网站零信任安全三步曲之第一步：HTTPS 加密

零信任是一种安全理念，同样非常适用于网站安全。网站零信任安全的核心之一就是不信任明文传输的 http 网站，所有浏览器都会提示“不安全”，这是对 http 明文传输的零信任。网站安全的基础安全是 https 加密，实现从浏览器(移动 App)到服务器端的信息传输加密，有效保障用户使用浏览器或移动 App 同云端服务器之间的机密信息的传输安全。

笔者发现有不少朋友完全误解了零信任，认为零信任就是身份认证，这可能是传统安全厂商都在专注于身份的零信任的原因。大家看看美国《联邦政府零信任战略》中的行动计划之一就是对明文网络流量的零信任，要求联邦政府机构必须加密所有 DNS 请求、 HTTP 流量和电子邮件流量，要求联邦机构在所有互联网可访问的 Web 服务和 API 中使用 HTTPS 加密。

要实现 HTTPS 加密当然离不开 SSL 证书，或称 TLS/SSL 证书、TLS 证书。但是，如何获取 SSL 证书，SSL 证书采用何种密码算法，如何部署 SSL 证书实现 HTTPS 加密，这里就有许多学问了，本文将详细讲解。

自从 Netscape 在 1994 年发明了 SSL 协议，互联网明文传输协议 HTTP 就变成了加密传输 HTTPS，用户必须向 CA 申请 SSL 证书，拿到 SSL 证书后必须在 Web 服务器上安装使用，当然 Web 服务器必须支持签发这张 SSL 证书的密码算法，浏览器也必须信任此 CA 签发的 SSL 证书，这样就形成了一个 HTTPS 加密的应用生态。目前已经成熟的生态仅支持 RSA 算法和 ECC 算法的 SSL 证书，我国的商用密码算法 SM2 SSL 证书应用生态还没有形成。

而自从 1994 年有了 SSL 证书实现 HTTPS 加密后，直到 2015 年 10 月出现 Let’s Encrypt 推出的 ACME 自动化部署证书协议，这 21 年来人们都是人工申请 SSL 证书和人工部署 SSL 证书，费时费力和费钱，而 Let’s Encrypt 的出现改变了这一切，主要有 3 个方面的改变：其一，实现了自动化部署 SSL 证书。用户只需在 Web 服务器上安装一个 ACME 客户端软件即可，甚至现在有些 Web 服务器已经直接集成了 ACME 客户端，用户只需配置 ACME 服务端网址即可。其二，实现了完全免费。这就为普及 HTTPS 加密打下了大规模普及实施的基础，但免费则一定是由机器自动化签发证书，也就只能做到仅验证网站域名，所以只能是低端 DV SSL 证书。这就带来的第三个改变：SSL 证书已经从证明网站身份和传输加密双功能降级为传输加密单功能，使得如何证明网站身份成为了一个新的问题，这个问题将在网站零信安全三步曲之第三步详细探讨解决方案。

无论是用户手动安装 SSL 证书，还是采用 ACME 方式自动部署 SSL 证书，都要求用户有

物理服务器，最少必须有云服务器，对于大量的虚拟主机用户来讲，安装 SSL 证书目前还是一个比较困难的事情。可喜的是，目前已经有虚拟主机服务提供商开始为用户提供 SSL 证书部署支持，这得益于 SNI 技术的广泛支持，当然也有来自浏览器提示“不安全”的压力推动。

部署 SSL 证书实现 HTTPS 加密除了传统的在服务器上安装 SSL 证书外，还可以把从 CA 申请到的 SSL 证书手动配置到 CDN 和云 WAF 上使用，一些做得比较好 CDN/WAF 服务提供商，如 Cloudflare，则直接自动配置好 SSL 证书，这是第二种自动化部署 SSL 证书实现 HTTPS 加密的解决方案，这个解决方案也将在网站零信安全三步曲之第二步详细探讨。

上面讲的是 SSL 证书如何申请和如何部署的问题，下面讲讲签发 SSL 证书的算法，目前的国际标准只允许使用 RSA 和 ECC 算法，操作系统、浏览器和 Web 服务器也只支持这两种算法签发的 SSL 证书。这是摆在我国希望推广国密 SM2 SSL 证书的现实，我国必须建立一个从操作系统，至少从浏览器(包括移动 App)和 Web 服务器都支持国密算法(SM2/SM3/SM4)的生态体系，当然还必须包括 CDN 和云 WAF 服务的国密算法和国密 SSL 证书的支持，只有这样才能无缝实现国密 HTTPS 加密。想必读者现在应该不难理解为何零信技术的第一个产品是支持国密算法和国密 SSL 证书的浏览器了，因为浏览器是互联网的入口，是国密证书应用生态系统的关键核心部件。

针对网站零信任安全三步曲之第一步的 HTTPS 加密，零信技术的口号是不为用户提供 SSL 证书，因为这不是用户所需要的，用户需要的是 HTTPS 加密，所以我们直接提供 HTTPS 加密服务，用户只需按要求做一次 CNAME 解析就可以自动完成域名验证，零信云 SSL 服务自动为用户签发所需的 SSL 证书并自动配置到云 WAF 上使用，只需再做一次 CNAME 域名解析即可启用云 WAF+HTTPS 加密服务。这是目前为止用户最省心的 HTTPS 加密解决方案，用户无需向 CA 申请 SSL 证书，无需在服务器上安装 ACME 客户端软件，只需做两次 CNAME 解析即可全自动实现 HTTPS 加密，与用户是否有物理服务器，是否是虚拟主机无关，只要是能访问的网站即可。这就是零信网站安全云服务，基于阿里云 WAF 服务和自研云 SSL 服务打造，完美快速全自动实现 HTTPS 加密，默认采用速度更快的 ECC 算法实现，用户可选启用国密 SM2 算法实现 HTTPS 加密，零信浏览器将优先采用 SM2 算法实现 HTTPS 加密。

网站实现了 HTTPS 加密，则所有浏览器都不再显示“不安全”，而且显示加密锁标识。零信浏览器创新地集成了网站安全体检评级服务，此服务的评分标准把 HTTPS 加密占比 60%，因为 HTTPS 加密是网站安全的基础安全保障，是网站安全三步曲的第一步。这一步的 SSL 安全体检评级会从 SSL 证书、协议支持、密钥交换和加密套件强度等 4 个维度来检测打分，分别占比 60%、12%、12%和 16%。通过这 4 个维度的检测就可以全面了解 HTTPS 加密的安全状况，确保 SSL 证书的正确部署和使用，可靠地实现 HTTPS 加密。

而为了打造国密证书应用生态，零信浏览器不仅支持国密算法和国密 SSL 证书，而且是优先采用国密算法实现 HTTPS 加密。而为了让用户感知网站已经部署了国密 SSL 证书，零信浏览器创新地在地址栏增加了一个国密加密标识“m”，让访问访问者对这个网站是否采用了国密加密保护一目了然，并且明确提示此网站是国密合规的。优先采用国密算法的完全免费的零信浏览器为打造国密证书应用生态的重要一环-HTTPS 加密的普及提供了坚实的网站安全商用密码保护应用基础。

总之，为了网站安全，必须对明文网络流量零信任，特别是政府网站和政务网站都必须强制 HTTPS 加密，并且必须是优先采用国密算法实现 HTTPS 加密。零信技术网站安全解决方案不仅让用户全自动实现了 HTTPS 加密，实现了网站零信任安全三步曲的第一步，而且让用户可以使用零信浏览器实时了解这一步的实际实施结果，以简单明了的方式对比了解使用零信网

站安全云服务之前后的网站安全状态的提升情况，让用户对自己的网站安全状况放心，以便可以专注于做好自己的业务。

王高华

2022 年 6 月 20 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。