SOHO 路由器脆弱性的分析和验证

李翔豪， 王轶骏， 薛 质
（上海交通大学 电子信息与电气工程学院，上海 200240）

[摘 要] SOHO 路由器作为现今家庭和中小型办公环境中普及度极高的网络接入设备，其安全性之重要不言而喻。加之目前国内外对网络设备，尤其是路由器的攻击越发流行，因此，本文对 SOHO 路由器脆弱性和相应攻击面的研究具有重要价值，是相关学术领域研究的大势所趋。主要研究分析和归纳总结了 SOHO 路由器脆弱性方面的相关技术和研究成果，包括远程侦测技术、漏洞利用技术和后门驻留技术等。首先是远程侦测技术，用来实现对路由器类型和版本的精准探测；其次是漏洞利用技术，用来获取路由器的管理权限甚至是系统权限；最后是后门驻留技术，用来在获取路由器权限的基础上实现长期的隐蔽控制。这里为今后在设计、改进 SOHO 路由器的安全防御技术和策略等方面提供基础支撑。

[关键词] SOHO 路由器；远程侦测；漏洞利用；后门驻留；脆弱性分析
[中图分类号] TP316 [文献标志码] A [文章编号] 1009-8054(2016)08-0095-06

Analysis and Verification of SOHO Routers Vulnerability

LI Xiang-hao, WANG Yi-jun, XUE Zhi
(School of Electronic Information and Electrical Engineering, Shanghai Jiaotong University, Shanghai 200240, China)

[Abstract] As a network access facility, the SOHO router is highly popular in family and office today, so it's security is of great importance. Nowadays cyber attack aiming at network equipment, especially SOHO routers, is gradually popular at home and abroad, so it is necessary to research on vulnerabilities and attacking methods, and also it is represents the general trend in the related research fields. This paper focuses on researching and concluding both the technologies and results about the SOHO router's vulnerabilities, including remote detection technology, exploit technology, and resident backdoor technology. Firstly, the remote detection technology, which is used to accurately detect router's type and version, is studied. Then, exploit technology is researched to get administrator privileges, even get the system authority. Finally, resident backdoor technology is is used as controlling the router covertly in a long-term based on getting the administrator privilege. This paper may provide basis SOHO router's support in the both design and improvement of security techniques and strategy in the future.

[Key words] SOHO router; remote detection; exploit; resident backdoor; analysis of vulnerability

0 引言

近年来，SOHO 路由器的普及程度越来越高，随之而来的安全性问题也层出不穷。现在许多用户在使用个人终端时，都将 SOHO 路由器作为接入网络的第一道网关设备，是网络通信的重要环节。但是，SOHO 路由器在设计、制造方面偏向于面向用户，往往提供简明易懂的界面、方便快捷的设置步骤，使用户能方便、快捷的实现上网行为；但也正是这有别于企业级路由设备的设计理念差异，导致 SOHO 路由器存在严重的脆弱性隐患，很容易产生各种安全问题。除了常见的被“蹭网”等，一些 APT 攻击也正是基于 SOHO 路由器的脆弱性而产生的。攻击者通过暴力、漏洞、或者社工方式可以轻易取得 SOHO 路由器的最高权限，进而实施网络劫持、信息窃取、网络钓鱼等攻击行为，直接威胁个人用户和企业单位的数据安全。此外，水平更高的攻击者还能通过对 SOHO 路由设备固件的逆向分析和漏洞挖掘来实施更为强大和精确的 APT 攻击[1]。

所谓“知己知彼，百战不殆”，为了能够第一时间及时对 SOHO 路由器的安全问题进行快速响应，减少因路由器漏洞和后门爆发带来的危害和损失，就需要我们对 SOHO 路由器进行脆弱性的分析，获悉各类路由器潜在的安全隐患，由此才能更有针对性的找到相应防御的方法。

因此，本文主要研究分析、归纳总结 SOHO 路由器脆弱性方

* 收稿日期：2016-03-16

面的研究技术和成果，首先是 SOHO 路由器的远程侦测技术，能够对路由器的类型和版本进行精准探测；然后是 SOHO 路由器的漏洞利用技术，包括内存溢出、固有后门漏洞的挖掘和分析，能够对目标路由器进行权限获取；最后则是 SOHO 路由器的后门驻留技术，能够对目标路由器进行隐蔽控制和流量转发。本文希望通过对上述脆弱性分析技术的归纳总结和趋势展望，来为下一步提出针对性的安全防御策略和方法提供重要积累和基础支撑。

1 SOHO 路由器的远程侦测技术

SOHO 路由器的远程侦测是对路由器发起攻击的基础，这是因为能否对设备类型、型号、功能等信息进行准确判定将会直接影响着后续攻击的成功率。远程侦测旨在通过网络自有协议和网络设备特定协议来判断目标路由器是否在线，进而通过与其进行数据包交互的方式来提取其设备指纹特征，并对比指纹特征数据库来获得目标路由器设备的具体信息。

一般来说，SOHO 路由器可用以作为主机指纹特征的对象主要包括 MAC/OUI 指纹和应用服务指纹这两类，如图 1 所示。

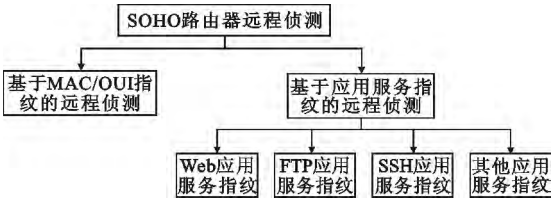

图 1 SOHO 路由器远程侦测技术的分类

1.1 基于 MAC/OUI 指纹的路由器侦测技术

MAC/OUI 指纹指的是固化在网卡设备中硬件地址（即 MAC，Media Access Control Address 地址）的前 3 个字节，是用来唯一标识该网卡的生产厂商（即 OUI）。因此，在内部网络进行路由器的远程侦测，就可以直接获取目标路由器的 MAC 地址，然后读取其中的 OUI 部分，并通过 IEEE 公布的 OUI 分配表来查找该地址对应的组织，就能获得目标路由器的生产厂商了[3]。这种基于 MAC/OUI 指纹的探测方式，其优点在于能够较为精确的判定路由器的生产厂商，但其缺点也很明显，一是无法获取系统精确版本信息；二是只能在内网中进行探测。

1.2 基于应用服务指纹的路由器侦测技术

基于应用服务指纹的探测则是利用目标路由器所开放的众多应用服务，包括 Web、FTP、SFTP、SSH、Telnet、SNMP 等，通过探测这些服务所返回的问候标语（banners）来获取其品牌、型号、固件版本号、服务版本号等诸多详细信息[3]。这种方式既适用于外网探测也适用于内网探测，是相对比较方便和可靠的远程侦测方式。

●Web 应用服务指纹

在 Web 服务返回的头部信息中，一般通过增加 WWW-Authenticate 字段来对用户身份进行认证，而各路由器厂商一般均在 Basic 字段（基本认证）中增加厂商信息。这里以 TP-Link N 系列路由器为例，该系列路由器的 HTTP 返回头部如下所示：

HTTP/1.1 401 N/A

Server: Router Webserver

Connection: close

WWW-Authenticate: Basic realm = " TP-LINK Wireless N Router WR941N"

Content-Type: text/html

从中可以清晰的看到，该设备为一台 TP-Link WR941N 无线路由器。

此外，厂商也往往会在 HTML 页面中添加公司名称、商标、设备信号等信息，以提供用户更人性化的登录界面。以 D-Link DIR-610 路由器为例，页面信息中有如下特殊字段可作为指纹特征使用：

<td>Product Page: DIR-610</td>

在探测过程中，如果返回页面中包含该字段，一般就可认为该目标为一台 D-Link 无线路由器。

●FTP 应用服务指纹

这里以 D-Link 公司生产的 DSL 系列无线路由器为例，该系列路由器会在 21 端口开启 FTP 服务并持续监听，等待用户连接向路由器传送文件用以升级系统固件。用户一旦与路由器建立 TCP 连接，设备会向用户发送如下问候标语信息：

220 Ftp firmware update util

user(62.215.* .* :(none)):

通过该信息，即可判断该设备为 D-Link DSL 系列路由器。

●SSH 应用服务

这里以 Cisco 公司的路由器为例，该公司的绝大部分设备均搭载了自行开发研制的 IOS（Internetwork Operating System）操作维护系统，该系统通常会在 22 端口开启 SSH 服务以远程管理路由器。用户发起连接请求后，设备在交换自己的 RSA 公钥的同时，就会向用户发送如下问候标语信息：

SSH-2.0-Cisco-1.25

该信息表明目标设备为一台运行 1.25 版本 IOS 系统的 Cisco 路由器，同时 SSH 版本号为 2.0。

此外，SFTP、Telnet 等应用服务指纹特征都与上述这些服务类似，此处就不再赘述。

现今，国内外已经诞生了 RouterScan 等路由器远程探测软件，以及 Zoomeye、Shodan、Censys 等大规模监测平台。其中 RouterScan 是俄罗斯安全团队 Stas'M 开发的一套路由器安全测试工具，它可以指定 IP 段对路由器进行暴力破解、信息提取等安全测试，支持各种品牌型号的路由器，善于发现大量已知的路由器或

服务器设备并提取相应信息，特别是无线网络加密信息，包括接入点的名称和密钥，并确定路由器品牌和型号，甚至可以对部分有漏洞的路由器进行漏洞利用和渗透。Zoomeye、Shodan、Censys则是国内外的一些安全团队和公司所打造的面向全球网络的设备监测系统和平台，旨在对全网范围内的服务器、摄像头、打印机、路由器等联网设备进行信息采集并提供可视化智能检索[4]。

2 SOHO 路由器的漏洞利用技术

当攻击者获知目标路由器的类型及其型号版本之后，就会尝试利用针对该路由器的各类漏洞进行攻击，直至最终获取其权限为止。漏洞利用成功之后，攻击者一般就能够进入后台管理界面，更改路由器的重要配置信息（比如 DNS 服务器的设置等），升级路由器固件引入后门等；甚至还能够直接获取到执行目标系统命令的 Shell 接口，从而获取系统底层信息，执行流量转发命令，植入系统后门等。

SOHO 路由器作为一种嵌入式设备，可视为特殊的小型计算机，也存在着各种类型的漏洞，主要可分为如下四类：身份认证脆弱性漏洞、Web 配置界面漏洞、缓冲区溢出型漏洞和固有后门型漏洞[5]。如图 2 所示。

图 2 SOHO 路由器漏洞利用技术的分类

在这四类漏洞中，身份认证脆弱性漏洞为攻击者进入目标网络提供先决条件，Web 配置界面漏洞为攻击者获取路由器 Web 管理界面提供了可能性，而后两类漏洞，即缓冲区溢出型漏洞和固有后门型漏洞能够帮助攻击者获取目标路由器的 Web 配置管理权限，甚至是系统本身的最高权限，因此风险威胁较大，检测难度也较大。

2.1 身份认证脆弱性漏洞利用技术

绝大部分的 SOHO 路由器都具有 Wi-Fi 功能，供电脑、手机、智能家电等支持无线功能的终端设备接入并分享互联网。提供 Wi-Fi 功能的路由器一般都需要进行身份认证才能够被允许接入其内部网络，因此攻击者往往需要首先破解 Wi-Fi 接入密码后才能够接入目标内部网络，然后再利用路由器本身的漏洞来进一步获取其权限。

目前，SOHO 路由器使用的身份认证加密算法主要包括 WEP、WPA、WPA2 和 WPA/WPA2-PSK 等。其中 WEP 由于受其采用的 RC4 的加密算法限制，攻击者能够非常容易的获取到加密密钥，安全性较差，因此已经不再被广泛采用了[6]。而 WPA 与 WPA2 作为目前在大部分设备中使用的加密方式，相较于 WEP 而言的安全性大大提高。在使用较复杂密码的情况下，单纯依靠暴力破解的攻击方式则需要较长时间。然而，由于一般用户的安全意识较弱，在设置密码时仍有不少不良习惯，包括简短的数字组合、电话号码、生日等容易被猜测的密码。因此攻击者可以收集到用户相关信息，辅以社会工程学的方法，创建有针对性的字典，从而实施高效的暴力破解。此外，攻击者还可以利用现今越来越强大的分布式云架构和大数据平台来生成以前无法想象的大容量彩虹表（Rainbow Table），然后在后台进行离线暴力破解[7]。

即使用户为 Wi-Fi 的身份验证设置了非常复杂的密码组合，还是仍然有被破解的可能性，这是因为目前的路由器厂商为简化终端接入路由器的过程而引入了 WPS（Wi-Fi Protected Setup）技术，即 Wi-Fi 安全防护设定。用户仅需按下无线路由器上的 WPS 按钮或者输入正确的 PIN 码，即可完成无线密码的验证，从而在客户端与路由器之间建立安全链接。首先，PIN 码一共 8 位，其中最后一位为校验位，因此在破解时只需考虑前 7 位即可；接着，如果 PIN 码的前 4 位验证失败，路由器就会向客户端发送 EAP-NACK 信息；因此，最终攻击者仅需要在找到一个前 4 位和后 3 位的 PIN 码组合即可，大约有 1 1000（10^4+10^3）种可能[8]。在实际破解中，攻击者通常平均只需要尝试 5 500 次就可以完成 Wi-Fi 身份验证的密码破解。此外，某些 SOHO 路由器，比如贝尔金（Belkin）路由器，还会将 WPS 的密钥生成算法固化在硬件中，一旦被攻击者获知之后，就可以基于该算法进行快速破解。

2.2 Web 配置界面漏洞利用技术

SOHO 路由器为了便于用户管理，一般都为用户提供了图形化的 Web 配置页面。因此，一些常见的 Web 攻击方式，如 SQL Injection（SQL 注入）、CSRF（跨站请求伪造）、XSS（跨站请求脚本）、RCE（远程命令执行）、File Inclusion（文件包含等），也会对路由器带来威胁[9]。

攻击者可以通过 SQL 注入非法获取或修改路由器中包括用户身份在内的数据库内容。而借助 CSRF，攻击者则可通过在网页中注入恶意 JavaScript 代码，在用户使用浏览器期间自动运行，以借用用户身份，访问受限的 Web 页面（管理界面等），从而达到修改路由器配置的目的。这些攻击所引发的路由器数据泄漏和配置修改，会引发后续的 DNS 劫持等更多高威胁、持续性的攻击。

近年来，典型的 Web 配置界面漏洞利用示例如下：

●TEW-654TR 路由器的登录页面（/my_cgi.cgi）存在 SQL 注入漏洞，输入类似“' or '1' = '1”这样的万能密码即可绕过登录验证进入 Web 管理界面[10]。

●D-Link DSR 系列路由器的登录脚本（/scgi-bin/platform.cgi）不正确过滤用户提交的输入，允许远程攻击者利用漏洞提交定制的 SQL 查询来绕过验证[11]。

●D-Link DIR-320 路由器的脚本(/model/__show_info.php) 存在文件包含漏洞,可被攻击者利用读取系统敏感配置文件[13]。

●TP-Link TL-WR840N 系列路由器存在 CSRF 漏洞,攻击者可以诱使路由器管理员访问一个恶意的网站,然后利用这个漏洞导入一个攻击者构造的配置文件,从而可以修改包括路由器的防火墙、远程管理等所有的配置项[13]。

2.3 缓冲区溢出型漏洞利用技术

缓冲区溢出攻击的原理是在将大缓冲区向小缓冲区复制的过程中,由于对小缓冲区的边界未经检查或检查不严格,导致小缓冲区不足以接收整个大缓冲区的数据,从而使得超出部分覆盖了与小缓冲区相邻的内存中其他数据,最终引发内存溢出问题。攻击者利用这一点就能够使得正常执行的程序流程跳转到攻击者所指定的代码(通常为精心编写的 Shellcode) 上去,从而对路由器设备造成严重后果,比如拒绝服务、执行远程 Shell,获得用户级权限、甚至是系统级别的权限。

现今针对 SOHO 路由器的缓冲区溢出漏洞攻击大多数还是栈溢出攻击。但与传统 PC 采用的 x86/x64 架构复杂指令系统不同,大多数采用 Linux 嵌入式操作系统的 SOHO 路由器使用的是 MIPS 指令系统,该指令系统属于精简指令系统。MIPS32 架构的函数调用方式虽然与 x86/x64 系统有很大的区别,比如没有 EBP (栈底指针) 寄存器,通过 $ a0 ~ $ a3 等寄存器而非堆栈来传递函数参数,将叶子函数的返回地址直接存入 $ ra 寄存器中等等。但是通过研究分析发现,传统的针对 x86/x64 的栈溢出攻击对 MIPS 系统仍然有效: 只要所调用的函数中是非叶子函数,并且有缓冲区溢出漏洞,就可以覆盖父函数的返回地址,从而劫持程序执行流程; 而在叶子函数中,如果存在可以溢出大量数据的情况,那么也存在覆盖父函数返回地址达到劫持程序执行流程的可能性。

针对 SOHO 路由器的栈溢出漏洞攻击主要面对的挑战是目标系统中启用的 DEP(Data Executive Protection,数据执行保护) 技术。DEP 的基本原理是将数据所在的内存页,包括栈和堆等,设置 NX/XD 属性标记来指明不能从该内存执行代码,这样当程序产生溢出,恶意代码试图在数据段执行指令的时候,CPU 就会产生异常而不去执行指令。因此,攻击者需要利用 ROP(Return-Oriented Programming,返回导向编程) 技术,在堆栈中构造一连串的参数和返回地址,利用目标系统中已加载的合法模块中的指令片断完成特定的 Shellcode 功能,从而绕过 DEP 防护机制。

●针对 SOHO 路由器的 ROP 技术

和其他程序一样,SOHO 路由器所加载的程序里一般都会包含大量的返回指令,如“jr $ ra”等,它们往往位于函数的尾部,或者函数中部需要返回的地方,从某个地址到“jr $ ra”指令之间的二进制序列被称之为“gadget”。所谓的 ROP 技术就是攻击者事先搜索程序内存空间中所有以这种返回指令结尾的 gadget 代码片断,使其按照前后顺序依次拼接起来,完成诸如内存读写、算术逻辑运算、控制流程跳转、函数调用等特定功能的操作,并最终组合起来完成复杂的功能[14]。为了将目标系统中的各个 gadget 代码块拼接起来,需要使用一个事先准备好、包含各条指令结束后下一条指令地址的特殊返回栈。攻击者会构造一个特殊输入向量以填充函数的栈空间。首先,让指向攻击者所构造的栈的指针跳到 gadget A 中,在执行完 gadget A 中的代码序列后,通过位于 gadget A 尾部的 jr $ ra 回到栈中,然后再执行 gadget B,执行后跳到 gadget C,这样依次进行下去。因此,只要目标栈的容量足够大,就一定能够达到完成全部功能代码(Shellcode) 执行的目的。

ROP 技术利用的一个难点在于,要在整个内存空间中搜索所需要的 gadget 代码链需要花费很长的时间。但一旦完成了“搜索”和“拼接”,那么这样的攻击将是难以抵挡的,因为它是用的都是内存中的合法代码。值得注意的是,ROP 技术具备图灵完整性,也就是说,如果程序能实现,那么 ROP 就肯定有一个对应的序列及堆栈。而现今绝大多数存在漏洞的 SOHO 路由器程序,攻击者通过 ROP 技术基本都可以构造出一个完整的 gadget 代码序列出来[15]。

2.4 固有后门型漏洞利用技术

SOHO 路由器的固有后门漏洞指的是路由器厂商开发的产品本身存在出厂后门设置,攻击者可以利用该后门绕过安全控制来获取路由器的访问控制权限。这类漏洞往往是由于路由器生产厂商在开发、管理和控制时候为了方便而引入的,也有可能是发布产品时出于某种目的而遗留的问题。

近几年被曝出有后门的路由器就覆盖了包括 D-Link、Tenda、Linksys、Netgear、Netcore/Netis、ZTE、Cisco 在内的等多家国内外知名厂商,如下所列:

●D-LINK(友讯) DIR-100 系列路由器的 Web 服务器程序(/bin/webs) 后门。攻击者只需将浏览器的 User-Agent 字段修改为“xmlset_roodkcableoj28840ybtide”后访问路由器,即可无需经过验证访问路由器的 Web 管理界面修改设备设置[16]。

●NetCore(磊科) 路由器的 IGDMPTD 程序后门。该程序会随路由器启动,并在公网上开放 53413 端口,存在一个“硬编码”写入设备固件的后门口令(从第 9 个字节开始的“netcore”字符串)[17]。攻击者可利用该后门口令登录路由器后读取系统文件,执行任意系统命令,从而控制路由器。

●Tenda(腾达) 多款路由器的后门。如果设备收到以字符串“w302r_mfg”为开头的一个 UDP 数据包,即可触发此漏洞执行各类系统命令[18]。

●ZTE(中兴) F460/F660 系列 SOHO 路由器的后门。任何用户都可以直接访问该设备一个命令执行的 Web 界面(/web_shell_cmd.gch) ,以 root 权限执行任意命令[19]。

3 SOHO 路由器的后门驻留技术

当攻击者获得目标路由器的权限之后，就可以将定制好的后门程序植入到路由器之中，达到长期驻留及隐蔽控制的目的，其中涉及到路由器后门的植入驻留技术以及路由器后门的定制开发技术。

目前市面上的 SOHO 路由器按照运行的系统大致可以分为两类：基于嵌入式 Linux 的分时操作系统以及基于 Vxworks、uC/OS-II、Zynos 之类的实时操作系统。有研究人员对目前市面上两万多种路由器固件进行了分析识别，在不考虑不能识别系统类型的部分路由器固件情况下，基于 Vxworks 实时操作系统的设备不超过 7%，因此绝大多数嵌入式设备都是基于 Linux 的分时操作系统，或者类 Unix 系统[20]。考虑到系统类型不同，不同路由器涉及到的具体后门驻留技术与实现方法亦不尽相同。

3.1 路由器后门的植入驻留技术

由于 SOHO 路由器的文件系统会在上电后由 Bootloader 从可读写的 FLASH 闪存动态加载进内存之中，对内存所做的任何修改都会在系统重启后消失，而 FLASH 中存储的根文件系统一般都是不可修改写入的，因此在一般情况下，攻击者都是通过固件升级的方法来实现路由器后门的植入和驻留的。

对于基于嵌入式 Linux 系统的 SOHO 路由器而言，由于这类路由器有着 Linux 系统的共性，其固件中一般包含有完整的文件系统，因此攻击者可以通过解包固件来获得完整的文件系统，然后将已经编译好的后门程序放置进去，并对固件进行重新打包。现今常见的打包方式包括 cramfs、squashfs、jffs2、cpio 等。而对于基于 Vxworks 等实时操作系统的 SOHO 路由器来说，由于这类路由器的文件系统一般只存放 html 等类型的静态文件，所有的可执行代码都放置在一个内核之中，因此攻击者会将编译好的后门代码插入到原有文件代码的缝隙之中，并修改系统程序调用相关部分，从而使得插入的代码获得执行。

此外，路由器的厂商为了保证固件的有效性，通常在固件刷入之前会对其进行严格的校验。使用的校验算法除常见的 CRC32、md5 外，还可能包含开发商自定义的校验方法。因此，攻击者在修改完固件之后，还需要对校验值进行相应的修改，防止固件刷入失败。

3.2 路由器后门的定制开发技术

当攻击者实现了路由器后门植入之后，就可以自由地实施各类攻击行为，比如流量转发、中间人劫持等，不同于漏洞，利用后门植入所进行的攻击危害往往更大。

基于嵌入式 Linux 系统的 SOHO 路由器后门开发相对比较简单，由于厂商一般会根据 GPL 协议公布系统的内核代码以及编译所使用的工具链（ToolChain），因此可以直接使用 C 等高级语言进行后门程序的开发。而对于基于 Vxworks 等实时操作系统的 SOHO 路由器来说，由于这类系统的耦合度较高，系统闭源，加之系统较为精简，缺乏可供分析调用的符号表，因此很难使用 C 等高级语言进行开发，一般都会使用底层的汇编语言进行编写。

虽然水平高超的攻击者可以通过自行开发代码来实现后门驻留，但目前而言，往往先通过更改系统的 NAT（Network Address Translation，网络地址转换）表来实现流量的转发，并在此基础上进一步实现中间人劫持、恶意代码替换植入等行为。由于 NAT 表是系统自带的管理工具，因此该方法具有通用、简便、轻巧等特性，应用面极广。例如，在基于嵌入式 Linux 系统的 SOHO 路由器中，可以使用系统自带的 iptables 命令来灵活的控制 NAT 表的转换策略。攻击者可以通过添加 DNAT（Destination Network Address Translation，目的地址转换）规则来将流经路由器系统的数据包转发到攻击者的服务器[21]。

具体来说，当路由器系统接收到某个匹配 DNAT 规则的数据包时，将会修改该数据包的目的地址为攻击者搭设的服务器地址，从而将数据包先转发至攻击者服务器中；当攻击者服务器接收到该路由器转发的数据包后，再次转发到真正的目的地址。不难发现，作为中间人的攻击者服务器可以在获取数据包后，对其进行解析处理、信息提取、日志记录等攻击操作。而从目的地址返回的数据包同样将通过攻击者服务器后再次转发至路由器，此时攻击者服务器将会相应修改该返回数据包的源地址，即将攻击者服务器地址隐藏为真实目的地地址，从而完成整个数据表的流转过程。整个流程对于路由器用户而言非常隐蔽，难以发现。

下面列举了一些可实现劫持某些特定类型流量的 iptables 命令：

劫持 DNS 请求

```
iptables -t nat -I PREROUTING -p udp --dport 53 -j DNAT --to <攻击者服务器 IP>:<攻击者服务器监听端口>
```

劫持 HTTP 请求

```
iptables -t nat -I PREROUTING -p tcp --dport 80 -j DNAT --to <攻击者服务器 IP>:<攻击者服务器监听端口>
```

4 结语

近几年，随着互联网的大规模普及，路由器作为网络基础设施中重要的组成部分，其安全性的需求也逐年提升。不难预见，对于路由器的安全攻防，将在产生、发现、利用以及应急响应等更多层次上展开。

首先是路由器系统的代码编写安全，路由器上游厂商应当将安全审计列入系统开发的重要环节，在源代码级别上分析和检查函数输入输出。特别是对危险函数和用户输入入口进行代码审计工作，以排查安全漏洞。同时，由于目前市面上大多数基于 Linux 系统的 SOHO 路由器设备出于成本的考虑采用了低版本内

核，因而安全性较差。随着类似路由器这样的嵌入式设备性能进一步增强和元器件成本降低，厂商应引入更新版本的内核以启用安全增强补丁，从而实现内存访问控制和地址随机化这样的安全功能。

其次为了防范路由器的后门植入，目前已经有部分厂商开始陆续将签名校验技术加入到了固件升级的过程之中。因此，按照这种发展趋势，攻击者如果无法通过特殊途径窃取到厂商证书的话，那么就将无法把定制修改过的固件成功植入到路由器之中了。但是，攻击者可能还会通过证书伪造的方法来绕过签名校验，这已经在传统的 Windows 恶意代码（比如火焰病毒）中存在过成功的应用案例，未来也有可能会应用在路由器系统的后门攻击之中，这的确需要安全研究人员和厂商持续跟踪并思考对抗之策。

最后，相比与 Windows 或 Linux 主机安全而言，路由器设备的安全应急响应工作还不够完善，存在厂商发布补丁滞后，用户部署补丁缺乏意识、操作复杂、难以完成等问题。因此如何建立有效的安全响应机制，把损失和破坏降低到最低限度也是未来针对 SOHO 路由器安全防范工作的重点和难点。

参考文献：

[1] Cui A，Costello M，Stolfo S J. When Firmware Modifications Attack：A Case Study of Embedded Exploitation [C] //Network and Distributed System Security Symposium. San Diego，CA United States：ISOC，2013：24-27.

[2] 隋新. 主机特征信息被动识别的研究与实现 [J]. 科学技术与工程，2013(03)：652-658.

[3] 王永杰，鲜明，王国玉等. 基于指纹分析的 Web 服务探测技术 [J]. 计算机工程，2005(17)：26-27.

[4] Bates R，Istance H.Zooming interfaces!：Enhancing the Performance of Eye Controlled Pointing Devices [C] //Proceedings of the Fifth International ACM Conference on Assistive Technologies. Edinburgh，United Kingdom：ACM，2002：119-126.

[5] 唐有武.基于漏洞攻击技术的路由器攻击研究与实现 [D]. 四川：电子科技大学，2012.

[6] 刘永磊，金志刚.WEP 协议攻击方法研究 [J]. 计算机工程，2010(22)：

[7] Gold S.Cracking Wireless Networks [J]. Network Security，2011(11)：14-18.

[8] Zisiadis D，Kopsidas S，Varalis A. Enhancing WPS Security [C] //IFIP Networking. Prague，Czech Republic：IEEE，2012：21-23.

[9] 吴明峰，张永胜，李园园等. Web 服务攻击技术研究 [J]. 计算机技术与发展，2012(01)：213-216.

[10] Craig. Exploiting Embedded Systems [EB/OL]. 2011 [2016-06-12]. http://www.devttys0.com/2011/09/exploiting-embedded-systems-part-2/.

[11] Exploit D B. D-Link DSR Router Series - Remote Root Shell Exploit [EB/OL]. 2012 [2016-06-18]. https://www.exploit-db.com/exploits/30062/.

[12] Security Focus. Multiple D-Link DIR Series Routers 'model/__show_info.php' Local File Disclosure Vulnerability [EB/OL]. 2013 [2016-06-18]. http://www.securityfocus.com/bid/64043.

[13] Secure Works. TP-Link TL-WR840N Configuration Import Cross-Site Request Forgery(CSRF) [EB/OL]. 2015 [2016-06-12] https://www.secureworks.com/research/swrx-2015-001.

[14] 王炜，赵旭，吴少华. 揭秘家用路由器 0day 漏洞挖掘技术 [M]. 北京：电子工业出版社，2015：134-139.

[15] Craig. MIPS ROP IDA Plugin [EB/OL]. 2013 [2016-06-14]. http://www.devttys0.com/2013/10/mips-rop-ida-plugin/.

[16] IceArmour. 我是如何反编译 D-Link 路由器固件程序并发现它的后门的 [EB/OL].2011 [2016-06-12]. http://www.freebuf.com/articles/wireless/14964.htm/.

[17] 知道创宇. Netcore / Netis 路由器后门应急概要 [EB/OL]. 2015 [2016-06-14]. http://blog.knownsec.com/2015/01/a-brief-analysis-of-netcore-netis-leak-emergency/.

[18] Craig. From China，With Love [EB/OL].2013 [2016-06-18]. http://www.devttys0.com/2013/10/from-china-with-love/.

[19] 知道创宇. ZTE SOHO ROUTERWEB_SHELL_CMD.GCH 远程命令执行 分析概要 [EB/OL].2015 [2016-06-14]. http://blog.knownsec.com/2015/01/analysis-of-zte-soho-routerweb_shell_cmd-gch-remote-command-execution/.

[20] Chen D D，Egele M，Woo M. Towards Automated Dynamic Analysis for Linux-based Embedded Firmware [C] //Network and Distributed System Security Symposium. San Diego，CA United States：ISOC，2016：21-24.

[21] 陈岚.Iptables 规则集优化的设计与实现 [D]. 湖北：武汉科技大学，2008.

作者简介：

李翔豪（1984—），男，硕士研究生，主要研究方向为信息安全；

王轶骏（1980—），男，硕士，讲师，主要研究方向为网络攻防及系统安全；

薛　质（1971—），男，博士，教授，主要研究方向为计算机通信及信息安全。