基于个人移动端的 SSL 协议安全技术与教学应用

李明坤[1],胡曦明[1,2*],李 鹏[1,2]
(1. 陕西师范大学 计算机科学学院,陕西 西安 710119;
2. 现代教学技术教育部重点实验室,陕西 西安 710119)

摘 要:随着以个人移动端为支点的移动新经济飞速发展,作为网络安全服务核心的 SSL 协议面临更加严峻的安全威胁,移动互联网产教协同发展迫切需要 SSL 协议个人移动端安全技术创新。以此为牵引,首先深入分析 SSL 协议体系结构和安全机制,在此基础上提出了真实网络环境下基于手机、笔记本电脑和 PAD 等个人移动端的 SSL 协议安全技术总体架构并详细说明了技术环节和个人移动端配置方法等关键技术,进而实现了移动互联网络下 SSL 协议 X.509 证书伪造和链接跳转篡改的攻击,详细阐述了攻击原理、实现流程、关键操作与配置以及数据测量与可视化分析等具体环节。疫情期间的在线实验应用表明,该技术可有效支持居家学习环境下“停课不停练”,为网络安全技术创新开拓实践新途径。

关键词:个人移动端;安全套接字层协议;安全技术;网络安全;教学应用
中图分类号:TP393 **文献标识码**:A **文章编号**:1673-629X(2021)06-0094-07
doi:10.3969/j.issn.1673-629X.2021.06.017

SSL Protocol Security Technology and Teaching Application Based on Personal Mobile Terminal

LI Ming-kun[1], HU Xi-ming[1,2*], LI Peng[1,2]
(1. School of Computer Science, Shaanxi Normal University, Xi'an 710119, China;
2. Key Laboratory of Modern Teaching Technology of Ministry of Education, Xi'an 710119, China)

Abstract: With the rapid development of the new mobile economy with personal mobile terminal as the fulcrum, SSL protocol, as the core of network security service, is facing more severe security threats. The collaborative development of mobile Internet industry and education urgently needs the innovation of SSL protocol personal mobile terminal security technology. Based on the analysis of SSL protocol architecture and security mechanism, we propose the overall framework of SSL protocol security technology based on mobile phones, laptops and PAD in real network environment, and describe in detail the key technologies such as technical links and personal mobile terminal configuration method, and then realize the authentication of SSL protocol X.509 certificate in mobile Internet. The attack principle, implementation process, key operation and configuration, data measurement and visual analysis are described in detail. The online experimental application during the epidemic period shows that the technology can effectively support the "stop class and keep practicing" in the home-based learning environment, and open up a new practical way for the innovation of network security technology.

Key words: personal mobile terminal; secure sockets layer protocol; security technology; network security; teaching application

0 引 言

作为提供信息加密、身份验证和完整性验证等安全服务支撑 HTTPS 安全链接的 SSL 协议(secure sockets layer),面临会话劫持攻击、剥离攻击和数据密文解密攻击等多种攻击[1-4]。有关移动终端的 SSL 安全分析表明,安智网和 360 手机安卓市场近 6 万个应用软件中约有 59.25% 的应用软件使用了与 SSL 相关的 API,存在可信证书链缺陷的软件占 77.1%,SSL 错误忽略缺陷的软件占比 33.29%,不可信证书链攻击成功的软件占比 17.39%,无域名认证攻击成功的软件占比 15.22%[5];即使大部分网络银行类 APP 完整实现了 SSL 证书公钥绑定,也依然存在诸多安全隐患。

反观高校 SSL 协议安全技术应用发展现状:一方面,SSL 协议作为计算机相关专业的教学重点得到了广泛关注和持续研究;但另一方面,SSL 协议安全技术

收稿日期:2020-06-18 **修回日期**:2020-10-20
基金项目:陕西省科技计划重点研发项目(2020GY-221)
作者简介:李明坤(1999-),男,研究方向为计算机科学与技术;通讯作者:胡曦明(1978-),男,博士,讲师,教育硕士导师,研究方向为智慧教育、计算机教育。

长期停留于基于 PC 真机或仿真平台局限在学校实验室的内部网络环境中实施的传统模式,例如:华南师范大学石硕基于“PC+服务器”开展 SSL 实验[6];海南经贸职业技术学院黄雪琴采用仿真平台开展 SSL 协议实验[7];温州大学黄辉使用 ASA 模拟器开展 SSL 实验[8]。在高校建设面向移动互联网新经济深化产教融合培养网络安全卓越工程师的背景下,探索在真实的移动互联网环境下,基于手机、笔记本电脑和 PAD 等设备的新型 SSL 协议个人移动安全技术和实验应用成为了富有时代性、紧迫性和教育价值的新课题。

1　SSL 协议及其安全机制

1.1　SSL 协议

SSL 协议在 TCP/IP 分层模型中工作在传输层和应用层之间,为互联网环境中的两个通信进程提供安全及数据完整性保障。从协议体系结构上来看,SSL 协议分为上下两个协议子层,上层是 SSL 握手协议簇(SSL Handshake Protocol),具体包括 SSL 握手协议(SSL Handshake Protocol)、修改密文协议(Change Cipher Protocol)和告警协议(Alert Protocol);下层是 SSL 记录协议(SSL Record Protocol),具体定义了两种报文,分别为发送信息报文(Send Information Packet)和接受信息报文(Accept Information Packet)。

SSL 握手协议负责通信双方的身份验证、参数协商和交换密钥以建立安全的加密通道,修改密文协议负责将参数更新信息进行加密、压缩并告知对端,告警协议负责在通信异常时向对端发出警告或致命两类报文。SSL 记录协议分别定义了发送信息报文和接受信息报文,接受信息报文对接收的加密数据进行解密、合并和传输,发送信息报文则对发送数据进行加密、分组和传输。

1.2　SSL 安全机制

如图 1 所示,SSL 记录协议首先将应用数据分为多个片段并对片段进行压缩,随后附上由安全哈希协议或消息摘要等算法生成的加密 MAC 作为消息身份验证代码,然后根据双方协商的加密方式与参数对数据进行加密,最后封装 SSL 首部[9]。SSL 握手协议簇通过客户端和服务器之间四个阶段的会话协商机制,建立起安全的数据传输通道,具体过程如下。

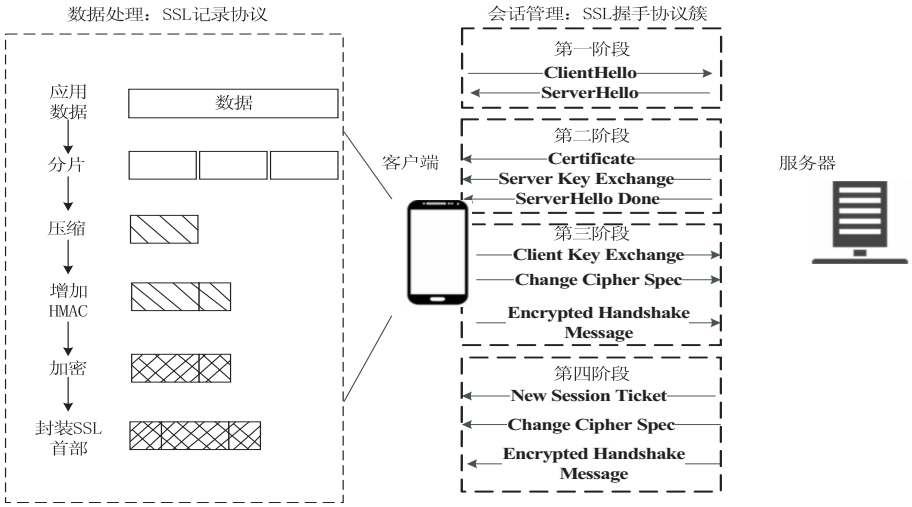

图 1　SSL 协议安全机制

(1)Hello 阶段。

客户端与服务器分别向对方发送 ClientHello 和 SeverHello 报文,客户端发送一个随机数给服务器,客户端与服务器相互交换加密套件(Support Ciphers)与版本信息(SSL Version)等安全信息。

(2)服务器认证阶段。

服务器向客户端发送 Certificate、Server Key Exchange 和 ServerHello Done 等身份证书报文实现自身身份验证并与客户端交换公钥与参数。在 Certificate 报文中,服务器需要向客户端发送整个证书链,包括服务器 CA(数位凭证认证机构)、中间 CA 以及到达可信的根 CA 所需要的所有中间证书。大部分公共签名机构 CA 不直接在服务器证书上签名,中间 CA 是由根 CA 对其签名验证的,由根 CA 离线存储以保证信息的安全。个人移动端一般仅信任根 CA,这样服务商同样需要向其他 CA 申请证书,多级递进确保证书的安全。在 SSL 协议握手期间服务器会向客户端发送整个证书链。

(3)客户端发送共享密钥和加密套件阶段。

客户端首先向服务器发送包含组装共享密钥的预主密钥、一个随机数和加密套件的 Client Key Exchange 报文,服务器收到预主密钥后,将预主密钥与收到的两个随机数组合生成共享密钥,然后通过 Change Cipher Spec 报文通知服务器之后的报文会用

共享密钥加密,在此基础上客户端发送握手信息摘要经加密成的 Encrypted Handshake Message 报文,以便于服务器验证共享密钥的有效性。

(4)服务器发送用户注册信息阶段。

服务器向客户端发送包含客户端登陆会话所需 Session 信息的 New Session Ticket 报文,然后发送 Change Cipher Spec 报文通知客户端之后的报文同样采用共享密钥加密,最后服务器同样发送 Encrypted Handshake Message 报文将握手信息摘要发送给客户端,以便于客户端接受后确认共享密钥的有效性。

2 SSL 协议安全技术设计

在分析 SSL 协议和 SSL 安全机制的基础上,该文探索基于手机、笔记本电脑等个人移动端在真实互联网环境下构建 SSL 协议安全技术系统,实现轻量化、便携化的 SSL 协议攻击与防御。

2.1 总体架构

基于个人移动端的 SSL 协议安全技术总体架构包含四个模块,如图 2 所示。

(1)攻击方模块:由笔记本电脑组成,与服务器和客户端在同一网络环境下,负责对客户端模块进行证书伪造攻击、跳转篡改攻击等 SSL 攻击操作。

(2)SSL 服务器模块:由内容服务器组成,负责与客户端建立 HTTPS 链接。由于攻击对象为 SSL 客户端,该安全技术不会对服务器造成任何不良影响,因此既可以自行搭建私网服务器,也可以采用公网的服务器。该文以百度服务器与 163 邮箱服务器为例,以更加真实地测试 SSL 安全。

(3)SSL 客户端模块:由手机、PAD 等个人移动设备组成,与服务器建立 HTTPS 链接,作为被攻击方。

(4)数据测量与分析模块:由笔记本电脑组成,负责对 SSL 攻击进行数据测量和可视化分析,而如何从 SSL 客户端获取数据是安全技术的难点。

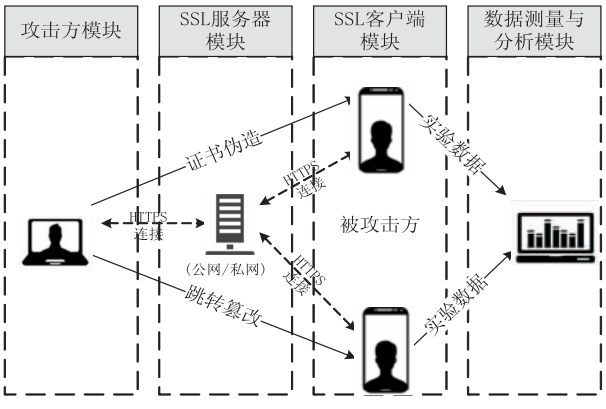

图 2 基于个人移动端的 SSL 协议安全技术总体架构

2.2 技术环节

基于个人移动端的 SSL 协议安全技术环节如图 3 所示。

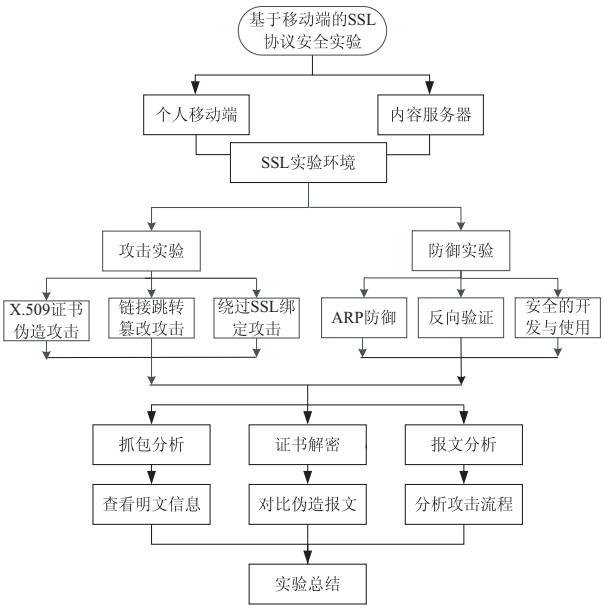

图 3 基于个人移动端的 SSL 协议安全技术环节

技术环节总体上分为:搭建环境、攻击与防御、测量分析。首先采用“个人移动端+内容服务器”搭建技术环境,在此基础上可以开展 X. 509 证书伪造、链接跳转篡改和绕过 SSL 绑定攻击等多种 SSL 典型攻击以及 ARP 防御、反向验证和安全开发与使用等防御,在实现过程中通过实时抓包分析、证书解密等方法实现对实现过程的数据测量和可视化分析。

3 SSL 协议安全技术实现

3.1 个人移动端配置

整个安全技术需要基于手机、笔记本电脑等个人移动端设备完成 SSL 攻击、防御与测量分析等一系列复杂功能,包括证书伪造、链接跳转篡改、手机抓包等,而这部分正是整个安全技术的难点所在。该文以常见的 X. 509 证书伪造攻击和链接跳转篡改攻击为例,实现过程中使用到的设备有一台 HP 8GRAM+1TROM/I5 /GTX1050TI 笔记本电脑,作为攻击方和数据测量与分析的设备;一台 MI 骁龙 835/6GRAM+64GROM 手机,作为客户端和数据测量与分析的设备;一台 SSL 服务器 BAIDU HTTPS SERVER/163 HTTPS SERVER,作为 SSL 服务器。

在此基础上,该安全技术所用的手机和笔记本电脑等个人移动设备配置方法,如图 4 所示,包括关键步骤、详细操作和工具实例。

3.2 X. 509 证书伪造攻击

(1)攻击原理。

在 SSL 客户端访问一个基于 SSL 加密的 Web 时,需要三个步骤验证证书服务器的有效性[10]:①该证书的主题名与访问服务站点的名称一致性;②该证

书的有效期限;③该证书与证书链中数字签名的匹配。若以上步骤有任意一个没有通过,SSL 协议就会向客户端发出警告,指出证书存在安全问题。此时需要用户来决定是否继续使用,攻击方由此利用用户安全意识缺乏进行攻击,若用户选择信任不安全的证书,或者被攻击方恶意控制将伪造的证书加入信任列表,从而造成基于 X.509 证书伪造的 SSL 会话劫持攻击。

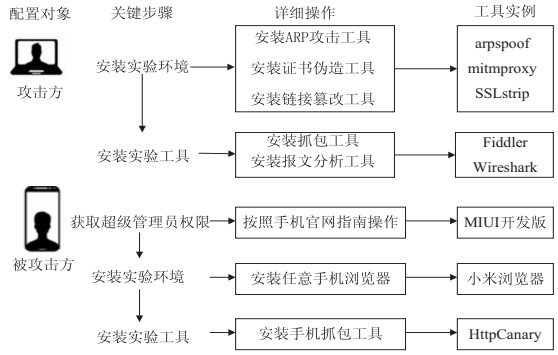

图 4　个人移动端软件环境配置

(2)实现流程。

基于 X.509 证书伪造的攻击流程如下:

①HTTPS 连接协商:攻击方同时与客户端、服务器发出 HTTPS 连接协商,攻击方截获并转发客户端与服务器之间的所有请求与响应。当攻击方截获客户端发给服务器的 ClientHello 请求时,记录随机序列在内的相关信息之后再转发给服务器。

②攻击方代替客户端对服务器进行验证:该步骤为证书伪造攻击的关键步骤,当攻击方截获服务器发给客户端的响应及服务器证书时,保存包括随机序列和 session 的相关信息,将数据包中的证书重组替换为伪造的 X.509 证书,重新打包数据之后转发给客户端。

③攻击方截获服务器与客户端交换的密钥:客户端发送密钥给服务器,攻击方截获密钥再转发给服务器,若服务器要求对客户端进行认证,则攻击方需要截获用户证书并重新打包转发。

④攻击方基于伪造的 X.509 证书实施攻击:攻击方利用伪造的证书同时和服务器与客户端建立 HTTPS 链接,但服务器与客户端并不知道攻击方作为中间人劫持了 HTTPS 链接,随后服务器与客户端之间传输的数据都可以被攻击方明文解析。

(3)操作与关键配置。

X.509 证书伪造攻击在攻击方和被攻击方通过命令行输入命令和浏览器建立 HTTPS 链接等方式,共需要五个步骤完成。X.509 证书伪造攻击的操作步骤与关键配置如表 1 所示。

表 1　X.509 证书伪造攻击操作与关键配置

对象	操作步骤	关键配置
攻击方	步骤一:对目标 IP 进行 ARP 攻击,使得被攻击方与服务器之间的通信被截获	ipconfig route -n arpspoof -i eth0 -t 192.168.0.1 -r 192.168.0.102
	步骤二:配置监听端口并开启路由转发,保持被攻击方与服务器之间正常通信	iptables -t nat -APREROUTING -p tcp -dport 443 -j REDIRECT --to-port8888 echo 1> /proc/sys/net/ipv4/ip_forward
	步骤三:启动攻击代理软件 mitmproxy,截获服务器 SSL 证书并伪造证书	mitmproxy -T --host -w mitmproxy.log
被攻击方	步骤四:安装并信任伪证书	使用浏览器访问 mitm.it 并下载 android 端的证书。在设置中安装伪证书
	步骤五:与百度 HTTPS 服务器建立 SSL 链接	在浏览器地址栏输入 www.m.baidu.com 并访问

(4)数据测量与可视化分析。

根据被攻击方抓包得到的报文可以看到攻击方保持了证书 id 等外部信息不变,但实则替换了证书内部的加密协商相关字段值,由此达到攻击方可以明文解密被攻击方与服务器之间 HTTPS 链接的目的。

攻击方进行 X.509 证书伪造攻击之后,使用 fiddler 对被攻击方的 HTTPS 访问请求进行抓包分析,如图 5 所示。攻击方从截获的报文中可以监控被攻击方的网络访问记录,本例访问了百度移动端站点 www.m.baidu.com;在此基础上,攻击方通过 X.509 证书伪造攻击可以进一步窃取被攻击方的个人私密信息,如被攻击方的 cookie 值。在被攻击方通过 HttpCanary 抓包,可以验证攻击方窃取的 cookie 值的真实性。

3.3　链接跳转篡改攻击

(1)攻击原理。

使用者在申请 HTTPS 链接时有两种实现方式[11],一种是在输入网址时添加前缀 https://指定该链接为 HTTPS 链接,另一种是使用者如果没有指定链接是 HTTP 还是 HTTPS,浏览器会默认为 HTTP 类型,

此时跳转到 HTTPS 就需要利用 HTTP 的 302 状态来重定向为 HTTPS 链接。大部分人图方便并不会采用第一种实现方式,而第二种实现方式就给了攻击方攻击的机会[12]。一个完全由 SSL 加密的 HTTPS 通信变成了加密的 HTTPS 通信和明文传输的 HTTP 会话混合的传输方式,如果 HTTP 通信被劫持,那么 HTTPS 会话也会遭到劫持。

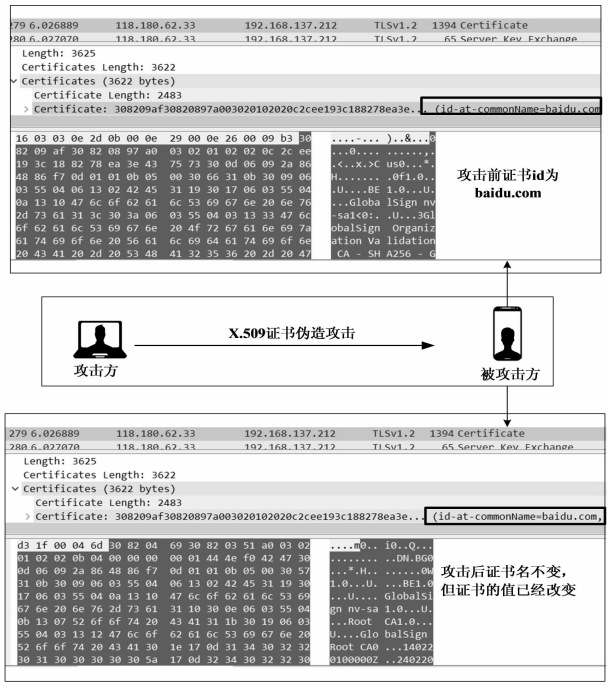

图 5 证书对比分析

(2)实现流程。

基于链接跳转篡改攻击流程如下:

①HTTPS 链接协商:攻击方分别向客户端、服务器发出 HTTP 和 HTTPS 链接协商,攻击方截获并转发客户端与服务器之间的所有请求与响应。

②攻击方替换服务器 HTTPS 流量中的信息:攻击方截获服务器发给客户端的 HTTPS 流量,攻击方解析该数据包并将其中的<a href="https://...">替换成<a href="http://...">,将 Location:https://...替换成 Location:http://..,保存修改的 URL 后,重新打包数据并转发给客户端。

③攻击方转发修改客户端 HTTP 流量中的信息:攻击方截获并解析客户端发给服务器的 HTTP 请求,与之前保存的 URL 对比之后,若存在要修改的 HTTP URL,则替换为原 HTTPS URL,重新打包数据并转发给服务器。

④攻击方维持与客户端和服务器之间的虚假 HTTPS 链接:分别与客户端和服务器维持 HTTP 和 HTTPS 链接。

(3)操作与关键配置。

链接跳转篡改攻击在攻击方和被攻击方通过命令行输入命令和浏览器建立 HTTPS 链接等方式,共需要四个步骤完成。链接跳转篡改攻击的操作步骤与关键配置如表 2 所示。

表 2 链接跳转篡改攻击操作与关键配置

对象	操作步骤	关键配置
攻击方	步骤一:对目标 IP 进行 ARP 攻击,使得被攻击方与服务器之间的通信被截获	ipconfig route -n ettercap -i wlan0 -T -M arp:remote /-t 192.168.0.1// /192.168.0.102//
	步骤二:配置监听端口并开启路由转发,保持被攻击方与服务器之间正常通信	iptables -t nat -APREROUTING -p tcp -dport 443 -j REDIRECT --to-port8888 echo 1> /proc/sys/net/ipv4/ip_forward
	步骤三:启动 HTTPS 过滤攻击软件 SSLStrip,将被攻击方请求的 HTTPS 链接篡改为 HTTP 链接	sslstrip -l 10000
被攻击方	步骤四:访问 163 邮箱站点(www.mail.163.com),并利用跳转机制建立 HTTPS 链接	在浏览器地址栏输入 www.mail.163.com 并访问

(4)数据测量与可视化分析。

攻击方进行链接跳转篡改攻击之后,使用 fiddler 对被攻击方的 HTTPS 访问请求进行抓包分析,如图 6 所示。攻击方从截获的报文中可以看到被攻击方与服务器之间建立的会话都是 HTTP 链接,本例中被攻击方与 163 邮箱移动站点建立了 HTTP 链接,地址栏信息为 http://smart.mail.163.com。由于链接跳转篡改攻击将 HTTPS 链接篡改为了 HTTP 链接,攻击方可以轻易窃取被攻击方的个人私密信息,如被攻击方的 cookie 值。如图 7 所示,在被攻击方通过 HttpCanary 抓包,可以验证攻击方窃取的 cookie 值的真实性。

3.4 SSL 协议的个人移动端防御

SSL 协议的个人移动端防御的关键在于如何有效防止攻击方与服务器和客户端建立虚假的 HTTPS 链接,具体可从四个方面实施。

(1)ARP 防御。

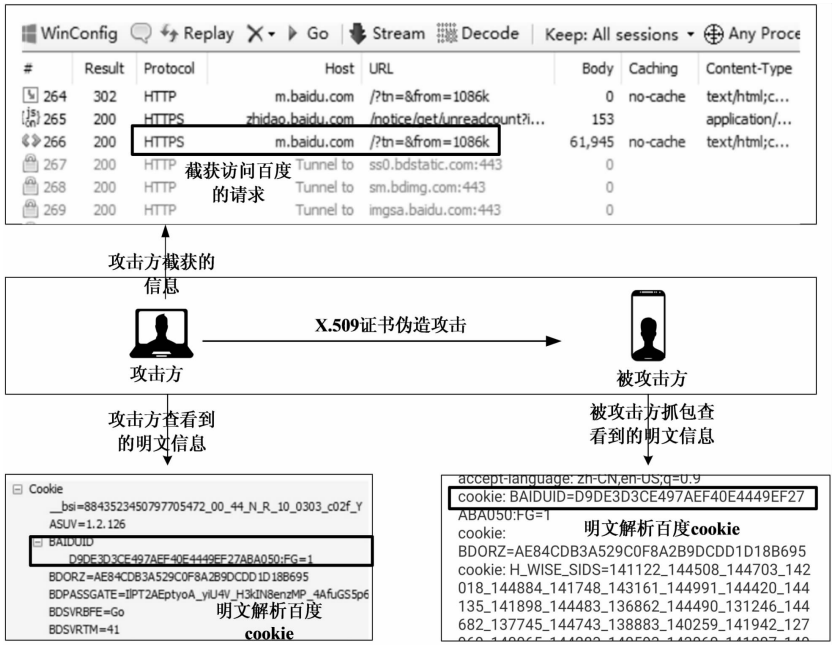

图 6　数据可视化分析

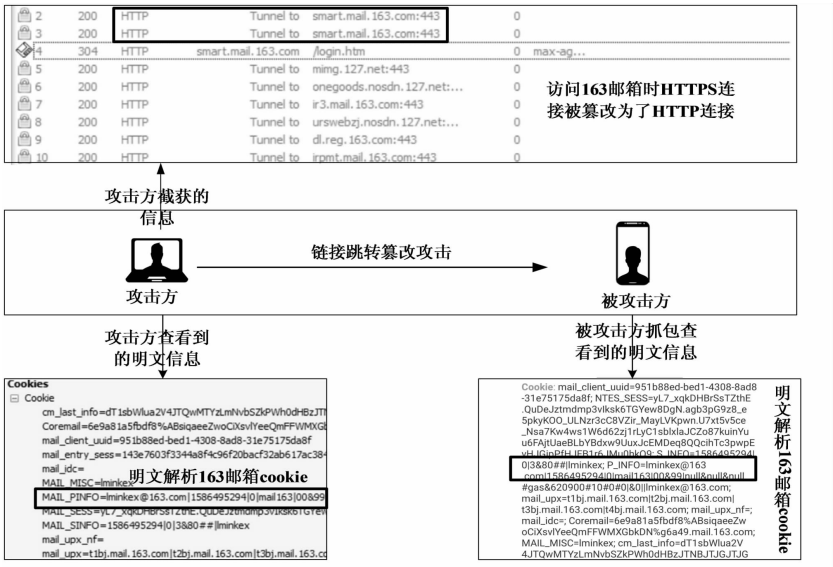

图 7　攻击端截获的信息

在证书伪造攻击和链接跳转篡改攻击中都需要攻击方接入网络并对被攻击方进行 ARP 攻击,因此针对 ARP 欺骗、DNS 欺骗等网络欺骗的防御方法同样适用于 SSL 攻击防御。常用的有动态 ARP 检测、静态 IP-MAC 绑定和安装 ARP 防火墙等[13]。

(2)提高用户安全意识。

证书伪造攻击需要用户安装并信任伪证书,链接跳转篡改攻击则利用了用户缺乏直接建立 HTTPS 链接的安全意识,因此用户良好的安全意识可以有效防止 SSL 攻击。例如,在网上注册、登陆等需要提供私密信息时,选择带有 https://前缀的网址;更换使用 360 等具有安全防护功能的浏览器并及时更新;尽量避免使用未知的 wifi 热点。

(3)反向验证。

SSL 协议中仅要求在建立 HTTPS 链接时,客户端验证服务器的身份,使得攻击方可以作为中间人伪装成客户端或服务端与对端建立虚假的 HTTPS 链接,因此服务器要求反向验证客户端身份可以防止 SSL 攻击。例如,服务器在建立链接与通信过程中也要求客户端使用证书与数字签名验证自身身份。

(4)提高开发者安全意识。

在对于 78 名 Android 和 IOS 开发者调查中发现,仅 14 名开发者意识到不完整实现 SSL 协议会遇到很多安全问题[14]。证书伪造攻击利用了开发者对于证书绑定实现的忽视,因此开发者良好的安全意识可以减少受到 SSL 攻击的可能。例如,完整的实现 SSL 相关接口;使用 SSL Pinnng 技术将证书与应用程序绑定[15-16]。

4 应用实效性分析

基于个人移动端的 SSL 协议安全技术可以完全依托个人移动端实现真实网络环境中的 SSL 协议攻击与防御,使得学生在居家条件下仍然可以利用手机、笔记本电脑等个人设备完成实验,从而实现学生居家边学边做“停课不停练”。针对本校 2017 级计算机科学与技术专业创新班学生开展问卷调查,全班 46 人共收回有效问卷 42 份,结果表明该技术具有轻量化、实景化、便携化和个性化的独特优点。

(1)技术效能对比。

超过 95% 的学生有计算机和手机,83% 的学生在疫情期间习惯使用手机上网课,80% 的学生在疫情期间习惯使用计算机上网课。

根据调查问卷的结果,50% 的学生认为基于计算机的实验技术在易操作性上有优势,分别有 56%、49%、46%、65% 的学生认为基于手机的实验技术在易配置、直观性、真实性和成本低方面有明显优势,而仅有 20% 的学生认为基于仿真的实验技术在实验真实性方面有微弱的优势。

(2)实验模式创新。

师生可以在远程同步进行实验,教师可以通过示范、答疑等方式对实验的重难点分析解决。这种理论与实践一体化的教学模式为有效破除高校人才培养存在的“眼高手低”“高分低能”等现实弊病提供了切实可行的教学模式创新空间。

根据调查问卷的结果,96% 的学生认为教学中的同步实验是很有必要的,79% 的学生认为手机实验能很好的实现教学与实验的同步,但仅 41% 的学生认为手机实验能代替传统计算机实验与仿真实验,大部分学生对于手机实验替代传统实验并不乐观,而以手机为支点结合笔记本电脑等个人移动设备的实验方式应用范围更加广泛。

5 结束语

随着 5G 移动网络的快速普及,个人移动端用户规模和应用领域将迎来新一轮高速发展,以手机为支点的新应用、新业态和新模式进一步渗透融入国民经济和社会生活。该文提出基于手机、笔记本电脑等个人移动端的 SSL 协议安全技术设计,并具体实现 X.509 证书伪造和链接跳转篡改等典型 SSL 攻击。疫情期间,该技术的应用实现了学生在居家环境下开展网络安全实验“停课不停练”,形成了以学习体验为核心的个人掌上移动实验室,经过实践检验具有轻量文章、实景化和便携化的优点,为网络安全技术创新开拓实践新途径。

参考文献:

[1] 刘新亮,杜瑞颖,陈 晶,等. 针对 SSL/TLS 协议会话密钥的安全威胁与防御方法[J]. 计算机工程,2017,43(3):147-153.

[2] 邓 真,刘晓洁. HTTPS 协议中间人攻击的防御方法[J]. 计算机工程与设计,2019,40(4):901-905.

[3] 韦俊琳,段海新,万 涛. HTTPS/TLS 协议设计和实现中的安全缺陷综述[J]. 信息安全学报,2018,3(2):1-15.

[4] EL-HAJJ W. The most recent SSL security attacks: origins, implementation, evaluation, and suggested countermeasures [J]. Security & Communication Networks,2012,5(1):113-124.

[5] 方慧鹏,应凌云,苏璞睿,等. 移动智能终端的 SSL 实现安全性分析[J]. 计算机应用与软件,2015,23(7):272-276.

[6] 石 硕,汪海涛. 局域网中的 SSL 实验[J]. 实验室研究与探索,2005,24(7):50-54.

[7] 黄雪琴,耿 强. 一种基于改进的 SSL 协议仿真测试方法[J]. 实验室研究与探索,2015,34(6):124-127.

[8] 黄 辉,张纯容. 基于 ASA 防火墙实现的 SSL-VPN 实验仿真[J]. 实验室研究与探索,2015,34(11):111-113.

[9] BHARGAVAN K, BRZUSKA C, FOURNET C, et al. Downgrade resilience in key-exchange protocols[C]//2016 IEEE symposium on security and privacy (SP). San Jose: IEEE,2016.

[10] 沈若愚,卢盛祺,赵运磊. TLS1.3 协议更新发展及其攻击与防御研究[J]. 计算机应用与软件,2017,34(11):264-269.

[11] 张 明,许博义,郭艳来. 针对 SSL/TLS 的典型攻击[J]. 计算机科学,2015,42(6A):408-412.

[12] 张恒伽. 基于中间人攻击的 HTTPS 协议安全性分析[D]. 上海:上海交通大学,2009.

[13] 王晓妮,韩建刚. 基于免疫网络的 ARP 攻击防御方案研究与实施[J]. 计算机技术与发展,2019,29(4):95-99.

[14] FAHL S,HARBACH M,PERL H,et al. Rethinking SSL development in an applied world[C]//Proceedings of the 2013 ACM SIGSAG conference on computer & communications security. New York:ACM,2013:49-60.

[15] BHOR M,KARIA D. Certificate pinning for android applications[C]//2017 international conference on inventive systems and control (ICISC). Coimbatore:IEEE,2017:1-4.

[16] RAMÍREZ-LÓPEZ F J,VARELA-VACA A J,ROPERO J, et al. A framework to secure the development and auditing of SSL pinning in mobile applications:the case of Android devices[J]. Entropy,2019,21(12):1136.