

个人资料



justFWD

关注

原创

36

等级： 访问： 24万+

积分： 2545 排名： 1万+

勋章：

最新文章

间的关系

工具党如何干掉某讯手游的反修改器功能

超简单的il2cpp游戏修改教程

对抗某讯手游保护解密U3D脚本DLL



突破https——https抓包

2017年12月10日 20:48:57 阅读数： 8575 标签： https抓包 ca证书 [更多](#)

加密阶段学习了https原理，现在开始尝试破解，工具主要是burp suite， fiddler/charles与之类似。

一些概念性的东西

中间人攻击

在中间人攻击中，攻击主机通常截断客户端和服务器的加密通信。攻击机以自己的证书替代服务器发给客户端的证书。通常，客户端不会验证该证书，直接接受该证书，从而建立起和攻击机的安全连接。这样，客户端发送的数据，都会被攻击机获取和解密。

Certificate Pinning

证书锁定Certificate Pinning是SSL/TLS加密的额外保证手段。它会将服务器的证书公钥预先保存在客户端。在建立安全连接的过程中，客户端会将预置的公钥和接受的证书做比较。如果一致，就建立连接，否则就拒绝连接。

Certificate Pinning在手机软件中应用较多。因为这些应用连接的服务器相对固定，可以预先将服务器的X509证书或者公钥保存在App中。例如，苹果应用商店Apple App Store就预置了这个功能。当使用中间人工具或者Fiddler之类的工具拦截数据，就会造成应用商店无法联网的情况。

https代理抓包原理

简单来讲，就是burp充当客户端与服务端通信，得到服务端的响应之后用自己的证书充当服务端与app通信。

登录

注册

破解手段

根据不同的认证过程需要使用相应的手段进行破解。

使用系统CA库的破解

个人分类

手游逆向与保护	4篇
Android逆向	34篇
Android开发	18篇
Windows	4篇

归档

2017年12月	3篇
2017年11月	1篇
2017年10月	1篇
2017年3月	1篇
2017年2月	1篇

展开

热门文章

让APK只包含指定的ABI
阅读量：27072
阿里系UTDID库生成唯一性ID分析
阅读量：18942
360加固之libjiagu.so脱壳及dex dump
阅读量：15297
某梆企业版加固脱壳及抽代码还原方法
阅读量：12366
Android 6.0敏感权限新特性及使用方法
阅读量：11807

最新评论

Winlo使用笔记
WZD023：在线吗,有事请教 QQ179983405 谢谢!

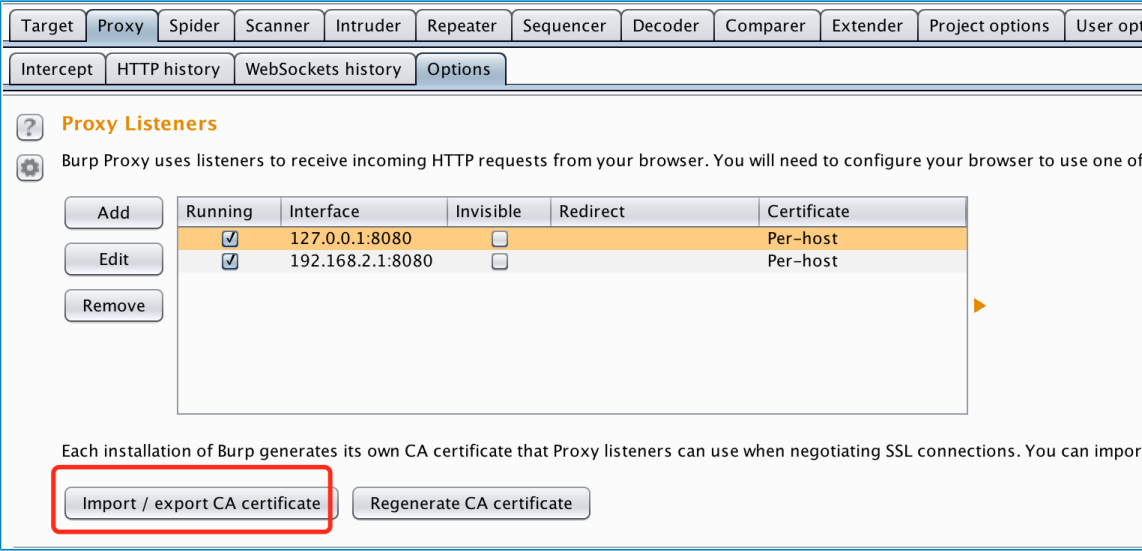
安卓浏览器，Mac下的Chrome浏览器都是使用系统的信任证书做验证。另外像下面这类代码请求https，应用也是通过系统信任证书做验证。

```
URL url = new URL("https://www.baidu.com/");
HttpsURLConnection urlConnection = (HttpsURLConnection) url.openConnection();
urlConnection.connect();
System.out.println(urlConnection.getResponseCode());
```

对于这种情况，将burp suite等工具的CA证书安装到系统中就可破解。如下是安卓上安装burp证书的过程。

1. 导出burp CA证书

点击Proxy -> Options 在Proxy Listeners 面板处的import/export CA certificate



导出burp CA

2. 将证书上传到手机，直接点击就可以安装了。

PC上的firefox浏览器维护着一套受信凭据，点击 首选项->高级->证书->查看证书，在证书机构中导入就可以了，如下图

阿里系UTDID库生成唯一性ID分析

w112121: 厉害

fiddler Android下h...

weixin_40468698: 你好: 使用fiddler出现了问题
希望能帮忙解答下 谢谢啊! 问题描述: APP使用I.
..

WinIo使用笔记

xzl1126: 楼主! 你好! 请问有java的样例嘛? 我是
win7 64位! JDK是32位的。使用的是winio32...

360加固之libjiagu.so...

qq_42055278: "北京地铁" apk, dump 出来的so
文件头被填充了 0x7fbaed294000: 0x...

联系我们



请扫描二维码联系客服

webmaster@csdn.net

400-660-0108

QQ客服 客服论坛

关于 · 招聘 · 广告服务 · 网站地图

©2018 CSDN版权所有 京ICP证09002463号

百度提供搜索支持

经营性网站备案信息



Firefox导入证书

另外burp suite出于安全考虑, 每次安装都会重新生成一套CA证书, 所以如果重新安装了burp, 要记得将系统中的CA证书更新。

接受所有证书的app

网络110报警服务
中国互联网举报中心
北京互联网违法和不良信息举报中心

如果应用代码中使用如下代码，则会接受所有证书(不对证书做验证)，此时直接通过代理就可以抓包。像这代码一般都是放在爬虫里抓数据的。

```
1  static SSLSocketFactory trustAllSocketFactory() throws Exception{
2      TrustManager[] trustAllCerts = new TrustManager[]{
3          new X509TrustManager() {
4              public java.security.cert.X509Certificate[] getAcceptedIssuers() {
5                  return null;
6              }
7          }
8      };
9      public void checkClientTrusted(X509Certificate[] certs, String authType) {
10     }
11     public void checkServerTrusted(X509Certificate[] certs, String authType) {
12     }
13 };
14 SSLContext sslCxt = SSLContext.getInstance("TLSv1.2");
15 sslCxt.init(null, trustAllCerts, null);
16 return sslCxt.getSocketFactory();
17 }
18
19
```

Certificate Pinning

前几年的app虽然也都用了https协议，但只需要简单地通过设置代理就能抓到；从去年开始遇到的几个app都不能走代理抓包了，一设置代理就说网络有问题，联不上网。通过前面的学习总算知道是怎么回事了。原来他们都使用了证书绑定技术，证书绑定简单来说就是app只信任自己内置的证书，如果服务端的证书与app内的信任证书不符，客户端主动拒绝连接，从而造成“网络无法访问”。如下是引用自[stackexchange](#)的关于证书验证与绑定的相关评论。

Typically certificates are validated by checking the signature hierarchy; MyCert is signed by IntermediateCert which is signed by RootCert, and RootCert is listed in my computer's “certificates to trust” store.

Certificate Pinning is where you ignore that whole thing, and say trust this certificate only or perhaps trust only certificates signed by this certificate.

So for example, if you go to google.com, your browser will trust the certificate if it's signed by Verisign, Digicert, Thawte, or the Hong Kong Post Office (and dozens others). But if you use (on newer versions) Microsoft Windows Update, it will ONLY trust certificates signed by Microsoft. No Verisign, no Digicert, no Hong Kong Post office.

Also, some newer browsers (Chrome, for example) will do a variation of certificate pinning using the HSTS mechanism. They preload a specific set of public key hashes into this the HSTS configuration, which limits the valid certificates to only those which indicate the specified public key.

所以我们可以有以下几个方式破解：

1. 李代桃僵

反编译app，替换cer为burp的证书后重新打包。如果有反二次打包机制，可以通过xposed hook相关方法来替换证书。

另外可以从app内取出cer文件并导入浏览器，就可以用浏览器访问app的url。

2. 釜底抽薪

用xposed或修改smali控制创建连接的SSLSocketFactory，使它不加载信任库。

另外app内的证书可能有两种格式

- .cer/.der

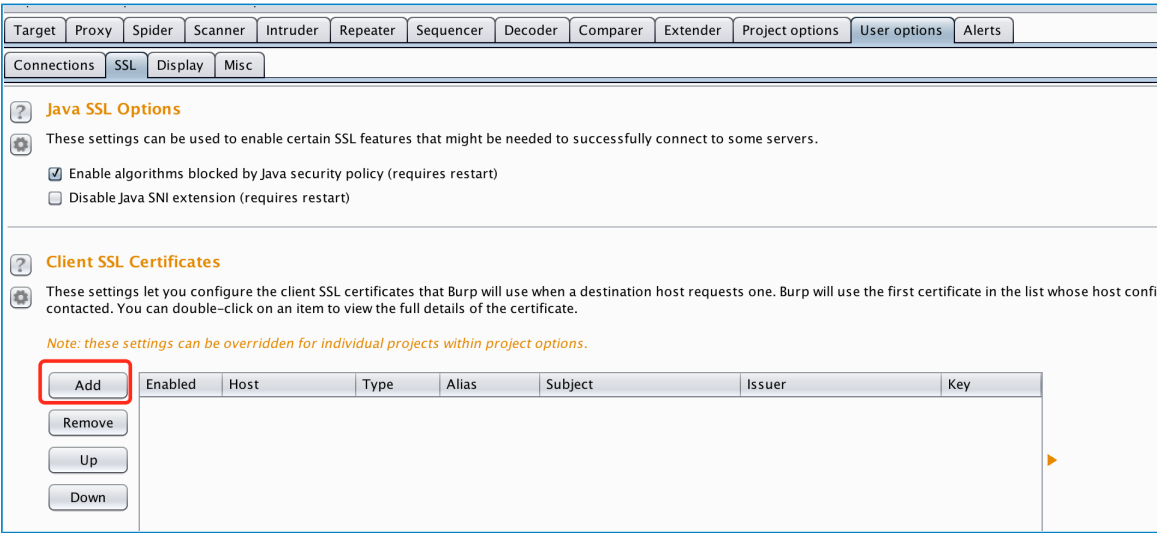
如果是.der证书，按以下步骤

1. 逆向，取出.cer证书文件
2. 用burp的证书替换掉app内的证书，app重新打包

- .bks

如果是keystore文件就简单了，先取出来，如果是单向认证，用keytool把burp的证书导入使之成为truststore内的一条就可以了；

如果是双向认证，除了加入truststore或替换cer文件，还要把keystore加入burp中，添加之前需要将它转换成pkcs12格式。如下图



burp添加keystore

android 4.X通过设置wifi代理可以为所以应用设置代理，但在5.x版本中设置的wifi代理只能为浏览器使用，如果要为app设置代理需要root后安装全局代理工具(如proxydroid)。

charles 为什么能抓https的包？原理是什么？

众所周知，http明文传输，https加密就是为了在传输层禁止暴露明文，但是为什么抓包工具又能抓到? 岂不是和https的设计矛盾了?? 简单的说就是中间人攻击，也就是“man-in-the-m...

想对作者说点什么？

我来说两句

wireshark抓取https加密报文，并解密

6.6万

首先你要有证书，而且这个证书需要是.pem格式的。Window的证书管理导出来的是.pfx文件。这个格式在官网上...


HTTPS抓包详细分析

2万

专题二：实际抓包分析本文对百度搜索进行了两次抓包，第一次抓包之前清理了浏览器的所有缓存；第二次抓包...

在windows下使用Charles对移动终端**抓包(https请求)**  4696

1、简介 Charles是目前最强大最流行的http抓包调试工具， Mac、 Unix、 Windows各个平台都支持。特别是做AP...

Window下使用Charles对手机的**Https请求进行抓包**  1.4万

1.首先安装Charles软件，在我上传的资源中有破解版（传送门） 另外还要注意，Charles软件运行需要java环境...

抓包工具Fiddler的使用教程（十二）下：Fiddler抓取HTTPS  1.1万

在教程十二（上）， 我们也了解了HTTPS协议， 该教程就和大家分享Fiddler如何抓取HTTPS 抓包工具Fiddler的...

HTTPs握手流程抓包解析  6063

TLS Handshake Flow： 以下是访问 https://github.com 的 wireshark 抓包截图： C->S： Client Hello S->C： Serve...




杭州人有福了！ 70周年纪念银币震撼上市

泽熙电子 · 顶新

Fiddler死活抓不了**HTTPS**包解决办法  4.9万

有些同学可能已经按照我们正常的流程在feiddler中设置好了https抓包，但死活抓不了。未设置的同学先按 https:...

 **[强烈推荐]HTTP/HTTPS抓包工具 HTTP Analyzer 5.1.1 破解版**

2010年04月26日 15:12

https实践之 抓包分析流程  2293

概述： 本文主要研究HTTPS协议的流程，通过抓包分析握手过程，主要将围绕HTTPS优化进行展开。 探究： 1...

关于**HTTPS的抓包**  16

工具： charles/fiddler； 安卓模拟器（我选择了夜神模拟器）， 一台配置还过得去的win之前公司的app出于安全性...

Https 抓包  33

1、 windows下安装charles，看到此文章的用户相信都已经安装了charles，如果还真的没安装，麻烦就自行搜索...

一步一步教你 **https 抓包**  4875

在 Mac 上常用的抓包软件是 Charles，网上关于 Charles 的教程很多，这里介绍另一个抓包神器 mitmproxy。mit...

- 让你的程序支持https以及https的抓包 1234
iOS9推出的时候，苹果希望大家使用https协议，来提高数据传输之间的安全性。下面我就从最简单的代码介绍， ...



耳鸣千万不可小视，几招教你解决...

上海华肤医院 · 顶新

- Charles抓包https接口指南 1.6万
Charles抓包https接口 作为一名iOS攻城狮，如果你没有听说过青花瓷这款软件，我只能说你还是回家洗洗睡吧。 ...

- fiddler-实现https抓包 581
1. fiddler设置-fiddler options-https项进行设置，如下： 2. ie代理设置：连接-局域网设置 ...

- wireshark https 抓包 2392
概述网上wireshark监听https的教程非常少，基本都是转载的同一篇，并且我实践后并不好使，没有办法，只能自...

- 突破微信授权，获取任意微信网页源代码（含https） 4520
chrome对需要微信授权登录的页面无能为力、微信官方提供的调试工具很不稳定，按下不表。这里使用Charles抓...

下载

HTTPS抓包浏览器

2014年01月12日 10:48

下载

https访问github.com的Wireshark抓包文件

2017年06月04日 08:52


- fiddler抓包HTTPS请求 6.9万
fiddler抓包HTTPS请求 跟着教程来，保证100%成功抓HTTPS包 教程开始安装fiddler首先准备一台可以上网的wind...

- Fiddler抓包使用教程-Https 2783
转载请标明出处：http://blog.csdn.net/zhaoyanjun6/article/details/72956016 本文出自【赵彦军的博客】 开启 Ht...

- fiddler pc https 抓包 3.3万

原理fiddler抓包原理fiddler 调试器注册到操作系统因特网服务中，系统所有的网络请求都会走fiddler的代理，所以f...

- 使用Charles进行https抓包 5760
使用Charles进行https抓包



腰椎病人的福音，小小一张纸，贴上就会好，快学起来

博舍 · 顶新

- MAC使用charles对https进行抓包 1293
1. Charles安装官网下载安装Charles:https://www.charlesproxy.com/download/2. 设置手机http代理并且安装证书...

- charles mac下https抓包和iphone https抓包 4577
1:去官网下载安装包 charles 我这次使用的是最新版本4.0.2（破解文件自己去搜，找不到在评论中问我） 2：本机...

- 使用Fiddler对移动设备上的HTTP/HTTPS抓包 1887
Fiddler是著名的抓包工具，经常跟HTTP/HTTPS打交道的人并不陌生。

- android使用Charles抓包https请求 1.3万
以前使用抓包神器fiddler抓包还是很厉害的，听说过Charles一直没用过，只从换了mac，fiddler就没发用了，只能...

- Fiddler 如何抓取手机app包以及抓取https 响应 9148
Fiddler安装 此处略。我们需要安装Fiddler软件，版本需要在4.0以上，尽量越高越好。 普通https抓包设置 打开Fid...

- fiddler 手机 https 抓包 4.3万
fiddler手机抓包原理fiddler手机抓包的原理与抓pc上的web数据一样，都是把fiddler当作代理，网络请求走fiddler...