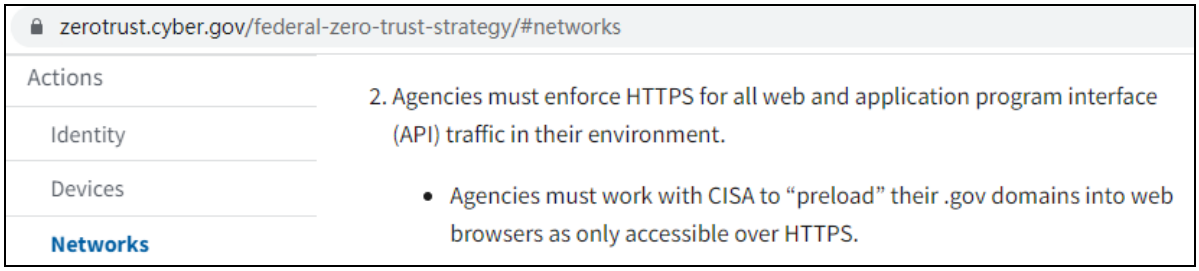
HSTS 就是对 HTTP 的零信任

HSTS 是英文 HTTP Strict Transport Security (http 严格传输安全)的缩写，这是一个征求意见版的 RFC6797 标准，意在制定一个标准，使得浏览器只能使用 https 协议访问某个网站。为此，谷歌还专门设置了一个 HSTS 预加载申请网站，用于用户提交域名以包含在谷歌浏览器的 HSTS 预加载列表中，这是一个硬编码到谷歌浏览器中的 HTTPS 网站列表，大多数浏览器(Chrome，Firefox，Opera，Safari，IE 11 和 Edge)也使用基于谷歌浏览器的 HSTS 预加载列表。

HSTS 是一个为了确保浏览器只使用 https 加密连接网站的安全措施，是对 HTTP 明文传输流量的零信任，得到了许多网站的支持。美国联邦政府管理和预算办公室(OMB)于 2022 年 1 月 26 日正式发布了《联邦政府零信任战略》，以支持第 14028 号美国总统行政命令"改善国家的网络安全"，以使联邦政府机构的网络安全架构适应零信任原则。在“加密 HTTP 流量”部分，要求所有政府机构在所有互联网可访问的 Web 服务和 API 中都使用 HTTPS，而为了确保政府网站都支持 https 加密，从 2020 年开始主流浏览器自动 HSTS 预加载所有新注册的.gov 域名，并已宣布最终将整个美国政府专用.gov 域名全部预置为仅限 HTTPS 访问，这一要求将改善美国各级政府机构的安全性和零信任状况。这个措施也是对各个政府机构是否能自觉地执行 https 加密政策的零信任，因为采取这个措施后，浏览器不会使用 http 协议访问，如果没有部署 SSL 证书实现 https 加密的话，网站就无法访问。



当然，要实现强制 https 加密，用户只需在网站部署 SSL 证书时设置为自动把 http 访问跳转到 https 访问即可，并不需要把网站域名提交给 HSTS 预加载数据库。HSTS 预加载由于是硬编码，不仅预加载列表会很长，而且新增加的网站域名必须在下次更新时才能生效，这是一个非常低效率的解决方案，但仍然是值得学习的解决方案。

笔者在此呼吁：为了保障我国政府网站的安全和保护政务机密信息的安全传输，也应该要求强制采用 https 访问.gov.cn 域名的政府网站，所有.gov.cn 域名的网站不能通过 http 访

问，只能是 https 访问。这项强制措施完成后可以进一步要求只能采用 SM2 加密算法的 https 加密访问。当然，不一定必须采用 HSTS 的笨办法，我们可以有更高效的更简单的方法。

王高华

2022 年 2 月 8 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。