



论文题目:

恶意 WIFI 信息窃取的可能方式和对策研究

Information eavesdropping WIFI & countermeasure

所在院系: 信息科学技术学院

专业名称: 信息安全

姓名: 袁皓洁 学号: PB14210017

指导老师姓名: 王百宗 职称: 实验师

论文主题词: 恶意 WIFI 中间人 防御 TTL 检测

摘要

近年来 WIFI 技术迅速发展，覆盖了生活的各个角落；与此同时 WIFI 安全事件频发。本文先是站在攻击者的角度搭建了恶意热点，并模拟了 sslstrip、dns 劫持等多种攻击，分析各种攻击的原理或利用的漏洞，介绍了各种手段所使用的工具以供测试，并就其攻击特点及所能产生的威胁做了相应的评估比较。采用市面上已有的号称有 WIFI 安全性检查的安全软件对热点进行测试，结果出乎意料的没有任何效果。

于是在攻击测试的基础上，并依据接入公众热点的普遍为智能手机这一事实，本文提出了自己的一套防御体系。针对各种类型的抓包分析，采用双网路切换保证敏感信息安全；针对 dns 劫持访问钓鱼页面，采用 TTL 检测有效查验是否正常跳转；针对一些少见的进攻可能，依据大数据的思想提出协议库和自定义站点库，给予连接安全性未知的热点的用户以多角度的保护。

关键词：恶意 WIFI 中间人 防御 TTL 检测

Abstract

In recent years, the rapid development of WIFI technology leads to the its coverage of every corner in daily life. By the same time WIFI security incident happens frequently. The article first stands at the perspective of attacker to set up a malicious access point. And executed sslstrip, dns hijacking, and other attacks. The principles of analysis of various attack or exploit, and its characteristics and the threat of attacks that can be generated to do the appropriate Comparative evaluation. However, using the security software which already has function of WIFI security check for the AP test, unexpectedly results to nothing.

So on the basis of the attack executed during the test, and based the fact of universal access to public hotspots mostly link to smartphones, the paper presents its own set of defenses. For all types of packet capture analysis, dual switched network to ensure security of sensitive information. For dns hijacking which access to phishing page, TTL module checks whether it's a normal jump. According to data presented ideological agreement for a number of rare offensive library and custom site library, giving users multi-angle protection when accessing to an unknown AP.

KeyWords: Malicious AP; Mitm attack; Defense frame; TTL

目录

第一章：绪论	1
1.1 课题背景及意义	1
1.2 国内外研究现状	1
第二章：进攻原理介绍	2
2.1 简单抓包分析	2
2.2 SSLstrip（http 降级攻击）	2
2.3 SSLsniff（伪造证书攻击）	3
2.4 重定向和钓鱼页面	3
2.5 Drift-net 记录图片	4
第三章：攻击成果展示	5
3.1 单纯抓包	5
3.2 SSLstrip+抓包	7
3.3 SSLsniff	9
3.4 DNS 劫持+钓鱼页面	10
第四章：防御架构	12
4.1 防御架构基本思想	12
4.2 双网路的实现方法	13
4.3 TTL 检测	14
4.4 https 库、重要域名库和 MAC 库	15
4.5 被放弃的一些防御思路和原因简介	16
4.5.1 IP 库	16
4.5.2 识别敏感页面后自动完成双网路切换	16
4.5.3 基于时序完成 SSLsniff 检测	17
第五章：总结和未来工作展望	18
附录	19

第一章：绪论

1.1 课题背景及意义

随着近几年来无线数据传输技术迅猛发展和智能手机的快速普及，WIFI 由于其方便快捷的特点颇受人们青睐，如今大街小巷随处可见开放的公众热点。由 360 互联网安全中心发布的 2014 年中国手机使用状况报告显示^[1]，网民使用手机上网人群占比已提升至 83.4%，其中有 28.6%手机用户选择使用 WIFI 上网，56.74%手机用户表示流量不够用。

WIFI 给生活带来便利的同时也给用户安全带来了严峻的考验。近几年来 WIFI 安全事件频发，315 晚会的现场演示震撼了很多。而经测试，市面上最普及的几款号称具有对抗钓鱼热点的软件并没有起到任何作用。

如何有效地在开放热点中保护敏感信息成了大多数用户普遍面临的难题，相应防御架构的研究势在必行。

1.2 国内外研究现状

近些年来部分国内外学者在无线网络安全研究领域做出了卓有成效的贡献，可是很多是针对自身热点防止第三方接入窃取内部信息进行的研究，如有学者研究了如何防御无线局域网入侵，建立了一套相关系统^[2]；或者是对当前协议提出改善建议，如有学者提出了 Cookie-Proxy 协议^[3]以改善当前 Cookie 协议安全性的问题；强认证型的 SSL 协议改进与应用^[4] 提出了 SSL 协议中认证部分的改进。但是新的协议意味着消耗大量时间完成普及，对于用户来说真正希望的是能有一个可以立即生效的轻便的保护机制。而 WIFI 大范围普及仅仅是近两年的事，市面上并没有能够给出成熟的防御措施的公司。

第二章：进攻原理介绍

2.1 简单抓包分析

对于连接到热点上的用户，其传输的所有数据包都会经由路由器。恶意热点作为接入者的路由，有权限查看修改任何数据包。而对于自己的数据包是否被查看或修改过用户一无所知。

对经由路由的数据包作简单的过滤筛选就能找出包含关键信息的数据包，这类软件比较出名的包括 WireShark 和 ettercap 等。

但简单抓包带来的收益太过有限，稍有防范意识的网站就不会采用明文传输用户名密码之类的敏感信息。攻击者若想有所收获，必须辅以其他的工具改善抓得数据包的质量。而这些工具中最有效的就是 SSLstrip。

2.2 SSLstrip (http 降级攻击)

SSLstrip 是 Moxie Marlinspike 在 2009 年黑帽子大会上提出的一种信息窃取方式。众所周知我们上网过程普通访问采用较为简单快速而未经加密的 http 协议而只有在涉及重要信息传输时才会才用 https(http secure) 协议。这之间显然存在着过渡机制。过渡机制的技术细节是发送一个重定向包使浏览器重新载入页面并切换至 https 协议。https 协议采用了强劲的 SSL 加密，正面破解希望渺茫。而 SSLstrip 就是利用了这个过渡过程的漏洞，拦截下重定向包，阻止页面向 https 跳转，使用户敏感信息仍旧采用未经加密的 http 协议传输，然后在路由器上抓包分析，获得明文信息。

SSLstrip 的可怕之处在于用户很难察觉，几乎没有用户会特别留意浏览器地址栏里的网址前缀是 http 还是 https。有趣的是这个工具的作者还特意加了几行指令，把网址栏前面的图标换成了一把小黄锁，让人觉得安全放心。

SSLstrip 攻击在钓鱼热点信息窃取中出现频率是绝对的第一。相较与其他攻击，SSLstrip 工具操作简单，获取的信息含金量高。而且最重要的一点是，无论在任何引擎上搜索“钓鱼热点搭建教程”，前几页几乎全部是采用 SSLstrip 抓获某个网站的明文账户密码。

但是比较注重安全的公司已经着手防范 SSLstrip 了，如 Baidu 就在 http 协议下仍旧传输密文。

2.3 SSLsniff（伪造证书攻击）

SSLsniff 利用的漏洞可以说已经被修复了，但采用 SSLsniff 在现在依旧可以发挥作用。SSLsniff 设计的初衷是针对 IE 浏览器对证书检验过程中不检查“Basic Constraint”这个域值^[5]，导致有效但不具有签发能力的证书可以用来签发子证书，攻击者利用子证书和用户建立起 SSL 连接，同时与原网站依旧采用原证书通信，合法且域名一致的证书会使用户的浏览器相信攻击者就是要找的服务器，而攻击者可以利用手里的子证书解密消息，同时把消息用原证书加密后与服务器通信，既不影响用户正常上网，同时记录下了用户的敏感信息。

IE 在发现后很快修复了这个漏洞，于是现在采用这种攻击方式浏览器会告知用户当前访问页面证书无效。虽然会提示证书无效，但用户是拥有选择是否相信的权力的，而证书无效的例子还是很常见的，比如火车票售卖官网 12306 的购买页面就有着无效的证书，需要用户自行下载安装根证书。用户在平常习惯了证书无效的提示可能会导致警惕性下降，一不留神就可能被 SSLsniff 窃取信息。

这个工具证书会报错这一点会让有心的用户提高警惕，现在使用起来还要选择证书进行签发，可以说是一个有价值的工具，但比 SSLstrip 逊色许多。

2.4 重定向和钓鱼页面

分为 DNS 重定向和 IP 重定向。

IP 重定向很简单，Linux 防火墙就能够做到，即在目标 IP 吻合时修改 IP 为某指定值，使访问走向另一个页面。只需要短短几条 iptables 指令。

DNS 重定向就麻烦很多，搭建热点一般都使用 DNSchef 将 DNS 解析工作转发到别的公共服务器上，想要在域名解析这一步动手脚只能自己搭建 DNS 服务器。

IP 重定向和 DNS 重定向的目的都是让用户在访问某个特定页面时跳转到攻击者指定的页面。攻击者往往会制造一个与原来页面非常相近的钓鱼页面以骗取用户输入帐户名和密码。

IP 重定向使用起来很吃力，原因在于如今的网站大多有不只一个 IP 地址，很难确定到底会访问哪个，而且 IP 重定向后用户是可以看到当前访问页面的域名的，攻击者不可能申请到一个相同的域名。相比之下 DNS 重定向实现起来虽然麻烦，但效果比 IP 重定向好很多。DNS 重定向是将域名解析到一个攻击者指定的 IP 上，任凭一个域名有多少 IP 都难逃魔爪。同时由于是在解析过程动手脚，用户要访问的域名是不会变化的，就是说再细心的用户也无法从地址栏里看出端倪来。检验的唯一方法就是 ping 出这个网站的 IP。但这又面临一个问题，之前提到过一个网站有多个 IP，很难获取全部的 IP 加以对比。

鉴于钓鱼页面可以和原网页做的一模一样，用户几乎没有自行察觉的可能。而且虚假网页手法花样繁多，比如用户输完信息后提示错误然后跳转回真实页面，用户重输一次后就能继续在真实的网站上继续访问，这个时候几乎所有的用户都会怀疑自己第一遍输错了，殊不知第一遍是被假页面记录了下来然后才来到真页面。

2.5 Drift-net 记录图片

图片加密的成本较高因而传输过程中往往不加密，攻击者可以轻易浏览保存用户传输的图片。虽然不会涉及到财产上的威胁，但会给用户隐私上带来不小的困扰。

图片截获的实现过程很简单主要依靠一个叫 Drift-net 的小工具。能够以图片流的形式展示当前流经热点的未加密图片，攻击者可以选择性保存。

第三章：攻击成果展示

3.1 单纯抓包

单纯抓包可以拿到一些安全性较差的网站的信息，比如下图依次是综合教务系统学生登陆口、未勾选 SSL 安全登录的 USTCmail 以及某小众邮箱：

```

Terminal
File Edit View Search Terminal Help

CONTENT: ce=false&sendMailWithSms=false&sendMailWithSmsMode=&smimeEncrypt=false&smimeSign=false&showOneRcpt=false&autosaveHitCounter=false&account=doubihj%40mail.ustc.edu.cn&to=%22JERRY%22+%3C569389540%40qq.com%3E&smsAddress=&cc=&bcc=&subject=Re%3A+%E6%B5%8B%E8%AF%95&btnAddAttach=0&btnCreateImg=0&signSet=-1&chkSaveToSent=on&year=2016&month=7&day=10&hour=16&compinfo_minute=37

HTTP : 218.104.71.173:80 -> USER: PASS: 10 INFO: http://mis.teach.ustc.edu.cn/userinit.do
CONTENT: userbz=s&hidjym=&userCode=pb14210&passWord=10&check=tl63

HTTP : 222.222.32.84:80 -> USER: jackwifitest PASS: yhj123123 INFO: http://vipmail.hebei.com.cn/web2/login_template/18.html
CONTENT: username=jackwifitest&mail_domain=vip.hebei.com.cn&password=yhj123123&verifynum_option=no&free_vip=vip&lang=gb

HTTP : 220.181.7.225:80 -> USER: nidaye733 PASS: 685943b0f6656d8fd12536effd1c5cb410d0d17aabc5939ae063f2bdce4b7e01e08758db7dcb775594746c7c4819d9eacaf3a3d412633af869f15e18b2ecc4558adc70f8f1fef84ae356b786f5dcd13fb089f7096cf2b849af04e6f6c7c20f76f6e5245fb8d6931e6f8ceff24cd9ccd5ca279c9c3ce3ecd97515b95402f41bf6 INFO: http://tieba.baidu.com/?page=user
CONTENT: hone=0&safeFlag=0&u=http%3A%252F%252Ftieba.baidu.com%252F%3Fpage%253Duser%2526task%253DloginLayer%2526locate%253Dfooter_login&subpro=tbwap&staticPage=http%3A%252F%252Ftieba.baidu.com%252Ftb%252Fmobile%252Fsglob

```

注意上图亮条下方为百度，密码是经过加密处理的

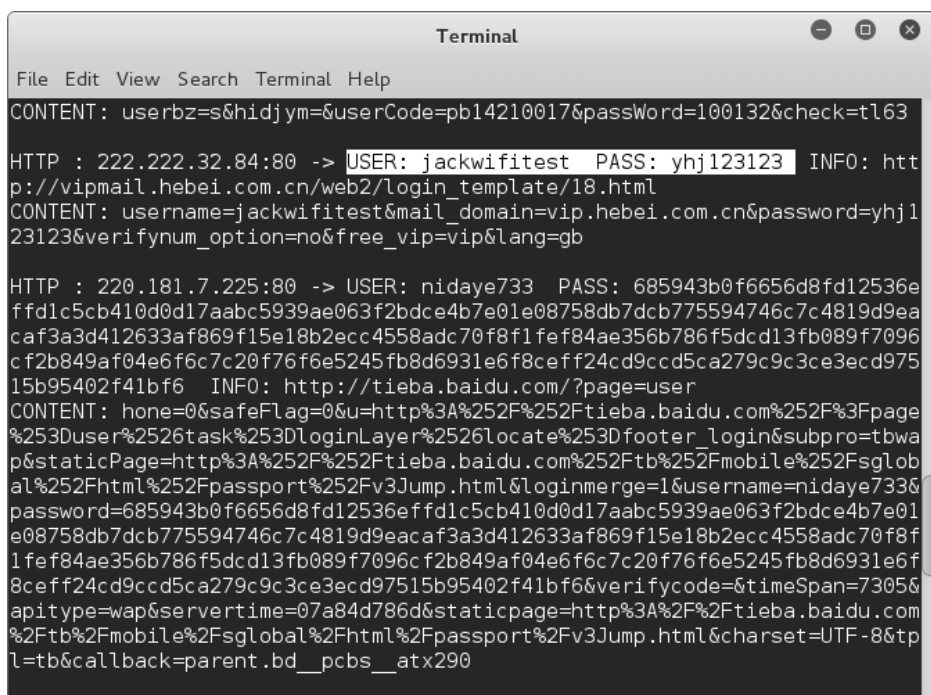
```

Terminal
File Edit View Search Terminal Help

HTTP : 220.181.7.225:80 -> USER: nidaye733 PASS: 2fd76537704a3f7f4ea689c3e56f4f102195236c36ba35e77e65ab6ce49726fdc8b6d960e6a178f7b22ba26d2d957a18611d0b8096dce0791210a011f201836458a1583989978bd97e5dff38193d9d8eb57a178d22d6a61b0aec531226e98454c30f7aee97ff8aca2b73ac616c11e9aea31f09757934dbbffa4e6d116fe09bc INFO: http://tieba.baidu.com/?page=user
CONTENT: hone=0&safeFlag=0&u=http%3A%252F%252Ftieba.baidu.com%252F%3Fpage%253Duser%2526task%253DloginLayer%2526locate%253Dfooter_login&subpro=tbwap&staticPage=http%3A%252F%252Ftieba.baidu.com%252Ftb%252Fmobile%252Fsglobal%252Fhtml%252Fpassport%252Fv3Jump.html&loginmerge=1&vcodestr=tcG1706e2935f21e2df029414d7de013338d56c980650037b8b&username=nidaye733&password=2fd76537704a3f7f4ea689c3e56f4f102195236c36ba35e77e65ab6ce49726fdc8b6d960e6a178f7b22ba26d2d957a18611d0b8096dce0791210a011f201836458a1583989978bd97e5dff38193d9d8eb57a178d22d6a61b0aec531226e98454c30f7aee97ff8aca2b73ac616c11e9aea31f09757934dbbffa4e6d116fe09bc&verifycode=0256&timeSpan=25078&apitype=wap&servvertime=dfb25115d5&staticpage=http%3A%2F%2Ftieba.baidu.com%2Ftb%2Fmobile%2Fsglobal%2Fhtml%2Fpassport%2Fv3Jump.html&charset=UTF-8&tpl=tb&callback=parent.bd_pcbs__3tsvmy

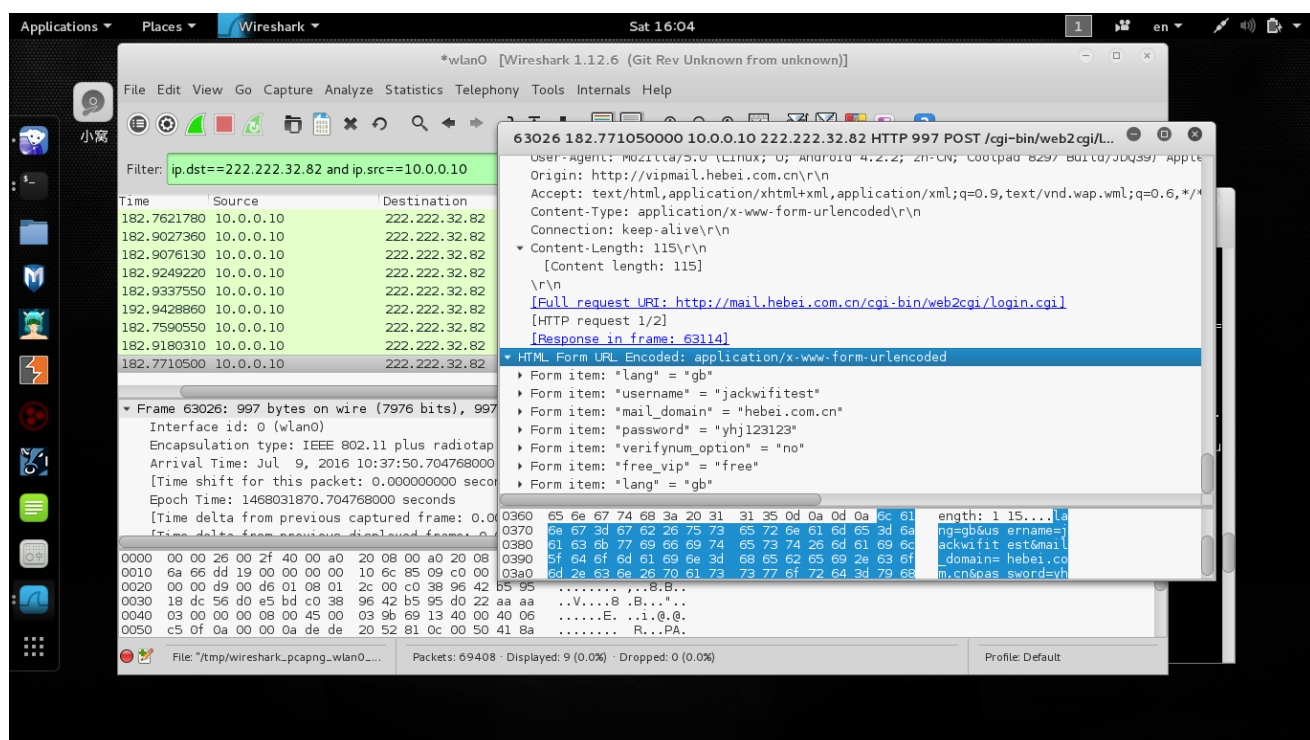
HTTP : 202.141.160.8:80 -> USER: do PASS: 70 INFO: http://email.ustc.edu.cn/coremail/index.jsp?nodetect=true
CONTENT: locale=zh_CN&uid=doubihj&nodetect=true&domain=mail.ustc.edu.cn&password=707196&action%3Alogin=

```



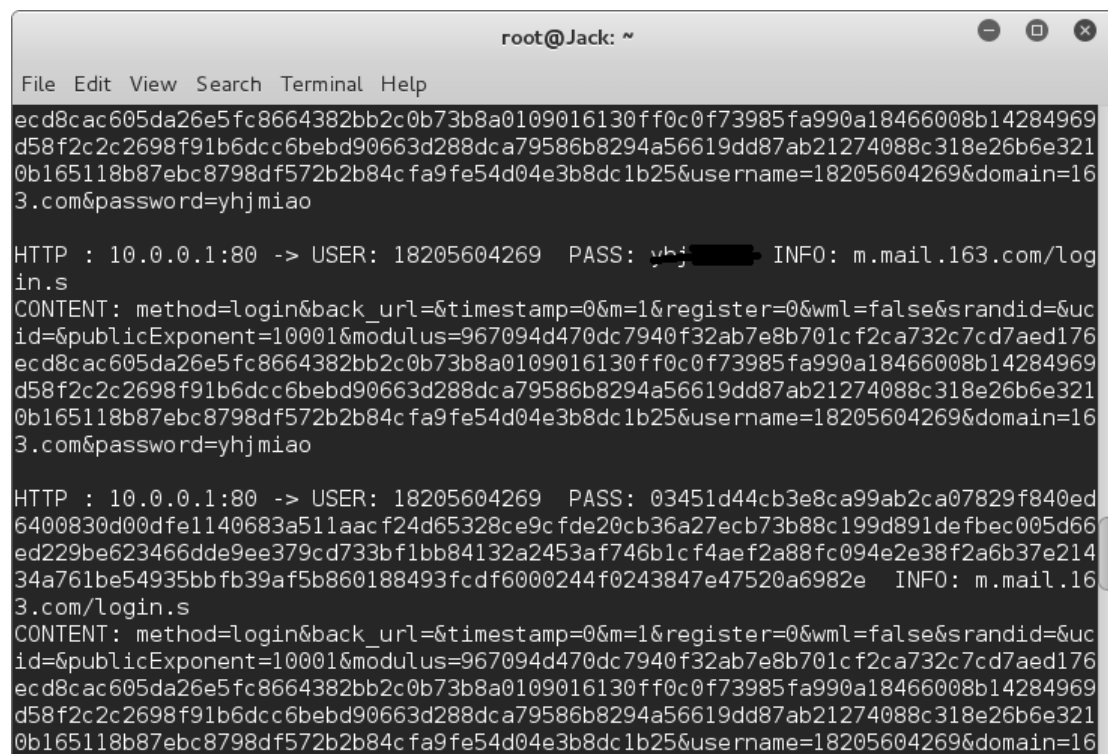
```
Terminal
File Edit View Search Terminal Help
CONTENT: userbz=s&hidjym=&userCode=pb14210017&passWord=100132&check=tl63
HTTP : 222.222.32.84:80 -> USER: jackwifitest PASS: yhj123123 INFO: http://vipmail.hebei.com.cn/web2/login_template/18.html
CONTENT: username=jackwifitest&mail_domain=vip.hebei.com.cn&password=yhj123123&verifynum_option=no&free_vip=vip&lang=gb
HTTP : 220.181.7.225:80 -> USER: nidaye733 PASS: 685943b0f6656d8fd12536effd1c5cb410d0d17aabc5939ae063f2bdce4b7e01e08758db7dcb775594746c7c4819d9eacaf3a3d412633af869f15e18b2ecc4558adc70f8f1fef84ae356b786f5dcd13fb089f7096c2b849af04e6f6c7c20f76f6e5245fb8d6931e6f8ceff24cd9cccd5ca279c9c3ce3ecd97515b95402f41bf6 INFO: http://tieba.baidu.com/?page=user
password=685943b0f6656d8fd12536effd1c5cb410d0d17aabc5939ae063f2bdce4b7e01e08758db7dcb775594746c7c4819d9eacaf3a3d412633af869f15e18b2ecc4558adc70f8f1fef84ae356b786f5dcd13fb089f7096c2b849af04e6f6c7c20f76f6e5245fb8d6931e6f8ceff24cd9cccd5ca279c9c3ce3ecd97515b95402f41bf6&verifycode=&timeSpan=7305&apitype=wap&servertime=07a84d786d&staticpage=http%3A%2F%2Ftieba.baidu.com%2Ftb%2Fmobile%2Fglobal%2Fhtml%2Fpassport%2Fv3Jump.html&charset=UTF-8&tpl=tb&callback=parent.bd__pcbs__atx290
```

上文中使用的过滤工具是 ettercap，能自动且有效地滤出包含用户名密码信息的包，相比之下 Wireshark 虽然有更强大的自定义过滤功能，但操作繁琐，很难滤出想要的东西，下面是 Wireshark 中找到需要信息的图：



3.2 SSLstrip+抓包

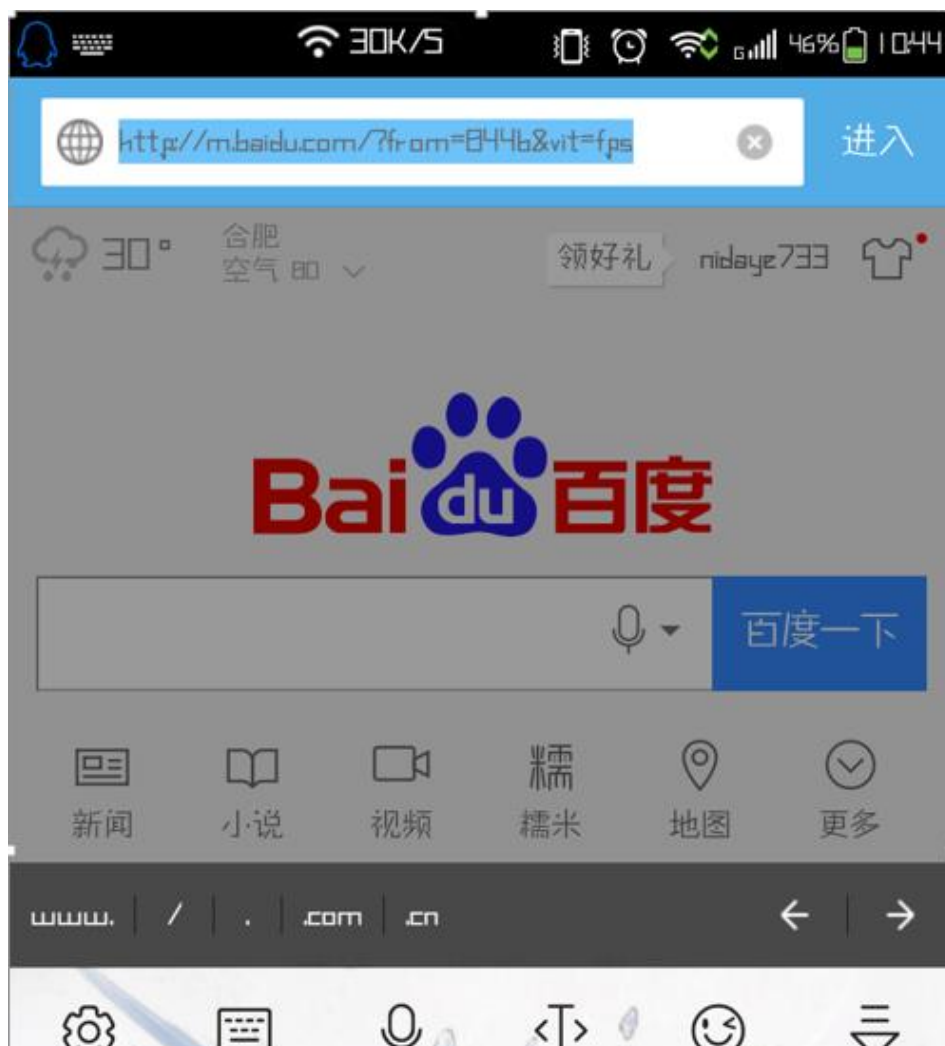
SSLstrip 攻击后可以获得大多数网站的明文帐户密码，如下图为截获的网易邮箱的帐户名密码：



观察可以看出地址栏前缀的变化，下图为正常访问时的地址栏：



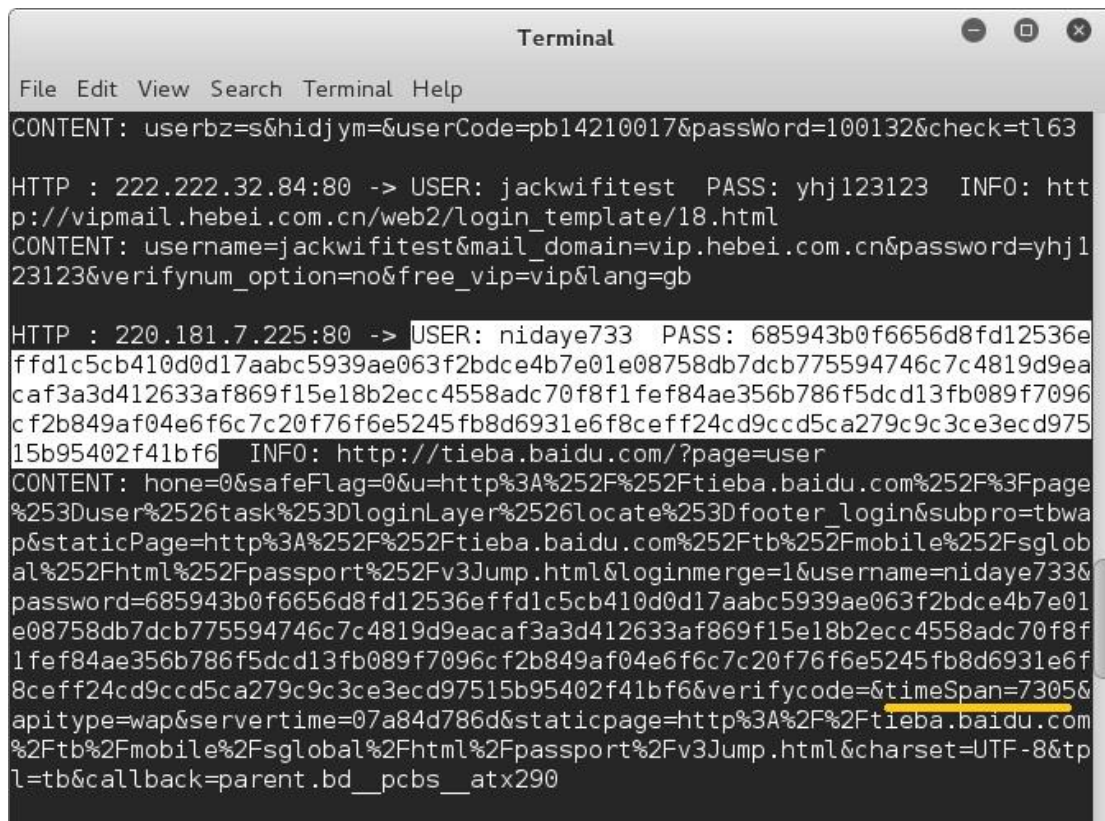
下图为经过 SSLstrip 攻击后的访问：



在这里值得一提的是百度的安全措施，无论是否是使用 SSLstrip 百度账号的密码都是密文，且多次抓出对应相同密码的密文均不相同，SSL 里有多种加密方式容易理解为何密文不同，http 协议下为什么每次都不一样？观察到抓出的包中有 timespan 一项，利用 timespan 作密钥加密密码就能做到每次抓得的均不相同。就算只是使用古典加密方式黑客也很难会有耐心去思考如何破解，毕竟恶意热点的建立者心态普遍是广撒网。

通过这些百度也在安全上给其他网站做出了良好示范，在这个计算机性能飞快的时代，少量的延迟可以极大地提高安全性。考虑到 SSLstrip 攻击，网站对于敏感信息即使是 http 下也应有加密举措。

下图为 SSLstrip 下抓得百度账号的数据包：



```
Terminal
File Edit View Search Terminal Help

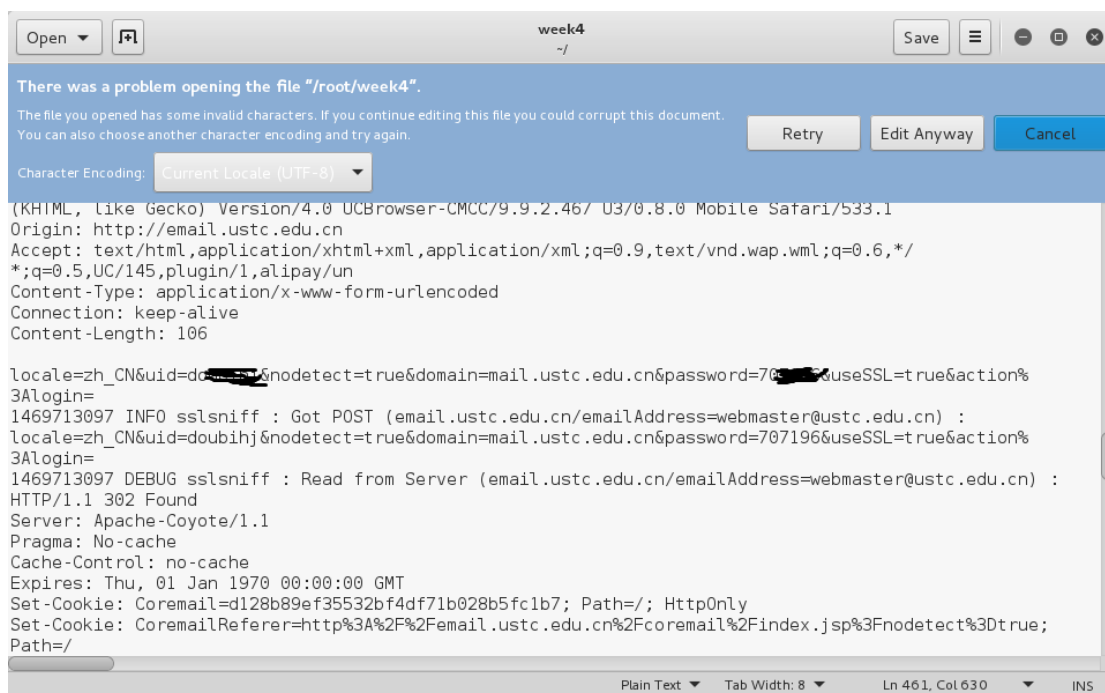
CONTENT: userbz=s&hidjym=&userCode=pb14210017&passWord=100132&check=tl63

HTTP : 222.222.32.84:80 -> USER: jackwifitest PASS: yhj123123 INFO: http://vipmail.hebei.com.cn/web2/login_template/18.html
CONTENT: username=jackwifitest&mail_domain=vip.hebei.com.cn&password=yhj123123&verifynum_option=no&free_vip=vip&lang=gb

HTTP : 220.181.7.225:80 -> USER: nidaye733 PASS: 685943b0f6656d8fd12536effd1c5cb410d0d17aabc5939ae063f2bdce4b7e01e08758db7dcb775594746c7c4819d9eacaf3a3d412633af869f15e18b2ecc4558adc70f8f1fef84ae356b786f5dc13fb089f7096cf2b849af04e6f6c7c20f76f6e5245fb8d6931e6f8ceff24cd9ccd5ca279c9c3ce3ecd97515b95402f41bf6 INFO: http://tieba.baidu.com/?page=user
CONTENT: hone=0&safeFlag=0&u=http%3A%252F%252Ftieba.baidu.com%252F%3Fpage%253Duser%2526task%253DloginLayer%2526locate%253Dfooter_login&subpro=tbwap&staticPage=http%3A%252F%252Ftieba.baidu.com%252Ftb%252Fmobile%252Fsglobal%252Fhtml%252Fpassport%252Fv3Jump.html&loginmerge=1&username=nidaye733&password=685943b0f6656d8fd12536effd1c5cb410d0d17aabc5939ae063f2bdce4b7e01e08758db7dcb775594746c7c4819d9eacaf3a3d412633af869f15e18b2ecc4558adc70f8f1fef84ae356b786f5dc13fb089f7096cf2b849af04e6f6c7c20f76f6e5245fb8d6931e6f8ceff24cd9ccd5ca279c9c3ce3ecd97515b95402f41bf6&verifycode=&timeSpan=7305&apitype=wap&servertime=07a84d786d&staticpage=http%3A%2F%2Ftieba.baidu.com%2Ftb%2Fmobile%2Fsglobal%2Fhtml%2Fpassport%2Fv3Jump.html&charset=UTF-8&tpl=tb&callback=parent.bd__pcbs__atx290
```

3.3 SSLsniff

SSLsniff 的测试对象是勾选了 SSL 安全登录的 USTCmail，效果如下：



```
Open [icon] week4 ~/ Save [icon] [icon] [icon] [icon]

There was a problem opening the file "/root/week4".
The file you opened has some invalid characters. If you continue editing this file you could corrupt this document.
You can also choose another character encoding and try again.
Character Encoding: Current Locale (UTF-8) [dropdown] [button] [button] [button]

(KHTML, like Gecko) Version/4.0 UCBrowser-CMCC/9.9.2.46/ U3/0.8.0 Mobile Safari/533.1
Origin: http://email.ustc.edu.cn
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,text/vnd.wap.wml;q=0.6,*/
;q=0.5,UC/145,plugin/1,alipay/un
Content-Type: application/x-www-form-urlencoded
Connection: keep-alive
Content-Length: 106

locale=zh_CN&uid=do[redacted]&nodetect=true&domain=mail.ustc.edu.cn&password=70[redacted]&useSSL=true&action%
3Alogin=
1469713097 INFO sslsniff : Got POST (email.ustc.edu.cn/emailAddress=webmaster@ustc.edu.cn) :
locale=zh_CN&uid=doubihj&nodetect=true&domain=mail.ustc.edu.cn&password=707196&useSSL=true&action%
3Alogin=
1469713097 DEBUG sslsniff : Read from Server (email.ustc.edu.cn/emailAddress=webmaster@ustc.edu.cn) :
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Pragma: No-cache
Cache-Control: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Set-Cookie: Coremail=d128b89ef35532bf4df71b028b5fclb7; Path=/; HttpOnly
Set-Cookie: CoremailReferer=http%3A%2F%2Femail.ustc.edu.cn%2Fcoremail%2Findex.jsp%3Fnodetect%3Dtrue;
Path=/

Plain Text Tab Width: 8 Ln 461, Col 630 INS
```


我们可以明显看出攻击过程生成的文档之大，从中找到有效的信息很花功夫，因为 SSLsniff 这个工具在攻击过程中是进行无差别记录的。

下图是访问时会提示的证书错误：



! 网站安全证书已过期或不可信
是否继续浏览

否，返回之前页面

是，继续浏览本网站（不推荐）

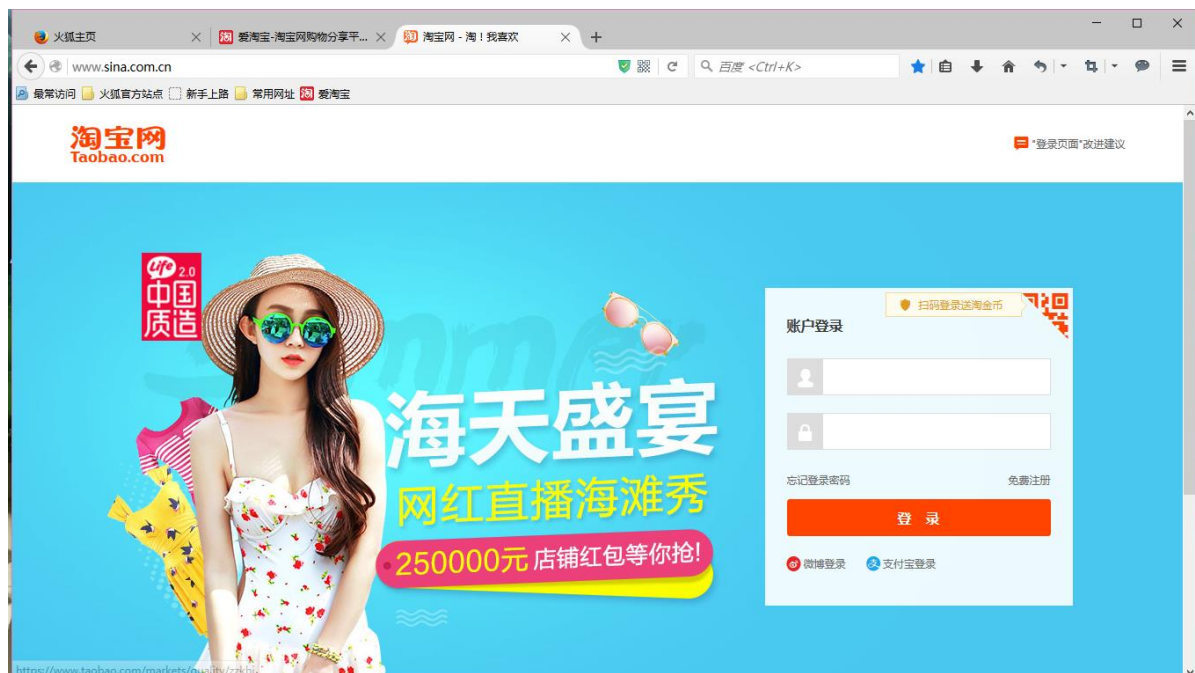


3.4 DNS 劫持+钓鱼页面

这里搭建 DNS 服务器时使用了 metasploit 中 auxiliary 功能里的 fakedns 模块，劫持目标为 www.taobao.com，反应如下：

```
Terminal
File Edit View Search Terminal Help
[*] 10.0.0.10:55411 - DNS - DNS bypass domain m.weibo.cn found; Returning real A records for m.weibo.cn
[*] 10.0.0.10:55411 - DNS - XID 55286 (IN::A m.weibo.cn)
[*] 10.0.0.10:38404 - DNS - DNS bypass domain apilocate.amap.com found; Returning real A records for apilocate.amap.com
[*] 10.0.0.10:38404 - DNS - XID 40452 (IN::A apilocate.amap.com)
[*] 10.0.0.10:38597 - DNS - DNS bypass domain ssl.baidu.com found; Returning real A records for ssl.baidu.com
[*] 10.0.0.10:38597 - DNS - XID 11338 (IN::A ssl.baidu.com)
[*] 10.0.0.10:3471 - DNS - DNS bypass domain restapi.amap.com found; Returning real A records for restapi.amap.com
[*] 10.0.0.10:3471 - DNS - XID 50987 (IN::A restapi.amap.com)
[*] 10.0.0.10:45881 - DNS - DNS target domain www.taobao.com found; Returning fake A records for www.taobao.com
[*] 10.0.0.10:45881 - DNS - XID 54899 (IN::A www.taobao.com)
[*] 10.0.0.10:62346 - DNS - DNS bypass domain log.mmstat.com found; Returning real A records for log.mmstat.com
[*] 10.0.0.10:62346 - DNS - XID 64152 (IN::A log.mmstat.com)
[*] 10.0.0.10:48091 - DNS - DNS bypass domain ynuof.alipay.com found; Returning real A records for ynuof.alipay.com
[*] 10.0.0.10:48091 - DNS - XID 26327 (IN::A ynuof.alipay.com)
[*] 10.0.0.10:13366 - DNS - DNS bypass domain qrlogin.taobao.com found; Returning real A records for qrlogin.taobao.com
[*] 10.0.0.10:13366 - DNS - XID 16121 (IN::A qrlogin.taobao.com)
[*] 10.0.0.10:56178 - DNS - DNS bypass domain img.alicdn.com found; Returning real A records for img.alicdn.com
[*] 10.0.0.10:56178 - DNS - XID 10955 (IN::A img.alicdn.com)
[*] 10.0.0.10:54078 - DNS - DNS bypass domain coolpush.coolyun.com found; Returning real A records for coolpush.coolyun.com
[*] 10.0.0.10:54078 - DNS - XID 4259 (IN::A coolpush.coolyun.com)
msf auxiliary(fakedns) >
```

我们可以看到淘宝的跳转是被伪造的。测试过程中页面的伪造使用了社会工程套件 social-engineer-toolkit 里的 sitecloner。由于制作的页面完全看不出差别，同时 dns 劫持不会改变用户要前往的域名。为了展示效果这里展示访问 sina 时被劫持到淘宝：



可以想象在访问淘宝时被劫持是否可能会有用户察觉。

测试结果展示：

```
root@Jack: ~/social-engineer-toolkit
File Edit View Search Terminal Help
[*] All fields captures will be displayed below.
[Credential Harvester is now listening below...]

('Array\n',)
('(\n',)
('    [TPL_username] => wifitest\n',)
('    [TPL_password] => 2333333333\n',)
('    [ncoSig] => \n',)
('    [ncoSessionid] => \n',)
('    [ncoToken] => b03509ece07fe539791bbd63e6f76f76fef04bb8\n',)
('    [slideCodeShow] => false\n',)
('    [loginsite] => 0\n',)
('    [newlogin] => \n',)
('    [TPL_redirect_url] => http://i.tao\n',)
('    [from] => taobaoindex\n',)
('    [fc] => default\n',)
('    [style] => \n',)
('    [css_style] => \n',)
('    [keyLogin] => false\n',)
('    [qrLogin] => true\n',)
('    [newMini] => false\n',)
('    [newMini2] => false\n',)
('    [tid] => \n',)
```

第四章：防御架构

4.1 防御架构基本思想

经过进攻结果展示和进攻原理分析，注意到最有效且隐蔽的攻击方式是 SSLstrip，除了地址栏前缀外没有别的影响，捕获的信息含金量高；其次是 DNS 劫持至钓鱼页面，制作精细的钓鱼页面加上完美的地址栏是无法仅凭观察识别的。

从使用普及率上 SSLstrip 同样是最高的，铺天盖地的关于 SSLstrip 的教程，加上工具的质量之高，适用对象之广，对于抱着广撒网心态的恶意热点搭建者来说，SSLstrip 必然会被使用。由于攻击者往往是一台 PC 作业，且很少有攻击者有自己的合法服务器，就算有也往往不敢在其上搭钓鱼页面，所以钓鱼页面一般只有某一个且搭建在路由上。

对于 SSLsniff 由于存在证书报错机制，与上述攻击相比隐蔽性会逊色很多。而且使用 SSLsniff 抓信息没有筛选功能，很有可能抓到敏感信息却筛选不出来。再有就是 SSLsniff 和 SSLstrip 是不能同时工作的，所与防御的重点不放在这里。

于是防御的重心就放在 SSLstrip 和 DNS 劫持到钓鱼页面上。

由于进行联网操作时热点拥有非常大的权限，客户端难以知道数据包是否被查看或拦截，识别工作在当前网络下进行很困难，但如今手机都可以通过数据流量上网，这为我们提供了一条安全便捷的数据通道，我们可以一少部分流量为代价保证重要信息传输的安全。在此提出双网路模块，实现方法在下文介绍。

热点搭建钓鱼页面使用的服务器往往就在路由上，也就是说我们访问遭到劫持后是瞬间就到达了钓鱼页面，没有经过任何跳转。这里介绍 TTL 的概念。TTL (time to live) 是 IPv4 包头的一个 8 bit 字段，表示当前数据包还能在网络上进行多少次转发，每进行一次转发该值会-1，减到零后路由器将会丢弃 IP 包并向 IP 包的发送者发送 ICMP time exceeded 消息。目的是防止一个到不了目的地的数据包在网络上无限次被转发。TTL 手机默认初始值为 64，访问正常页面后往往会得到 TTL 值为 20~50 的数据包。而对于搭建在路由器上的钓鱼

页面，访问的到的数据包 TTL 值不会减少。这在正常上网过程中几乎没有可能发生。因此提出 TTL 检测，实现方法下文介绍。

由于绝大部分时间我们连接的热点都是有安全保障的，防御机构可以在平时完成一些信息的采集形成配置文件（比如常访问的那些网站会 http→https 的跳转），通过对比历史信息给当前 WIFI 做出评估。这是 https 库的基本想法。

同时作为一个防御架构，我们不能只考虑大多数情况，对于钓鱼页面，如果攻击者有所准备提前将 TTL 值减至正常值，或是将钓鱼页面搭建在一个正常合法的服务器上，或是有一组钓鱼页面相互之间的链接不需要 DNS 劫持就能合法跳转，这时防御架构就很难发挥功效。而且单纯检测是否被劫持是非常困难的。这时也是有防御措施的，可以开启双网路确保 DNS 无法劫持，预置多数涉及财产的网页加上用户自定义一些认为重要的页面，在访问这些页面时给予提示，最大程度保证用户进行此类重要访问的安全。这是重要域名库的基本思想。

4.2 双网路的实现方法

鉴于当前市面上 android 智能机占比重最大，所以本文针对的均是 android 手机端的检测防护。

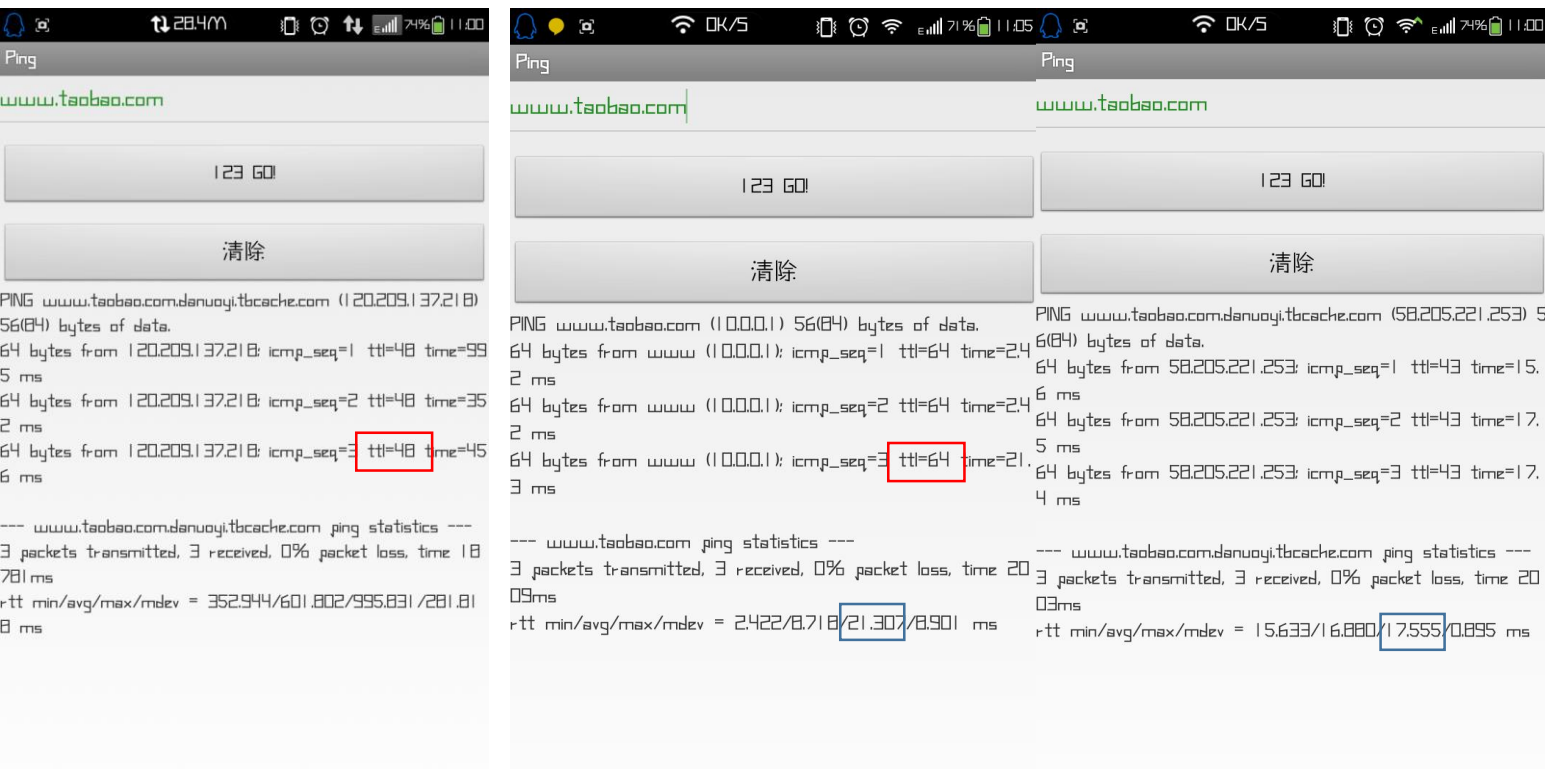
安卓手机设计时考虑到省电，默认连接 WIFI 后断开流量连接，。所以两种连接之间切换存在重新开启耗时的问题，切换过程往往需要 5~6 秒的时间。就用户体验来说切换网路是一个麻烦的事情。而我们之前已经说过数据流量在防止 SSLstrip 抓包上能发挥奇效，而且只是登录过程采用数据流量的话消耗也会很小。在传输无关紧要但量大的信息（如观看视频等）时再切回热点，继续蹭热点，这显然是最好的公众热点上网方式。然而正是因为那 5~6 秒来回切换的等待时间，加上认为自己不会碰到钓鱼热点的心理，很多公众才会遭了 SSLstrip 攻击者毒手。这里希望能够开发一个小工具，保持流量和热点双 IP 双连接同时存在，跳过重新开启的过程，用户可以通过屏幕上的悬浮窗实现一键迅速切换数据通道。

众所周知 android 系统采用的是 Linux 内核，而 Linux 系统是允许上述双 IP 双网路存在的，android 框架层存在热点连接后断开流量的机制。且有专利

提供了安卓双网路的实现方法^[6]，做法是屏蔽安卓原拨号驱动后重新编写程序实现拨号上网。

4.3 TTL 检测

下面给出正常页面访问和搭在热点服务器上页面访问 ping 结果的差别



中图的 TTL 值正如上文所说不会减少，这说明了 TTL 检测的可行性。

由左中两图我们同样可以看出 ping 出的时间差别也很大，搭在服务器上的连接起来时间远短于真实网站，是否可以以 ping 得时间来判别钓鱼页面呢？

观察到访问搭建在热点上的页面最常访问时间达到 21.3ms，而走正常 WIFI 访问真页面（右图）时 ping 出的时间则有 17.5ms 的，显然通过时间检测行不通。

TTL 检测可基于 popen() 函数来实现。popen() 函数用于 shell 执行命令的返回结果，我们可以利用 ping 来返回出 TTL 值以供检测。

4.4 https 库、重要域名库和 MAC 库

有了前述的 TTL 检测和双网路防护，用户已经有能力检测抵御绝大多数的攻击，而且上面的两种工具都是非常轻便简洁的。这里将提出 https 库和重要域名库两个相较之下略显臃肿的防御手段，用于针对一些非常的攻击者。

如果说攻击者拥有自己的合法服务器，并在服务器上搭好了一组可以互相合法访问的钓鱼页面，然后在某一个非登录页面处先劫持到钓鱼页面组中的一个。这时由于并不是登陆页面，用户不会选择开启双网路。当用户已经处在虚假页面中，虚假页面里的链接指向钓鱼页面，则此时开启双网路也无济于事，因为这个时候的访问过程是合法的。整个过程 TTL 检测都不可能报错，因为页面没有搭在热点上。

重要页面库的想法来自于 360 安全卫士在电脑用户访问淘宝时提示访问的是淘宝网的做法。当用户从某个虚假页面去访问某个登陆页面时，会开启双网路，这时不存在被 DNS 劫持的可能，所以抵达的页面域名不可能有假，但鉴于钓鱼页面的网址可以与真实网站很相似（如 icbc 和 lcbc），用户是很难分辨的，需要我们给予提示。这里的做法是提前将主流购物网站和银行网站网址置入库中，访问时域名正确提示用户访问到的是正确网站。同时提供给用户自定义库的功能，使用户在访问一些自己认为重要的网站时也能得到提醒。

或者说用户并不能做到每次都在合适时机开启双网路，这时需要有有效的 SSLstrip 检测机制。

https 库的做法是创建一个关于网址的数据库，记录下所有访问到的 https 页面。客户端随时监测浏览器的网址，发现当前网址存在于 https 库中而当下前缀是 http 时给予用户警告当前点存在攻击行为，提示用户开启双网路。参考了 HTTPS 协议中间人攻击的实现与防御^[7] 中的 History-proxy 思想，依据历史信息来给予用户识别能力。

https 库的思想在现实中已经有人着手实现，IETE 近年推出的 HSTS 项目即使得用户在一次使用 https 与某网站传输信息后，接下来的一年内都只会用 https 与之传输内容，且该服务器的证书无效时用户无法忽略警告进行访问。这将有效抵抗 SSLstrip 和 SSLsniff 的攻击。

但这些数据库的做法毕竟只是补充用，真正开发过程追求轻量和用户体验的话是可以把这两个库暂时放在一边的。

MAC 库用来记录被检验出来的恶意热点 MAC，用户连接热点后可进行 MAC 对比观察是否是曾被查出的恶意热点。这个库优点是攻击者不知道自己被拉入了某个黑名单，一次成功的查处可以给很多人便利；缺点是 MAC 修改很简单，攻击者一旦发觉可以轻易完成 MAC 变更。

4.5 被放弃的一些防御思路 and 原因简介

4.5.1 IP 库

考虑构建一个巨大的数据库存放所有网页对应的全部 IP，这样可以有效防御 DNS 重定向。

放弃原因是一个页面可以有太多 IP，而且就算费尽周折建好后也只能对付 DNS 重定向，对于 IP 重定向就毫无办法。

The screenshot displays a web application interface for IP lookup. The top navigation bar includes links for 'IP查询', 'IP批量查询', 'IP所在地批量查询', and '同IP网站查询'. The main input field contains 'www.bilibili.com'. Below the input, a table titled 'IP/域名www.bilibili.com的信息' shows the following data:

域名/IP	获取的IP地址	数字地址
www.bilibili.com	183.61.9.45	3074230573
www.bilibili.com	113.105.152.207	1902745807
www.bilibili.com	183.2.232.8	3070421000

Below the table, there is a section for '最近查询' (Recent queries) listing 'runddl.meibu.com', 'girlsoftball.com', 'skinsharp.cn', and '684w'. At the bottom, there is a code snippet for embedding the IP lookup results on a website.

On the right side of the screenshot, a Windows command prompt window is open, showing the execution of the command 'ping www.bilibili.com'. The output displays the IP address 223.93.140.66 and the results of four ping attempts, including response times and TTL values.

4.5.2 识别敏感页面后自动完成双网路切换

敏感页面的识别一直是个难题，网页的编写里没有固定的关键字来代表用户名栏和密码栏，关键字识别也没有用。这里进行了少量测试，测试结果：

关键字	登陆页面	任意非登录页面
登录	7/7	3/3
Login	7/7	3/3
Username	3/7	1/3
Password	4/7	1/3
用户名	1/7	1/3
密码	4/7	1/3

出现这样情况的原因有二：

1. 登陆页面没什么特别共有的特征，很多的用户名密码框都是加载的 script 来提高安全性。
2. 现在基本是个网站都有办法登录的，而且都是放在某个角落里点击登录，不影响用户正常浏览网页，这就是为什么我找的非登录页面里也会找到这些关键字。用户也很少会有除几个主流页面外的账户。

于是决定将网路切换权交给用户。

4.5.3 基于时序完成 SSLsniff 检测

这是从安全套接层中间人攻击与防护研究^[8]中看到的方法，文中提到 SSLsniff 攻击会在数量级上影响访问页面所需时间。本文同样进行了测试，但结果大相径庭，测得结果访问时间没有很大差别。

类型	n	均值	标准差
无中间人（文）	100	0.0273	0.0144
有中间人（文）	100	0.3643	0.3711
无中间人（测）	20	0.0244	0.0108
有中间人（测）	20	0.0213	0.0107

认为可能的原因如下：

1. 套件版本问题，我用的是最新的 sslsniff 工具，论文是 2013 年写的，可能这几年的更新把时间消耗这个问题给修复了。
2. 论文作者就没用套件，因为我使用的过程中根本不存在是否要解密后再加密，可能是作者自己写的代码，效率不如我下载的套件。

第五章：总结和未来工作展望

本文测试了恶意热点可能采用的各种攻击方式，分析了各种攻击方式的特点和局限性。在此基础上有针对性的提出了一套防御体系，采用一些现有的技术手段而不是提出一个新的协议来保障用户安全。但限于工作时间和开发经验并没有将这个系统全部实现，今后可以逐步实现这些设计。此外技术是在不断进步的，安全永远是相对的，只又不断改进自身才能适应需求。今后作者还会持续关注无线攻防技术动态，为网络安全事业献出自己的绵薄之力。

附录

参考文献:

- [1] 2014 年中国手机使用状况报告 360 互联网安全中心
- [2] 雷阳.基于无线入侵防御系统的中间人攻击 检测功能的设计与实现[D].华中科技大学,2014.
- [3],[7],[8]赵森栋.安全套接层中间人攻击与防护研究[D].哈尔滨工程大学,2013.
- [4] 李兴辉.强认证型的 SSL 协议改进与应用[D].重庆邮电大学,2012.
- [5] Callegati F, Cerroni W, Ramilli M. Man-in-the-Middle Attack to the HTTPS Protocol [J]. Security Privacy. 2009, 7(1):78-81
- [6] 基于安卓系统的多网络并用方法和系统,专利号 CN105357373A