



GreyFan: 一种 Wi-Fi 隐蔽信道攻击框架

马栋捷^{1,2}, 金成强^{1,2}, 陈园^{1,2}, 陈铁明^{1,2,3}

(1. 浙江工业大学计算机科学与技术学院, 浙江 杭州 310023;

2. 浙江省网络空间安全创新研究中心, 浙江 杭州 310023;

3. 之江实验室工业互联网研究中心, 浙江 杭州 311100)

摘要: 针对现实网络中诸如侧信道攻击、HID 攻击等传统的物理攻击, 物理隔离被认为是一种较为彻底的抵御网络攻击的安全防护手段。2018 年, 业界首次提出了一种物理隔离环境下的 Wi-Fi 隐蔽信道方法——Ghost Tunnel, 即在 Wi-Fi 尚未连接的状态下, 无线 AP 可成功将数据传给发起连接请求的计算机。提出了一种基于 Ghost Tunnel 方法的攻击框架——GreyFan, 利用该攻击框架攻击者可以对未连接 Wi-Fi 的用户实施无感知攻击, 如文件隐蔽传输、任意代码执行等, 并分析了相应的防御技术。

关键词: HID 攻击; 网络隔离; 隐蔽信道; GreyFan 攻击

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2019179

GreyFan: a network attack framework using Wi-Fi covert channel

MA Dongjie^{1,2}, JIN Chengqiang^{1,2}, CHEN Yuan^{1,2}, CHEN Tieming^{1,2,3}

1. College of Computer Science and Technology, Zhejiang University of Technology, Hangzhou 310023, China

2. Zhejiang Innovation Center of Cyberspace Security, Hangzhou 310023, China

3. Research Center of Industrial Internet, Zhejiang Lab, Hangzhou 311100, China

Abstract: For traditional physical attacks such as side channel attacks and HID attacks in real networks, physical isolation is considered to be a relatively complete security protection against network attacks. In 2018, a Wi-Fi hidden channel method in the physical isolation environment——Ghost Tunnel was firstly proposed, that is, in the state that Wi-Fi didn't connected, the wireless AP could successfully transmit data to the computer that initiates the connection request. An attack framework based on the Ghost Tunnel method——GreyFan was proposed. This attack framework enabled attackers to implement non-aware attacks on users who didn't connected to Wi-Fi, such as file concealed transmission and arbitrary code execution, etc. The corresponding defense technology was also analyzed.

Key words: HID attack, network isolation, covert channel, GreyFan attack

收稿日期: 2019-05-24; 修回日期: 2019-07-03

基金项目: 国家自然科学基金资助项目 (No.61202282, No.61772026); 国家自然科学基金与浙江省政府联合项目 (No.U1509214)

Foundation Items: The National Natural Science Foundation of China (No.61202282, No.61772026), The Joint Project of National Natural Science Foundation and Zhejiang Provincial Government (No.U1509214)



1 引言

隐蔽信道是一种违反安全策略的秘密传输信息的机制。它将数据报作为通信载体,将指定数据嵌入数据报文中,达到指定数据在网络中秘密输出而不被发现的目的。利用隐蔽信道,攻击者不仅可以目标主机中的数据信息传送到攻击机获取情报,还可以传送控制命令,控制目标主机。它不仅会对网络数据的安全造成危害,甚至还会损害计算机硬件^[1]。

基于隐蔽信道的网络攻击不需要复杂的计算机环境和操作条件,仅需要目标主机感染恶意客户端,即可将指定数据根据已经构建好的协议嵌入载体数据中,并与正常通信的流量混杂在一起,使其难以区分,从而隐藏通信通道。攻击机收到数据后进行响应,将嵌入的数据从伪装的数据报中分离出来,提取其中的关键数据。通过隐蔽信道进行攻击的方式往往让目标主机使用者难以察觉,隐蔽性极高^[2]。

随着对现代隐蔽信道技术研究的不断深入和反隐蔽信道攻击技术的持续发展,使用仅由 ICMP、HTTP 等协议构建的隐蔽信道作为攻击框架核心已无法满足实际应用中具有高隐蔽性、高安全性、高效率性的隐蔽信道攻击框架的迫切需求。因此,本文构建了一种隐蔽信道攻击框架——GreyFan 攻击框架。在架构上,该框架以 Ghost Tunnel 理论为基础,根据使用目的、使用对象、使用场景的不同,定义了全新的传输帧格式,设计了全新的传输协议,不仅保证了数据在传输过程中具有较好的稳定性和可靠性,同时还有效地将传输的数据进行了模块化划分,使各模块具有较好的规范性,使框架具有较好的扩展性;在功能上,利用该框架能够在不确定主机是否成功建立网络连接的情况下建立长连接的隐蔽信道,拥有远程控制、文件传输等功能,并可自主选择加密方式、发送分组初始量、发送分组间隔时间等,同时预留了异常检测逃避、系统实时监控等常用接口。

本文首先介绍了 GreyFan 攻击框架的研究背景,其次阐述了 GreyFan 攻击框架的基本结构、组成和功能,接着通过实验对该框架的可靠性、稳定性、通用性和时效性进行了验证,最后提出了对该种攻击框架的检测方法并进行总结。

2 相关工作

2.1 国内外对隐蔽信道的研究现状

隐蔽信道作为攻击框架的核心,它的构建使攻击框架的设计成为了可能。目前,国内外对于隐蔽信道的研究主要集中在从网络应用服务、网络协议和移动网络中寻找构建的可能性。

在网络应用服务方面,王娟等人^[3]提出了一种基于浏览器帮助对象(browser helper object, BHO)构建网络隐蔽信道的方法,这种方法不仅能躲避杀毒软件和防火墙,还能为流量隐蔽和代理穿透提供有利条件。

在信道建立方法以及网络协议方面,Ahmadzadeh 等人^[4]提出了利用差分通信信道导出公式来建立网络隐蔽通道的新方法;姬国珍等人^[5]实现了基于 ICMP 数据分组时间间隔的时分型隐蔽信道;李卫等人^[6]针对网络地址转换情况下信息传输行为和内容的强隐蔽需求,提出了一种适用于 NAT 环境的隐蔽信道构建方法;朱越凡等人^[7]利用互联网不可或缺的 NTP(network time protocol, 网络时间协议),设计了下行通道和上行通道分离的 NTP 隐蔽信道,提出了基于 NTP 的隐蔽信道构建机制。

在移动网络方面,Tan 等人^[8]针对 LTE 视频流提出了一种基于 VoLTE 的构建隐蔽定时信道的方法,该方法通过故意丢弃视频分组来调制屏蔽信息,进而构建隐蔽定时信道;Yang 等人^[9]提出现有移动系统可能会因受到恶意软件的攻击,而被迫改变无线网络接口的阻抗,从而迫使移动设备反射周围的 RF 信号,达到建立隐蔽信道传达信息的目的。Schulz 等人^[10]在智能手机上的 Wi-Fi 中构建隐蔽通道,通过在传输之前预先过滤 Wi-Fi

帧,利用信道状态信息(channel state information, CSI)在接收器侧提取嵌入信息。

这些隐蔽信道虽然具有隐蔽性强、传输效果好、灵活性高等特点,但是在物理隔离的条件下,这些隐蔽信道均无法正常使用。而目前,对在物理隔离环境下的隐蔽信道研究还基本处于空白。

2.2 物理隔离环境下的攻击方式

物理隔离指的是计算机禁止直接或间接地接入公网等非安全网络,它能够阻止重要计算机设备与非安全网络发生物理层面的接触。一般而言,在物理隔离环境下,计算机无法通过互联网被注入病毒或木马,避免了数据泄露或设备瘫痪等安全隐患,一定程度上提高了安全性。

然而,针对物理隔离环境同样也存在一些特别的攻击手段。U 盘攻击是一种将恶意代码存放于 U 盘的固件中,利用 U 盘在设备上的插拔使计算机设备被感染恶意代码的攻击方式;CD/DVD 攻击指的是利用 CD/DVD 等介质对 CD/DVD 的刻录软件的感染,从而完成对光盘类介质的感染,使光盘成为针对隔离网络的攻击工具和感染途径;水坑攻击是一种通过将恶意软件伪装成系统补丁、软件工具等常用软件,并利用社会工程学诱导计算机工程师下载、安装至物理隔离环境中的计算机,达到攻击目的的攻击方式;HID 攻击是一种将包含恶意脚本的 USB 设备模拟成人机交互设备,使计算机机会由于错误地将其识别为人机交互设备而导致执行攻击脚本的攻击方式。

这些针对物理隔离环境下的攻击方式虽然隐蔽性好,但对恶意软件在目标主机上的维护则较为困难,灵活性较差。

2.3 Ghost Tunnel 隐蔽信道

在 2018 年年初,一种 Wi-Fi 物理隔离环境下的隐蔽通信技术——Ghost Tunnel 首次 in HITB 国际会议上被提出,在 Wi-Fi 尚未连接的状态下,无线接入点可将数据传给发起连接请求的计算机。

攻击者首先建立一个具有特殊 SSID (service

set identifier, 服务集标识)的恶意无线接入点,并向周边发送 Beacon 广播帧宣告本网络的存在;当被感染了恶意软件的目标主机打开无线网络时,原本用于扫描所在区域内是否存在 IEEE 802.11 网络的 probe request 帧,可携带具有特殊含义的数据进行发送;当无线接入点收到客户端的请求帧后,原本用于对客户端的 SSID 探测请求进行应答的 probe response 帧,也可携带指定数据进行发送,由此构成的 Wi-Fi 隐蔽传输通道就称作 Ghost Tunnel。

Ghost Tunnel 技术在理论上为物理隔离环境下构建隐蔽传输信道或隐蔽操控目标主机提供了一种新的途径。但在实际环境中, Ghost Tunnel 技术无法解决复杂的电磁环境干扰带来的分组丢失、出错等问题;此外, Ghost Tunnel 技术未对传输的内容进行细节化、模块化,导致无法在其基础上扩展出新的功能。

3 GreyFan 攻击框架

基于现有的隐蔽信道传输技术,结合 Ghost Tunnel 技术,本文构建了一种名为 GreyFan 的隐蔽信道攻击框架,而利用该框架进行的攻击被称为 GreyFan 攻击。该框架可分为三层结构,框架结构如图 1 所示。第一层为 GreyFan 隐蔽信道模型,用于在攻击者与目标主机之间建立稳定的长连接;第二层为传输帧结构,用于规范不同应用下的传输帧所携带的具体内容,方便应用层功能的添加与修改;第三层为应用层,用于提供具体的功能,该框架可自主选择传输加密方式、发送分组初始量、发送分组间隔时间等,并预留了异常检测逃避、系统实时监控等接口,方便后续开发。目前,该框架可实现远程控制目标主机、向目标主机传输文件等功能。

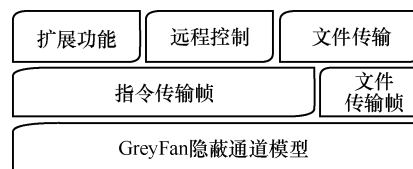


图 1 GreyFan 攻击框架结构



3.1 GreyFan 隐蔽信道模型

GreyFan 隐蔽信道模型为在 Wi-Fi 物理隔离的条件下建立稳定的隐蔽信道提供了基础。在 Wi-Fi 建立阶段, 无线接入点与客户端均采用 IEEE 802.11 协议中的管理帧进行通信, 管理帧主体为长度固定的字段和长度不定的信息元素。正是因为信息元素部分的内容可变, 因此给隐蔽信道的建立提供了可能。

信息元素通常包含 3 个部分: 元素 ID 字段、信息长度字段以及信息内容字段^[11], 如图 2 所示。元素 ID 字段用于标识每一种信息元素的类型, 信息长度字段标识第三部分的长度, 信息内容字段携带具体的信息。GreyFan 攻击在不建立完整 Wi-Fi 连接的情况下, 使 probe request 帧和 probe response 帧携带指定 ID 的冗余信息元素, 从而建立隐蔽通信通道。

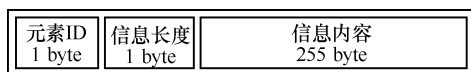


图 2 管理帧信息元素结构

攻击者与目标主机之间的基本通信流程如图 3 所示。目标主机在感染恶意程序后, 无论其是否连接网络, 均会主动发送携带含有特定元素 ID 的冗余信息元素的 probe request 帧; 攻击者在接收到 probe request 帧后, 解析其 ID 字段及具体信息内容, 判定目标主机是否处于准备状态, 并发送携带由恶意指令组成的冗余信息元素的 probe response 帧; 目标主机在收到 probe response 帧后, 解析其 ID 字段及具体信息内容, 并根据内容执行后续操作。

然而在现实环境下, 电磁环境复杂, 容易导致数据分组的丢失, 造成数据传输失败。因此, 被控端在发送 probe request 帧时, 帧内需要携带上一次收到 response 帧的时间的散列值; 而控制端在发送 probe response 帧时, 帧内需要携带本次帧发送时间的散列值。

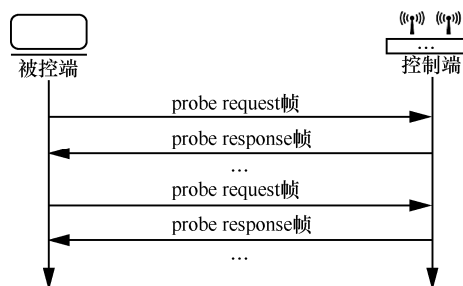


图 3 攻击者与目标主机之间的基本通信流程

此外, 计算机存在缓存机制, 会导致重复接收数据, 因此被控端在解析信息内容后, 将缓存该信息元素的散列值, 当再次收到 probe response 帧时, 将校验该帧内信息元素的散列值是否与缓存下的散列值相同, 若相同, 则不执行相关操作。

3.2 传输帧结构

在建立隐蔽信道通信的过程中, 传输帧携带的内容不仅关系到传输效率, 还会影响传输的可靠性。而在不同的应用场景下, 传输帧需要携带的信息也不尽相同。因此, 为了平衡传输的效率和可靠性, 同时为应用层提供一种可复用的帧结构、简化应用层的扩展难度, 根据帧工作性质的不同, 将帧分为指令传输帧及文件传输帧。

指令传输帧的帧信息元素结构如图 4 所示。

它将 255 byte 的冗余信息元素分为 4 个部分: 第一部分为特殊字段, 占 3 byte, 用于标识该帧用于执行命令; 第二部分为散列值字段, 占 8 byte, 用于可靠传输; 第三部分为具体命令信息字段, 占 240 byte, 用于携带需要传输的具体命令; 第四部分为保留字段, 占 4 byte, 用于未来扩展及优化。

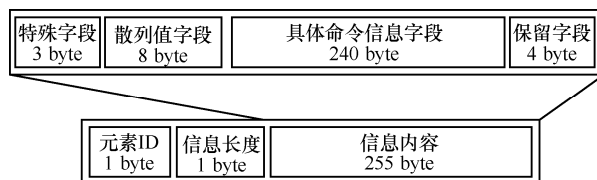


图 4 指令传输帧格式

文件传输帧的帧信息结构如图 5 所示, 它将 255 byte 的冗余信息元素分为 7 个部分, 各部分含义及用途见表 1。

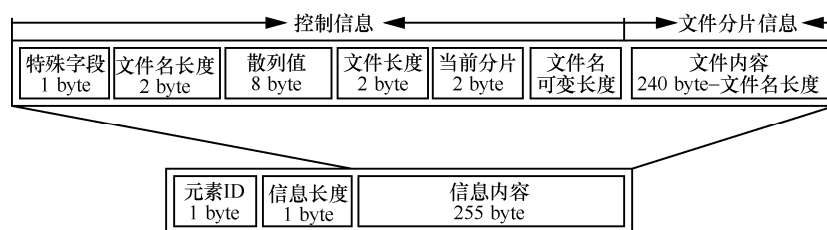


图5 文件传输帧格式

表1 文件传输帧功能解释

字节数/byte	含义	用途
1	特殊字段	标识该帧用于传输文件
2	文件名长度	标识文件名的长度, 用 16 进制表示
8	散列值	用于可靠传输
2	文件总长度	标识文件的总片数, 用 16 进制表示
2	当前分片序号	标识当前分片所属的位置, 用 16 进制表示
0 ~ 240	文件名	标识文件的保存名称, 可带具体路径
0 ~ 240 - 文件名长度	文件的具体内容	发送具体的文件信息

3.3 远程控制及文件传输

远程控制和文件传输是 GreyFan 攻击框架应用层中的具体应用。远程控制指的是无论用户是否建立网络连接, 攻击者均可无感知地操控目标主机, 进行执行脚本、开关计算机、修改计算机配置文件等敏感操作。文件传输指的是无论用户是否建立网络连接, 攻击者均可将本地文件无感知地传输至目标主机的指定目录下。

在远程控制应用中, 被控端与控制端均发送指令传输帧, 完成一次隐蔽远程控制, 被控端系统流程如图 6 所示, 控制端系统流程如图 7 所示。而在文件传输应用中, 被控端发送指令传输帧,

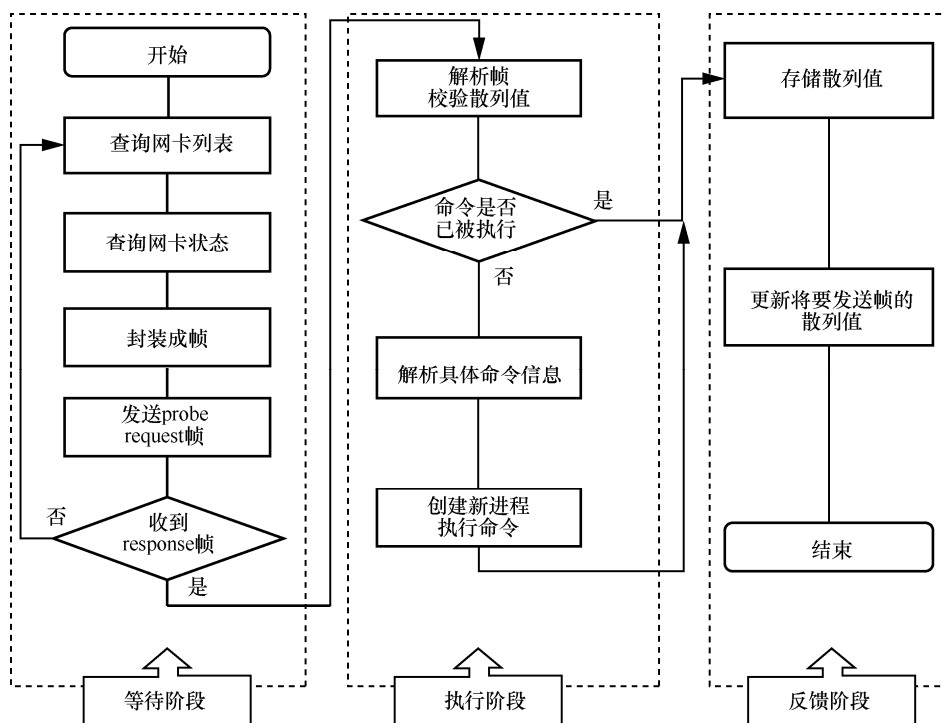


图6 远程控制时被控端系统流程

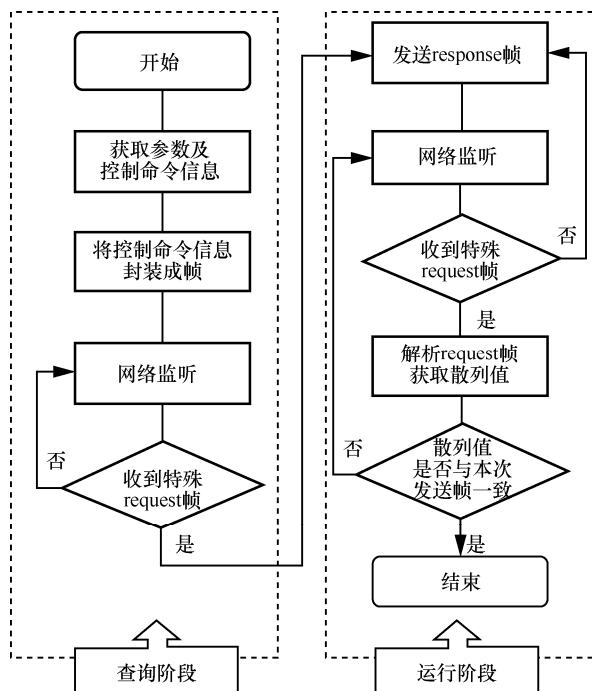


图 7 远程控制时控制端系统流程

控制端发送文件传输帧,完成一次隐蔽文件传输,被控端系统流程如图 8 所示,控制端系统流程如图 9 所示。

对于被控端而言，完成一次 GreyFan 攻击，需经历等待、执行和反馈 3 个阶段。在等待阶段，被控端调用系统 Wi-Fi 模块资源，持续发送包含特定信息头的 probe request 帧，并等待 probe response 帧，一旦收到，则进入执行阶段，否则依然处于等待阶段。在执行阶段，若进行远程控制，则解析帧内容，并创建进程，执行命令；若进行文件传输，则解析帧内容，并根据控制信息内的文件名字段按指定的保存路径保存文件信息。在反馈阶段，被控端需要将 probe request 帧内携带的时间散列字段更新为最新收到的 probe response 帧的时间散列值，若进行的操作为文件传输，还需将具体命令信息字段更新为被控端进行解析、接收和存储后的结果代码，之后持续发送，等待下一次命令或下一个文件。

对于控制端而言，完成一次 GreyFan 攻击，需经历查询和运行两个阶段。在查询阶段，控制端启动网络监听功能，持续监听是否收到含有指定信息头的 probe request 帧，一旦收到，则进入

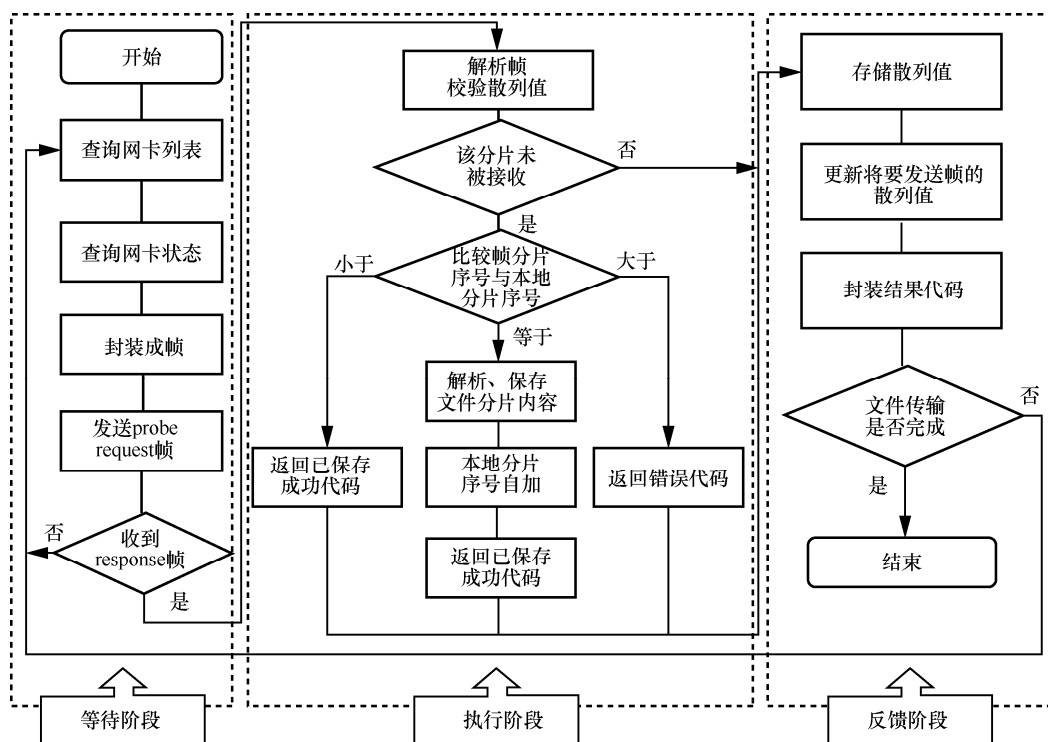


图 8 远程文件传输时被控端系统流程

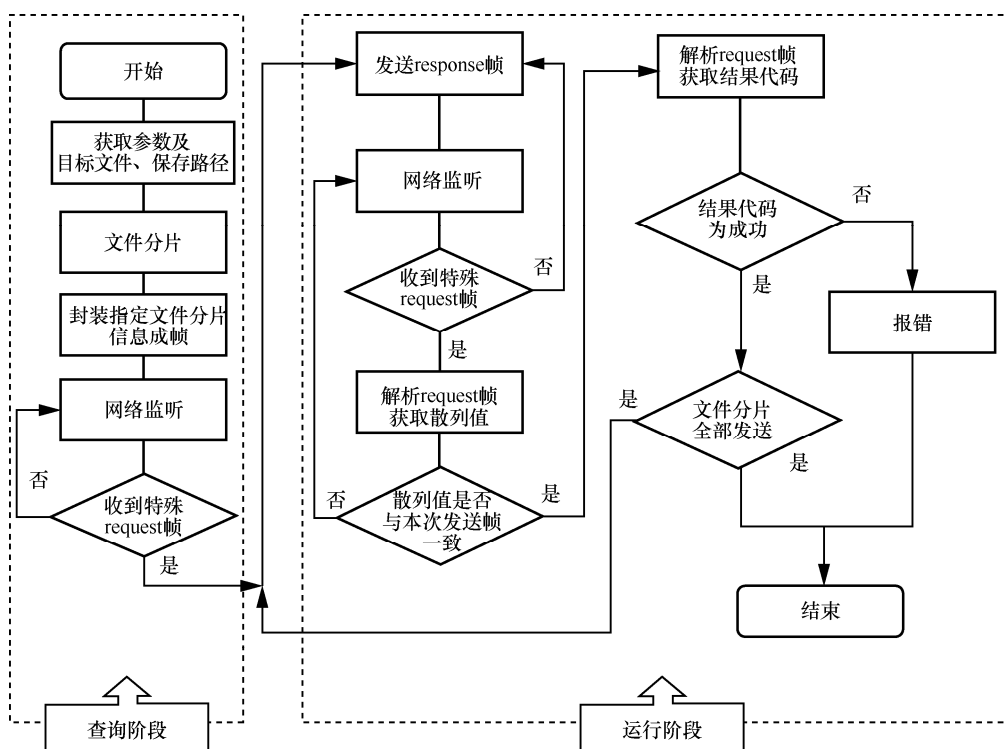


图9 远程文件传输时控制端系统流程

运行阶段，否则依然处于查询阶段；同时，如果需要执行文件传输，则还需将用户指定发送的文件进行分片。在运行阶段，若进行远程控制，则发送携带当前时间散列值及用户远程控制命令的 probe response 帧；若进行文件传输，则发送携带控制信息及文件分片信息的 probe response 帧。之后等待被控端返回包含当前发送帧所携带的时间散列值的确认信息 probe request 帧。如果超过一定时间依旧未收到确认信息，则增加发送分组量重新发送。

3.4 扩展功能

由于应用 GreyFan 攻击框架的场景不同，攻击者需要一次性发送的分组量也会有所不同。为了提高框架应用的灵活性，GreyFan 攻击框架可自主选择发送分组的初始量以及超时时间。当 GreyFan 攻击框架在超时时间内未成功接收到来自于被控端的消息响应时，则判定被控端未正常接收指令或信息，此时，控制端会在其上一次发

送分组量的基础上增加 100，并重新发送分组，以增加被控端成功接收的概率。

在文件传输中，由于外界干扰，传输的过程可能会被中断。因此，为了提高文件传输的可靠性及灵活性，GreyFan 攻击框架支持从断点续传功能，即当文件传输中断时，可从中断分片处或已完成传输分片处继续传输。

为了提高 GreyFan 攻击的隐蔽性，GreyFan 攻击框架支持自主选择是否加密及传输加密方式，目前 GreyFan 攻击框架支持的加密方式有 AES 加密和 RC4 加密。

为了使攻击者能够更好地使用 GreyFan 攻击，GreyFan 攻击框架预留了异常检测逃避、系统实时监控等接口，从而使攻击者能够更好地将该框架与其他系统对接。

4 实验与分析

本节针对远程控制和文件传输两种场景，分



别设计了多组对照实验,对 GreyFan 攻击框架的稳定性、时效性、可靠性和通用性进行了验证。

在硬件方面,控制端采用处理器为 Intel Core i5-3317U 的计算机,四核,主频为 1.7 GHz,内存 4 GB,华硕 UX32V 内置网卡,操作系统为 64 位 Kali 系统;被控端采用处理器为 Intel Core i7-6500U 的计算机,四核,主频为 2.5 GHz,内存 8 GB, Dell 灵越 15-5559 内置网卡,操作系统为 64 位的 Windows 7 系统。

在软件方面,控制端运行 GreyFan 攻击框架的控制应用程序,模拟攻击者;被控端运行更新至 2018 年 9 月最新病毒库的 360 杀毒软件、GreyFan 攻击框架的被控应用程序,模拟被恶意软件感染的目标主机。为了便于统计与分析,控制端与被控端详细的通信时间及过程分别打印至本地控制台。

为避免真实环境中其他网卡的干扰,实验环境为地下车库。

4.1 远程控制测试

在测试远程控制的稳定性、时效性和可靠性的实验中,将 Windows 环境下打开计算器的 cal 指令作为实验指令,将初始发送分组量设置为 500,将超时时间设置为 10 s,分别在控制端与被控端间隔为 10 m、15 m、20 m、25 m、30 m、40 m、45 m 的条件下进行实验,同一距离下测试 20 次。实验步骤如下。

在确定控制端和被控端的间距距离后,首先在被控端启动被控端应用程序,确定被控端已被激活。之后在控制端发送远程控制指令,并开始计时,直至被控端接收到指令并成功打开计算器后,记录下当前消耗时间,并将其作为被控端响应时间。由于 GreyFan 攻击框架要求被控端在执行完命令后需要返回确认信息给控制端,因此当控制端收到返回的信息后,停止计时,并将从被控端打开计算器到控制端接收到确认信息的时间作为控制端消耗时间。若控制端在传输过程中出

现错误、被控端未成功打开计算器或杀毒软件提示异常,则视为控制失败。

图 10 展示了在相隔距离不同的条件下,去除最大最小值后,被控端响应及控制端消耗的平均时间及时间标准差。图 11 展示了在相隔距离不同的条件下,被控端响应时间及控制端消耗的时间离散图。

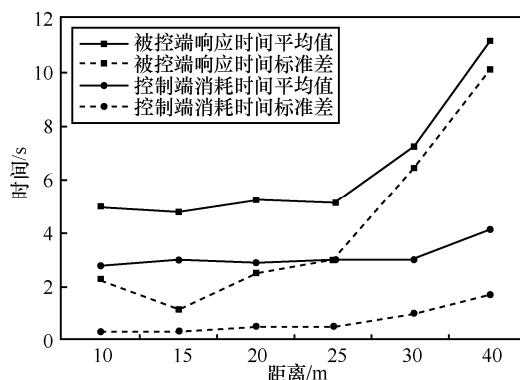


图 10 不同距离下被控端响应及控制端消耗时间平均值及标准差

从稳定性角度看,随着距离的逐渐增大,攻击的不稳定性逐渐上升。在实验中,当控制端与被控端之间的距离在 0~25 m 时,每次实验时的被控端响应时间和控制端消耗时间基本一致,说明此时 GreyFan 攻击框架具有较好的稳定性;在 25~45 m 时,被控端响应所消耗的时间和离散程度急剧上升,而控制端消耗的时间和离散程度也有所增加,说明此时攻击出现了不稳定性;当距离超过 45 m 时,攻击失效。

之所以随着距离的增大稳定性逐渐变差,是由于受到了实验双方内置网卡传输距离和计算机自身功率的限制:在距离较近的条件下,双方网卡均能够及时收到对方发送的 probe 帧,故每次测试消耗的时间基本一致,传输较为稳定。而当距离间隔较远时,实验双方可能会存在分组丢失的情况,然而由于 GreyFan 攻击框架具有可靠传输机制,当控制端发送控制命令后,一旦被控端丢失数据分组,则无法在规定时间内返回确认信息,控制端则会增加发送分组量,重新发送命令,因此被控端响应时间会急剧上升,其上升的幅度

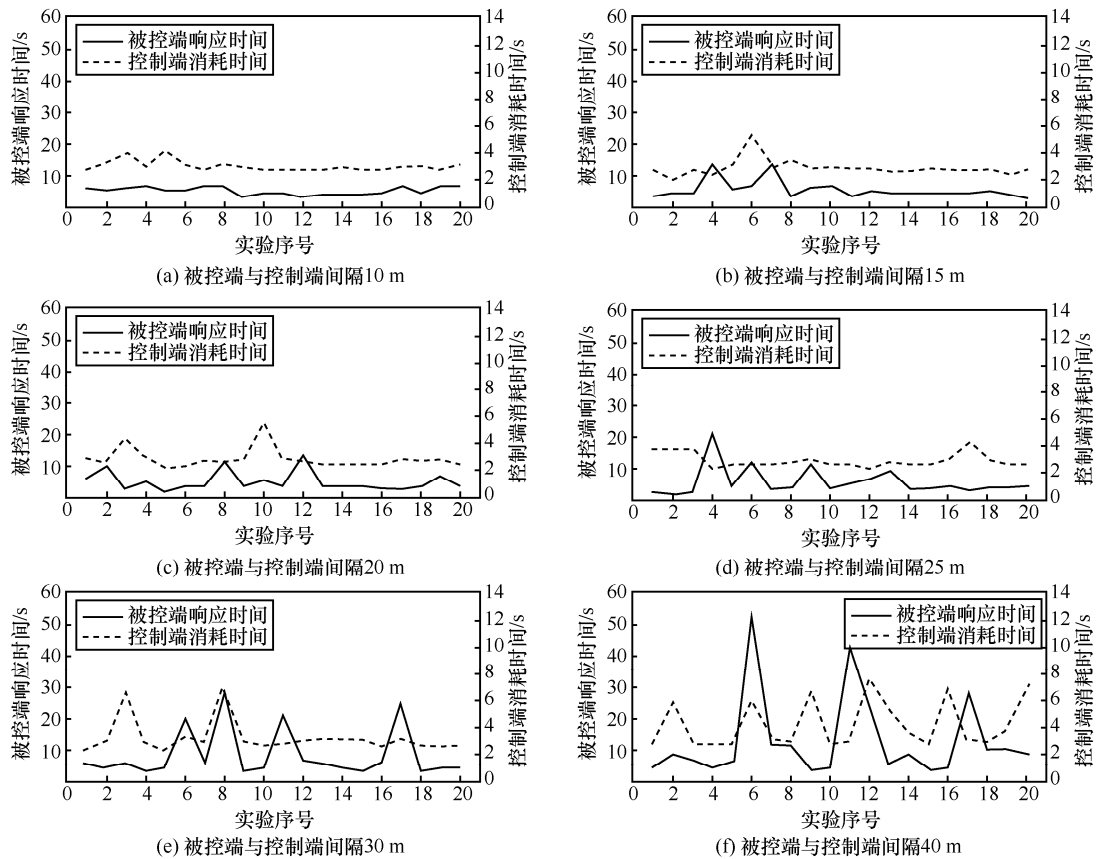


图 11 不同距离下被控端响应时间及控制端消耗时间离散图

与设定的超时时间有关；而当被控端返回的确认信息丢失时，由于该信息封装在 request 帧中，是不断发送的，因此，控制端消耗时间只是略微增加。当双方距离超过网卡能够接受的距离后，无论控制端如何增加发送的数据分组，被控端均无法接收，故攻击失效。综上所述，在使用 GreyFan 攻击框架时，为了增加控制的稳定性，控制端应当尽可能地在距离被控端周围较近的位置进行控制。

从时效性角度看，若被控端能够及时响应控制端发送的控制命令，其平均时间为 5~6 s，若控制端能够及时接收确认信息，其平均时间为 2~3 s。因此在近距离情况下，完成一次远程控制工作需要 7~10 s。而在远距离情况下，被控端响应时间为 5~55 s，而控制端消耗时间为 2~8 s。

之所以在近距离情况下被控端响应时间会比

控制端消耗时间长，是因为被控端在接收到控制端发送的 probe response 帧并解析后，还需要调用系统进程打开计算器，通过测算，该过程消耗的时间为 2~3 s。而控制端收到被控端发送的 probe request 帧确认信息并解析后，只需要进行一次判断运算，其消耗时间可忽略不计。因此，probe response 帧的实际传输时间与 probe request 帧的实际传输时间基本一致，为 2~3 s。

之所以在远距离情况下被控端响应时间远大于控制端消耗时间，是因为 GreyFan 攻击框架中的可靠传输机制。控制端重传的条件是当在设置的超时时间内未收到确认信息，则重传，而在本次实验中超时时间设置为 10 s，因此两次发送数据分组的间隔时间最小为 10 s，当多次在被控端响应阶段发生分组丢失情况时，被控端响应时间则成倍增加；而对于被控端发送的确认消息而言，



由于其确认消息被封装于 request 帧中, 而该帧不断向外发送以表示本机已被激活, 因此, 由于两次发送帧的时间间隔短, 当多次在控制端消耗阶段出现发送分组丢失时, 控制端消耗时间仅略微增长。

之所以完成一次远程控制工作需要两倍的传输时间加执行命令时间, 同样是因为 GreyFan 攻击框架中具有可靠传输机制, 该机制为了提高传输的可靠性, 要求控制端发送控制指令后, 需要等待被控端返回的确认信息, 否则将重新进行发送。因此牺牲了一定的传输效率。

从可靠性角度看, 在间隔 10~40 m 的测试条件下, 虽然执行的时间随着距离的不同不断波动, 但是所有命令最终均可以成功执行, 未出现控制失败的情况。而可靠性讨论的是被控端与控制端之间在能够正常通信的情况下完成预定功能的能力, 故在 40 m 以外的条件下, 被控端与控制端双方因受到计算机设备硬件的限制而无法攻击成功, 其不属于可靠性的讨论范畴。因此, GreyFan 攻击框架虽然牺牲了传输效率, 但是却拥有极高的攻击可靠性。

在测试远程控制的通用性实验中, 被控端与控制端间隔 20 m, 在控制端分别输入 Windows 环境下 15 大类共计 90 种命令, 检测被控端能否正常执行以及杀毒软件是否能够检测出风险。若被

控端未成功执行或杀毒软件检测出了病毒或进行了风险提示, 则该命令记为不可执行。测试命令个数与可执行命令个数的统计情况如图 12 所示。

从通用性角度看, Windows 环境下所有的 DoS 指令均可以正常运行, 其指令类别涵盖了复制操作、进程操作、目录操作、文件操作、时间操作、控制操作、环境变量操作、CMD 操作、网络操作、ACL 操作、计划操作、机器操作、驱动操作、硬盘操作和其他操作, 其中部分命令甚至涉及一些计算机的敏感操作。但在执行这些命令时, 计算机并未进行阻止, 并且成功绕过了运行在被控端上的杀毒软件。因此, GreyFan 攻击框架具有通用性。

4.2 文件传输测试

在测试远程文件传输的实验中, 在被控端与控制端间的距离间隔为 15 m 的条件下, 将一个大小为 500 byte 的 txt 文件作为测试文件, 初始发送分组量设置为 500, 超时时间为 10 s, 被控端存放文件的路径为 “1.txt”, 共测试 20 次, 实验步骤如下。

首先在被控端启动被控端应用程序, 确定被控端已被激活。之后在控制端发送远程文件传输指令, 将本地的文件发送至被控端, 并开始计时, 直到控制端收到最后一次返回的确认信息并提示

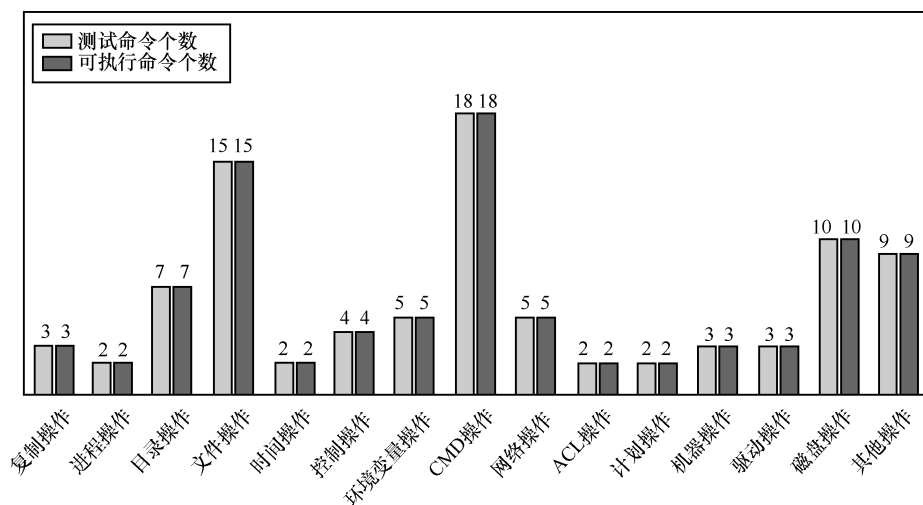


图 12 执行命令情况统计

完成传输后，停止计时，将这段时间记为远程传输文件的总消耗时间。若控制端在传输过程中出现错误、被控端接收的文件出现错误或杀毒软件提示异常，则视为传输失败。远程传输文件消耗时间及中断次数如图 13 所示。

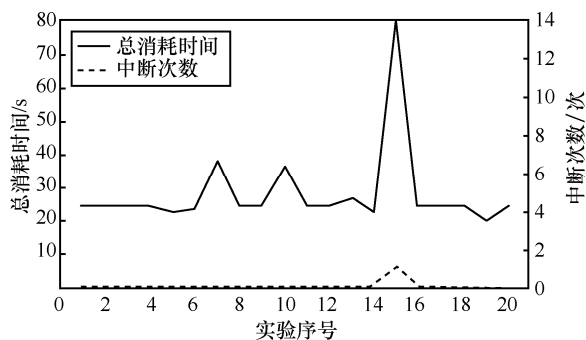


图 13 远程传输文件消耗时间及中断次数统计图

从时效性角度看，有 17 次传输测试花费的时间为 22~28 s，有 2 次传输测试花费了将近 40 s 的时间，有 1 次传输花费了将近 80 s 的时间。

之所以大部分测试的总耗时在 22~28 s，是因为在本实验中，一个文件传输帧可携带的具体内容字节数最高为 235 byte，因此 500 byte 的 txt 文件需要 3 个分片，即至少需要完成 3 次可靠传输，才能将文件发送至被控端。在控制端与被控端均能够良好地接收到数据分组的情况下，完成一次可靠传输需要 8 s 左右，因此，在预定的实验条件下，至少需要 24 s 左右的时间才能完成 500 byte 文件的传输。

之所以有少部分测试会有较高的总耗时，是因为在间隔为 15 m 的条件下，可能会出现被控端与控制端间通信数据分组的丢失，而由 GreyFan 攻击框架中的可靠传输机制可知，控制端判定一帧是否发送失败的条件是在超时时间内是否收到了被控端发送的确认信息，因此，在本实验中两帧的间隔时间至少为 10 s，这也导致了总消耗时间的增加。此外，由于 GreyFan 攻击框架支持断点续传，因此在第 15 次实验中发生中断故障后，需要人为再次启动命令程序，这势必会消耗大量

的时间。

从可靠性角度看，除了第 15 次传输测试外，其余测试虽然可能发生了分组丢失情况，但在可靠机制的保护下，最终均完成了传输任务，保证了传输的可靠性。而在第 15 次传输的过程中发生了中断的情况，主要是因为控制端在规定时间内未收到确认信息，下一次发送帧时需要增加发送分组量进行重新发送，然而发送 probe response 帧的过程需要占用较多的内存，故当发送分组量过大时，会导致内存不足，从而被迫中断。因此，虽然 GreyFan 攻击框架可以无限制地增大发送分组量以提高被控端接收的概率，但在实际情况下，由于受到缓存空间的限制，发送分组量是有上限的，而随着文件大小的增加，完成可靠传输的次数逐渐增加，因分组丢失而增加发送分组量的次数也随之增加，这也间接地增加了缓存的压力，提升了中断出错的概率。因此，文件传输在传输小型文件（如脚本文件）时，可靠性较高。

5 攻击检测与防御

GreyFan 攻击的关键在于对 IEEE 802.11 协议中管理帧的发送与接收，而对于操作系统系统和杀毒软件而言，它们并没有对其进行防御或检测，这也是被控应用程序能够在运行时成功绕过杀毒软件检测和系统防火墙防御的重要原因。因此，为了保护用户的个人财产和隐私不受到侵犯，在主机层面和网络层面提出了防御 GreyFan 攻击的方法。

5.1 主机层面

CPU 使用率指的是计算机中运行的程序所占用的 CPU 资源，表示计算机在某个时间点的程序运行情况。利用 GreyFan 攻击框架进行攻击的目的往往是窃取信息、破坏系统等，这势必会消耗系统的部分 CPU 资源。因此可检测 CPU 使用率，并重点关注使用率最高的前 3 个任务，当所属任务的分类属于报文接收和发送类任务时，可考虑采



取暂时关闭 Wi-Fi 模块等措施, 达到防御的目的。

5.2 网络层面

WIPS (wireless intrusion prevention system, 无线入侵防御系统) 指的是能够监测无线范围内未授权的接入、并能自动采取应对措施的网络设备^[13]。在网络、空间内部署该系统后, 可利用该系统对区域内的无线网络环境进行实时监听。一旦识别出攻击行为, 则通过多种渠道立即阻断对应的 2.4 GHz 和 5 GHz 的频段, 同时记录下 Wi-Fi 设备的特征、攻击行为样本并报告管理员, 达到拦截、阻断、取证、追踪的目的。

因此, 可利用 WIPS 解析无线管理帧内容, 验证其是否具有 GreyFan 攻击的特征信息^[12], 如信息元素中的元素 ID 字段存在非特定内容等, 从而达到识别 GreyFan 攻击行为的目的。

6 结束语

针对在物理隔离环境下建立隐蔽信道的需求, 本文提出了一种 Wi-Fi 隐蔽信道攻击框架——GreyFan 攻击框架。实验测试表明, GreyFan 攻击框架能够执行的指令丰富, 具有较强的通用性, 且在半径为 25 m 的攻击范围内具有良好的可靠性和稳定性, 适合在网络环境不佳的情况下传送较小的本地文件。对于 GreyFan 攻击, 可以通过在主机层面监控计算机资源使用率或在网络层面利用网络嗅探解析帧内容的方式进行防御。

此外, GreyFan 攻击框架仍然可以在反检测方面进行改进。如在执行窃取、破坏等攻击任务时, 可采用延时等待的方式进行攻击, 即每隔一段时间攻击一次, 以达到降低 CPU 使用率、逃避主机检测的目的; 可以将有效载荷的内容通过 RSA 加密算法进行加密和混淆, 以降低对有效载荷内容的识别。下一步将重点研究 GreyFan 攻击框架的新功能以及探究如何利用机器学习对 GreyFan 攻击进行智能识别, 帮助

人们降低网络空间的威胁。

参考文献:

- [1] DAKHANE D M, DESHMUKH P R. Active warden for TCP sequence number base covert channel[C]//International Conference on Pervasive Computing, Jan 8-10, 2015, Pune, India. Piscataway: IEEE Press, 2015: 1-5.
- [2] ZANDER S, ARMITAGE G, BRANCH P. Covert channels and countermeasures in computer network protocols[J]. IEEE Communications Surveys & Tutorials, 2007, 9(3): 44-57.
- [3] 王娟, 郭永冲, 王强, 等. 基于 BHO 的网络隐蔽通道研究[J]. 计算机工程, 2009, 35(5): 159-161, 164.
WANG J, GUO Y C, WANG Q, et al. Research of network covert channel based on BHO[J]. Computer Engineering, 2009, 35(5): 159-161, 164.
- [4] AHMADZADEH S A, AGNEW G. Turbo covert channel: an iterative framework for covert communication over data networks[C]//IEEE INFOCOM, April 14-19, 2013, Turin, Italy. Piscataway: IEEE Press, 2013: 2031-2039.
- [5] 姬国珍, 谭全福. 基于数据包时间间隔的隐蔽通道实现及检测方法研究[J]. 通信技术, 2018, 51(1): 189-194.
JI G Z, TAN Q F. Covert channel implementation based on between-packet time intervals and detection method[J]. Communications Technology, 2018, 51(1): 189-194.
- [6] 李卫, 嵩天. 适用于 NAT 环境的隐蔽通道构建方法[J]. 计算机工程与应用, 2018, 54(17): 103-109.
LI W, SONG T. Covert channel applying to NAT environment[J]. Computer Engineering and Applications, 2018, 54(17): 103-109.
- [7] 朱超凡, 马迪, 王伟, 等. 一种 NTP 协议隐蔽通道[J]. 计算机系统应用, 2017, 26(5): 119-125.
ZHU Y F, MA D, WANG W, et al. Covert channel based on NTP protocol[J]. Computer Systems & Applications, 2017, 26(5): 119-125.
- [8] TAN Y A, XU X, LIANG C, et al. An end-to-end covert channel via packet dropout for mobile networks[J]. International Journal of Distributed Sensor Networks, 2018, 14(5).
- [9] YANG Z, HUANG Q, ZHANG Q, et al. NICSscatter: backscatter as a covert channel in mobile devices[Z]. 2017.
- [10] SCHULZ M, LINK J. Shadow Wi-Fi: teaching smartphones to transmit raw signals and to extract channel state information to implement practical covert channels over Wi-Fi[C]//The 16th Annual International Conference on Mobile Systems, Applications, and Services Table of Contents, June 10-15, 2018, San Francisco, California, USA. [S.l.:s.n.], 2018: 256-268.
- [11] WU K, WEI Z S, TEACHER W Z. A study on the application

of intrusion detection technology to WLAN[C]//IEEE International Conference on Communication Software and Networks, May 27-29, 2011, Xi'an, China. Piscataway: IEEE Press, 2011: 344-346.

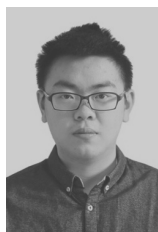
- [12] 谭彦, 厉萍, 卢洪涛, 等. Wi-Fi 无线钓鱼攻击分析及应对技术研究[J]. 电信科学, 2013, 29(Z2): 143-146, 151.

TAN Y, LI P, LU H T, et al. Wi-Fi wireless phishing attack analysis and coping technology research[J]. Telecommunications Science, 2013, 29(Z2): 143-146, 151.

- [13] 高波, 潘毅明, 黄国瑾. 基于城域网的运营级 WLAN 组网技术[J]. 电信科学, 2015, 31(10): 199-203.

GAO B, PAN Y M, HUANG G J. Technology of WLAN in operation level based on metropolitan area network[J]. Telecommunications Science, 2015, 31(10): 199-203.

[作者简介]



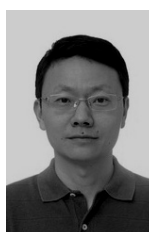
马栋捷 (1994-), 男, 浙江工业大学计算机科学与技术学院硕士生, 主要研究方向为信息安全。



金成强 (1995-), 男, 浙江工业大学计算机科学与技术学院硕士生, 主要研究方向为信息安全。



陈园 (1994-), 女, 浙江工业大学计算机科学与技术学院硕士生, 主要研究方向为物联网安全。



陈铁明 (1978-), 男, 博士, 浙江工业大学计算机科学与技术学院教授, 主要研究方向为网络空间安全与大数据智能分析。