手机 App HTTPS 加密宝典

笔者在多种场合同朋友讲过手机 App 编程使用 https 加密的各种安全问题，记得有一年公司信息安全工程师测试了几款网银 App，发现每一款都有 https 加密的安全问题，不知道现在是否已经得到改进。但是，笔者同多名不同行业的 App 开发工程师沟通过，发现多年前发现的问题现在仍然存在。为此，笔者特抽空把手机 App 中普遍存在的安全问题整理成宝典呈现给读者。

大家都知道，手机 App 一般都有注册和登录操作，同时也要同服务器端交互各种用户机密数据，为了保护密码安全和机密信息安全，必须采用 https 协议实现同服务器端的加密通信，如果没用启用 https，是一定不能通过苹果应用商店审核的。但是，如果仅仅是启用 https 加密还是不够的，常见的安全问题有如下五种情况：

第一：不判断 SSL 证书绑定的域名是否正确

启用 https 同服务器握手，服务器会返回 SSL 证书绑定的域名，如果返回的 SSL 证书绑定的域名同用户请求连接的网址不一致，则应该终止连接。如：App 发起 https://login.domaina.com 连接，返回的 SSL 证书却是绑定 login.domainb.com 域名，这时候如果 App 不判断域名是否匹配就稀里糊涂的与之连接，把用户在 App 中输入的银行卡密码就交给了假冒网银服务器！域名不匹配绝大多数是遭遇了中间人攻击，这种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(如果这个 App 是网银 App 的话)。但是，如果 App 能实时验证域名是否匹配就能防范这类攻击。

第二：不判断 SSL 证书是否可信

这个问题也比较普遍，在网上查了一下相关问题，居然有多篇文章教用户无需调用证书验证函数。如果用户知道必须验证域名是否匹配，但是不知道需要验证服务器证书是否是操作系统信任的证书，或者验证是否是 App 信任的证书，则一样可能会遭遇 DNS 劫持后的中间人攻击，把用户的机密信息乖乖的交给了假冒网银系统。因为操作系统不信任的自签 SSL 证书是可以使用 OpenSSL 命令随意制作的，即使 App 会验证连接的域名是否同证书匹配，但是由于 App 不验证 SSL 证书是否可信，则仍然会中招。

比较可靠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，如支付系统，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。

第三：不判断 SSL 证书是否已经吊销

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。而 App 如果在同服务器握手时不验证证书是否被吊销的话，则如果某张网银用的 SSL 证书的确是已经泄露的话，则攻击者就可以用这种证书来成功实现中间人攻击。但是，如果 App 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中间人攻击。

第四：不判断 SSL 证书是否已经过期

这是一个低级错误，但是大多数 App 经常犯这个错误。SSL 证书都是有有效期的，如果过期了就会更新成新的有效期证书。但是，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中间人攻击，如果 App 同服务器握手时不检查证书是否过期，则就中招了！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。

第五：不支持国密算法和国密 SSL 证书

这是一个新问题，因为在目前的非常不确定的国际环境下，重要网站部署国密 SSL 证书是必须，所以手机 App 必须支持国密算法和国密 SSL 证书，以便能正确与服务器端实现国密 https

加密通信。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 证书被吊销或断供，则手机 App 就无法实现正常加密通信，无法保障 App 的数据通信安全。

这一点特别值得常用的手机 App 的高度重视，早点着手升级改造 App 以便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，必须未雨绸缪和有备无患。

以上前四大证书问题常用浏览器在 https 访问网站时是都有判断的，这就是为何有些用户看到浏览器会显示安全警告信息，但是 App 开发者往往并不是懂 PKI 技术的专业人士，不会了解 https 连接还有这么多名堂，以为只要在服务器上部署好 SSL 证书，App 编程启用 https 连接即可。其实这远远不够，App 在使用 https 协议同服务器握手时一定要检查以上前四种情况都没有问题后才能同服务器正常交换数据，只有这样，才能真正保证 https 加密能起到保护机密数据的作用。而对于第五个问题，目前许多国产浏览器都已经支持国密算法，常用的移动 App 也必须尽快支持。

笔者呼吁所有 App 开发者在看到此文后马上检查你开发的 App 是否已经做了以上五项检查，如果没有做到，马上改进并发布更新版本。而看到此文的朋友如果不是 App 开发者，但自己单位或朋友单位有 App 的话，请告知 App 开发者马上检查 App 程序，尽快堵住这个已经存在的很久的安全漏洞。也在此呼吁做 App 安全检测的朋友，在检测用户 App 时一定要特别留意检查 App 是否有这些问题，帮助用户及时堵住这个漏洞。这样的话，就可以大大提升我国手机 App 的安全水平，让 App 用户的数据更安全，让我国的互联网更安全。

王高华

2022 年 9 月 22 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。