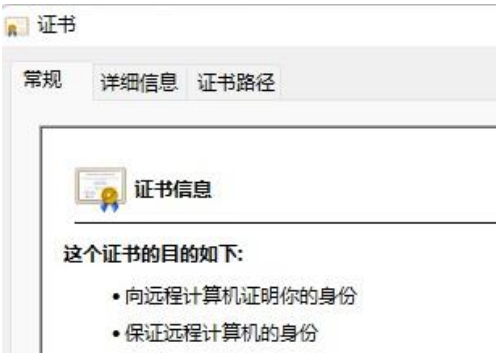
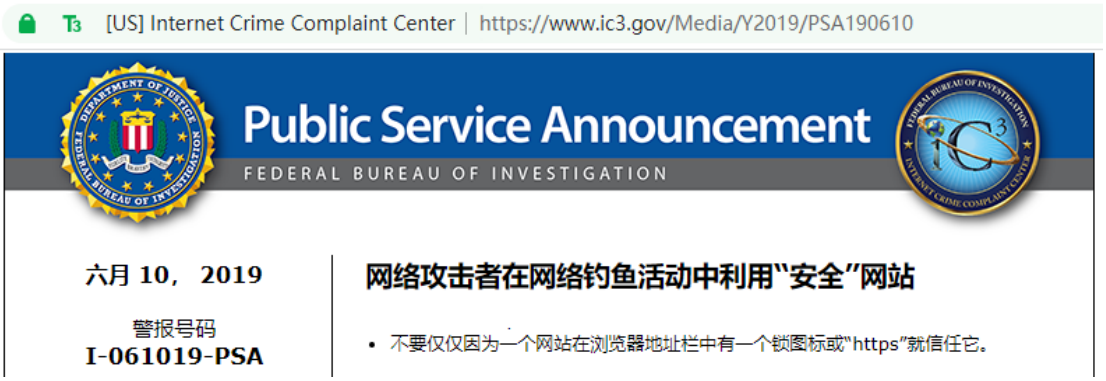
网站零信任安全三步曲之第三步：可信认证

零信任是一种安全理念，同样非常适用于网站安全。所有浏览器都 HTTP 网站显示为“不安全”，这就是对未通过可信身份认证的网站的零信任。也许有读者会说，浏览器对 HTTP 网站显示为“不安全”是因为这个网站没有部署 SSL 证书实现 HTTPS 加密，这个理由是正确的。但是，我们再想一想 SSL 证书是什么，它就是 CA 在完成了对网站的身份认证后签发 SSL 证书来证明网站的可信身份的，这张证书同时可以用于传输加密交换加密密钥用。所以，归根结底，这就是所有浏览器对没有通过认证的网站的零信任，会显示为“不安全”。大家可以点击加密锁标识查看 SSL 证书的用途就能验证我的观点，如下图所示，SSL 证书的目的是“向远程计算机证明你的身份，保证远程计算机的身份”，是用于证明网站的可信身份的，加密只是一个副功能，其主要功能是服务器身份认证。

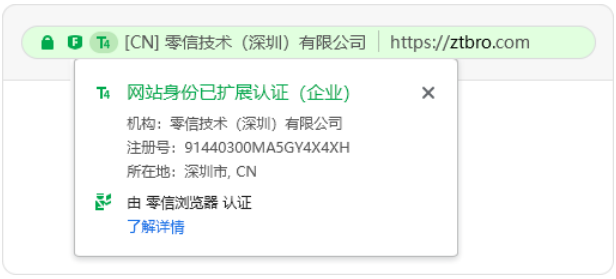


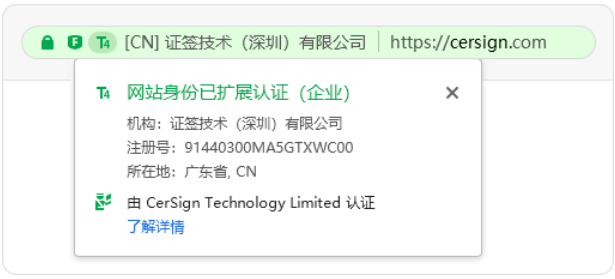
笔者在博文《网站零信任安全三步曲第一步：HTTPS 加密》中详细讲解了如何实现网站零信任安全三步曲的第一步的 HTTPS 加密，这是网站安全的基础。但是，网站仅有 HTTPS 加密还是不够的，还需要云 WAF 防护，这就是第二篇博文《网站零信任安全三步曲第二步：云 WAF 防护》所讲的内容。网站有了 HTTPS 加密和云 WAF 防护，仍然是不够的，还需要网站身份的可信认证。如果实现 HTTPS 加密的 SSL 证书是已经验证网站身份的 OV SSL 证书或者 EV SSL 证书，则就完美地完成了网站安全的三个保障要求：HTTPS 加密、云 WAF 防护和可信认证。

可惜的是，目前全球已部署 SSL 证书的网站中有 83%的网站部署的是未验证网站可信身份的 DV SSL 证书，这使得假冒欺诈网站也可以有 HTTPS 和云 WAF 防护，但相信大家都不会认为这个假冒欺诈网站是安全的。美国联邦调查局互联网犯罪投诉中心向消费者发出警告-不要信任一个网站仅仅是因为浏览器地址栏显示 https 加密锁标识，如下图所示(中文为机器自动翻译)。这是对网站身份的零信任和对 HTTPS 加密的零信任。

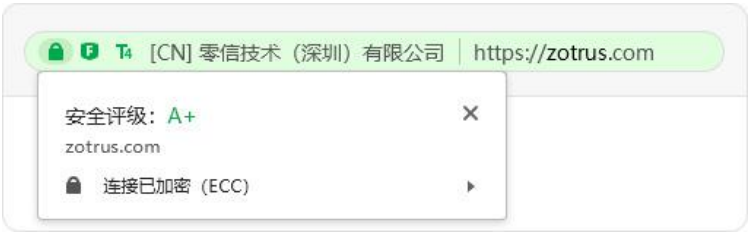


所以，网站零信任安全还需要有独立的网站身份认证服务来弥补 DV SSL 证书的网站可信身份认证缺失这个安全短板，网站身份可信认证是网站安全的第三个重要要素，同 HTTPS 加密和云 WAF 防护一样重要！零信技术的解决方案就是零信网站可信认证服务，部署了 DV SSL 证书的网站主可以申请网站可信认证服务，由零信浏览器来自动获取网站可信身份数据并在地址栏直接展示，如下左图所示。而对于已经部署了已验证身份的 IV SSL、OV SSL 和 EV SSL 的网站，零信浏览器则直接读取 SSL 证书中的 O 字段信息来展示网站可信身份，如下右图所示。点击可信认证标识，不仅会展示详细的网站身份信息，而且会展示此网站的身份由谁认证。





零信浏览器的地址栏展示网站可信身份，让网站访问者对网站的真实可信身份一目了然，能有效增强网站访问者的在线信任。对于网站是否通过可信认证，在零信浏览器创新集成的网站安全体检评级中占比 20%，有了可信认证能有效提升网站安全评级级别。



总之，为了网站安全，必须对没有通过认证的网站身份零信任，所以浏览器都会显示“不安全”。零信浏览器始终验证网站可信身份，并全球独家率先恢复对部署了最严格的网站身份认证的 EV SSL 证书和 EV 认证的网站展示绿色地址栏和单位名称，率先创新地对部署了 OV SSL 证书和 OV 认证的网站展示浅绿色地址栏和单位名称，对部署了 IV SSL 证书和 IV 认证的

网站展示浅绿色地址栏和个人姓名，完美实现了网站零信任安全三步曲的第三步。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或申请了网站可信认证之前后的网站安全状态的提升情况(安全评级级别会上升)，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 24 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。