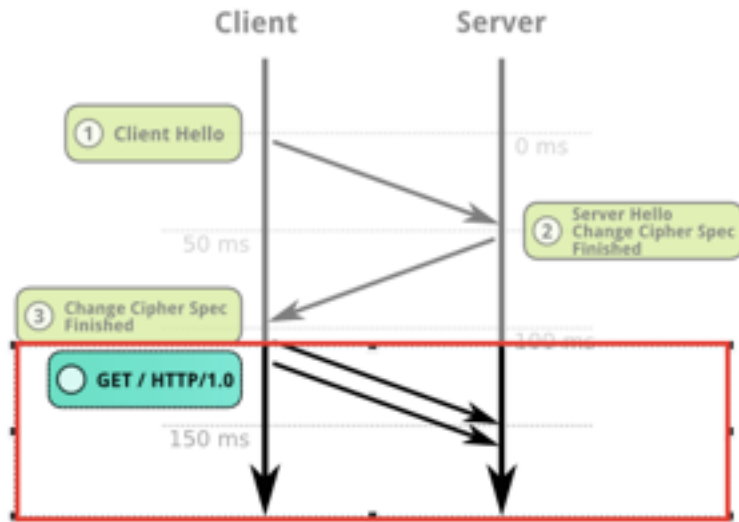
日志监控:

`$ssl_protocol $ssl_cipher`

`$ssl_session_id`

`$ssl_session_reused`





keepalive_timeout=75
keepalive requests=100

日志监控：
\$connection_requests > 1

- *TLS full handshake % =*

*(! keepalive + ! session_reused) / total_conn * 100%*

各种算法的性能			
DHE+RSA	ECDHE+RSA	RSA+RSA	ECDHE+ECDSA
基线	21%	73%	92%

- OpenSSL 1.02a比1.0.1m的ECDSA签名能力提高1.5倍
- 大型网站建议使用硬件加速卡，性价比更高
- 关闭TLS压缩



用户体验



手淘App			
	首页	搜索	购物车
2G	4%	31%	6%
3G	23%	26%	9%
4G	-5%	9%	3%
WiFi	12.7%	29%	6%

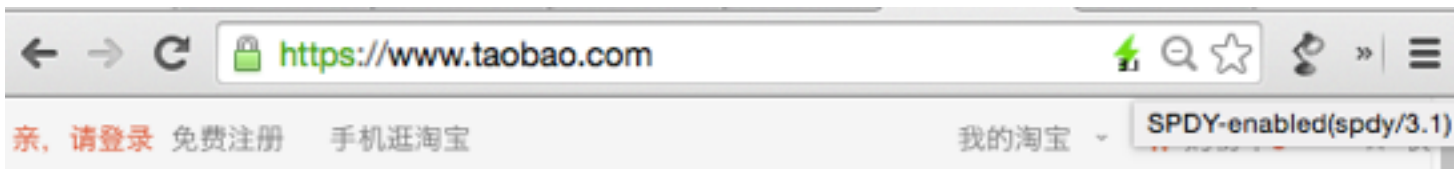
H5（100KB页面）	
2G	15%
3G	6%
4G	-1%
WiFi	3%

PC								
	淘宝 首页	淘宝 详情	淘宝 搜索	淘宝 购物车	天猫 首页	天猫 详情	天猫 搜索	聚划 算
平均	0%	-3%	-3%	0%	3%	-1%	-1%	7%
99th	15%	1%	-10%	-2%	17%	21%	2%	3%



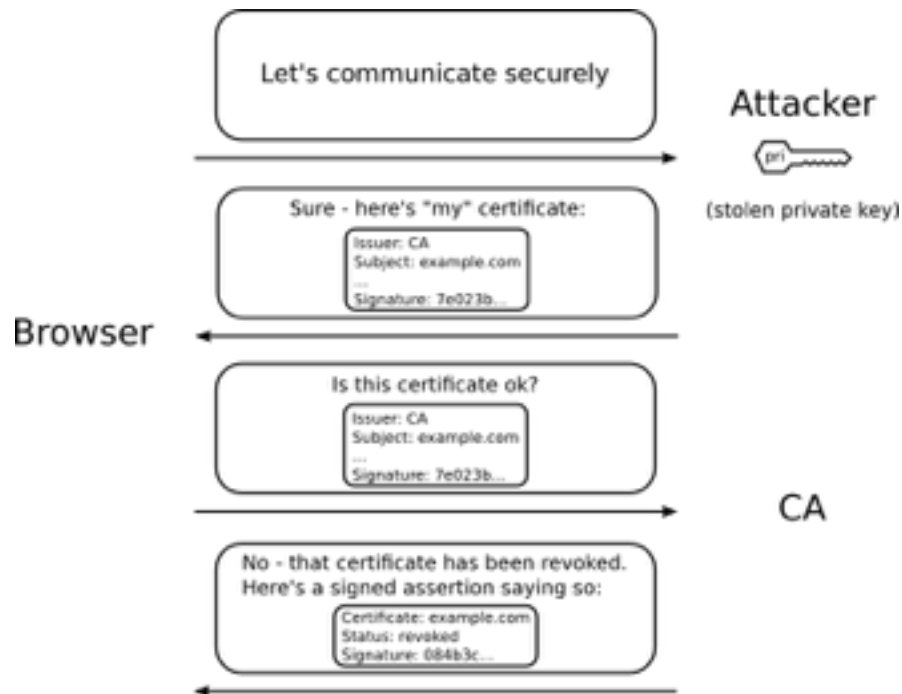
SPDY3.1 & HTTP2

- 多路复用降低TLS握手、连接数、TCP丢包
- *HTTP/2 and SPDY indicator: <http://lwurl.to/3SSC2>*



- 只支持SPDY3.0是不够的
- 未来支持HTTP/2, 用户支持SPDY/HTTP2比率: 70%/20%

OCSP check



- OCSP check需要500ms
- IE/Firefox默认会进行OCSP检测

OCSP Stapling

- 50%支持
- 只能发送一级证书状态
- 注意证书链大小

其他优化措施

- TCP内核优化
- False Start
- CDN Early Termination
- 适当调整TLS Record Size
- 预加载
- 图片域名合并
- 去掉资源合并以及Inline资源



其他优化措施

- TCP内核优化
- False Start { ECDHE
减少一个RTT
- CDN Early Termination
- 适当调整TLS Record Size
- 预加载
- 图片域名合并
- 去掉资源合并以及Inline资源



其他优化措施

- TCP内核优化
- False Start
- **CDN Early Termination - 动态内容也可以做加速**
- 适当调整TLS Record Size
- 预加载
- 图片域名合并
- 去掉资源合并以及Inline资源

其他优化措施

- TCP内核优化
- False Start
- CDN Early Termination
- 适当调整TLS Record Size
- 预加载
- 图片域名合并
- 去掉资源合并以及Inline资源



其他优化措施

- TCP内核优化
 - False Start
 - CDN Early Termination
 - 适当调整TLS Record Size
 - 预加载
 - 图片域名合并
 - 去掉资源合并以及Inline资源
- DNS-Prefetch
Preconnect
Prefetch
Flush HTML Early
PreRender



其他优化措施

- TCP内核优化
- False Start
- CDN Early Termination
- 适当调整TLS Record Size
- 预加载
- 图片域名合并
- 去掉资源合并以及Inline资源



3

如何选择证书



	展现	单域名	多域名	泛域名	多个泛域名
DV		支持		不支持	
OV		支持			
EV		支持		不支持	
e.g		www.taobao.com	www.taobao.com www.tmall.com www.1688.com	*.taobao.com	*.taobao.com *.tmall.com *.1688.com

各种证书的加密强度都是一样的
个人用户可以尝试免费的Let's Encrypt

4

安全和兼容性

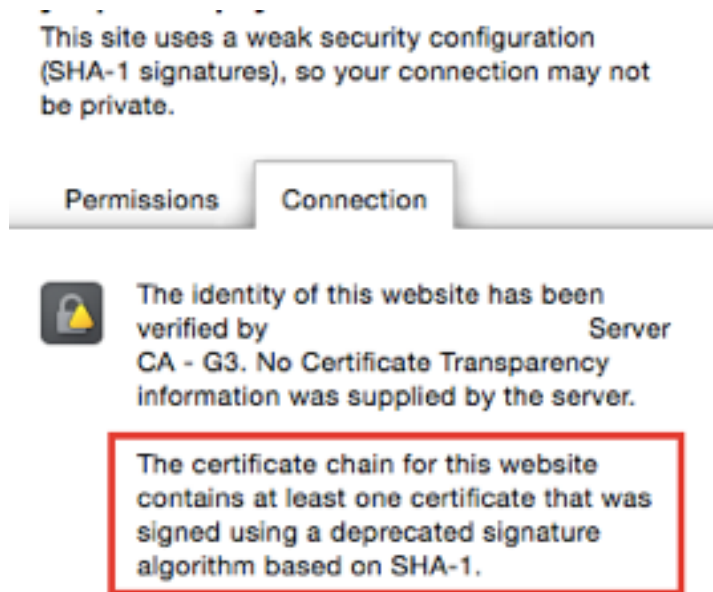


Modern compatibility

For services that don't need backward compatibility, the parameters below provide a higher level of security. This configuration is compatible with Firefox 27, Chrome 22, IE 11, Opera 14 and Safari 7.

- Ciphersuite: ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK
- Versions: TLSv1.1, TLSv1.2
- RSA key size: 2048
- DH Parameter size: 2048
- Elliptic curves: secp256r1, secp384r1, secp521r1 (at a minimum)
- Certificate signature: SHA-256
- HSTS: max-age=15724800


https://wiki.mozilla.org/Security/Server_Side_TLS



SHA1证书过期


1. 2016年开始CA不再颁发SHA1，2017年开始浏览器不再支持SHA1证书
2. WindowsXP SP2/Android<2.3不支持SHA256证书



 <https://www.taobao.com>


www.taobao.com
Your connection to this site is private.

Permissions **Connection**

 The identity of this website has been
verified by a certificate.


Transparency information was supplied by the server.


[Certificate Information](#)

 Your connection to www.taobao.com is encrypted using a modern cipher suite.

The connection uses TLS 1.2.

The connection is encrypted and authenticated using AES_128_GCM and uses ECDHE_RSA as the key exchange mechanism.

 **Site information**
You first visited this site on Jun 15, 2015.

 *.taobao.com

Signature Algorithm	SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters	none
Valid Before	Friday, May 29, 2015 at 8:00:00 AM China Standard Time
Valid After	Sunday, June 12, 2016 at 7:59:59 AM China Standard Time

1. SHA1证书过期时间不超过年底

2. 多证书支持



- HSTS可以阻止SSLStrip

- 防止80端口被劫持
- 让用户不能忽略证书错误
- 减少2个RTT
- IE11/Android4.4/Opera都不支持
- PreloadList - <https://hstspreload.appspot.com/>

```
Request URL: https://www.alipay.com/
Request Method: GET
Status Code: 200 OK

▼ Response Headers view source
Connection: keep-alive
Content-Encoding: gzip
Content-Type: text/html; charset=utf-8
Date: Tue, 28 Jul 2015 07:20:02 GMT
Expires: Sun Jan 01 1995 00:00:00 GMT+0000 (CST)
Pragma: no-cache
Request-Id: 0ae1051314380680023766540
Server: Tengine/2.1.0
Set-Cookie: spanner=aSQ0xeb1flrQ3WDM5nB4veue1
Strict-Transport-Security: max-age=31536000
```

Your connection is not private

Attackers might be trying to steal your information from
.com (for example, passwords, messages, or credit cards).

[Hide advanced](#)

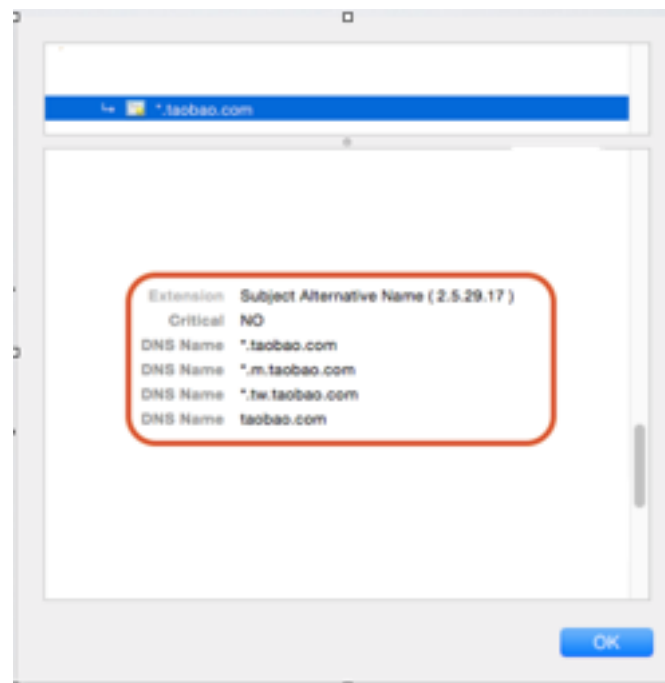
[Reload](#)

.com normally uses encryption to protect your information. When Chrome tried to connect to .com this time, the website sent back unusual and incorrect credentials. Either an attacker is trying to pretend to be .com, or a Wi-Fi sign-in screen has interrupted the connection. Your information is still secure because Chrome stopped the connection before any data was exchanged.

You cannot visit .com right now because the website uses HSTS. Network errors and attacks are usually temporary, so this page will probably work later.



- SNI (Server Name Indication)
可以在TLS握手的时候告诉服务器我要访问什么域名，这样一个IP:443就可以部署多个证书
- 但是IE6~IE8/XP不支持SNI协议

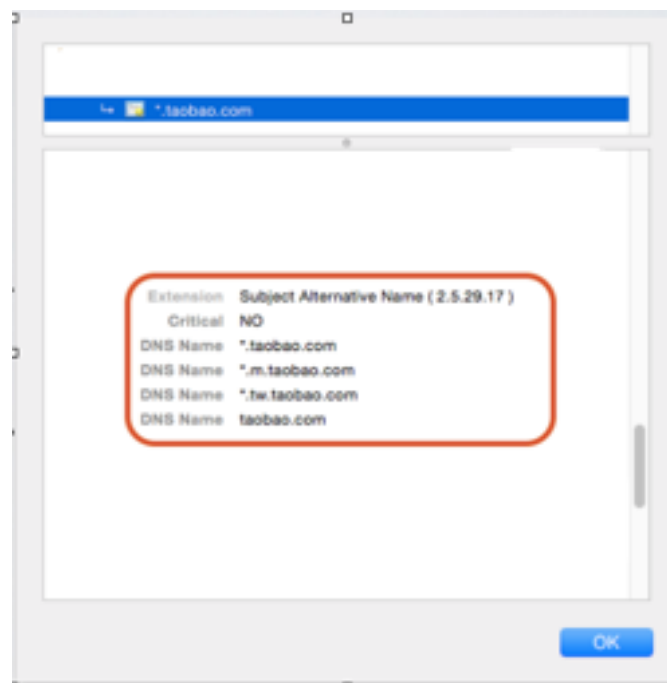


解决方案：多泛域名证书（WildCard SAN Certificate）



多泛域名证书还可以在多个域名之间复用连接如果：

- 多个域名合在一张证书里面并且证书有效
- 域名指向到同一个IP
- 使用SPDY3.1 or HTTP/2





代码改造

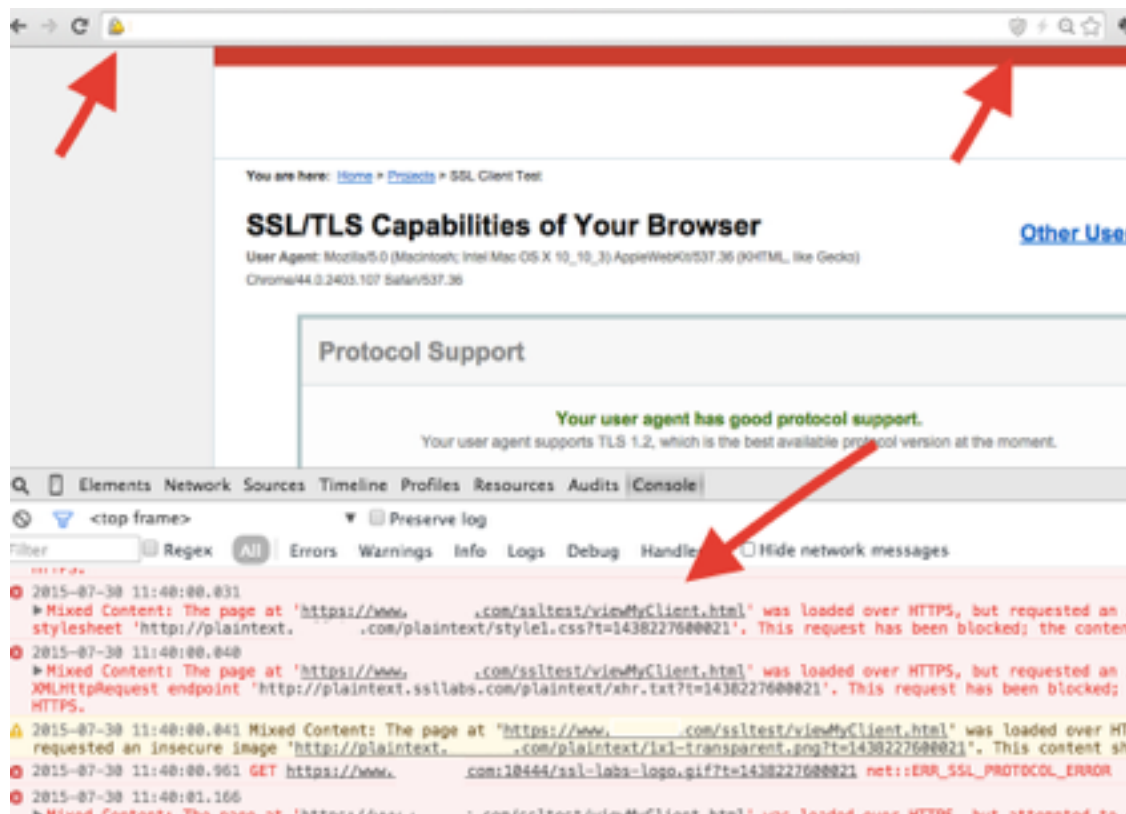
http:// => //

缺点:

1. 无线老版本对//解析不支持
2. 有些中间件不支持

```
href="//gtms03.alicdn.com/tps/i3/TlOjaVFl4dXXa.JOZB-114-114.png" r
href="//g.alicdn.com/tb-mod/??tb-pad/1.0.1/index.css,tb-sitenav/1.
sysbanner/1.0.0/index.css,tb-banner/1.0.3/index.css,tb-top-spy/1.0
search/1.0.5/index.css,tb-logo/1.0.5/index.css,tb-gr/1.0.0/index.c
promo/1.0.2/index.css,tb-tmall/1.0.0/index.css,tb-belt/1.0.0/index
ifashion/1.0.6/index.css,tb-market/1.0.2/index.css,tb-market2/1.0.
diet/1.0.8/index.css,tb-apollo/1.0.0/index.css,tb-market-furnitur
market-pannel/1.0.2/index.css,tb-notice/1.0.3/index.css,tb-member/
conve/1.0.7/index.css,tb-apps/1.0.3/index.css,tb-feature/1.0.0/ind
footprint/1.0.2/index.css,tb-discover-shop/1.0.2/index.css,tb-cust
cat/1.0.0/index.css,tb-rmdimg/1.0.0/index.css,tb-channel/1.0.1/ind
guang/1.0.1/index.css,tb-channel2/1.0.3/index.css,tb-channel-edu/1
sale/1.0.0/index.css,tb-helper/1.0.0/index.css,tb-footer/1.0.0/ind
fixedtool/1.0.0/index.css"><link rel="stylesheet" href="//g.alicdn
page/tbindex/1.0.71/index-min.css"><script src="//g.alicdn.com/??k
```





黄三角：图片、POST
盾牌：JavaScript、异步
调用、字体、iFrame、
Flash、视频

利用Webkit内核自动
检测URL是否HTTPS友好

- 图片：图片空间自动搬家工具
- 视频：Flash包一层
- 国内地图：高德
- 国外地图：？
- Referer丢失：<meta name="referrer" content="origin">或者
window.name
- SEO问题：
 - 国内：部分支持HTTPS抓取，但还不支持//
 - Google：http://lwurl.to/3SQ3J





推荐

1. SSLabs: <http://lwurl.to/3SR0K>
2. Ivan Ristić: 《Bulletproof SSL and TLS》、
《OpenSSL Cookbook》
3. Ilya Grigorik: <https://istlsfastyet.com/>、
《Yesterday's perf best-practices are today's
HTTP/2 anti-patterns》、《High-Performance
Browser Networking》
4. 百度https实践: <http://lwurl.to/3SR0L>




总结


1. 尽可能降低TLS新建的比率
2. 使用ECC算法，ECDSA证书需要CA支持
3. 使用最新内核、Webserver、OpenSSL的稳定版本
4. 建立性能监控，找到HTTPS的性能瓶颈
5. SPDY3.1&HTTP/2对用户体验提升最大
6. HTTP/1.1的最佳实践在HTTP/2可能不再适用
7. 黄三角和盾牌一定需要去除
8. 使用多证书解决Chrome将SHA1标记为黄色的问题
9. 多泛域名证书能极大的降低运维成本
10. HSTS一定要支持
11. 使用//同时提供http&https的服务
12. 经常使用ssllabs等网站检测TLS配置





 @阿里技术保障



 @阿里技术保障

谢谢~!

Q&A

tony.lizy@alibaba-inc.com

