密码讲堂第 7 讲 ｜ 浏览器是如何验证 SSL 证书的？

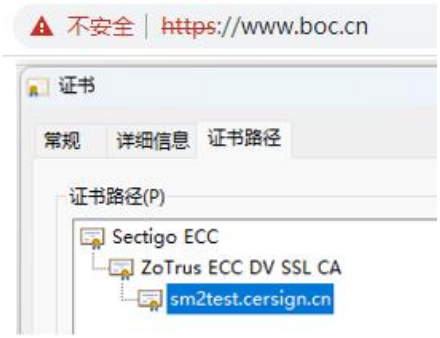
前几讲都在讲 SSL 证书，这一讲讲一讲浏览器是如何验证 SSL 证书的，浏览器在 CA/浏览器论坛中被定义为 SSL 证书的 Consumer(消费者)，什么是消费者？消费者是上帝哦。这就是为何笔者一直在说浏览器厂商在 CA/浏览器论坛中是强势方，那我们就看看强势在哪？

浏览器是用户上网的入口，当然需要担当起保护用户上网安全的责任。当用户使用浏览器以 http 方式上网时，浏览器会提示“不安全”，这不是浏览器吓唬用户，是真的不安全，因为 http 是明文传输协议，从浏览器到云端服务器之间明文传输的信息非常容易被非法窃取和非法篡改。笔者很遗憾的看到现在的微信等常用 APP 的内置浏览器访问 http 网站时并没有提示“不安全”，这实际上是在伤害用户！

如果用户使用浏览器访问的网站启用了 https 协议，则浏览器就开启了 SSL 证书的验证流程，主要有如下 9 个方面的验证，各个浏览器的验证项都有所不同，但是主流浏览器基本上都会验证前 5 项。

1. 验证 SSL 证书绑定的域名是否正确

浏览器使用 https 协议同 Web 服务器握手时，首先会从服务器返回的 SSL 证书中解析出证书绑定的域名，如果 SSL 证书绑定的域名同用户请求连接的网址不一致，则浏览器提示“不安全”并终止连接。如下左图所示，本地 host 解析 www.boc.cn 到另一个网站: sm2test.cersign.cn 的 IP 地址上，浏览器会提示“不安全”，具体错误信息是：ERR_CERT_COMMON_NAME_INVALID (域名不匹配)，因为此网站部署的 SSL 证书绑定的域名不是 www.boc.cn 而是 sm2test.cersign.cn，如下右图所示，这就有效地保护了用户不会被假冒银行的网站所欺骗。



但是，目前的各种 APP(包括微信)连接 https 服务时不判断域名是否匹配就稀里糊涂的与之连接，这会导致用户在假冒的银行网站输入的银行卡密码！域名不匹配绝大多数是遭遇了 DNS 攻击指向了假冒网站，而不判断域名是否匹配的问题就让攻击者轻松得到了用户的银行卡密码。但是，如果 APP 能想浏览器一样实时验证正在连接的 Web 服务器的 SSL 证书中绑定的域名是否匹配的话就能防范这类攻击。各种 APP 同浏览器一样都是上网客户端软件，都应该学习浏览器是如何正确验证 SSL 证书的，这是笔者讲浏览器是如何验证 SSL 证书的主要目的。

2. 验证 SSL 证书是否可信

浏览器在验证了证书绑定的域名同用户访问的域名一致后，就要验证 SSL 证书是否是浏览器信任的证书。浏览器使用 https 协议同 Web 服务器握手时就获得了网站部署的 SSL 证书和证书链，首先验证 SSL 证书是否是所声称的中级根证书签发，如果是则继续验证中级根证书的签发者是谁，一般就是浏览器信任的顶级根证书，如果是已经预置信任的某个顶级根证书签发的中级根证书，则表明证书链可信。但这时候浏览器不会马上显示加密锁标识，还需要做其他判断。

如果签发 SSL 证书的根证书不是浏览器信任的，则浏览器会提示“不安全”，具体错误信息是：ERR_CERT_AUTHORITY_INVALID (根证书不受信任)。但是，这个必须验证证书是否可信的步骤很多 APP 也没有做到，后果非常严重，因为假冒银行网站可以自签一张绑定正确的网银网址的 SSL 证书，如果 APP 不验证 SSL 证书是否是操作系统信任的证书，或者验证是否是 APP 信任的 SSL 证书，则一样可能会遭遇 DNS 劫持后的中间人攻击。安全的做法是不仅要验证 SSL 证书是操作系统信任的证书，而且应该验证证书是否是由本单位指定的 CA 机构的中级根证书签发，以防止可能的从操作系统信任的其他 CA 非法获得的绑定服务器域名的证书的恶意攻击。而对于一些重要的系统，如政务 APP、支付 APP，笔者推荐定制本单位专用中级

根证书来为这些系统签发 SSL 证书，这样就能做到 APP 只信任本单位专用中级根证书签发的 SSL 证书，只有这样才能做到万无一失。

为了防止浏览器把可信的 SSL 证书由于无法验证证书链而误判为不信任的证书，用户必须在部署 SSL 证书时同时附上中级根证书，这样浏览器在同服务器握手时就能快速验证证书链，快速显示加密锁标识。而零信浏览器同时做了更多的改进，如果握手时没有拿到中级根证书，则会通过证书中的 AIA 信息去获取中级根证书，并在验证后写入本地数据库供下次使用。如果证书中没有 AIA 信息或 AIA 网址不可用，而本地库也没有中级根证书信息，则只能认为是不可信证书了。

3. 验证 SSL 证书是否已经吊销

浏览器在验证了 SSL 证书是可信根签发后，还会查验 SSL 证书是否被吊销，这是通过访问证书中的“CRL 分发点”字段来获取证书吊销列表信息后验证证书序列号是否在证书吊销列表中，或者通过访问证书中的 OCSP 服务网址来验证证书是否被吊销。鉴于 OCSP 访问涉及到用户隐私问题，CA/浏览器论坛计划弃用 OCSP 服务。

一般情况下，如果用户怀疑证书私钥有可能泄露的话(如关键人员离职或服务器被攻击)，则必须向 CA 申请吊销此证书，重新申请一张新的 SSL 证书，所以浏览器在访问网站时会检查吊销列表，如果证书被吊销，则浏览器一定会显示为“不安全”，具体错误信息是：ERR_CERT_REVOKED (证书已吊销)。但是，笔者发现多个常用的 APP 并没有检查服务器证书是否被吊销，则非常危险，因为如果某个网银用的 SSL 证书的确是已经泄露的话，则攻击者就可以用这张证书来成功实现中间人攻击，因为这张 SSL 证书是浏览器信任的 SSL 证书。但是，如果 APP 能像浏览器一样实时验证证书是否已吊销的话，则就能及时发现并终止连接，能有效防止攻击者使用已经吊销的证书用于窃取网站的机密信息攻击。

4. 验证 SSL 证书是否已过期

浏览器在验证了 SSL 证书是可信根签发并且没有被吊销后，还会查验 SSL 证书是否过期，因为所有 SSL 证书都是有效期的，目前的标准是一年。用户必须在证书过期前续期证书，否则浏览器会显示“不安全”，具体错误信息是：ERR_CERT_DATE_INVALID (证书已过期)。

笔者发现有许多常用的 APP 居然不检查证书是否已经过期，如果攻击者获得了网银系统的已经过期的 SSL 证书，并且部署此过期证书用于攻击网银系统，则网银 APP 同服务器握手时不检查证书是否过期，则就会遭遇假冒银行网银系统的攻击！但是，如果 APP 能实时检查

证书是否过期的话，则一旦发现证书已经过期则马上终止连接，能有效防止攻击者利用过期证书的攻击。

谷歌正在推动 SSL 证书有效期缩短为 90 天，也就是说这个政策的改变可能会导致大量的人工部署和管理的 SSL 证书会在过期时由于忘了续期而使得用户无法通过浏览器正常访问。所以，大家从这里应该也能理解到 SSL 证书的自动化管理是何等的重要，实现了自动化管理，就不用担心证书已过期而忘了续期。

5. 验证 SSL 证书是否已透明公开披露

在谷歌牵头推出证书透明之前，浏览器在完成了以上 4 个步骤的检查后会正常显示加密锁标识，读者如果看过其他类型主题的文章应该就是这些内容了。但是，考虑到 CA 系统可能会被攻击而导致恶意签发浏览器信任的绑定某个域名的 SSL 证书用于恶意攻击，或者 CA 机构由于操作失误或系统错误而错误签发了绑定某个并不是用户申请的域名的 SSL 证书，怎么办？这些 SSL 证书都能正常通过以上 4 个步骤的检查。这就要靠证书透明机制来起保护作用了，谷歌浏览器要求所有 CA 机构必须把待签发的 SSL 证书提交到通过谷歌浏览器认证的证书透明日志系统中获得日志签名数据，并把日志签名数据写入到 SSL 证书的“SCT 列表”字段中。浏览器在最后一步会验证证书透明信息，如果证书中没有 SCT 列表字段，或者 SCT 列表字段中的日志签名信息不可信，则浏览器一样会显示“不安全”，如下左图显示，具体错误信息是：“ERR_CERTIFICATE_TRANSPARENCY_REQUIRED”(要求证书透明)，这是目前谷歌浏览器针对所有国际 SSL 证书如果没有提交证书透明日志系统的安全警告。而针对没有提交国密证书透明日志系统的情况，零信浏览器目前的处理方式如下右图所示，只是提示“国密证书不透明”，计划在 2023 年 7 月 1 日之后会同谷歌浏览器一样提示“不安全”，如下左图一样的提示。

6. 验证网站是否采用国算法实现 https 加密

这是零信浏览器增加的验证步骤，会在浏览器握手时询问 Web 服务器是否支持国密算法和国密 SSL 证书，如果支持，则优先采用国密算法实现 https 加密。这一点在目前的非常不确定的国际环境下变得非常重要，重要网站部署国密 SSL 证书是必须的。如果不支持国密算法，则只能采用 RSA 算法同服务器 https 加密通信，但是一旦这张用于 https 加密的 SSL 证书被吊销，则浏览器就无法正常访问网站，会像第 3 步验证一样显示为“不安全”而无法正常实现 https 加密通信。

如果网站部署了国密 SSL 证书，则零信浏览器会优先采用国密算法实现 https 加密，并在地址栏的加密锁标识后面增加显示国密加密标识，让用户对网站是否国密合规一目了然。

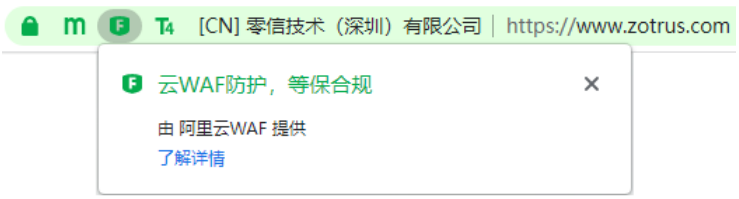
目前笔者还没有发现那个 APP 支持国密 https 加密，这值得各种网银 APP 和政务 APP 高度重视，早点着手升级改造 APP 以支持国密算法和国密 SSL 证书，只有这样才不至于出现一旦发生证书被非法吊销的极端情况时用户无法使用手机 APP，影响移动业务的正常运转，必须未雨绸缪提前做好准备才能有备无患。

7. 验证并展示网站可信身份

这是零信浏览器全球独家特色服务，零信浏览器在完成了所有 SSL 证书安全验证后会读取 SSL 证书中的身份认证级别 OID，如果是 EV SSL 证书，则显示绿色地址栏和展示 SSL 证书中的 O 字段单位名称，如下左图所示。如果是 OV SSL 证书，则显示浅绿色地址栏和展示 SSL 证书中的 O 字段单位名称。鉴于目前 85%的网站部署的都是无网站身份信息的 DV SSL 证书，零信浏览器独家创新提供了网站可信认证服务，并对通过 EV 认证的网站一样显示绿色地址栏和展示通过认证的单位名称，填补了 DV SSL 证书的身份缺失，如下右图所示。

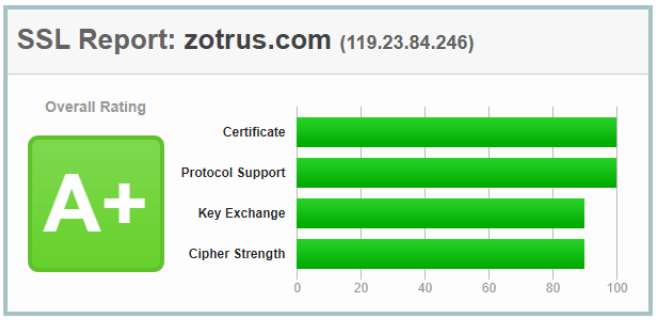
8. 验证并展示网站是否有 WAF 防护

这是零信浏览器全球独家特色服务，零信浏览器认证并预置了国内和国际知名的云 WAF 厂商的云 WAF 服务特征数据，如果网站有云 WAF 防护，则会在地址栏展示云 WAF 防护标识。虽然这个功能同 SSL 证书验证无关，但是一个网站是否安全，仅有 https 加密是不够的，必须同时有 WAF 防护。此验证功能仅在网站部署了 SSL 证书才会验证并展示，因为仅有 WAF 防护而没有部署 SSL 证书则网站一样是不安全的，浏览器只会显示“不安全”，不会展示 WAF 标识，没有启用 https 加密的 WAF 防护是没有意义的投资。



9. 完成所有验证后给网站安全打分

这也是零信浏览器全球独家特色服务，零信浏览器会在完成所有 SSL 证书验证后根据 SSL 证书的类型、SSL 协议支持、密钥交换、密码强度等四个维度来对 SSL 证书的部署做一个全面的 SSL 安全体检打分，再加上网站是否有 WAF 防护，是否有可信身份认证等指标给网站打一个安全分，让用户对网站的安全情况一目了然。这个体检打分标准是参考著名的 Qualys SSL Labs 的 SSL 体验打分标准的，如下左图所示为零信浏览器对零信官网的体检打分，如下右图所示为 SSL Labs 为零信官网的打分，都是 A+。



从以上讲解的浏览器 SSL 证书验证过程可以看出，用户在地址栏看到加密锁标识时浏览器是做了多个步骤的验证的，只有通过这些验证才会显示加密锁标识，浏览器才会让用户安全地同服务器交互。这个严格的证书验证过程非常值得 APP 开发者和 APP 运营者学习，自己开发和运营的 APP 在连接服务端之前一定也要做这些验证，否则 APP 是不安全的 APP，无法保障用户同服务器之间交互的机密信息安全。

笔者专门把浏览器如何验证 SSL 证书作为密码讲堂的一堂课的主要目的就是让 APP 开发者和运营者能借鉴非常成熟的浏览器的 SSL 证书验证过程来完善和提升 APP 同服务器通信时的安全水平，因为在移动互联网时代，用户使用手机的时间已经超过了浏览器，APP 的安全至关重要，不仅关系到 APP 用户更是关系到 APP 运营方的用户数据安全和运营数据安全，一定要高度重视。只有所有 APP 都安全了，才能真正提升我国的互联网安全水平。

下一讲内容预告 | 第 8 讲 什么是证书透明？什么是国密证书透明？

本讲讲一讲如何保障 SSL 证书的安全可靠供给，仅有根证书信任机制是不够的，必须还有一个监督机制来及时发现恶意签发或错误签发的 SSL 证书。

王高华

2023 年 3 月 21 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。