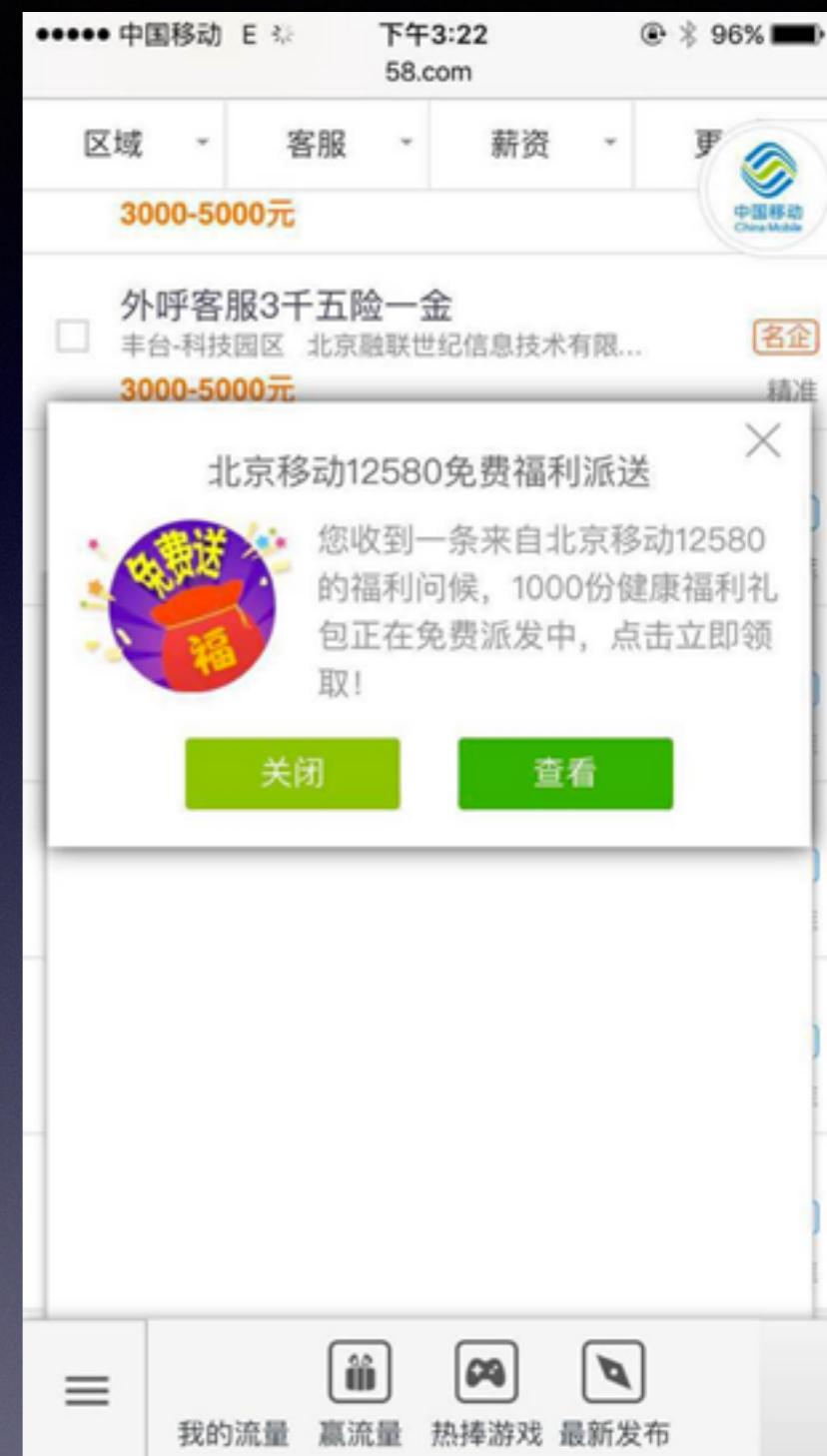


HTTPS

和运营商劫持说拜拜

一、为什么要上 HTTPS



Structure Sequence

https://www.google.com.hk
<unknown>
https://www.baidu.com
https://ss1.bdstatic.com
https://ss0.bdstatic.com
https://sp1.baidu.com
https://sp0.baidu.com
http://music.163.com
http://www.gstatic.com
http://10.20.13.51:8000
https://e.crashlytics.com
https://raw.githubusercontent.com
https://safari-extensions.apple.com
http://rm.api.weibo.com
https://baidu.com
http://www.google.com

Overview Request Response Summary Chart Notes

1 0Í□□□□□□□< Mv § bÎÌÅHuða]H€ P¾% " Gf(² Eöpl±AäÅý z<9 ,µøÒ h©ý o à
1 -ÇÑÑ-í ,çÔE "íi3 ù[Vh ÁÌÀºÅvÖ,ÁìµäÖii·ð³\$ H@-
2 "Äb|ñkV Y p 9 ð_ú oo a}vTIQZCø VþÅÉÖ kcæ FPÐ]Ö· 9@ûÒaI-è ü,å±
Â K ðÊ R c -Ù □)□□□□□=vÇÄá c□ÅWu PÜ¶-cÓ- ¥ Oá-(«ÅSSÈ □í□
□□□□□>D,5½dµ öÉyÜ eä í ÙxèD^ &rÈ}y|åg T tÙ±[i'õ± Ä>[mØ0 C\$+a 7Só
í l'NzEÁø·NVì U&1, G})L ý/a| 6 Øù/I^ÙIU a£K ÔdëK (xyo ÅluS ÄC<€]:ÍX±
U H ¥ iïõ ^] i! í Bd@vü a dq ðoË þ è ° U-çKdæB\à*µ □)□□□□□?7
\$7ûøt " zLqÊ b- ð { øÇ9C \$J-3 □í□□□□@W} µ-øM CR ØÖÆ- a! RP û
£>w °èÜÑX©l¾_-¼pþß- -ù s%CÁí xmD \t È£I~ÈØÖUøb *i.!¢ Qf\$ ôü ¼×âîO}
_.~6í|j ²aG1lò=- ÈÅ«¶Jº ®õ[]t û·uñt \$ô Ôçªu Iqx /ä è*Éáæ Â rÓ-t@ øÈí½
é " vÀ R é¹ d,Éà·èn 'ü©m» □%□□□□□Ae"Aù³b,¶ø 8Ú ½åg"(Ù·í+ e«¿
m □Ð□□□□□Býd ³ \$² ø4 ,èµ SÈrÓì De Áo D ?£óùÆÜ ¢e g§
°ioÔhÝi¤¤[7Ã ò#ºo hïàò w ñæË Gp€ I|òC 6 è ä¹÷îþÙµ) □ì _ÅÙó6úO
rÚ(OÛsU}48 èüPi 2 Ó ýÇiÜÖy.~Lñ ||+k -ä , H:à_r) Z À E SJÝ Nô
B ïæ:!® 9 4 ûn □)□□□□□Cj» N Taiþ-, vïéâ2 » -võ=jå~G6 □É□□□
□□□D½ þø]T?I_}·6 R·ã□¥êM
3 På°}åázUeJø ~x2 x³ ð®'P Õä _2SÉé3 È °
4 H#V> -S ,mił oí@EA_Eçuo Qa-e P3Uç , YQ /z'a9 -Ù %4E;O, · O, ;J,z:= - /@!z>·
SÍ4·Æí6 Ø AFÉ z) □rBu a&é va69-nø03 Yaó- Äf □é!< □)□□□□□Fr3W

Structure Sequence

https://www.google.com.hk
<unknown>
https://www.baidu.com
https://ss1.bdstatic.com
https://ss0.bdstatic.com
https://sp1.baidu.com
https://sp0.baidu.com
http://music.163.com
http://www.gstatic.com
http://10.20.13.51:8000
https://e.crashlytics.com
https://raw.githubusercontent.com
https://safari-extensions.apple.com
http://p4.music.126.net
https://safebrowsing.google.com

Overview Request Response Summary Chart Notes

1 0E□□□□□ 1 1ä üßÇV Ü~Dk`
2 sÀËºMØLP'Ë ïzQØ Ä~Y úðÓ€ªJØ Ö&Ä
3 MºEOS6 awU ç□□□□□ |Ø ïrB a-\dUQð+ ®: é ô é÷ iöy²F"4W² Uä k¥Ùè
k í í % å_u l ¾s7zoÀz#imFQN ù·ù/ ' Ç n¹ ;Y Q# õSsÆ½ C¢ Ú¥'«'nCO
®ÿâÑ .F,- Á þ®¼/g °Ð□ "Ø _å~& ©,!y°é iØ5 ØhL € ïdþW½ q < A-!ØY¥¤s
@½¤ ú<Ñ®=ç© .6P
4 Ö Y" ;y å!Ö Èò³/ ,IÅM#vÊ ® Tñ5ß-ó>@ÙóC }wNëxT¥]| ½ñç ÄG uø G®ÙS·Ef
øgÉ (: · \$,YlähÅ -gÊÖYÖ e¿Ðò" 4 álóAb ä>5é§ èyWY ïnæÂ Áéö+- ?H[
àWÐòT'¿ Y@í Ë¤{Çøl¥Ó"y - i¶H Åxä²räÓÛð· ê,Z¶ òO7 çÃ' qtºô £ I
ZËÙ·Øßð Á-h VÇ sëT 2m) _OBØ(<ú @ ÁØ«;a]£äº?i ¥-ì Ñ t □)□□□
□□□ 'Y6K^cD >'xu yT[-Uï \ï"é □.□□□□□ -&iõù¶FÉÆ ð4 Ú2 à @S
□óÃ2Ý ýh~üì AE □□□□□ úk¤ ÆO(z{é¹ÃÃ"- 7Wt6~naWÓ- u ?Ö5
%H Öè u iáÛ7 wØ?_nE ý"¥ [5zþóÉ ~p», XHþIïê-C i*fË2â O ÅS kZ®4{ Äßó
äç-\$, ua o-ðøa?26
5 X à·ëmää ^/³é <SC.QmvÀP?Ô|Ëä~3¤Uí ³Eí;Ù<VÁ¹rÝú +½ +üw?ïôf Üe¶
9ÂæC ²Ac¹IP² À i ~äN [Æ "³xìU'K ,}ÆN# · e iB1òë© x 3 JéÑ i+È- "Û ùkN]
12 var GFrom="";
13 var GClient="";
14 var GPLatform="other";

关于抵制流量劫持等违法行为的联合声明

我们六家公司(今日头条、美团大众点评网、360、腾讯、微博、小米科技),在此联合表达共同诉求:呼吁有关运营商严格打击流量劫持问题,重视互联网公司被流量劫持,可能导致的严重后果。

进一步说明,目前的移动互联网环境下,流量劫持方式主要分为两类:

- 1、域名劫持,表现在用户正常联网状态下(如3G、4G和WiFi等状态),目标域名会被恶意地错误解析到其他IP地址,造成用户无法正常使用服务。
- 2、数据劫持,对于返回的内容,会在其中强行插入弹窗或嵌入式广告等其他内容,干扰用户的正常使用,对用户体验构成极大伤害。

放任流量劫持将带来以下严重后果:首先,遵守市场规则的公司不能得到褒奖,商誉和利益被严重伤害,而违法违规者却受到鼓励;其次,用户使用我们的产品,意味着和我们之间形成严格的服务契约,流量被劫持,等于用户不能得到约定服务,从而导致利益受到损害;第三点,也是最让人忧虑的地方在于,我们提供的信息服务,都是依照国家法律,并在有关部门监管下完成,而劫持流量者提供的信息服务,完全脱离监管,甚至可能传播诈骗、色情等低俗甚至严重违法信息,如任由非法劫持泛滥,将造成无法挽回的恶果。

上述两类劫持和偷卖流量等行为,已有多项证据直接指向某些机构。鉴于劫持行为已涉嫌违反中国法律,如《电信条例》等,因此,我们在对恶意劫持做技术识别和拦截之外,也向有关监管部门报案。

我们发表联合声明,是为引起全社会重视,我们不排除视事态发展,进一步采取联合行动的可能。

最后,我们再次呼吁,打击包括流量劫持在内的违法行为,不仅关乎互联网产业健康发展,也是包括运营商在内的所有游戏参与者的义务和责任。我们期待社会各界充分重视问题的严重性,采取共同措施抑制劫持,共同打造一个健康、诚信、有序的市场环境。

特此声明!

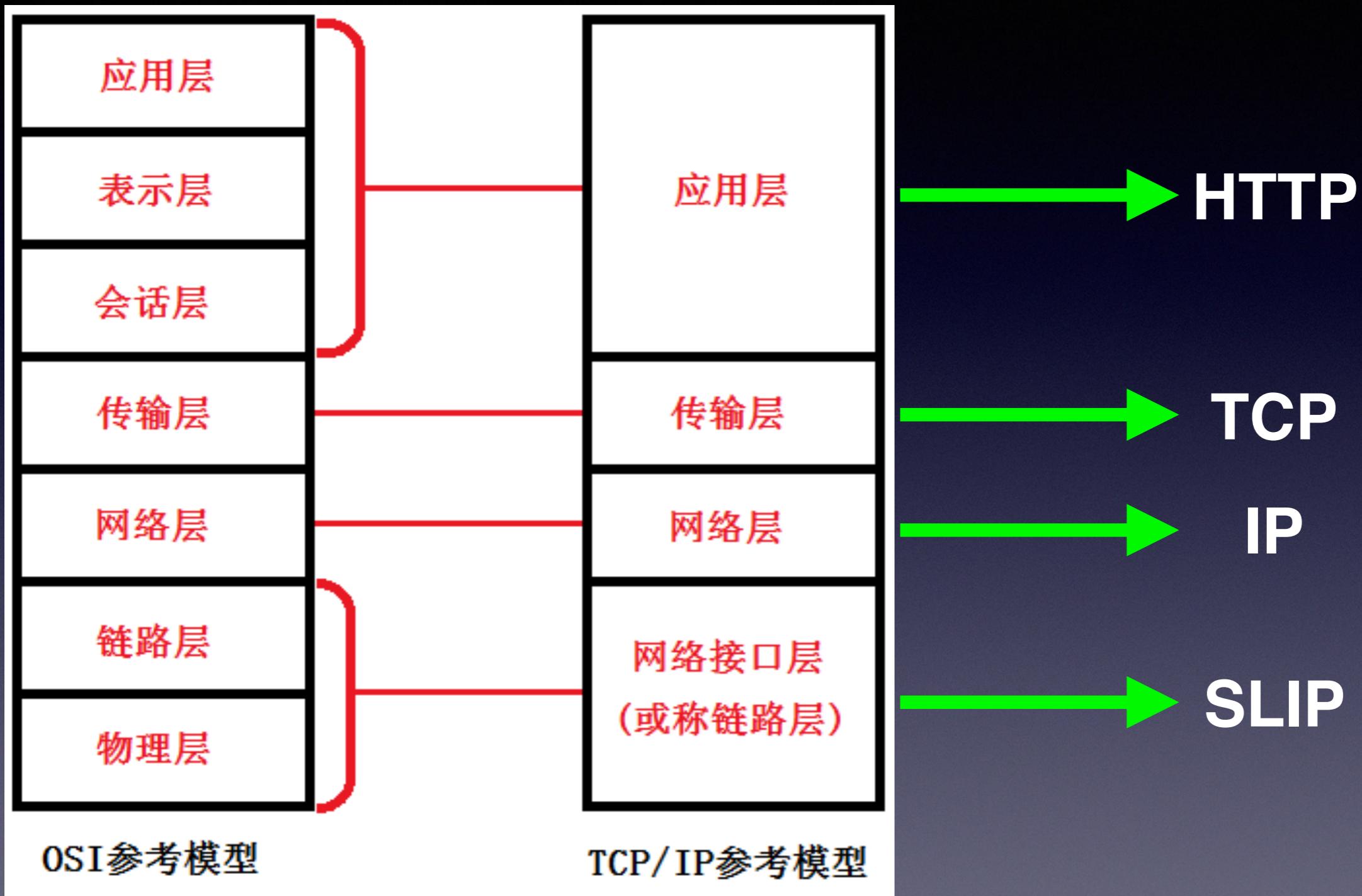
联合声明企业(按汉语拼音首写字母排序)
今日头条、美团大众点评网、360、腾讯、微博、小米
科技

HTTPS 趋势

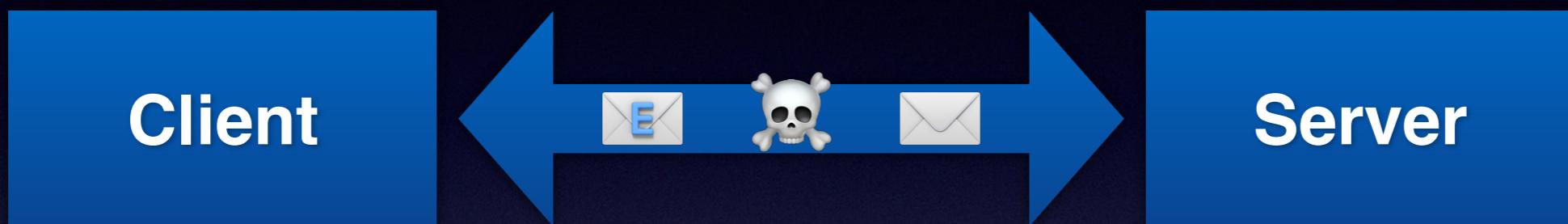
- Chrome/Firefox：将 http 标记为不安全
- Apple 要求 2017 年前上架 APP 全部采用 HTTPS
- 下一代 HTTP 协议只用于 HTTPS 网址
- Google / Baidu 搜索排名会给 HTTPS 网站加权
- 美国要求2016年底所有政府网站必须是HTTPS



二、HTTPS为什么比HTTP安全



HTTP 为什么不安全



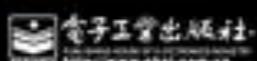
- 明文传输，数据没有加密，通信双方没有认证
- 窃听：第三方节点可以获知通信内容
- 冒充：第三方节点可以冒充他人身份参与通信
- 篡改：第三方节点可以修改通信内容



程序员的自我修养

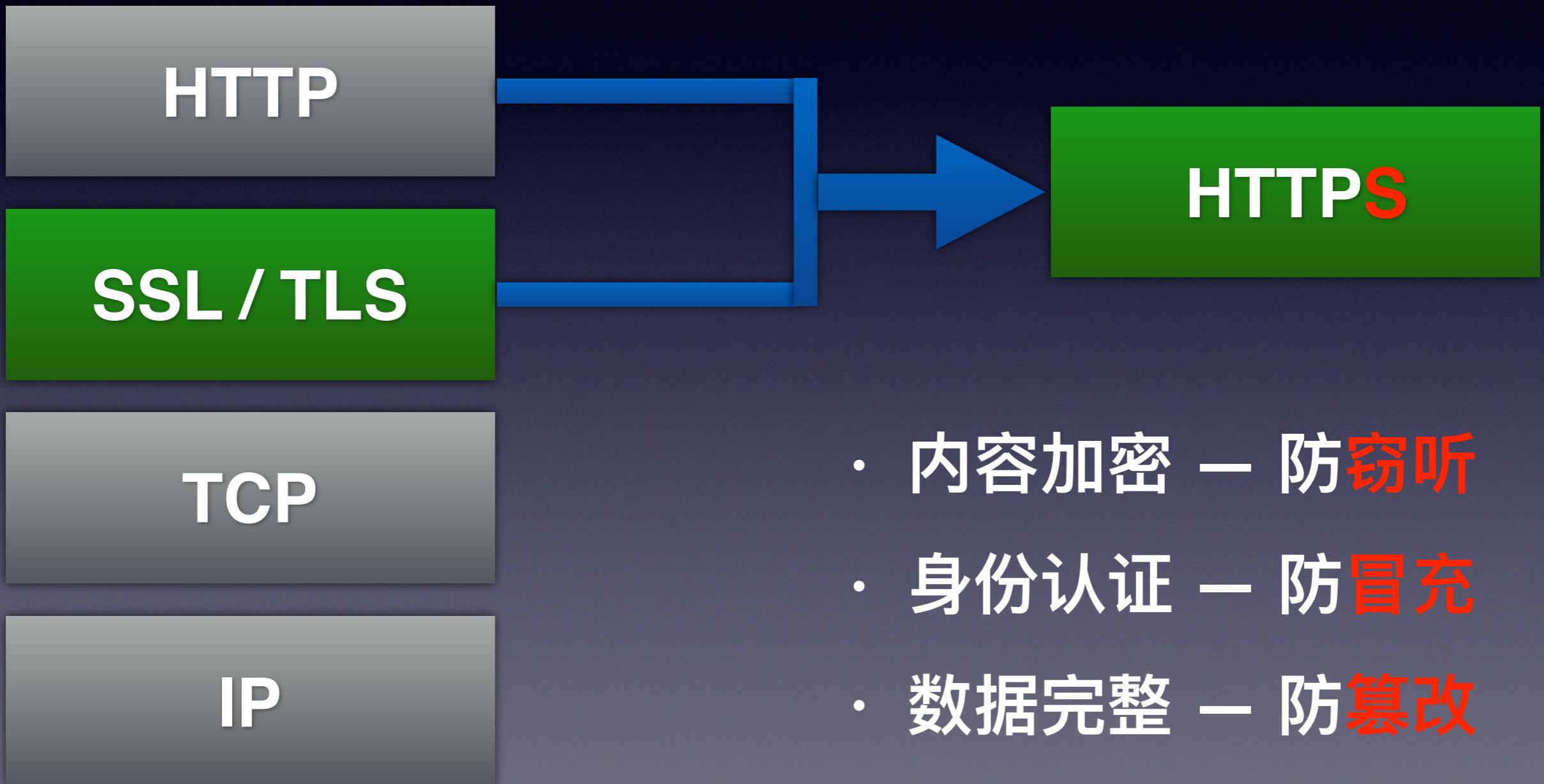
——链接、装载与库

俞甲子 石凡 潘爱民 著



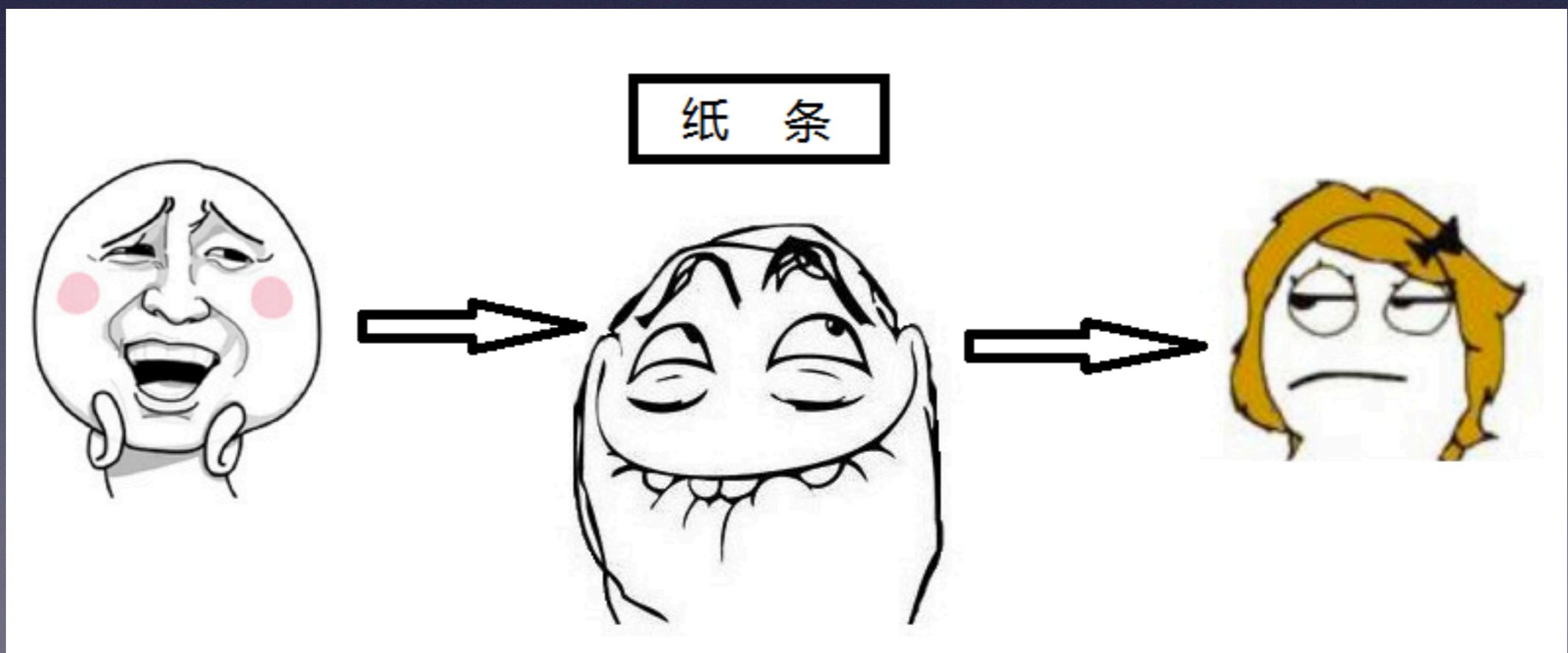
“计算机科学领域的任何问题，
都可以通过添加一个中间层来
解决。”

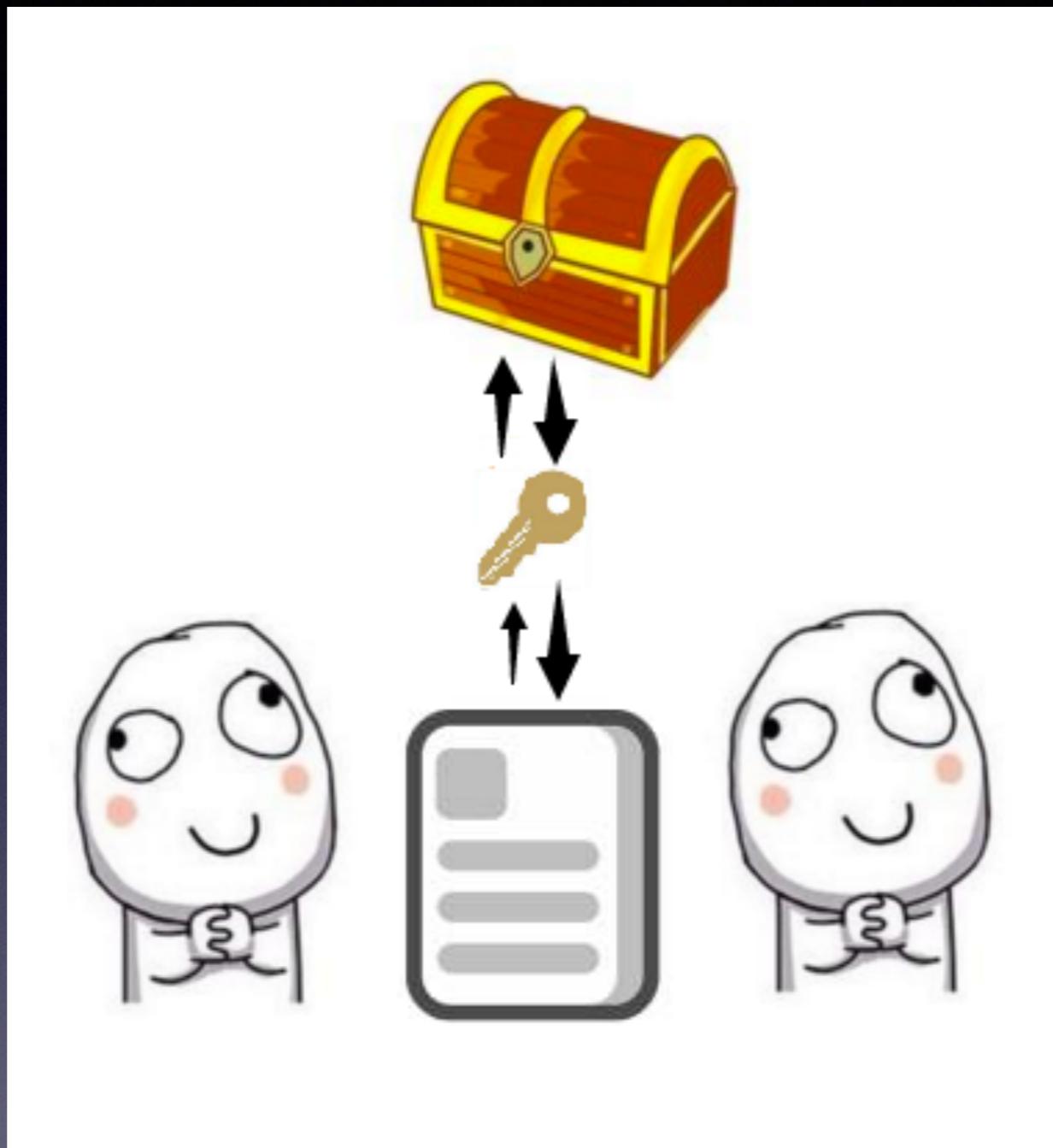
HTTPS 协议的目标



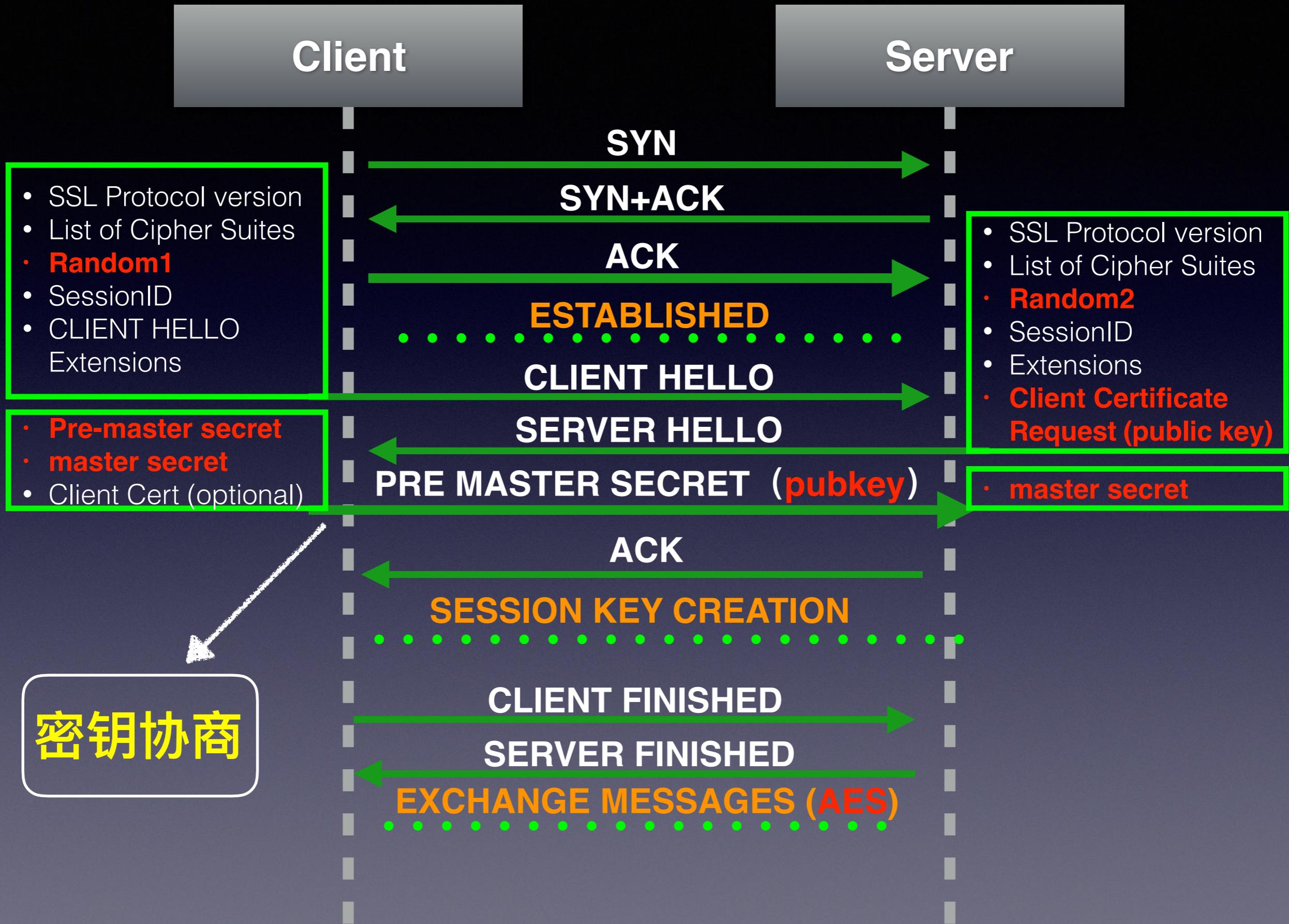
1、內容加密

- 我正在教室上课，非常想和迷人的小丽说话，但小丽离我好远，没办法，只能“传纸条”了。
- 我在纸条上写好内容，希望途径的小明根据指示帮我传给小丽。 (HTTP协议)
- 不要脸的小明居然偷看我的纸条！





- 我先用暗号 (AES key) 加密内容，但怎么把 key传给小丽呢？写在纸条上小明也能看到👀
- 有了！我先用RSA生成一对密钥k1、k2。
- 我把k1写在纸上传出去，小明知道了也没用，因为k1加密只有k2能解密， k2在我手上 😜
- k1给了小丽， 小丽准备一个AES key，用k1加密key，传给我。
- 我用k2解出key， 现在全教室只有我们俩知道key 😊
- 我和小丽聊天不怕窃听啦。

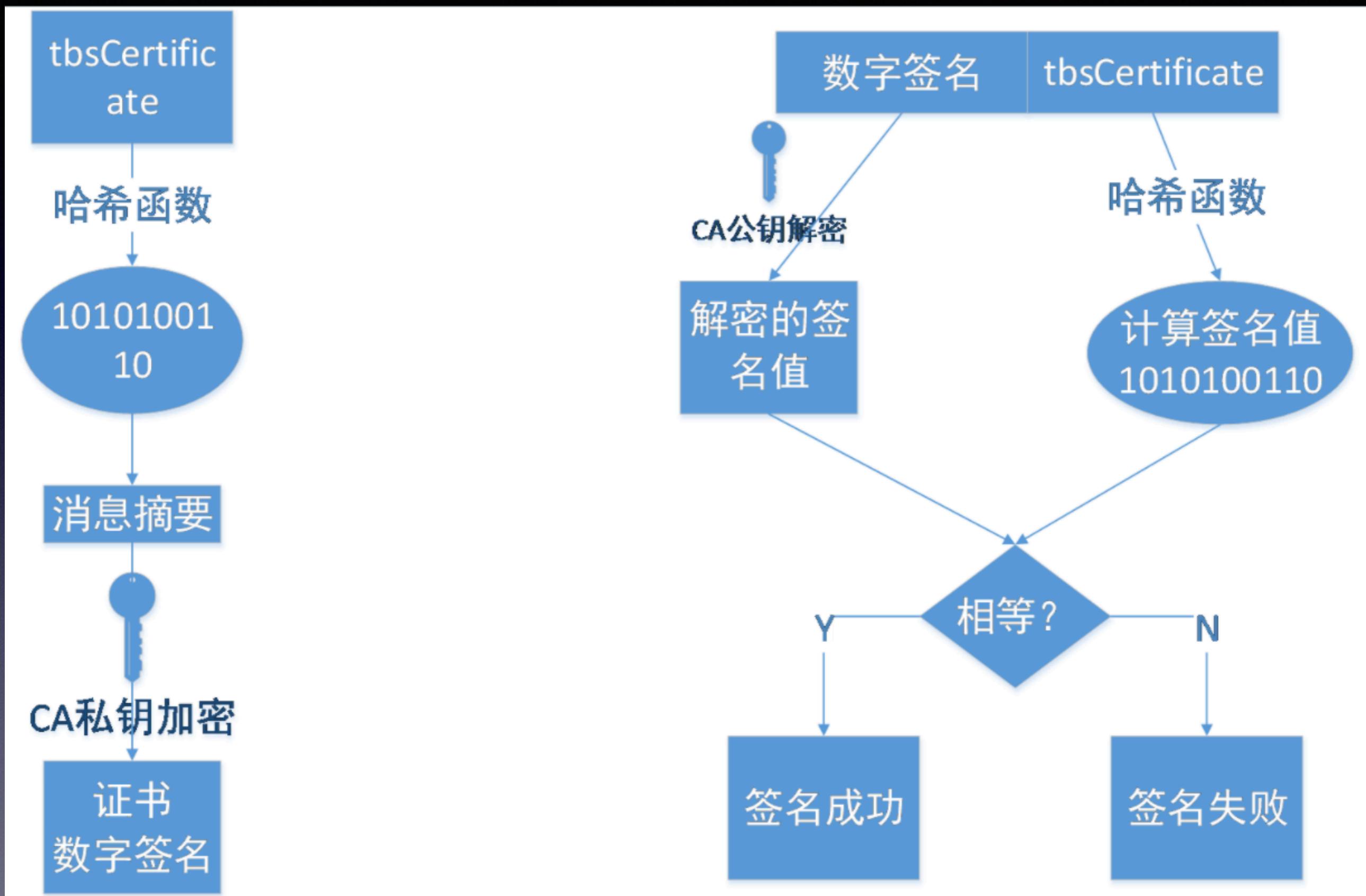


2、身份认证

- 我发现今天小丽的字怎么突然变这么丑了 😕
- 靠@！！搞了半天我是在跟小明聊天 😡😭
- 当我要和小丽进行密钥交换的时候，小明把纸条扣了下来，假装自己是小丽并伪造了一个key，然后用k1加密了key发给我。
- 我以为是和小丽完成了密钥交换，实际上是和小明 😭



- 我的同桌小华是小丽最信任的朋友。要是让小华 (CA) 在上边盖个章 (数字证书)，小丽就知道是我传给她的纸条啦。
- 等等，万一小明自己伪造一个章盖上去咋办？
- 让小华在章后边加一个防伪标签 (数字签名)。先对章进行安全哈希生成消息摘要，然后用小华自己的私钥加密。
- 小丽拿到纸条后，先用小华的公钥解密，得到一个消息摘要1，然后她也对章做一次哈希得到摘要2，比较摘要1==摘要2？



关于数字证书

- 作用：身份授权、分发公钥
- 数字签名签发和校验用的是CA自己的公私钥，跟数字证书中注册者生成的公钥不是一回事
- 数字签名跟后续内容加密的过程相反。
- 从哪获取CA的密钥对？它们是否可信？（OS/浏览器内置）



您的连接不是私密连接

攻击者可能会试图从**kyfw.12306.cn**窃取您的信息（例如：密码、通讯内容或信用卡信息）。 NET::ERR_CERT_AUTHORITY_INVALID

自动向Google报告可能出现的安全事件详情。[隐私权政策](#)

高级

返回安全连接

3、数据完整性

- 小明：“不给我看， 那我就瞎改你们的内容！”
- 虽然我给小丽的纸条内容加了密， 但阻挡不了小明瞎改。
- 我把数据的哈希结果也写到数据中， 小丽解密后对比数据的哈希结果， 不一致说明被篡改了。
- openssl现在使用的完整性校验算法有两种： MD5/SHA。

HTTPS如何避免三大风险

- 1、内容加密：RSA-AES
- 2、身份验证：数字证书、数字签名（RSA-SHA）
- 3、数据完整：MD5/SHA

三、 HTTPS耗性能吗

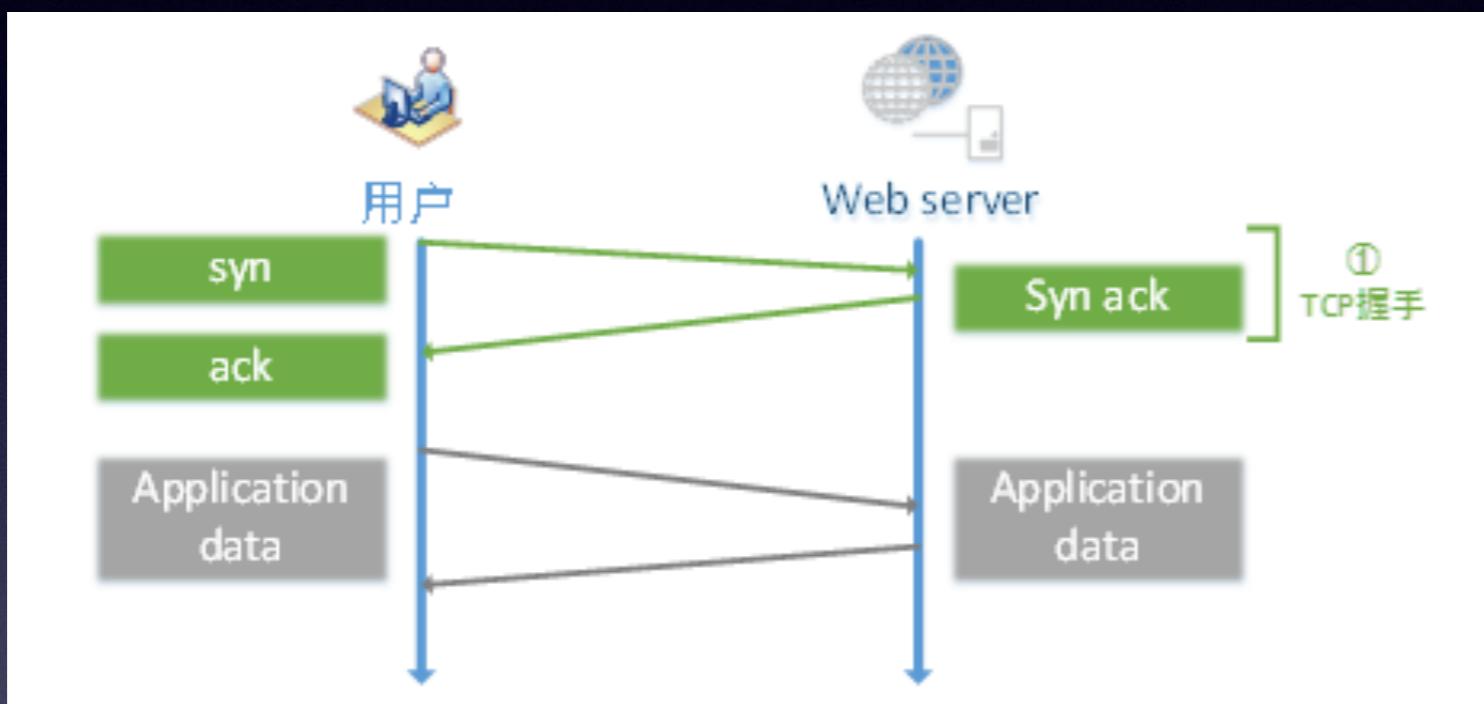
HTTPS 对速度的影响

- 协议交互所增加的网络 RTT。

RTT(Round-Trip Time) —— 往返时延。表示从发送端发送数据开始，到发送端收到来自接收端的确认（接收端收到数据后便立即发送确认），总共经历的时延。

- 加解密相关的计算耗时。

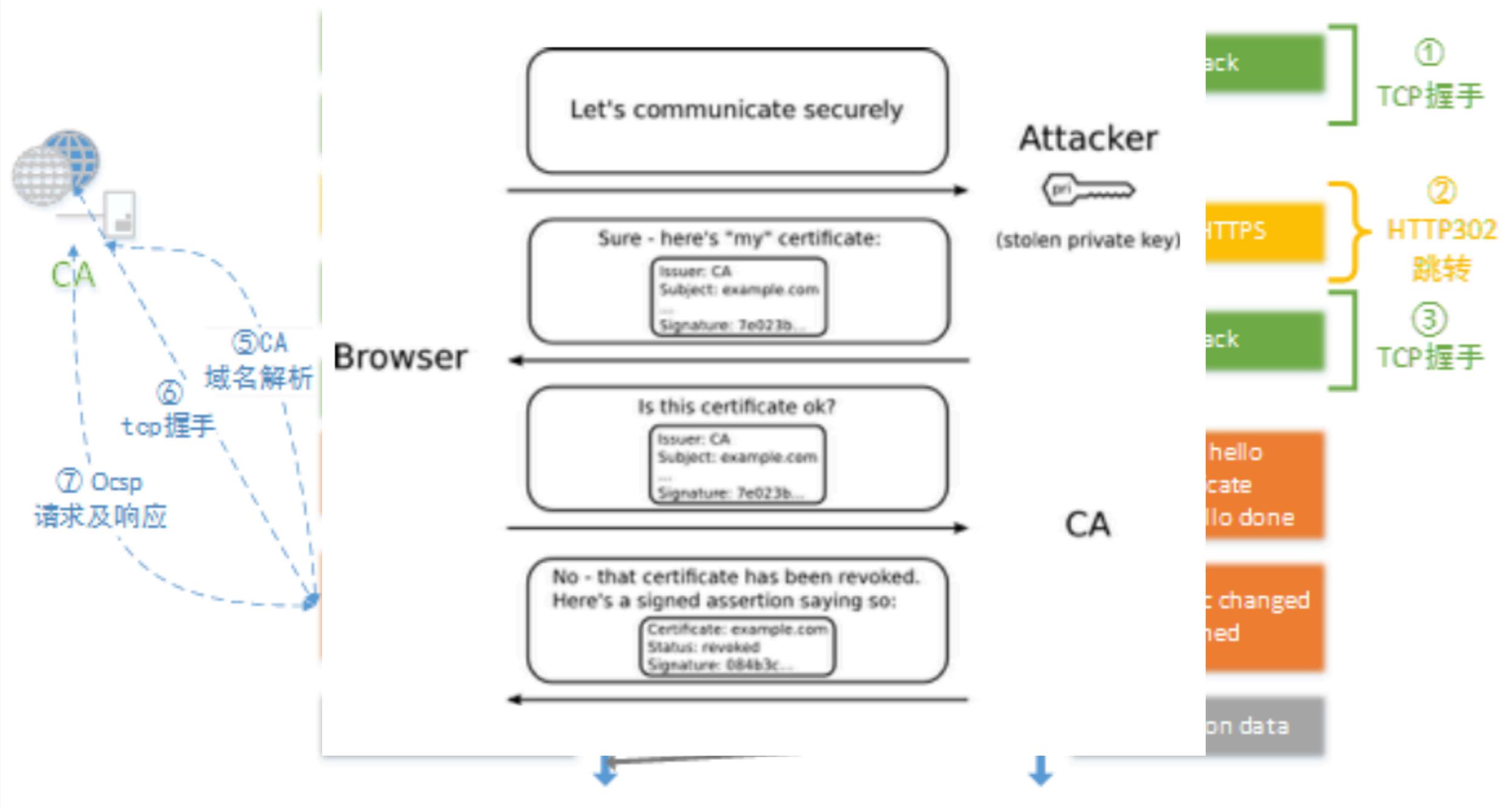
网络耗时



- 只需 1 个RTT
- 访问过程中没有消耗计算资源的地方



OCSP check



只有不到 0.01% 的请求可能经历全部上述步骤

计算耗时

- 浏览器
 - 证书签名校验 (SHA+RSA)
 - 密钥协商, RSA 公钥加密 pre-master-secret
 - 应用层数据 AES 加解密
 - 应用层数据一致性校验

计算耗时

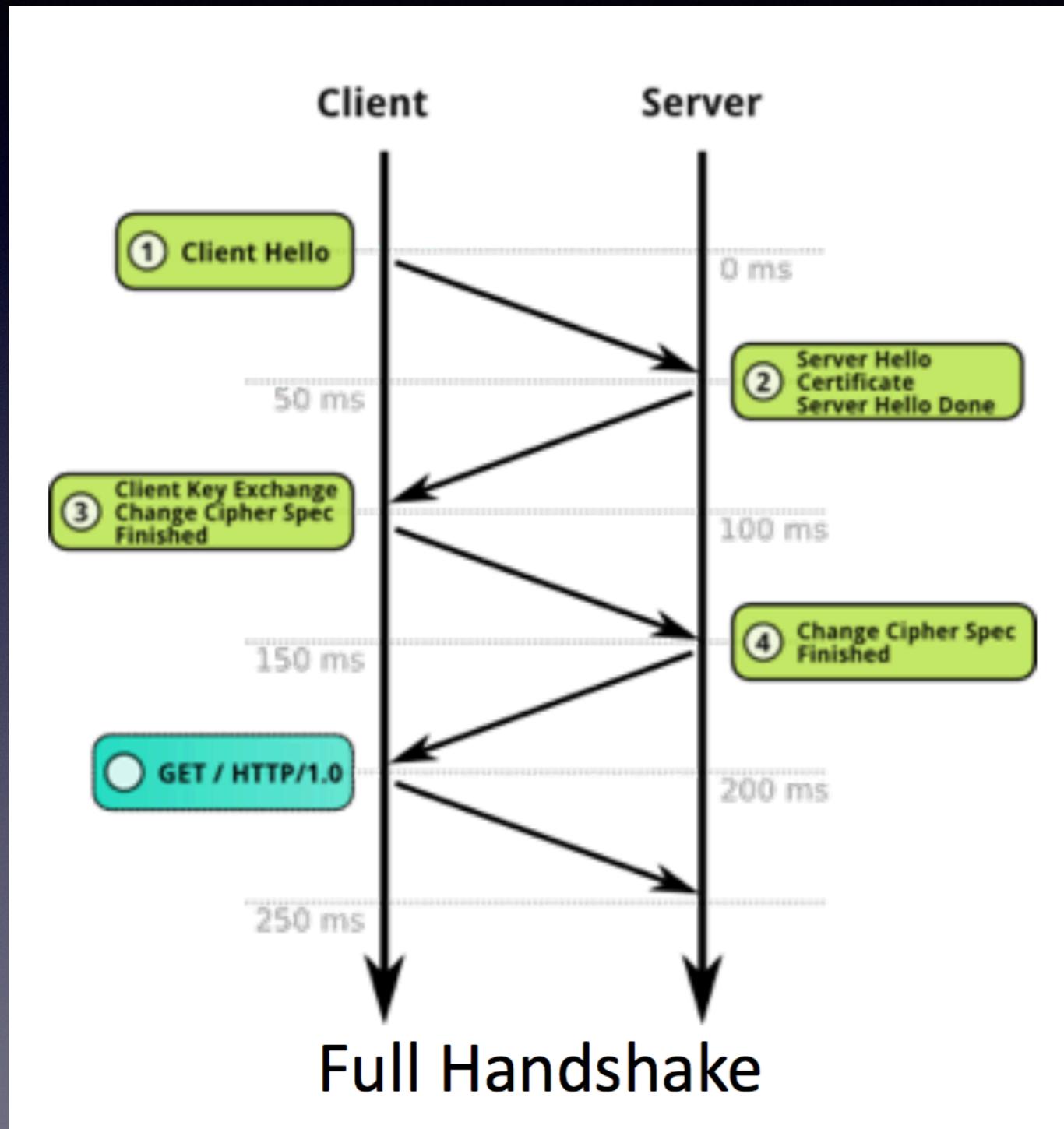
- 服务端
 - 密钥协商， RSA 私钥解密 pre-master-secret
(很耗性能的一步)
 - 应用层数据 AES 加解密
 - 应用层数据一致性校验

计算耗时

- 客户端
 - 手机端单纯计算增加的延迟至少在 50ms 以上。
 - PC 端也会增加至少 10ms 以上的计算延迟。
- 服务端
 - 计算延迟在 5ms 以上。

四、如何优化 HTTPS

服务器性能



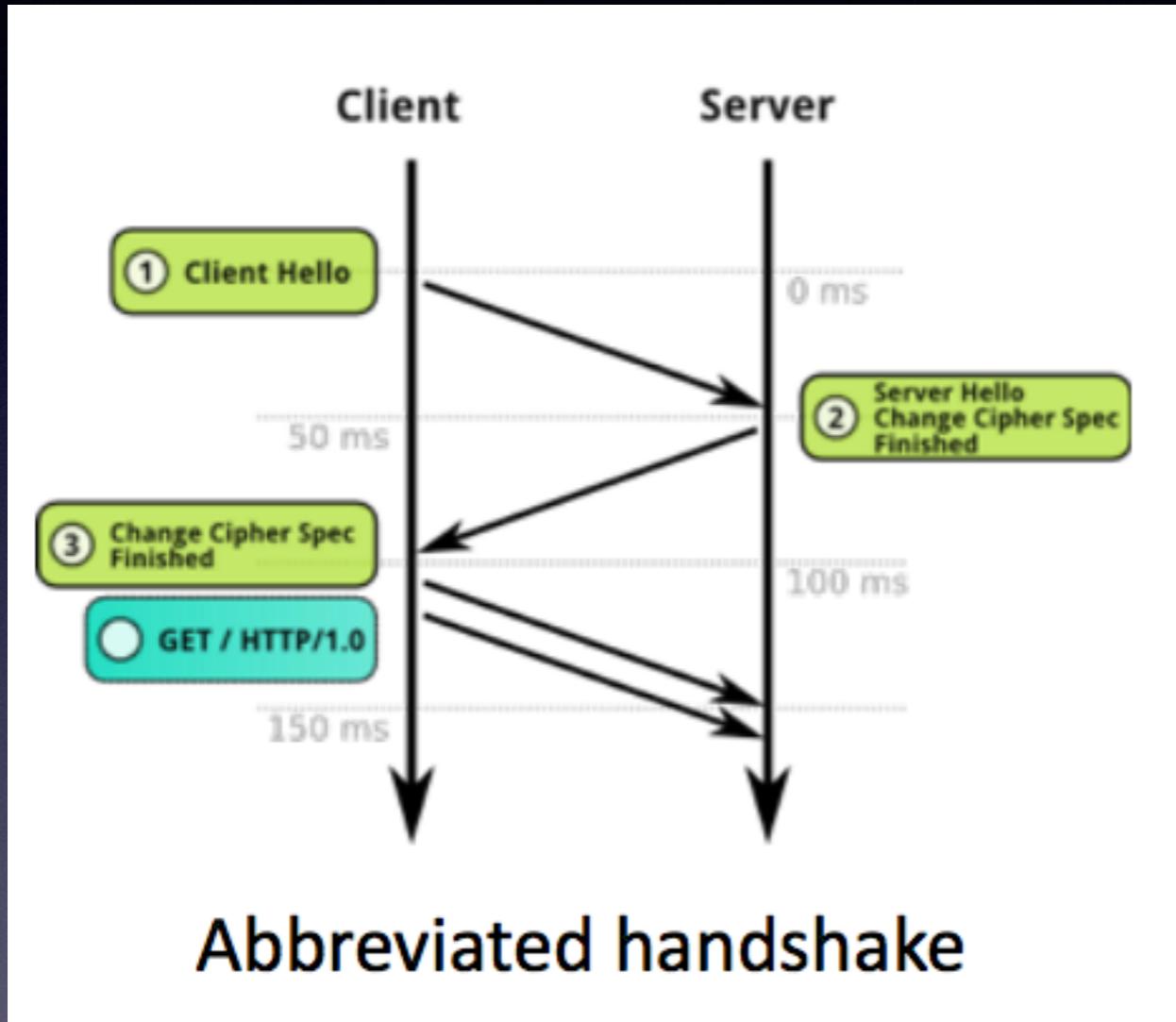
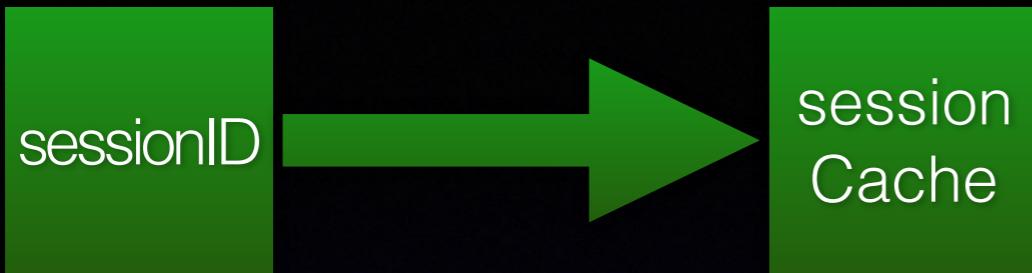
非对称加密

- TLS握手

对称加密

- 数据加解密

尽可能减少TLS握手



Session Cache: 
服务端存储 session、兼容性高

Session Ticket:
客户端存储 session、60% 支持，
支持集群模式



No.	Time	Source	Destination	Protocol	Length	Info
1...	2016-03-14 03:31:35.607699	192.168.3.106	123.59.27.9	TLSv1.2	279	Client Hello
1...	2016-03-14 03:31:35.640282	123.59.27.9	192.168.3.106	TCP	54	443 → 37472 [ACK] Seq=1 Ack=226 Win=15544 Len=0
1...	2016-03-14 03:31:35.641068	123.59.27.9	192.168.3.106	TLSv1.2	1514	Server Hello
1...	2016-03-14 03:31:35.641214	123.59.27.9	192.168.3.106	TCP	1514	[TCP segment of a reassembled PDU]
1...	2016-03-14 03:31:35.641289	123.59.27.9	192.168.3.106	TCP	1230	[TCP segment of a reassembled PDU]
1...	2016-03-14 03:31:35.648646	192.168.3.106	123.59.27.9	TCP	60	37472 → 443 [ACK] Seq=226 Ack=1461 Win=65535 Len=0
1...	2016-03-14 03:31:35.648738	192.168.3.106	123.59.27.9	TCP	60	37472 → 443 [ACK] Seq=226 Ack=2921 Win=65535 Len=0
1...	2016-03-14 03:31:35.648854	192.168.3.106	123.59.27.9	TCP	60	37472 → 443 [ACK] Seq=226 Ack=4097 Win=65535 Len=0
1...	2016-03-14 03:31:35.681571	123.59.27.9	192.168.3.106	TLSv1.2	1225	Certificate
1...	2016-03-14 03:31:35.693119	192.168.3.106	123.59.27.9	TCP	60	37472 → 443 [ACK] Seq=226 Ack=5268 Win=65535 Len=0
1...	2016-03-14 03:31:35.703813	192.168.3.106	123.59.27.9	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted ...
1...	2016-03-14 03:31:35.742988	123.59.27.9	192.168.3.106	TLSv1.2	296	New Session Ticket, Change Cipher Spec, Encrypted H...
1...	2016-03-14 03:31:35.750410	192.168.3.106	123.59.27.9	TLSv1.2	672	Application Data
1...	2016-03-14 03:31:35.822885	123.59.27.9	192.168.3.106	TCP	54	443 → 37472 [ACK] Seq=5510 Ack=970 Win=16686 Len=0
1...	2016-03-14 03:31:35.995086	123.59.27.9	192.168.3.106	TLSv1.2	1108	Application Data

▶ Transmission Control Protocol, Src Port: 443 (443), Dst Port: 37472 (37472), Seq: 5268, Ack: 352, Len: 242

◀ Secure Sockets Layer

◀ TLSv1.2 Record Layer: Handshake Protocol: New Session Ticket

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 186

◀ Handshake Protocol: New Session Ticket

Handshake Type: New Session Ticket (4)

Length: 182

◀ TLS Session Ticket

Session Ticket Lifetime Hint: 300

Session Ticket Length: 176

Session Ticket: 7cc22fe1f32d09e01743238837971d940a30199f2d29f60d...

▶ TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec

▶ TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message

客戶端性能

- HTTP/2 Enabled: true
- SPDY/3.1 Enabled: null
- Use Alternative Service: null
- ALPN Protocols: h2,http/1.1
- NPN Protocols: null



HTTP/2 sessions

[View live HTTP/2 sessions](#)

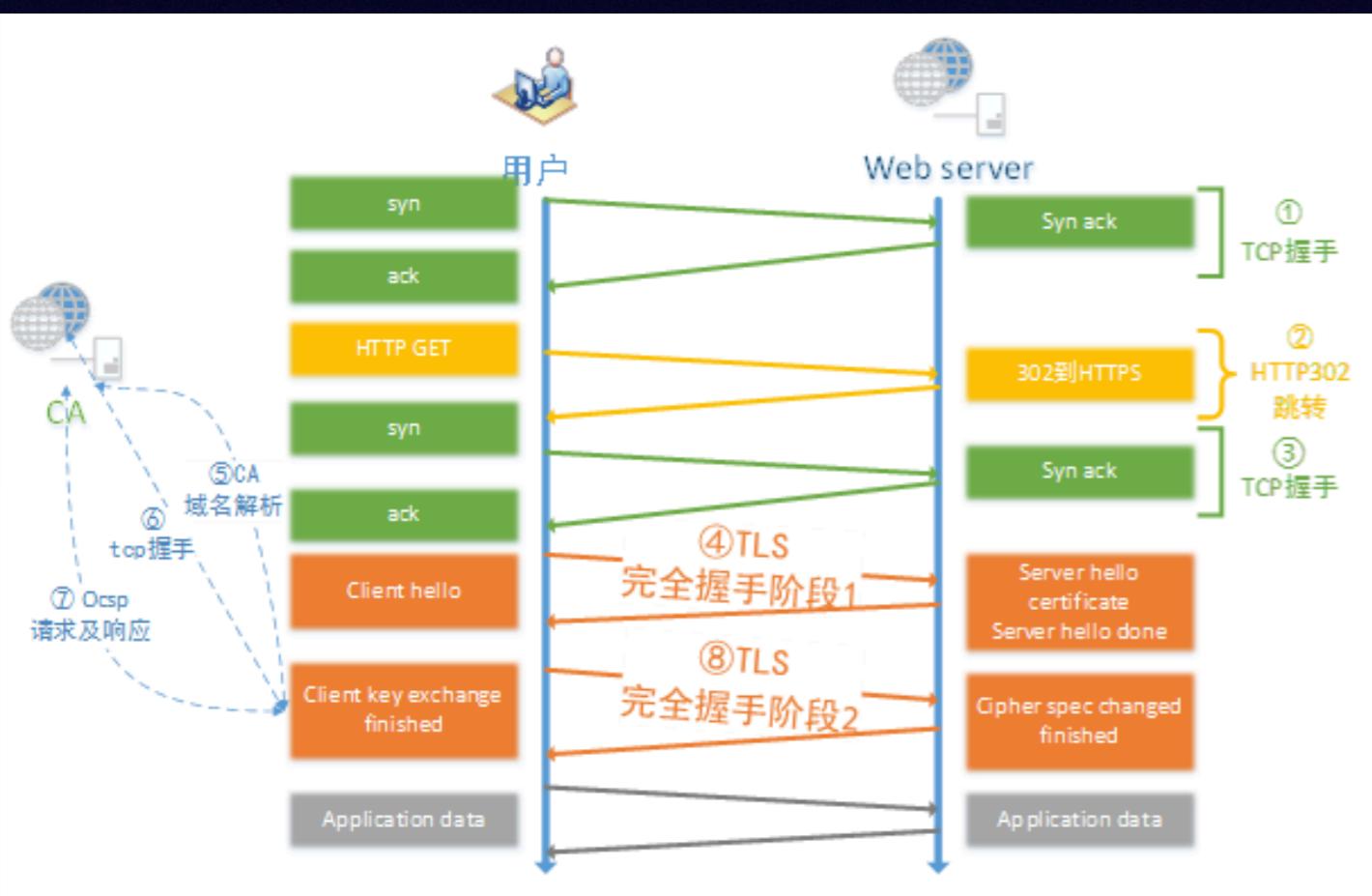
Host	Proxy	ID	Negotiated Protocol	Active streams	Unclaimed pushed	Max	Initiated	Pushed	Pushed and claimed	Abandoned	Received frames
ald.taobao.com:443	dev-proxy.oa.com:8080	291958	h2	0	0	128	1	0	0	0	3
ecpm.tanx.com:443	dev-proxy.oa.com:8080	292137	h2	0	0	128	8	0	0	0	16
g.alicdn.com:443	dev-proxy.oa.com:8080	292318	h2	0	0	128	1	0	0	0	3
gm.mmstat.com:443	dev-proxy.oa.com:8080	292148	h2	0	0	128	14	0	0	0	28
gw.alicdn.com:443	dev-proxy.oa.com:8080	292282	h2	0	0	128	10	0	0	0	31
img.alicdn.com:443	dev-proxy.oa.com:8080	292158	h2	0	0	128	35	0	0	0	153
suggest.taobao.com:443	dev-proxy.oa.com:8080	292335	h2	0	0	128	1	0	0	0	2
tce.alicdn.com:443	dev-proxy.oa.com:8080	292138	h2	0	0	128	2	0	0	0	6

客户端性能

- OCSP Stapling
 - OCSP Check 需要 500ms
 - IE/Firefox默认会进行OCSP Check



客户端性能



- TCP Fast Open: syn+application data
- HSTS(HTTP Strict Transport Security): 避免302
- False start: 完全握手第二个阶段+应用数据

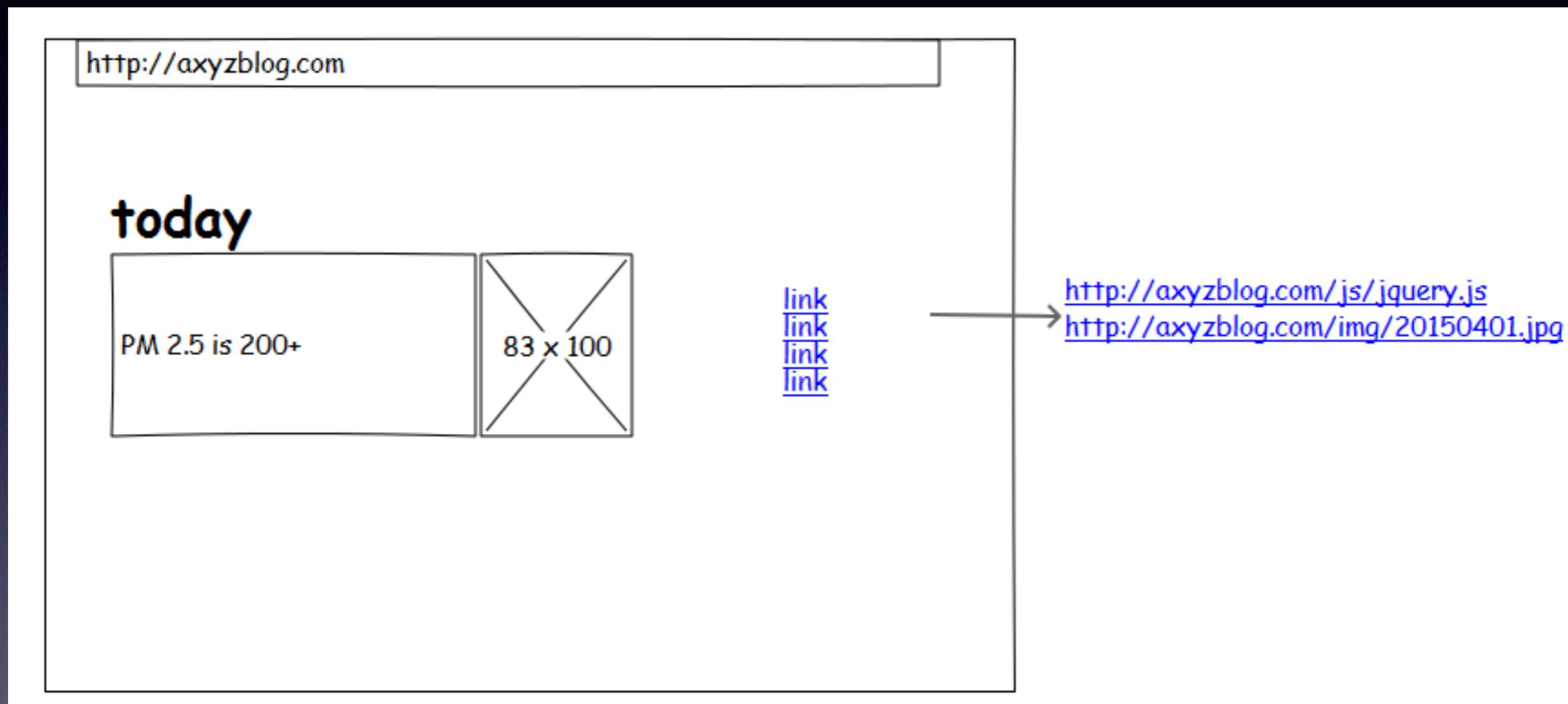
五、HTTP加个S很难吗

为什么强调全站？

- 主域名上https远远不够，主域名加载的js/css/image资源没上的话，https是没意义的。
- 浏览器的限制可能会导致网站基本功能无法使用。

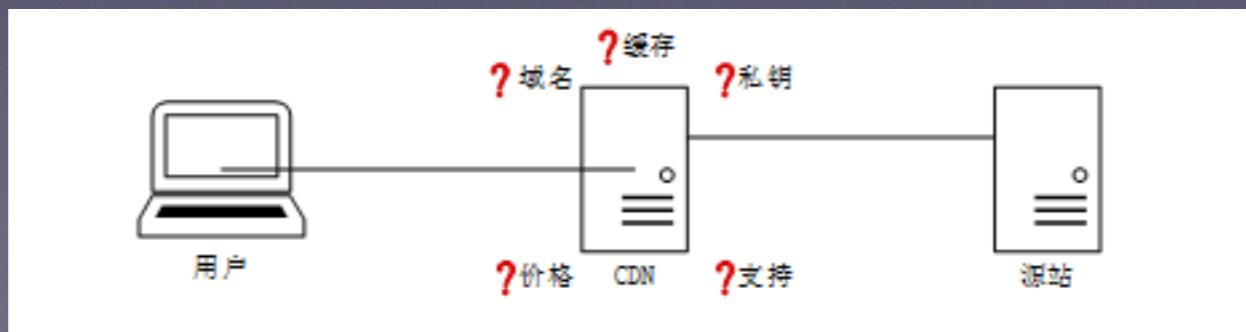
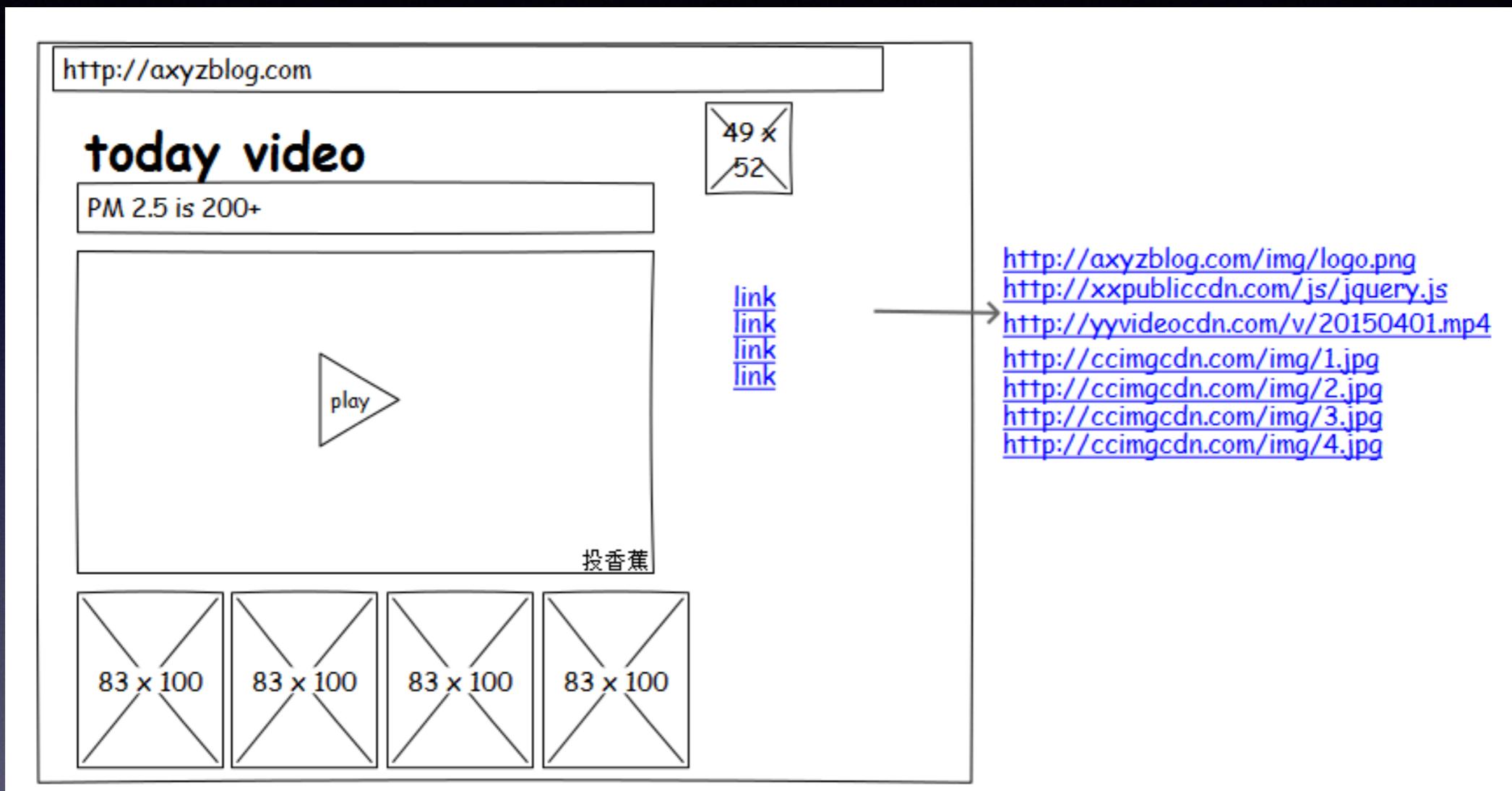


简单的个人站点



http —————> https

复杂的个人站点



简单的大型站点

- 简单：资源只从本站的主域，主域的子域，或者自建 / 可控的 cdn 域名加载，几乎没有第三方资源。
- 几乎不允许使用多样化的第三方资源。

复杂的大型站点

- 复杂：从本站的非主域，或者第三方站点的域名有大量的第三方资源需要加载，多出现在一些平台类，或者有复杂内容展现的网站。
- 尽可能推动所有相关域名升级为支持 HTTPS。

<http://www.bigaxyzblog.com/img/logo.png>
<http://static.bigaxyzblogcdn.com/js/jquery.js>
<http://v.bigaxyzblogcdn.com/v/20150401.mp4>
<http://image.bigaxyzblog.com/2.png>



<https://www.bigaxyzblog.com/img/logo.png>
<//static.bigaxyzblogcdn.com/js/jquery.js>
<//v.bigaxyzblogcdn.com/v/20150401.mp4>
<//image.bigaxyzblog.com/2.png>

<//www.third1.com/img/1.jpg>
<//www.third2.com/flash/2.swf>
<//static.third3cdn.com/img/2.swf>

- 第三方资源怎么办？

- 超小型个人站点：1天就能申请证书、改造完成。
- 大型站点：
 - Google 部署 https 花费了 1-2 年
 - 将证书从 1024 位升级到 2048 位花了 3 个月
 - 百度花费一年，2015.3 全量上线
 - 阿里历时数月，涉及上百万页面，2015.10 完成