iOS HTTPS 防中间人攻击

参考:
iOS 客户端 HTTPS 防中间人攻击实践
iOS安全系列之一：HTTPS
iOS安全系列之二：HTTPS进阶
SSL/TLS协议运行机制的概述

SSL 证书校验

HTTPS 相对 HTTP 来说其实是多了一层 SSL对信息加密以及证书校验的流程, 黑客为了获取到相关信息, 采用中间人攻击的手段来截取 HTTPS 信息。
我们先来看一下 SSL 是如何建立的安全通讯通道, 这里涉及到三个角色: Client,Server,以及 Ca(证书签发机构). Ca 主要用于解决 Client 与 Server 信任的问题, 一般流程是 Ca 通过签发证书的方式, 来确认 Client 与 Server 之间的身份, CA 一般向 Server 签发证书, 然后告知 Client, 该 Server 是可信任的, 这里有一个问题就是 Client 如何确认 CA 是信任的, 操作系统本身会内置一些 知名的 CA 的公钥, 这些知名 CA 在签发证书的时候会通过审核确认， 确保 Server 的身份和其所宣称的一致。

所有中间人攻击都是 围绕 CA 来进行的

解决方法

- 对通讯信息加密.一般使用 AES 256 对传输内容进行加密.
- 对证书 文件进行校验,主要对其 公钥与服务器证书公钥进行校验对比. 这里要注意证书过期
- 采用随机数 + 时间戳的方式增加到参数上, 服务器进行校验, 来防止重放性攻击.
- 使用 参数拼接的加密方式以及 同一套加密算法来对传输内容加密。
- 对证书校验如果一定要对证书时间做校验, 如果证书过期了, 服务器返回 规定的状态码,然后去请求下载最新证书.