Web生态安全 之 HTTPS应用

张伟伟

2017/04

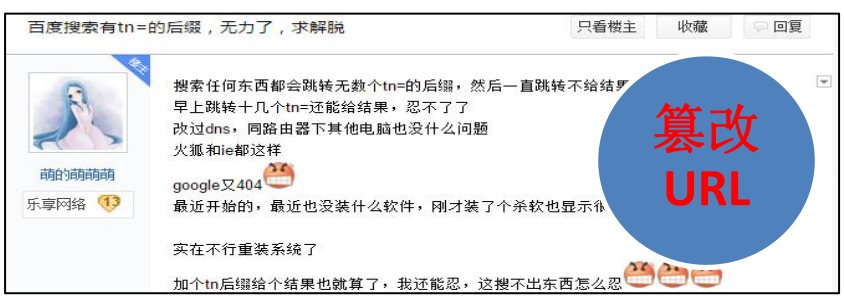
个人介绍

- **百度运维部/BFE（统一前端）**
- 工作经历
  - 2014年7月入职百度，先后参与了百度安全搜索、移动端网络优化等项目
  - 工作经历：SSLVPN、WAF、防火墙/路由器等

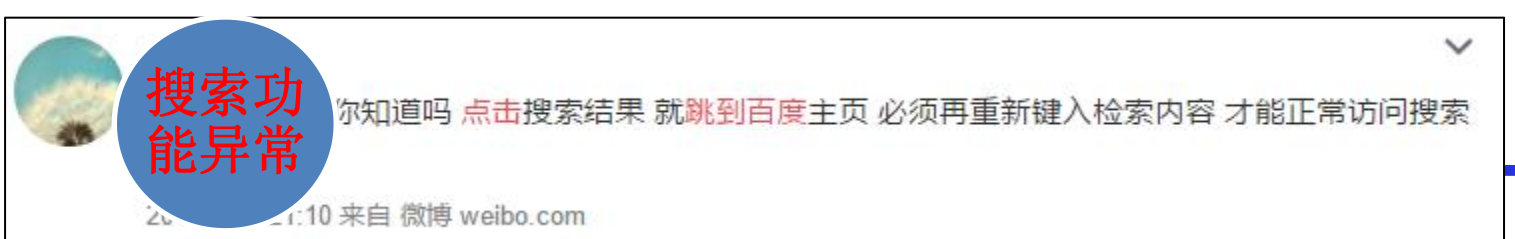
遇到过的问题


左看右转
百度又挂了？搜索任何东西都会跳到一个空白页？
2014-2-22 09:19 来自 微博手机版
收藏
转发
评论 2
卡蒂苟萨-Sorceress
救命……为什么chrome现在不能正常使用百度搜索，一搜就成空白页？！
空白页


问：只在网上百度了一下
来说有免费的彩超加药
流，说是在北京朝阳区的十里河医院，还给了验
女 36岁 分类：其他 浏览23次
2015-03-04 17:52
证码，这事靠谱吗？会是骗局吗？
窃听用户隐私

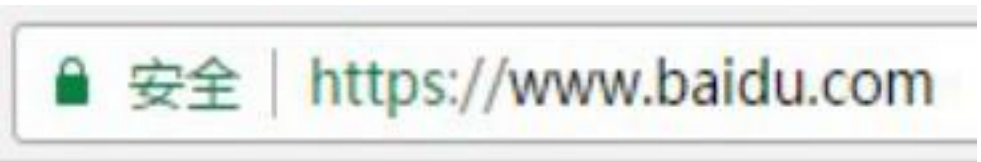

百度搜索有tn=的后缀，无力了，求解脱
只看楼主
收藏
回复
搜索任何东西都会跳转无数个tn=的后缀，然后一直跳转不给结
早上跳转十几个tn=还能给结果，忍不了了
改过dns，同路由器下其他电脑也没什么问题
火狐和ie都这样
google又404
最近开始的，最近也没装什么软件，刚才装了个杀软也显示
实在不行重装系统了
加个tn后缀给个结果也就算了，我还能忍，这搜不出东西怎么忍
萌的萌萌萌
乐享网络
篡改URL

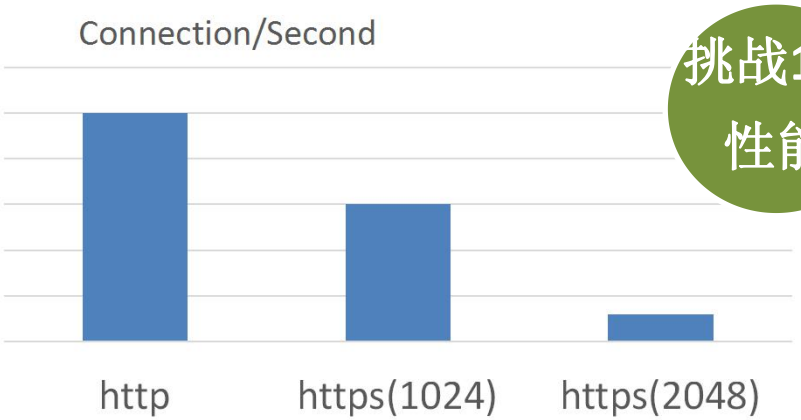

网名很难取诶
贵阳花溪移动运营商有疑似DNS劫持行为！望网民朋友们引起注意！详细现象为每次点击移动版百
度（www为电脑版，m为移动版）会自动转跳到搜狗
一个重定向链接
302重定向


你知道吗 点击搜索结果 就跳到百度主页 必须再重新键入检索内容 才能正常访问搜索
:10 来自 微博 weibo.com
搜索功能异常


百度
网页
地图
贴吧
新闻
更多
百度一下
m.baidu.com 12k
插播广告

解决方案和挑战



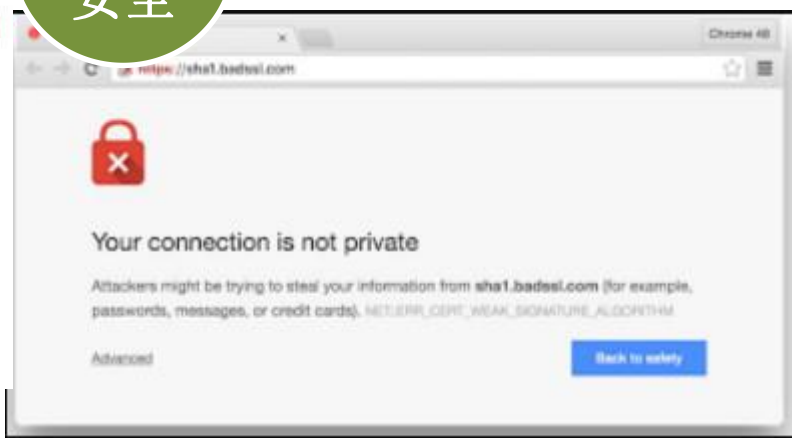


挑战1：性能

HTTP cps 2W+

HTTPS cps 2000-3000

挑战2：安全



挑战3：可用

主要内容 – “四要素”

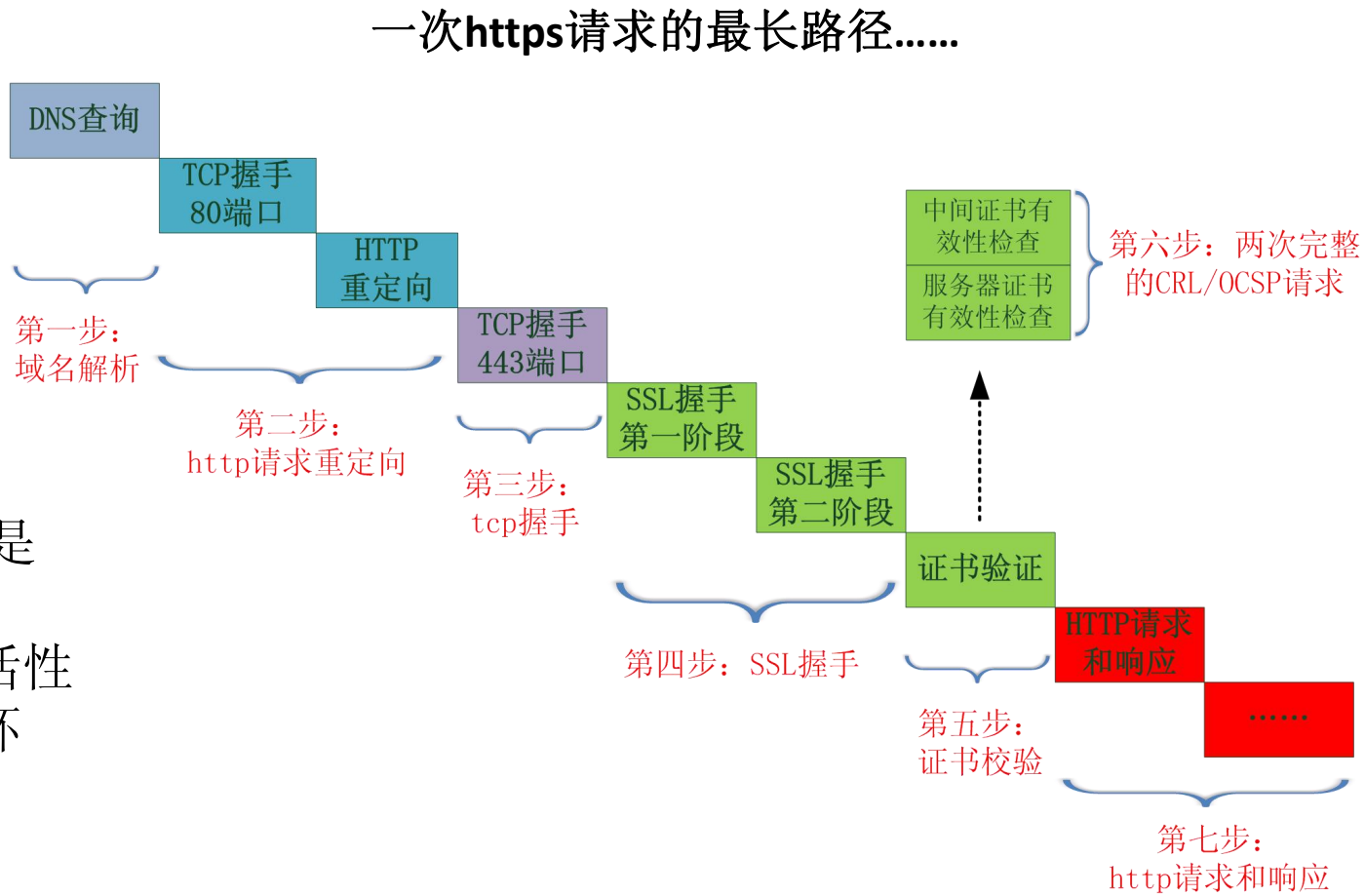
1. 性能优化
2. 连通率和可用性
3. 安全
4. 稳定

HTTPS应用 – “性能优化”

内容摘要：

- HTTPS访问过程
- 常规优化
- 定制优化

HTTPS访问过程



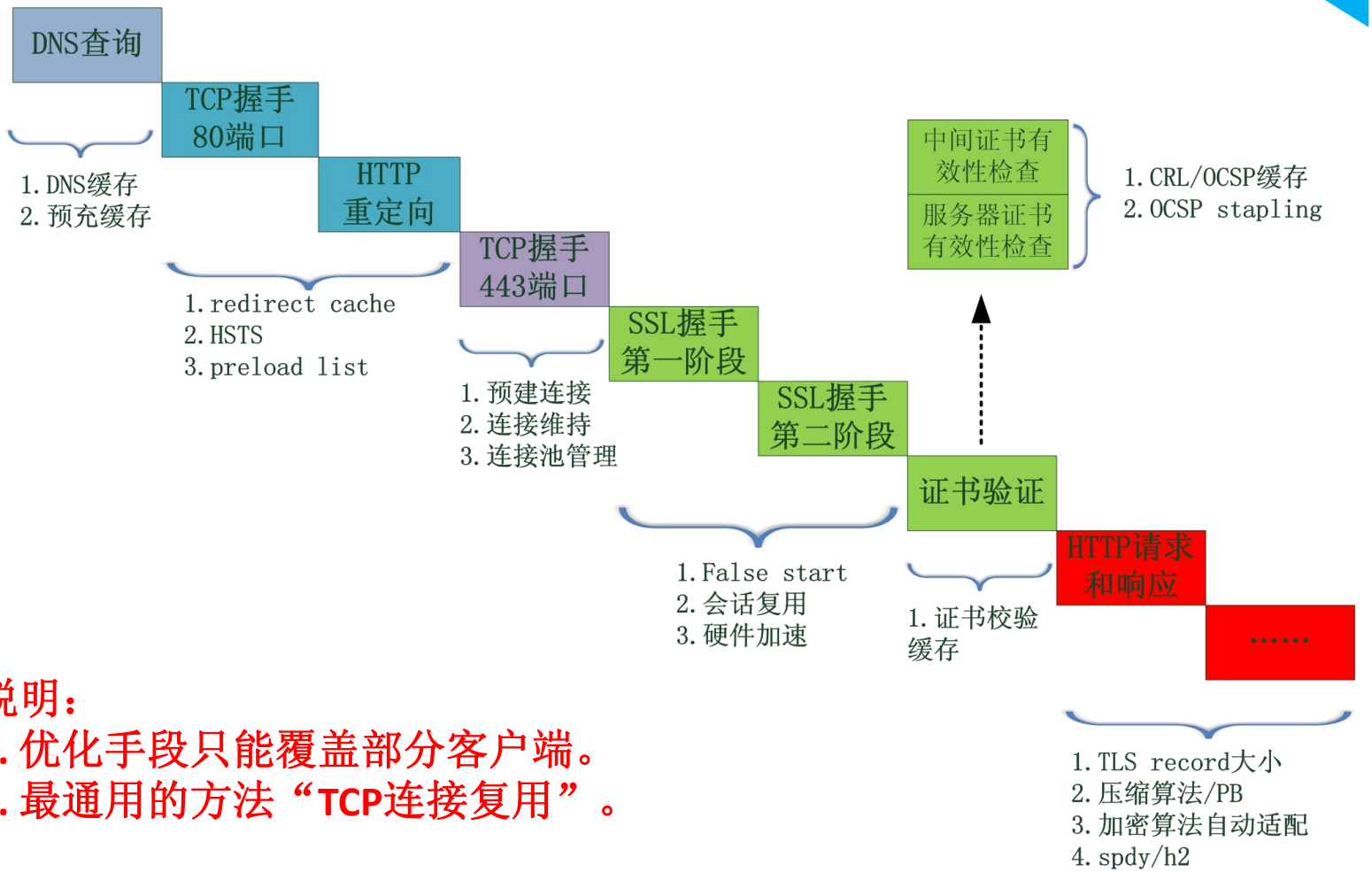
要点说明：

- HTTPS增加的不只是SSL握手
- “证书验证”的灵活性
- 为什么存在重定向环节？

HTTPS常规优化

主要优化点：

- 消除网络延迟
- 减少CPU运算
- 节省流量
- 提前渲染



说明：

1. 优化手段只能覆盖部分客户端。

2. 最通用的方法“TCP连接复用”。

HTTPS定制优化

- DNS解析
  - ✓ HTTPDNS
  - ✓ DNS cache
- SSL握手
  - ✓ 实现100% 1-RTT握手（False Start和会话复用）
  - ✓ 完善SSL session复用策略，提高会话复用率
  - ✓ 基于TLS1.2协议的0-RTT 握手协议
- 证书验证
  - ✓ 时间容错
  - ✓ 证书监控
  - ✓ 证书校验cache
- 数据传输
  - ✓ 加密算法优化（根据CPU适配）
  - ✓ 新的压缩算法

解决了哪些问题：

- VIP的正确性、合理性
- 减少网络延迟
- 节省CPU资源
- 容错
- 发现异常
- 减少CPU运算
- 速度
- 节省流量

HTTPS应用 – “连通率和可用性”

内容摘要：

- **协议版本和加密套件**
  - 兼容性 vs 安全性
- 时间错误
- 劫持
- **证书可用性**

证书可用性 – 证书适配

- **适配方案：** 根据客户端的特征，选择不同的证书提供服务。
- **适配规则：**
  - 系统要求，比如iOS ATS（ECDHE）
  - 协议安全性，比如TLS1.2协议
  - 兼容低版本系统和SDK，比如TLS协议 + SNI扩展
  - 客户端特性，比如TLS1.2协议 + ALPN扩展（spdy、h2等协议）
  - ……

证书可用性 – SHA-1证书“退役”

- 下线SHA-1证书影响范围
  - Mozilla下载量**减少了5%**
  - Cloudflare统计，中国有**6.08%浏览器不支持**
  - Facebook统计，全球有**3-7%浏览器不支持**
  - 百度统计，发现连通率**下降0.2~1%**
- 全面理解问题
  - 不完整的方案：只要客户端在SSL握手的协商算法和扩展签名算法中支持SHA-2算法，服务器返回SHA256签名证书就可以解决这个问题。
  - **补充说明：**客户端不支持SHA-2算法不仅发生在握手协商阶段，还包括浏览器对服务器证书的验证阶段。

https://www.facebook.com/notes/alex-stamos/the-sha-1-sunset/10153782990367929/

证书可用性 – Chrome VS Symantec

- **背景**
  - 16年11月，Chrome 53/54版本存在的bug导致这两个版本的浏览器和webview访问提供Symantec证书的服务时被拒绝。（影响范围涉及百度大部分HTTPS服务）

- **问题追踪**
  - Symantec官方11月14号：Chrome53升级到54版本；或重启浏览器
  - Symantec官方12月07号：升级到Chrome55版本，或者更换浏览器
  - 我们11月16号的分析结果：一是证书颁发机构是Symantec、GeoTrust、Thawte（都是Symantec公司旗下）；二是证书颁发日期晚于2016年6月1日；三是Chrome发版10周以后开始。

- 问题出现时，Chrome没有向服务器返回任何异常数据。
- 百度搜索后端统计，1个月之内可能受影响的访问量大约是2.2%以上（上升过程中,随着时间推移影响更大）。
- 百度统计所示，Chrome浏览器、以Chrome为内核的浏览器份额占据了60%以上。

关于证书的思考

- 如何选择证书？
  - 证书的**成本**能接受的范围？
    - 兼容性、服务质量
  - **服务类型**：金融服务、普通Web服务、APP服务？
    - 不同服务对服务证书的要求不一样
  - 对**速度**有严格要求？
    - 证书链长度、OCSP/CRL服务器节点分布等等
  - 行业**前沿动态**
    - SHA-2签名算法证书
    - 证书透明度（Certificate Transparency）支持
  - 能否承受因为**CA服务事故**带来的流量损失？
    - 2016年，多家CA厂商出现了重大事故，导致有的服务受损。

HTTPS应用实践 – “安全”

内容摘要：

- 私钥保护
- 安全等级
- 证书验证
- 证书伪造

私钥保护

- 私钥安全问题
  - 多个域名共用同一个证书（公钥）/私钥。 影响面大
  - 服务部署在IDC和CDN，或第三方服务平台。 环境复杂
  - 泄漏后，攻击者可以伪造服务端，劫持流量（篡改流量，窥探隐私）。 危害大

- 私钥保护方案
  - openssl genrsa -aes256 / nginx ssl_password_file
  - “私有”加密算法（算法组合、密钥选择、噪声干扰……）
  - 硬件保护

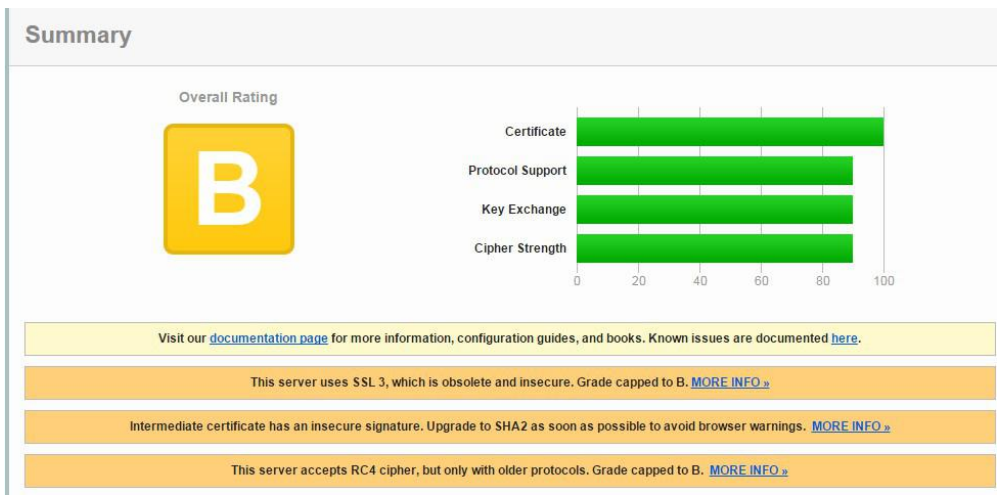
安全等级

- 影响因素
  - 证书
  - 协议版本
  - 加密套件
  - 协议/实现漏洞

两点说明：

- 协议/实现漏洞
  - 建立一套“发现、验证、修复”的应急响应机制
  - 尝试不同TLS协议栈
- 区分服务
  - 不同类型的服务提供不同安全等级

ssllabs： A+, A, B, C, ……



证书验证

- 证书检查被忽略或不充分
  - Google Play Security Alert

- 四个维度：
  - ✓ 域名
  - ✓ 时间
  - ✓ 证书链校验
  - ✓ 有效性检查

如何修复 TrustManager 实施方式不安全的应用

本文面向的是发布的应用中 X509TrustManager 接口实施方式不安全的开发者。具体而言，该问题是指在与远程主机建立 HTTPS 连接时实施方式会忽略所有 SSL 证书验证错误，从而使您的应用容易受到中间人攻击。攻击者可能会读取传输的数据（例如登录凭据），甚至更改通过 HTTPS 连接传输的数据。要查看受影响应用的完整列表，请访问开发者控制台。

为了正确处理 SSL 证书验证，请更改您的自定义 X509TrustManager 接口的 checkServerTrusted 方法中的代码，指定在服务器提供的证书不符合您的预期时生成 CertificateException 或 IllegalArgumentException 错误。如有技术问题，您可以在 Stack Overflow 上发帖咨询（使用"android-security"和"TrustManager"标签）。

请尽快解决此问题并增加升级版 APK 的版本号。从 2016 年 5 月 17 日起，Google Play 将禁止发布 X509TrustManager 接口实施方式不安全的任何新应用或应用更新。

要确认您所做的更改是否正确，请将更新后的应用版本提交至开发者控制台，并在 5 小时后回来查看。如果应用并未正确升级，系统将会显示警告。

尽管这些具体问题可能不会影响每个实施 TrustManager 接口的应用，但您最好不要忽略任何 SSL 证书验证错误。如果应用包含会让用户面临入侵风险的安全漏洞，那么我们可能会将其视为危险产品，因其违反了内容政策和开发者分发协议第 4.4 条的相关规定。

应用还必须遵循开发者分发协议和内容政策。如果您认为我们发送此警告的判断有误，请通过 Google Play 开发者帮助中心与我们的政策支持团队联系。

如何解决 HostnameVerifier 不安全的问题

本文面向的是在应用中采用不安全的 HostnameVerifier 接口实施方式的开发者。在与使用 setDefaultHostnameVerifier API 的远程主机建立 HTTPS 连接时，这种实施方式会接受所有主机名，从而使您的应用容易受到中间人攻击。攻击者可能会读取传输的数据（例如登录凭据），甚至更改通过 HTTPS 连接传输的数据。

从 2017 年 3 月 1 日起，只要新应用或应用更新采用的 HostnameVerifier 的实施方式不安全，一律禁止在 Google Play 发布。**您已发布的 APK 版本不会受到影响，但是，如果不解决此漏洞，您将无法为应用发布任何更新。**

需要执行的操作

为了正确处理主机名验证，请更改您的自定义 HostnameVerifier 接口中的验证方法，指定在服务器的主机名不符合您的预期时返回 False。

证书伪造

- 前提
  - DNS劫持/链路劫持
  - 客户端劫持
- 危害
  - 伪造服务端
  - 劫持流量（篡改流量/窥探隐私）

监控异常

- HPKP(HTTP Public Key Pins)
- 证书透明度(Certificate Transparency)
- 法律手段

不足？

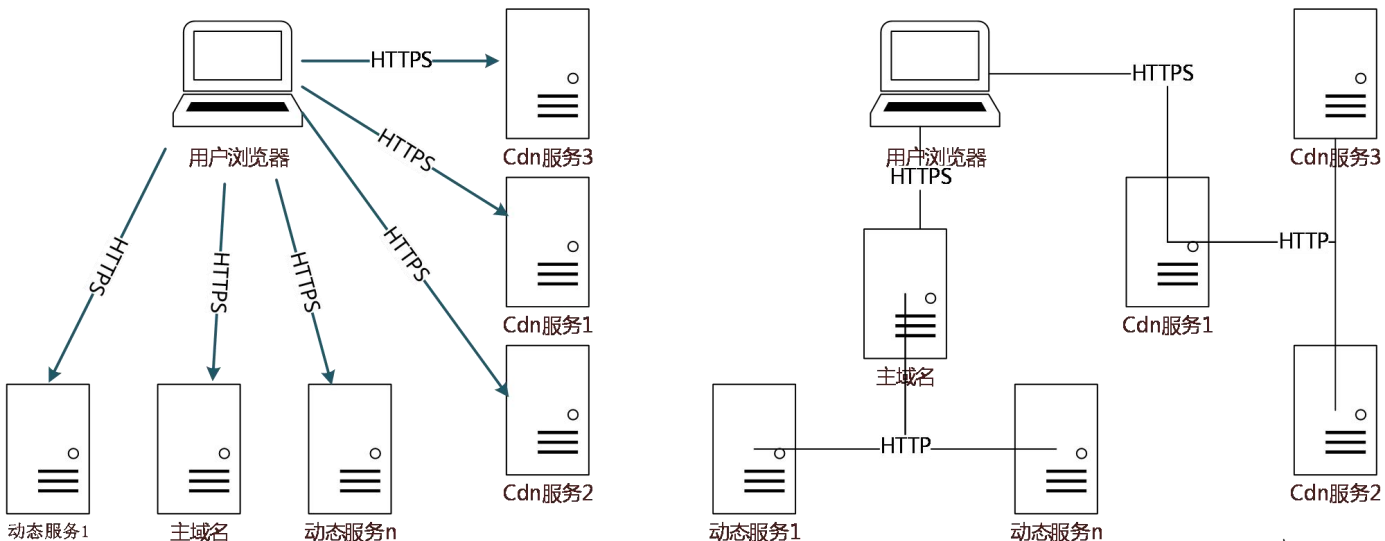
public-key-pins-report-only: pin-sha256="K87oWBWM9UZfyddvDfoxL+8lpNyoUB2ptGtn0fv6G2Q=";pin-sha256="IQBnNBEiFuhj+8x6X8XLgh01V9Ic5/V3IRQLNFFc7v4=";pin-sha256="9n0izTnSRF+W4W4JTq51avSXkWhQ88duS2bxVLfzXsY=";pin-sha256="JbQbUG5JMJUoI6brnx0x3vZF6jilxsapbXGVfjhN8Fg=";max-age=300;report-uri="https://reports.baidu.com/pkp-report/"

HTTPS应用实践 – “稳定”

Check点：

- **开发**
  - 自动纠错（容错意识）
  - 自动降级（自我保护意识）
- **上线变更**
  - 分级发布
  - 回滚/预案
- **监控和报表**
- **防攻击**
  - 容量保证
  - 异常流量监测
- **协议降级？**

其他 – 网站架构规划

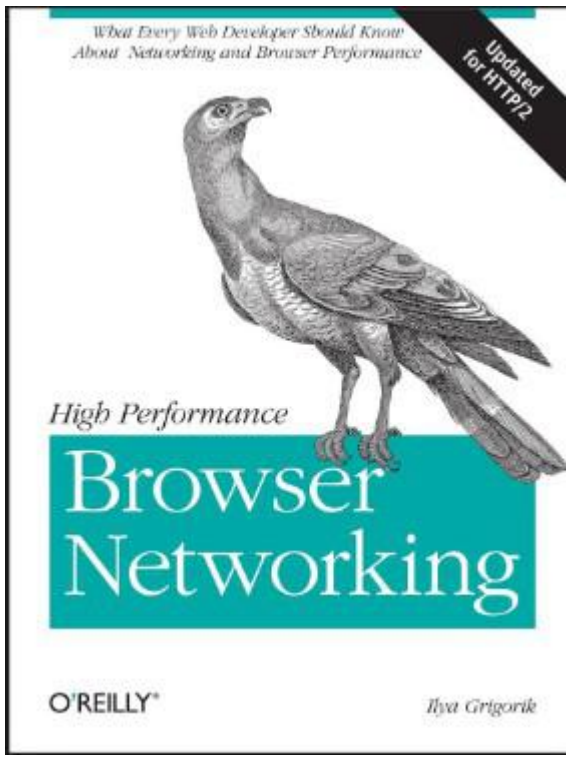

HTTPS
HTTPS
HTTPS
HTTPS
HTTPS
用户浏览器
Cdn服务3
Cdn服务1
Cdn服务2
动态服务1
主域名
动态服务n
用户浏览器
HTTPS
HTTPS
HTTP
Cdn服务3
Cdn服务1
主域名
HTTP
Cdn服务2
动态服务1
动态服务n

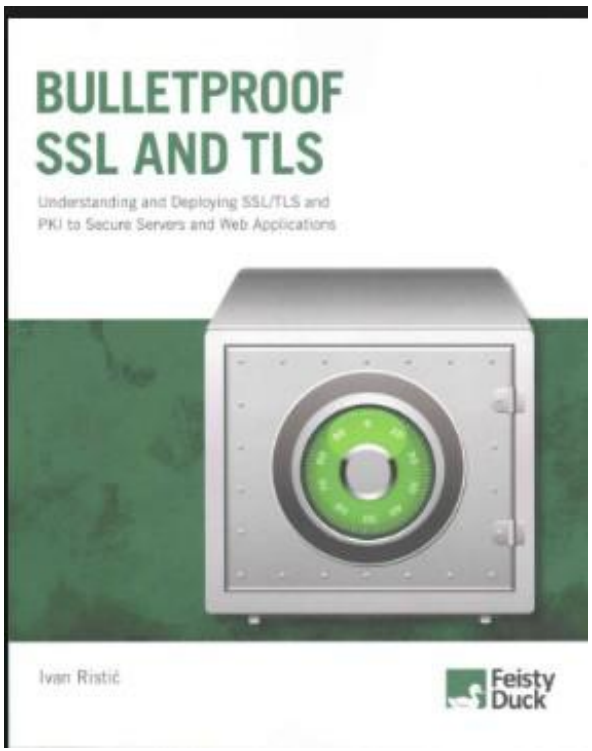
其他 – 改造建议

- 域名收敛
- 统一接入/公共服务
- 第三方资源
  - 访问质量
  - 证书弹窗

参考资料

http://op.baidu.com/





THANKS