多域 SSL 证书一定会退出历史舞台

多域 SSL 证书就是绑定多个域名的 SSL 证书，现在许多 CA 都已经支持绑定多达 1000 个域名，这的确方便了有许多域名需要部署 SSL 证书的应用，如 CDN 厂商的 https 支持，还有云服务提供商的上千台服务器的 SSL 证书。笔者看到的某某云的官网 SSL 证书部署的 SSL 证书绑定了将近 300 个域名，并且绝大数是通配证书。支持所有子域的通配证书如*.cersign.com 可以用于所有 cersign.com 子域的网站部署同一张 SSL 证书，多域证书中可以含单域证书和通配证书，一张这样的 SSL 证书就可以满足所有网站系统部署 SSL 证书的需要了，这视乎已经成为了大网站的标配和首选。但是，笔者认为：这种部署 SSL 证书的方式不可取，多域 SSL 证书迟早会退出历史舞台，并且应该早点尽快退出。

笔者为何得出这样的结论，这还得从为何出现了多域 SSL 证书说起。大家都知道，Web 服务器是支持一个 IP 地址部署多个网站的，大家都可以共用一个 80 端口来访问，因为 http 协议是带上了主机头信息的，即使是同一个端口访问，但是可以根据域名不一样就可以正确地访问不同的网站。但是，网站部署了 SSL 证书后，所有网站就共用一个 443 端口来实现 https 访问，但是由于 https 协议的 SSL 握手信息中并没有带上主机头信息，这样就不知道该同哪个网站实现 https 加密了，怎么办？这时候，多域 SSL 证书就出现了，把要部署 SSL 证书的网站的所有域名全部含在一张 SSL 证书中，无论哪个域名来访问，都可以用这张 SSL 证书来实现握手加密。

但是，这个解决方案意味着一个 IP 地址仍然只能部署一张 SSL 证书，如果要增加域名，增加 SSL 证书则又不行了，这就出现了新的解决方案—RFC 6066 SNI (Server Name Indication, 服务器名称指示)，让 TLS 协议支持握手时像 http 协议一样带上主机头信息，这就可以不受限制的在一个 IP 地址上启动 N 个 Web 服务和每个 Web 服务都部署一张独立的 SSL 证书，SNI 标准到现在已经 10 年了，所有客户端浏览器和服务器软件都已经支持 SNI 了，除非 10 年前还没有升级过的不安全的系统。

也就是说，由于 SNI 的出现和普及支持，原先产生多域 SSL 证书存在的技术基础已经不存在了，多域 SSL 证书是当时技术局限的产物，现在应该退出历史舞台了，这是我得出这个结论的主要理由之一。

但是，通过各大浏览器对 http 访问显示为不安全的共同努力，现在 https 已经成为了必须，多域 SSL 证书得到了有 N 多服务器需要部署 SSL 证书的云服务提供商和互联网公司的青睐，

(C) 2021 证签技术（深圳）有限公司

一张 SSL 证书绑定几十个域名是常态，绑定几百个域名也不少见。难道存在就合理？还是让笔者给大家算一笔经济账，看看部署多域 SSL 证书是否划算。

名称	大小	类型	修改日期
1. 单域SSL证书.cer	3 KB	安全证书	2021/12/3 07:57
2. 通配单域SSL证书.cer	3 KB	安全证书	2021/12/3 07:56
3. 多域218个域名SSL证书.cer	9 KB	安全证书	2021/12/3 07:56
4. 多域1000个域名SSL证书.cer	39 KB	安全证书	2021/12/3 07:56

一张单域名 SSL 证书包括通配单域 SSL 证书，都是只绑定一个域名的证书，对于常用的 RSA 2048 位 SSL 证书来讲，单域 SSL 证书文件大小在 3K 以内，如上图所示，而一个绑定 218 个域名的 SSL 证书大小为 9K，一个绑定 1000 个域名的 SSL 证书大小为 39K，浏览器访问网站时的 https 握手需要浏览器从服务器下载这张 SSL 证书(公钥)，对于每日访问量高达 1000 万次的大网站，则每次下载绑定 218 个域名的 SSL 证书的流量是比下载绑定一个域名的 SSL 证书流量多出 6K，乘以 1000 万次再乘以 365 天，每年多浪费了 2.11G 流量，按每 G 每年 8 万元计算，则每年因为使用多域 SSL 证书而多支出的带宽费用高达 16.88 万元！而且不仅仅是浪费流量，而且也多耗服务器资源，增加访问延时和影响用户体验。经测试，绑定 5 个域名以内在证书大小上是没有太多变化的。所以，笔者认为不应该部署绑定超过 5 个域名的多域 SSL 证书，以保证用户体验、减少带宽浪费和服务器资源浪费。

我再给大家算一下安全帐，云服务提供商喜欢用绑定通配域名的多域证书无非是可以用这一张 SSL 证书搞定所有网站应用，部署虚拟机时也可以快速复制镜像而实现快速部署。但是，这里面有一个巨大的安全隐患，如果这几百上千台服务器都用这一张 SSL 证书，如果这张 SSL 证书私钥泄露而必须吊销这张证书，则这一千台服务器的 SSL 证书全部需要重新部署新的证书，这个替换工作量就大了，而且还有可能影响服务器的正常运行。笔者就此问题专门写了一篇博文《为何 SSL 证书部署必须“一机一证”》，就是专门讲这个问题的，为了每台物理服务器的安全，必须为每台物理服务器独立使用一张独立私钥的 SSL 证书，这样才不至于其他一台服务器被黑而影响其他服务器的部署的 SSL 证书的正常使用。这个安全运维帐也要算，算下来当然是应该“一机一证”，那么这个“一证”就是只需要一张单域证书或者一张通配证书了。也就是说，从安全运维的角度也不应该使用多域证书。

现在，大家应该能理解我的观点了，从多域 SSL 证书的产生背景来看，技术上已经彻底解决了需要多域证书的问题，多域证书已经没有了存在的技术基础。从节省带宽和提升用户访问速度来看，其实使用多域证书太浪费带宽，也由于文件较大而会影响下载速度而降低用户体验，

(C) 2021 证签技术（深圳）有限公司

为了节省带宽费用和提升用户体验不应该部署多域证书。而从安全运维来看，更不应该把一张多域证书部署在多台服务器上，非常不安全并且大大增加运维人力成本。从这 3 个方面来看，我相信：多域 SSL 证书一定会因为被市场自然淘汰而退出历史舞台。

王高华

2021 年 12 月 9 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。

(C) 2021 证签技术（深圳）有限公司