**关注”千锋互联”微信公众号( ID: qianfengjiaoyu ),更多学习资源(电子书/面试题/简历模板/视频/公开课等等)与你分享**



**HTTPS逐渐取代HTTP**

互联网发展20多年，大家都习惯了在浏览器地址里输入HTTP格式的网址。但前两年，HTTPS逐渐取代HTTP，成为传输协议界的“新宠”。

早在2014年，由网际网路安全研究组织Internet Security Research Group(ISRG)负责营运的 “Let's Encrypt”项目就成立了，意在推动全球网站的全面HTTPS化；今年6月，苹果也要求所有IOS Apps在2016年底全部使用HTTPS；11月，Google还宣布，将在明年1月开始，对任何没有妥善加密的网站，竖起“不安全”的小红旗。

去年，淘宝、天猫也启动了规模巨大的数据“迁徙”，目标就是将百万计的页面从HTTP切换到HTTPS，实现互联网加密、可信访问。

更安全、更可信，是HTTP后面这个“S”最大的意义。HTTPS在HTTP的基础上加入了SSL/TLS协议，依靠SSL证书来验证服务器的身份，并为客户端和服务器端之间建立“SSL加密通道”，确保用户数据在传输过程中处于加密状态，同时防止服务器被钓鱼网站假冒。

**HTTP为什么过时了？**

很多网民可能并不明白，为什么自己的访问行为和隐私数据会被人知道，为什么域名没输错，结果却跑到了一个钓鱼网站上?互联网世界暗流涌动，数据泄露、数据篡改、流量劫持、钓鱼攻击等安全事件频发。

而未来的互联网网络链路日趋复杂，加重了安全事件发生。可能在星巴克被隔壁桌坐着的黑客嗅探走了口令，或者被黑了家庭路由器任由电子邮件被窃听，又或者被互联网服务提供商秘密注入了广告。这一切都是由互联网开始之初面向自由互联开放的HTTP传输协议导致的。

**HTTP数据在网络中裸奔**

HTTP明文协议的缺陷，是导致数据泄露、数据篡改、流量劫持、钓鱼攻击等安全问题的重要原因。HTTP协议无法加密数据，所有通信数据都在网络中明文“裸奔”。通过网络的嗅探设备及一些技术手段，就可还原HTTP报文内容。

**网页篡改及劫持无处不在**

篡改网页推送广告可以谋取商业利益，而窃取用户信息可用于精准推广甚至电信欺诈，以流量劫持、数据贩卖为生的灰色产业链成熟完善。即使是技术强悍的知名互联网企业，在每天数十亿次的数据请求中，都不可避免地会有小部分流量遭到劫持或篡改，更不要提其它的小微网站了。

**智能手机普及，WIFI接入常态化**

WIFI热点的普及和移动网络的加入，放大了数据被劫持、篡改的风险。开篇所说的星巴克事件、家庭路由器事件就是一个很有意思的例子。

**自由的网络无法验证网站身份**

HTTP协议无法验证通信方身份，任何人都可以伪造虚假服务器欺骗用户，实现“钓鱼欺诈”，用户根本无法察觉。

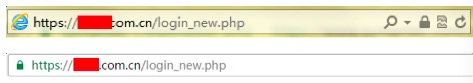
**HTTPS，强在哪里？**

我们可以通过HTTPS化极大的降低上述安全风险。



从上图看，加密从客户端出来就已经是密文数据了，那么你的用户在任何网络链路上接入，即使被监听，黑客截获的数据都是密文数据，无法在现有条件下还原出原始数据信息。

各类证书部署后浏览器呈现效果：



免费SSL数字证书（IE上，Chrome下）



OV SSL数字证书（IE上，Chrome下）

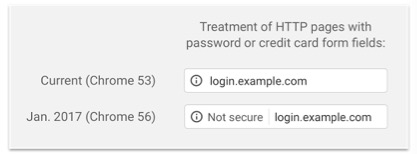


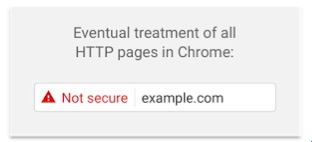
EV SSL数字证书（IE上，Chrome下）

**全世界都对HTTPS抛出了橄榄枝**

**浏览器们对HTTP页面亮出红牌**

谷歌、火狐等主流浏览器将对HTTP页面提出警告。火狐浏览器将对“使用非HTTPS提交密码”的页面进行警告，给出一个红色的阻止图标；Google Chrome浏览器则计划将所有HTTP网站用“Not secure”显注标识。





图片来源：Googleblog

对于一般用户来讲，如果是这样标识的网站，可能会直接放弃访问。

**苹果iOS强制开启ATS标准**

苹果宣布2017年1月1日起，所有提交到App Store 的App必须强制开启ATS安全标准(App Transport Security)，所有连接必须使用HTTPS加密。包括Android也提出了对HTTPS的要求。

**HTTP/2协议只支持HTTPS**

Chrome、火狐、Safari、Opera、IE和Edge都要求使用HTTPS加密连接，才能使用HTTP/2协议。

**HTTPS提升搜索排名**

谷歌早在2014年就宣布，将把HTTPS作为影响搜索排名的重要因素，并优先索引HTTPS网页。百度也公告表明，开放收录HTTPS站点，同一个域名的http版和https版为一个站点，优先收录https版。

**英美强制要求所有政府网站启用HTTPS**

美国政府要求所有政府网站都必须在2016年12月31日之前完成全站HTTPS化，截至2016年7月15日，已经有50%政府网站实现全站HTTPS。英国政府要求所有政府网站于2016年10月1日起强制启用全站HTTPS，还计划将service.gov.uk提交至浏览器厂商的HSTS预加载列表，只有通过HTTPS才能访问政府服务网站。

**超级权限应用禁止使用HTTP连接**

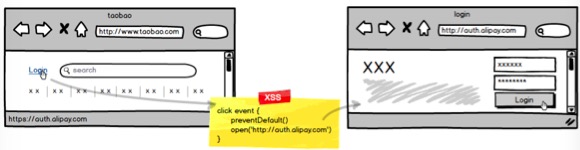
采用不安全连接访问浏览器特定功能，将被谷歌Chrome浏览器禁止访问，例如地理位置应用、应用程序缓存、获取用户媒体等。从谷歌Chrome 50版本开始，地理定位API没有使用HTTPS的web应用，将无法正常使用。

**只有部分网页可不够，全站HTTPS才是最佳方案**

很多网站所有者认为，只有登录页面和交易页面才需要HTTPS保护，而事实上，全站HTTPS化才是确保所有用户数据安全可靠加密传输的最佳方案。局部部署HTTPS，在HTTP跳转或重定向到HTTPS的过程中，仍然存在受到劫持的风险。

**情况一：从HTTP页面跳转访问HTTPS页面**

事实上，在 PC 端上网很少有直接进入 HTTPS 网站的。例如：支付宝网站大多是从淘宝跳转过来，如果淘宝使用不安全的 HTTP 协议，通过在淘宝网的页面里注入 XSS，屏蔽跳转到 HTTPS 的页面访问，那么用户也就永远无法进入安全站点了。

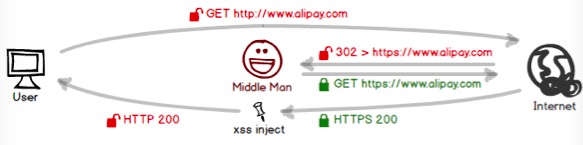


图片来源：EtherDream《安全科普：流量劫持能有多大危害？》

尽管地址栏里没有出现 HTTPS 的字样，但域名看起来也是正确的，大多用户都会认为不是钓鱼网站，因此也就忽视了。也就是说，只要入口页是不安全的，那么之后的页面再安全也无济于事。

**情况二：HTTP页面重定向到HTTPS页面**

有一些用户通过输入网址访问网站，他们输入了 www.alipaly.com 就敲回车进入了。然而，浏览器并不知道这是一个 HTTPS 的站点，于是使用默认的 HTTP 去访问。不过这个 HTTP 版的支付宝的确也存在，其唯一功能就是重定向到自己 HTTPS 站点上。劫持流量的中间人一旦发现有重定向到 HTTPS 站点的，于是拦下重定向的命令，自己去获取重定向后的站点内容，然后再回复给用户。于是，用户始终都是在 HTTP 站点上访问，自然就可以无限劫持了。



图片来源：EtherDream《安全科普：流量劫持能有多大危害？》

而**全站HTTPS化可以确保用户在访问网站时全程HTTPS加密，不给中间人跳转劫持的机会。**国外各大知名网站（PayPal,Twitter,Facebook,Gmail,Hotmail等）都通过Always on SSL（全站https）技术措施来保证用户机密信息和交易安全，防止会话劫持和中间人攻击。



图片来源：Symantec《Protect the Entire Online User Experience: with Always On SSL》

那么问题来了，为什么HTTPS百般好，全世界却还有过一半的网站，还在使用HTTP呢？

首先，**很多人还是会觉得HTTPS实施有门槛**，这个门槛在于需要权威CA颁发的SSL数字证书。从证书的选择、购买到部署，传统的模式下都会比较耗时耗力。目前，主流CSP都集成了多家证书颁发机构的SSL证书，部署过程也相对更容易一些。因“麻烦”和“门槛”而不HTTPS化的现象，预测也将有所缓解。

**第二是性能**。HTTPS普遍认为性能消耗要大于HTTP。但事实并非如此，用户可以通过性能优化、把证书部署在SLB或CDN，来解决此问题。举个实际的例子，“双十一”期间，全站HTTPS的淘宝、天猫依然保证了网站和移动端的访问、浏览、交易等操作的顺畅、平滑。通过测试发现，经过优化后的许多页面性能与HTTP持平甚至还有小幅提升，因此HTTPS经过优化之后其实并不慢。

**最后是安全意识**。相比国内，国外互联网行业的安全意识和技术应用相对成熟，HTTPS部署趋势是由社会、企业、政府共同去推动的。不过，随着国内等保、网络安全、P2P监管措施的普及，HTTPS也有望造福更多网民。

**关注”千锋互联”微信公众号( ID: qianfengjiaoyu ),更多学习资源(电子书/面试题/简历模板/视频/公开课等等)与你分享**

