

博客学院下载GitChatTinyMind论坛APP问答商城VIP会员活动招聘ITeye

写博客发Chat传资源登录注册

个人资料



五二言

关注

原创18

等级: 访问: 1万+
积分: 359 排名: 23万+
勋章:

最新文章

原

【微信你妹】中间人攻击截获微信数据

0

2016年01月25日 00:15:59

阅读数: 6530

标签: 微信 通信 https 网络安全

中间人 更多

版权声明: 本文为博主原创文章, 未经博主允许不得转载。 <https://blog.csdn.net/wueryan/article/details/50533974>

前言

最近由于项目的需求, 需要获取微信图文的点赞数以及阅读数。相关的接口已经通过抓包软件fiddler定位到了, 但是这两个接口需要传递一个key值才能获取到响应的数据, 而这个key的参数不仅动态变化, 而且还是通过微信的自定义的协议进行传递通信, 所以按照一般的手段, 很难获取到这个值。

缺失key值, 就无法获取到图文的点赞数以及阅读数, 反过来说, 只要解决了获取key参数的问题, 那么这个获取点赞数以及阅读数的问题就会迎刃而解。

这里提供两种思路。

第一种思路则是从key的生产源头出发——即破解微信android的源码, 对其进行修改后重编, 此时即可获取到key值。这种方法胜在稳定, 然而需要读懂微信的源码以及规避微信的数字签名校验等机制。

第二种思路则是从通信过程入手, 采用中间人攻击对key进行截获转发到我们自身的服务器。

目前笔者采用了第二种思路来作为解决问题的方法。

相关概念以及知识点

计算机就称为中间人。

(2) HTTPS

HTTPS是基于SSL/TSL的HTTP, 在HTTP协议的基础上, 添加了SSL/TSL的数据传输加密机制。

(3) HTTPS通信流程

登录注册

【技术员的工具箱】四步十分钟生成一千万条数据进行性能测试

Spring AOP初探 (二)

Spring AOP初步了解

Spring Bean的生存日记

个人分类

编程师札记	3篇
设计模式与代码规范	2篇
项目与产品之道	3篇
事务，零失误	3篇
知平问答	3篇

展开

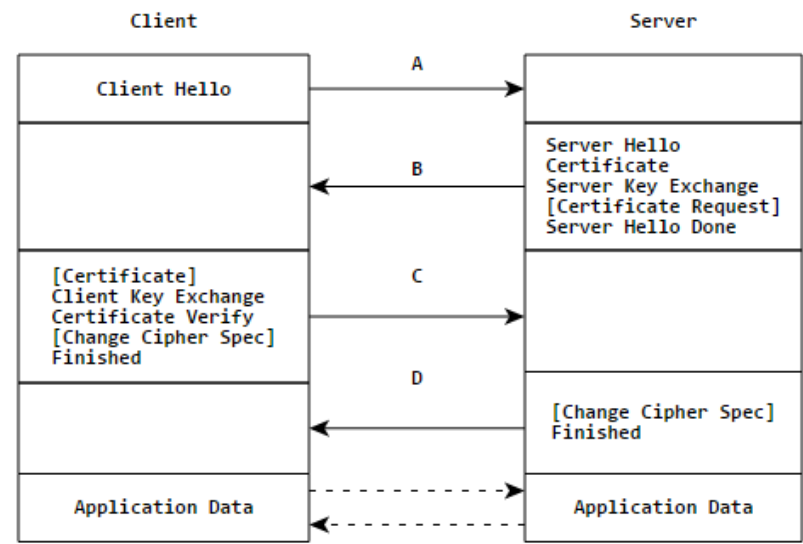
归档

2016年8月	2篇
2016年6月	2篇
2016年5月	1篇
2016年3月	1篇
2016年2月	1篇

展开

热门文章

【微信你妹】中间人攻击截获微信数据	阅读量：6517
【知乎问答】为什么很多看起来不是很复杂的网站，比如 Facebook 需要大量顶尖高手	阅读量：2013
关于项目的构建与打包	阅读量：1731
【懒程序员的日常】接口文档绝对是个混账！	阅读量：1070
学习技巧以及学习方法的总结	阅读量：748



简单说下HTTPS通信流程。

- 1) 握手阶段，客户端告知服务端以下信息：本地支持的加密套件以及准备产生Master Secret的随机数。
- 2) 服务端接收到客户端的申请并鉴定后，产生一对私钥与公钥，同时颁发证书，此时服务端将私钥保存起来，公钥附带在证书信息中，随后返回证书给客户端。
- 3) 客户端检测证书的合法性，并产生一个PreMaster Secret，用服务端传过来的公钥进行加密后，返回给服务端。
- 4) 此时客户端和服务端共同拥有一样的PreMaster Secret以及随机数，这时候将其合并在一起，变成Master Secret，这串数据可以解析出来客户端的加密的key以及服务端加密的key。
- 5) 双方开始进行通信

(4) 截获和篡改HTTPS实现原理

我们可以伪造CA证书对微信的https进行破译。

- 1) 首先我们的本地服务器会截获客户端的消息，此时客户端还没有微信的服务端进行握手行为。
- 2) 之后我们伪造客户端的请求向微信服务端发送请求，服务端返回证书，获取到CA证书后，拿到里面的公钥。

最新评论

【微信你妹】中间人攻击截获微信数据

Tilyp: 这个现在还能行得通吗? 我配置的不能到外网去

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

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

- 3) 服务端伪造自己的CA证书，之后对客户端的请求进行返回伪造的CA证书。
 - 4) 客户端用了我们的伪造证书里的公钥进行加密，传给我们的本地服务端，我们截取到数据后，用自己的CA证书进行解密，然后在利用微信的服务端证书进行加密重新传给微信服务端
- 由于我们有两边的密钥，所以数据对于我们来说是透明的。

方案实施

(1) 通过修改本地的host文件对微信客户端的域名进行劫持，继而转向我们的本地服务端。

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com           # source server
#       38.25.63.10       x.acme.com               # x client host


# localhost name resolution is handled within DNS itself.
#   127.0.0.1       localhost
#   ::1             localhost

127.0.0.1 mp.weixin.qq.com
#127.0.0.1 res.wx.qq.com
```

(2) 在本地搭建HTTPS服务器，并且自签名数字证书。

如何搭建HTTPS服务器？可以去nginx官网上下载安装包，之后只要对配置进行修改，指向准备分发数据的Tomcat即可。

配置如下：

```
2 #user nobody;
3 worker_processes 1;
4
5 #error_log logs/error.log;
6 #error_log logs/error.log notice;
7 #error_log logs/error.log info;
8
9 #pid logs/nginx.pid;
10
11
12 events {
13     worker_connections 1024;
14 }
15
16
17 http {
18     include mime.types;
19     default_type application/octet-stream;
20
21     #log_format main '$remote_addr - $remote_user [$time_local] "$request" '
22     #                 '$status $body_bytes_sent "$http_referer" '
23     #                 '"$http_user_agent" "$http_x_forwarded_for"';
24
25     #access_log logs/access.log main;
26
27     sendfile on;
28     #tcp_nopush on;
29
30     #keepalive_timeout 0;
31     keepalive_timeout 65;
32
33     #gzip on;
34
35
36     # another virtual host using mix of IP-, name-, and port-based configuration
37     #
38     #server {
39     #     listen 8000;
40     #     listen somename:8080;
41     #     server_name somename alias another.alias;
```

```
42
43     #     location / {
44     #         root     html;
45     #         index    index.html index.htm;
46     #     }
47     #}
48
49
50     # HTTPS server
51     #
52     #server {
53     #     listen      443 ssl;
54     #     server_name localhost;
55
56     #     ssl_certificate      cert.pem;
57     #     ssl_certificate_key  cert.key;
58
59     #     ssl_session_cache    shared:SSL:1m;
60     #     ssl_session_timeout  5m;
61
62     #     ssl_ciphers  HIGH:!aNULL:!MD5;
63     #     ssl_prefer_server_ciphers  on;
64
65     #     location / {
66     #         root     html;
67     #         index    index.html index.htm;
68     #     }
69     #}
70
71     server {
72         listen      80;
73         listen      443;
74         server_name localhost;
75
76         ssl          on;
77         ssl_certificate      server.crt;
78         ssl_certificate_key  server_nopass.key;
79
80
```

```
81         location / {
82             proxy_pass http://127.0.0.1:8080;
83             proxy_set_header Host $host;
84             proxy_set_header X-Real-IP $remote_addr;
85             proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
86         }
87     }
88 }
```

关于自签名证书

生成密钥

openssl genrsa -des3 -out server.key 2048

转化成免密密钥

openssl rsa -in server.key -out server_nopass.key

生成一个证书请求

openssl req -new -key server.key -out server.csr

自己签发证书

openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt

- (3) 搭建Tomcat，模仿微信编写相应的Servlet接口。
- (4) 完成配置，用微信客户端发送请求，观测本地服务器的Servlet接口是否已经接收到了数据。

参考资料

[Https\(SSL/TLS\)原理详解](#)

想对作者说点什么？

我来说两句

Tilyp： 这个现在还能行得通吗？ 我配置的不能到外网去 （07-06 14:43 #1楼）



第三方apk实时获取微信聊天消息记录

1.3万

说明：纯属发烧而生 第一步：安装apk的手机进行root 因为需要读取微信聊天记录信息表，所以手机需要root，...

利用fiddler 截获微信传输数据（方便抓取公众号信息）

3.3万

前言：本文章是搭配《批量获取微信公众号》一文，介于群里朋友很热情，我就趁着上班测完bug 来撰写该文章...

截获各种IM Messenger的聊天记录

1400

对于当前流行的各种即时聊天工具，截获聊天内容大致有两种办法。第一种，分析通信协议。第二种，通过...

Wireshark抓包微信Web详细分析HTTPS通信中TLS/SSL工作原理

1.2万

简介HTTPSHTTPS(Hypertext Transfer Protocol Secure)是一种网络安全传输协议，是一种用于在不可信网络上...

Wifi密码破解与局域网抓包监听（小白--纯工具版）

7万

工具介绍： 1，wifi密码破解：CDlinux.iso ：一个Linux系统，集成了wifi密码的PIN码破解软件。2，Mac地址修...

服务器数据抓包（原来微信图片真的可以抓包看的）

3.1万

在我们开发的时候，有时需要抓包，看一下服务器的返回数据，来校验自己请求的参数和返回的参数是否正确。...



杭州人有福了！70周年纪念银币震撼上市

泽熙电子 · 顶新

微信交互数据包分析

2030

该篇文章主要对微信交互数据报文进行了抓包分析，抓包可以用wireshark通过hub抓取wan口数据包，也可以通...

Android 窃取手机中微信聊天记录

9326

这几天事情比较多，可还是想尽快写下这篇文章。本以为微信的聊天记录以我本人现存能力获取不到，但经过一...

利用Fiddler手机抓包对ONE·APP网页爬虫实现电影资讯微信Java开发

1.1万

实现电影资讯微信订阅号Java开发。 1. 利用Fiddler抓包工具，通过手机代理抓取ONE电影请求； 2. 使用jackson...

破解无线路由器，获得微信等上网信息 8278

翻到一个帖子，感觉很有用，因此转载到博客，有利于提高安全意识。 都是年轻人，肯定少不了无线路由器...

相关热词 [ii 微信](#) [微信this](#) [微信for](#) [微信 ii](#) [微信的if](#)

抓取微信图文信息 974

class AdvertisementAction extends BaseAction{ public \$token; public \$id; public \$wecha_id; publi...

微信朋友圈马赛克图片 -- 抓包破解 7367

微信已经修复这个 bug 了， 所以如果只是想免费看微信朋友圈马赛克图片可以不用看此文了。 想了解抓包的可...

移动端防止被抓包 4000

微探星座 2016-10-27 11:20 最近在调试一个bug的时候没有其它好的办法了，用到了抓包这么个方式才发现问题...



耳鸣千万不可小视，几招教你解决...

上海华肤医院 · 顶新

netty 实现https服务器 1512

0 概述 netty 通过JDK的SSLEngine，以SslHandler的方式提供对SSL/TLS 安全传输的支持，极大的简化了开发工...

APP中https证书有效性验证引发安全问题（例Fiddler可抓https包） 5823

前言： 在实际项目代码审计中发现，目前很多手机银行虽然使用了https通信方式，但是只是简单的调用而已， ...

HTTPS连接过程以及中间人攻击劫持 5008

HTTPS连接过程https协议就是http+ssl协议，如下图所示为其连接过程： 1.https请求 客户端向服务端发送https...

Https单向认证和双向认证 5.7万

HTTPS单双向认证过程

[下载](#) **微信62数据**源码

[下载](#) **微信**信息获取软件

2014年08月08日 11:24

程序员撩妹，一撩一个准，哈哈  4996
给大家分享这些聊天记录之前，先分享一段非常经典的找女朋友套路！如果没有过硬的追人技术，放弃今生只爱她...

python教你用**微信**每天给女朋友说晚安  110
但凡一件事，稍微有些重复。我就考虑怎么样用程序来实现它。 这里给各位程序员朋友分享如何每天给朋友定时...

ettercap进行简单的arp欺骗和**中间人攻击**  592
请遵守法律法规，严守道德底线，禁止使用相关技术危害他人信息安全。 攻击主机平台：kali-linux 被攻击主机： ...

针对SSL的**中间人攻击**演示和防范  2104
1 中间人攻击概述 中间人攻击（man-in-the-Middle Attack, MITM）是一种由来已久的网络入侵手段，并且在今天...



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

如何抓**微信**的请求  6180
最近公司做了一个微信的项目，因为项目只能在微信中运行，要调试的话就必须抓包。PC怎么抓取到微信的包呢...

手工实现ARP**中间人攻击**  1680
<http://support.huawei.com/ecomunity/bbs/10170857.html> 手工实现ARP中间人攻击 本文档针对已学习了解A...

[转]**微信**端口及协议分析  1.4万
2015-3-3阅读386 评论0 <http://blog.newxd.com/7235.html> 有朋友公司需求如下，手机通过WIFI连接上网，而老板...

微信小程序--妹子demo  655
花了二天刷了一遍微信小程序官方文档,于是写了第一个小程序demo,算做入了个门吧。图片API来自gank.io 源代码...

Python撩妹实战——教你用微信每天给女朋友说晚安



570

能用朋友通红弄自动但凡一件事，稍微有些重复。我就考虑怎么样用程序来实现它。这里给各位程序员朋友分享如...

中间人攻击：你的信用卡数据是这样暴露的.....



181

NCR Corp研究人员展示了针对PoS终端和PIN输入设备的被动中间人攻击是如何绕过信用卡芯片和密码保护、而导...

1分钟教会你二进制撩妹（汉）读心术



619

近些年来，小魔发现，对于年轻的男女而言，一些传统的节日似乎都变成了情人节或者脱单节，就连“光棍节”，实...

下载 微信H5小游戏转你妹

2018年07月26日 22:24

微信与服务器端通信方式的变迁是为什么？



6096

最近发现系统的微信认证很慢，有的甚至连接不上，发不出消息，就到网上搜索了下，还真发现了关于微信的细微...

微信小程序敏感内容检测



122

获取access_token access_token是公众号的全局唯一接口调用凭据，公众号调用各接口时都需使用access_token...



仅剩1天！生肖纪念币大全1200元限量抢！再不出手就没了！

天腾测绘 · 顶新

Http的post请求和常见的编码,加解密,支付宝和微信支付的使用



5176

Http协议与请求 Post请求 Post请求与Get请求的区别 Get请求的参数是直接放在url后面的，而Post请求是放在请求...

如何使用Charles抓包并分析Http报文



2555

从Web安全的攻击防御方面来说，最多接触的应该就是Http协议了，当我们作为中间人（man-in-the-middle）查看...

微信开发（五）微信消息加解密 (EncodingAESKey)



5.1万

随着微信服务开发在越来越多的领域应用，应用的安全性逐渐被重视起来。本文主要阐述如何为微信的消息加密的...

		...
<div>下载 微信小程序(WeChatMeiZhi妹子图)</div>		2018年07月08日 22:35
<div>数学之美 代码撩妹的艺术</div> <div>微信小程序中使用贝塞尔曲线动态绘制心</div>		<div> 1626</div>
<div>中间人攻击之DNS劫持</div> <div>中间人攻击之DNS劫持</div>		<div> 1825</div>
<div>设计模式中的撩妹神技--上篇</div> <div>开篇前言 遇一人白首，择一城终老，是多么美好的人生境界，她和他历经风雨慢慢变老，回首走过的点点滴滴， ...</div>		<div> 4917</div>
<div>关于Diffie-Hellman密钥协商机制以及中间人攻击</div> <div>前两天学习了有关认证机制的内容，学到一个Diffie-Hellman密钥协商机制，阅读的文章说其极易受到中间人攻击...</div>		<div> 2966</div>
<div>苹果iCloud遭SSL中间人劫持，用户如何防范隐私泄露？</div> <div>近日，苹果iCloud服务器在中国被人使用SSL中间人劫持，部分地区用户隐私恐将不保。据了解，苹果iCloud网站...</div>		<div> 603</div>
<div>Android逆向之旅---静态方式破解微信获取聊天记录和通讯录信息</div> <div>微信现在是老少皆宜，大街小巷都在使用，已经替代了传统的短信聊天方式了，只要涉及到聊天就肯定有隐私消息...</div>		<div> 3.4万</div>
<div> 杭州人有福了！70周年纪念银币震撼上市</div> <div>泽熙电子 · 顶新</div>		
<div>Android利用Fiddler进行网络数据抓包</div> <div>http://www.trinea.cn/android/android-network-sniffer/ 主要介绍Android及iPhone手机上如何进行网络数据抓包， ...</div>		<div> 1.3万</div>
<div>java 实现微信搜索附近人功能</div>		<div> 419</div>

最近给andorid做后台查询数据功能，有一个需求是模仿微信的查找附近人功能。数据库中存储每个用户的经纬度...

ContentType("application/octet-stream");  1945


ContentType("application/octet-stream"); [问题点数： 40分， 结帖人Partys] 不显示删除回复 显示所有...

通过中间人攻击的方法拦截传输在https上的加密信息  1205

通过Charles来拦截移动端的登录密码，验证应用的安全性

Android安全之Https中间人攻击漏洞  898

HTTPS，是一种网络安全传输协议，利用SSL/TLS来对数据包进行加密,以提供对网络服务器的身份认证，保护交换...

中间人攻击(Man-In-The-Middle)&&Cain使用简介  5033

中间人攻击(Man-In-The-Middle) 局域网内通过向被攻击者和网关发送ARP请求或响应包来修改对方的ARP缓存(...

没有更多推荐了， [返回首页](#)