物理隔离网络对抗技术综述

孙德刚[1,2], 夏宇琦[1,2], 吕志强[1,2], 张 宁[1,2], 孔庆善[1]

[1] 中国科学院信息工程研究所第四研究室 北京 中国 100093
[2] 中国科学院大学网络空间安全学院 北京 中国 100049

摘要 物理隔离网络对抗是一种利用预先植入的软硬件在物理隔离网络内部与外部之间建立隐蔽信道的方式。它打破了该网络提供的隔离手段, 严重威胁了用户的信息安全, 受到了学术界的广泛关注。与传统网络对抗不同, 物理隔离网络对抗通过自行建立的隐蔽信道与外界进行通信, 而不是利用公共通信网与外界进行通信。本文从物理隔离网络对抗技术的起源入手, 简要地介绍了物理隔离网络对抗技术的相关背景。通过与传统网络对抗技术的对比分析, 介绍了物理隔离网络对抗技术的工作原理, 突出了隐蔽植入和隐蔽通信是物理隔离网络对抗技术的两大特点。根据物理隔离网络对抗技术的实施步骤, 提出了一种物理隔离网络对抗技术的分析模型, 该分析模型分为侦察跟踪、武器构建、隐蔽植入、行为执行、隐蔽通信、命令与控制、目标达成等七个阶段, 这为发现和分析新出现的物理隔离网络对抗技术提供了借鉴作用。结合当今物理隔离网络对抗技术的研究热点和对现有研究成果的调研分析, 分别介绍了电磁、声、光、热等隐蔽信道在物理隔离网络对抗技术中发挥的作用, 同时指出隐蔽性和传输性能是隐蔽信道急需解决的问题。参考物理隔离网络对抗技术的特点, 介绍了物理隔离网络安全标准、物理隔离网络检测防护技术、供应链安全管理等当前针对物理隔离网络对抗技术的防范措施。基于物理隔离网络对抗极其检测防护面临的诸多问题, 介绍了两者未来可能的研究方向。

关键词 物理隔离网络安全; 隐蔽植入; 隐蔽通信; 隐蔽信道
中图法分类号 TP309 DOI 号 10.19363/J.cnki.cn10-1380/tn.2023.03.08

A survey on in air-gapped network confrontation technology

SUN Degang[1,2], XIA Yuqi[1,2], LV Zhiqiang[1,2], ZHANG Ning[1,2] and KONG Qingshan[1]

[1] Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[2] School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

Abstract Air-gapped network confrontation is a way to establish a covert channel between the interior and exterior of the air-gapped network by using pre-embedded software and hardware. It breaks the isolation means provided by the network, seriously threatens the information security of users, and has attracted extensive attention from the academic community. Unlike traditional network confrontation, air-gapped network confrontation communicates with the outside world through self-established covert channels, rather than using public communication networks to communicate with the outside world. This paper starts with the origin of air-gapped network confrontation technology, and briefly introduces the background of air-gapped network confrontation technology. By comparing with traditional network confrontation technology, this paper introduces the working principle of air-gapped network confrontation technology, and highlights that two characteristics of air-gapped network confrontation technology are concealed implantation and convert communication. According to the implementation steps of air-gapped network confrontation technology, an analysis model of air-gapped network confrontation technology is proposed, which includes seven stages (reconnaissance and tracking, weapon construction, concealed implantation, behavior execution, covert communication, command and control, and target achievement) and provides a reference for discovery and analysis of the new air-gapped network confrontation technology. Combined with the research hotspot of air-gapped network confrontation technology and the investigation of the existing research results, this paper introduces the role of the covert channels such as electromagnetics, acoustics, optics, and thermology in air-gapped network confrontation technology, and points out that concealment and transmission performance are two problems that need to be solved urgently. Referring to the characteristics of air-gapped network confrontation technology, this paper introduces the air-gapped network security standards, air-gapped network detection and protection technology, supply chain security management and other current preventive measures against air-gapped network confrontation technology. Based on the problems faced by air-gapped network confrontation and detection protection, the possible research directions of them in the future are introduced.

Key words air-gapped network security; concealed implantation; covert communication; covert channel

通讯作者: 吕志强, 博士, 正高级工程师, Email: lvzhiqiang@iie.ac.cn。
本课题得到国家重点研发计划项目(No. 2018YFF01014303)资助。
收稿日期: 2020-03-03; 修改日期: 2020-03-20; 定稿日期: 2022-12-26

1 引言

物理隔离网络是一种计算机网络, 它是指不直接或间接与国际互联网或其他公共信息网络相联接的网络。不同于采用虚拟化技术的逻辑隔离网络, 物理隔离网络主要采用物理方法将内网与外网隔离, 从而避免入侵或信息泄漏的风险。物理隔离网络主要应用于情报[1-2]、军事[2-4]等政府部门和 SCADA[5]、金融[3]等非政府部门。然而, 针对物理隔离网络的对抗技术随之应运而生, 其危害程度也越来越严重。

物理隔离网络对抗技术最早出现在 20 世纪 80 年代, 荷兰学者 Wim Van Eck 发表了第一篇有关 CRT 显示器电磁泄漏的文章[6], 这让物理隔离网络中电子设备存在的电磁泄漏问题引起了广泛关注; 2013 年斯诺登事件曝光的 DROPMIRE、水蟒蛇(COTTONMOUTH)系列技术[7-9]和 2017 年 Vault 7 事件曝光的野蛮袋鼠(Brutal Kangaroo)[10]技术与冲击钻(Hammer Drill)[11]技术, 表明一些物理隔离网络对抗技术已经实战化; 而最新报道的物理隔离网络对抗技术则是对震网(Stuxnet)病毒感染物理隔离网络的细节进行了追踪报道和分析[12]。

计算机系统是物理隔离网络的重要组成部分, 本文将重点围绕物理隔离网络内的计算机系统开展研究工作。为此, 本文第 2 节给出了物理隔离网络对抗技术的工作原理和分析模型; 第 3 节根据目前的主流研究方向, 对电磁、声、光、热等隐蔽信道技术进行了梳理; 第 4 节从检测和防护角度, 介绍了物理隔离网络对抗技术的应对措施; 第 5 节对全文进行了总结。

2 工作原理与分析模型

传统的网络对抗技术利用计算机系统与公共通信网络(例如国际互联网)相连的特点, 进行中断、篡改、伪造等主动网络对抗行为和信息窃取、流量分析等被动网络对抗行为[13]。然而, 由于物理隔离网络先天不具有与公共通信网连接的特性, 相应的物理隔离网络对抗技术与传统的网络对抗技术具有明显的差异, 因此根据物理隔离网络的特点, 物理隔离网络对抗技术主要解决隐蔽植入和隐蔽通信的问题。下面从物理隔离网络对抗技术的工作原理与本文提出的分析模型说明两类对抗技术相同点和不同点。

2.1 工作原理

利用物理介质感染、供应链污染、非接触接入等入侵形式将含有恶意软硬件的植入模块隐蔽植入到物理隔离网络内的目标电子设备, 并结合电磁、声、光、热等不同的隐蔽信道实现目标电子设备与中继模块之间的隐蔽通信, 同时通过中继模块与远程操控中心之间的公共通信网络达到针对物理隔离网络的对抗目的。图 1 为物理隔离网络对抗系统拓扑图。

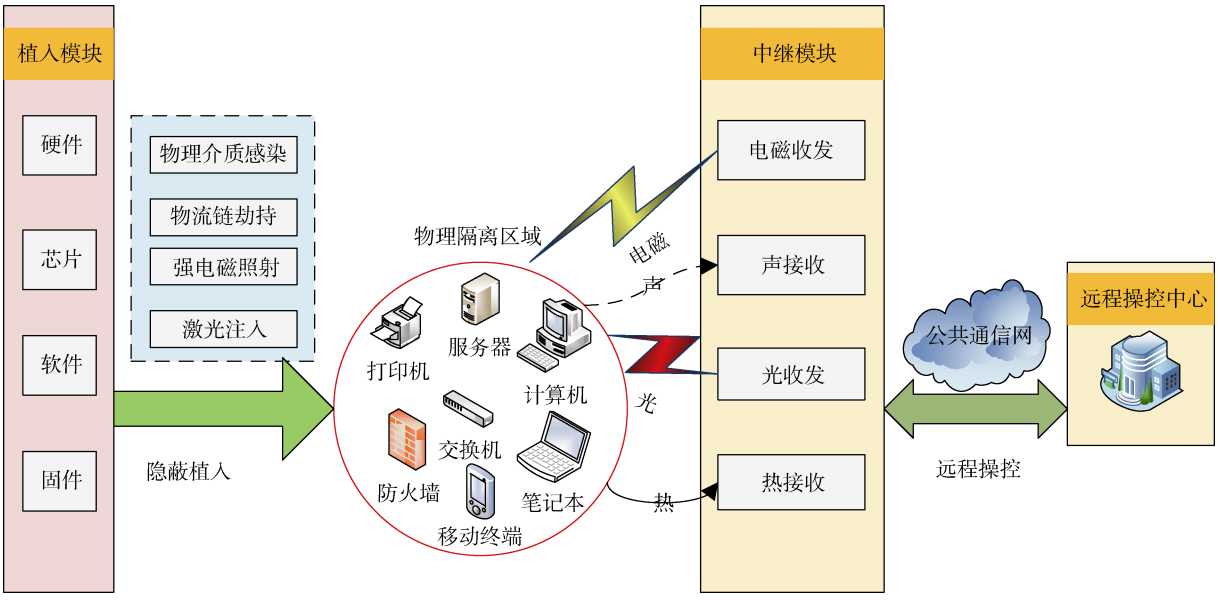

图 1 物理隔离网络对抗系统拓扑图

Figure 1 Air-gapped network confrontation system topology

从物理隔离网络对抗技术的工作原理分析, 隐蔽植入和隐蔽通信是区别于传统网络对抗技术的两大特点。传统的网络对抗技术是通过公共通信网络将恶意软件植入到目标电子设备, 而物理隔离网络

对抗技术则是通过物理介质感染、供应链污染、强电磁照射、激光注入等接触或近距离的入侵方式将恶意软硬件植入到目标设备; 传统的网络对抗技术是直接通过公共通信网络与远程操控中心建立连接, 而物理隔离网络对抗技术则是结合隐蔽信道(目标电子设备与中继模块之间)和公共信道(中继模块与远程操控中心)两种方式实现与远程操控中心建立连接。

2.2 分析模型

根据物理隔离对抗技术的工作原理和洛克希德-马丁公司的网络杀伤链(Kill Chain)模型[14], 该文提出了一种物理隔离网络对抗的分析模型。该分析模型可以分为七个阶段: 侦察跟踪、武器构建、隐蔽植入、行为执行、隐蔽通信、命令与控制、目标达成等七个阶段。物理隔离网络对抗技术分析模型如图 2 所示:

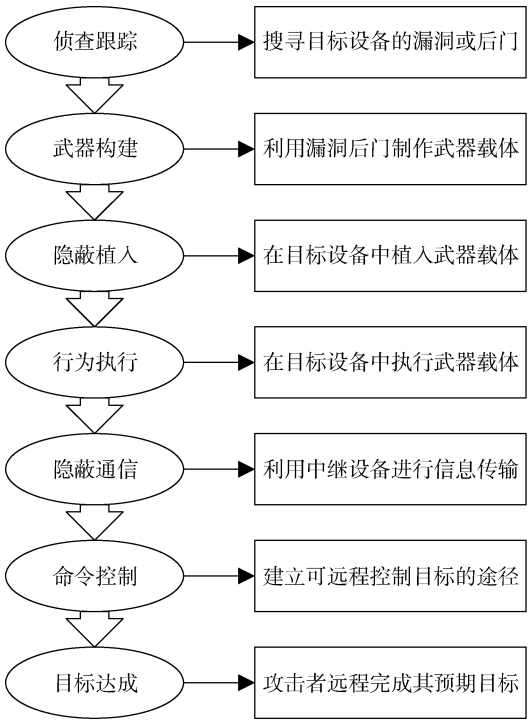

图 2 物理隔离网络对抗技术分析模型

Figure 2 Analysis model of air-gapped network confrontation technology

对于网络杀伤链模型来说, 敌对方主要通过网络实施侦查跟踪、武器构建、载荷投递、漏洞利用、安装植入、命令控制、目标达成等行为。物理隔离网络对抗技术的分析模型与网络杀伤链模型的区别主要体现在以下两点: 在物理隔离网络对抗技术的分析模型中, 敌对方需要利用隐蔽植入阶段将恶意软硬件植入到非网络连接的目标电子设备内部, 而在网络杀伤链模型中, 敌对方通过公共通信网络就可以实现恶意软件植入; 另外, 在本文提出的分析模型中, 敌对方通过隐蔽通信阶段可在非网络连接的目标电子设备与公共通信网络之间建立隐蔽信道, 而在网络杀伤链模型中, 敌对方仍然是直接通过公共通信网络与外界建立联系。因此, 隐蔽植入和隐蔽通信这两个阶段再次体现了物理隔离网络对抗技术的主要特点。

阶段 1. 侦查跟踪

侦察跟踪阶段是敌对方为达成目标, 进行探测、识别及确定目标电子设备的过程。传统网络对抗技术可以通过公共通信网络收集与目标电子设备相关的情报, 而收集处于物理隔离网络之内的政府、军队、金融、电信等拥有重要数据信息的部门情报, 由于目标电子设备没有与公共通信网络连接, 仅仅通过公共通信网络收集与目标电子设备相关的情报, 已经不足以获得完整的情报, 这就需要从其它方面入手进行侦查跟踪。

间谍活动是针对物理隔离网络的主要侦查跟踪手段。从 2019 年的雅虎新闻报道[12]获悉, 荷兰间谍利用多次进入伊朗核设施的机会, 持续收集离心机相关信息, 确定了离心机的具体型号、设备配置、网络状况等, 从而为震网病毒的研制和执行创造了充分的条件, 最终达到损坏离心机的目的。

阶段 2. 武器构建

武器构建阶段是指通过侦察跟踪阶段确定目标电子设备后, 准备物理隔离网络对抗武器的阶段。物理隔离网络对抗武器可由敌对方直接制造, 也可利用自动化工具来制造, 其发挥的作用不仅针对目标电子设备实施控制、窃取、监视、干扰、破坏、摧毁等行为, 而且担负着与物理隔离网络之外建立隐蔽通信的目的。特别值得注意的是, 物理隔离网络对抗武器在执行对抗属性的基础上, 不仅能够保证构建的软件或固件具有躲避计算机安全软件实时监控和防护的能力, 而且能够保证构建的硬件或芯片具有较强的隐蔽性, 不易被对方发现。

传统的网络对抗武器种类以软件(固件)为主; 而物理隔离网络对抗武器的种类不仅包括软件或固件, 而且包括硬件(芯片), 甚至以软硬件结合的方式构建武器。物理隔离网络对抗武器的软件种类与传统网络对抗技术中的恶意软件类似, 包括病毒、蠕虫、木马、后门、僵尸网络、Rootkit 等恶意代码[13]; 而物理隔离网络对抗武器的硬件种类包括处理器、存储器、输入/输出接口、无线收发等组成部分。

NSA 的 COTTONMOUTH 产品系列[7-9]是一套典

型的由硬件和芯片组成的物理隔离网络对抗武器。COTTONMOUTH 产品在建立隐蔽信道的同时, 也可以在目标计算机内植入恶意软件。为了确保硬件的隐蔽性, COTTONMOUTH 产品将数字模块、USB 集线器模块、路由模块、无线收发模块等硬件组成部分全部集成在 USB 线缆(COTTONMOUTH-I)或者计算机内的 USB 接口(COTTONMOUTH-Ⅱ和 COTTONMOUTH-Ⅲ)中。这种硬件设计方案通常会采用集成电路设计技术高度集成各个硬件模块, 减小硬件面积, 然后通过在计算机原有的组件上安装恶意硬件, 使人无法从计算机外观上觉察到恶意硬件的存在, 增加了恶意硬件被发现的难度。

阶段 3. 隐蔽植入

隐蔽植入阶段是指将制造完成的武器向目标电子设备植入的阶段。由于物理隔离网络不具有与公共通信网络连接的条件, 使得物理隔离网络对抗技术必须采用非网络手段实现隐蔽植入。传统网络对抗技术多数利用邮件、钓鱼网站等网络手段实现恶意软件的植入, 而物理隔离网络对抗技术会采用物理介质感染、供应链污染、强电磁照射、激光注入等多种方式实现软硬件的隐蔽植入。

对于物理介质感染的隐蔽植入方式, 敌对方通常会采用 U 盘或光盘等存储介质, 将恶意软件植入目标电子设备中。在维基解密最近曝光的 CIA-Vault7 文档中, “野蛮袋鼠(Brutal Kangaroo)”通过 U 盘入侵物理隔离网络[10]; 而“冲击钻(Hammer Drill)”是通过劫持 Windows 系统上的光盘刻录软件, 感染光盘这类数据传输介质的方式, 以达到入侵物理隔离网络目的[11]。该隐蔽植入方式需要利用内部人员有意或无意地将 U 盘或光盘插入到目标计算机中, 使目标计算机感染恶意软件。

在供应链污染的隐蔽植入方式中, 敌对方会利用电子设备的设计、制造、运输、安装、服务等供应链环节, 将恶意软件和硬件植入电子设备中。格林沃尔德在书中写到[15]: “NSA 经常收到或拦截目标电子设备, 该机构之后在目标电子设备中植入后门监视工具, 然后用厂家的密封条重新包装设备, 再继续运输。NSA 因此得以访问整个网络及其所有用户”。供应链污染是目前比较常见的隐蔽植入方式, 它与物理介质感染的植入方式类似, 都是一种接触式的隐蔽植入方式。

强电磁照射是一种特殊的隐蔽植入方式, 敌对方可以利用强电磁信号, 将恶意软件植入目标电子设备中。美军的“舒特(SUTER)”系统[16-18]是最典型的案例, 其工作原理是利用敌方电子信息系统的雷达、通信系统的天线为入口, 通过强电磁信号渗透进入敌方的防空网, 向其注入网络入侵算法和恶意程序, 或启动敌方控制器芯片后门, 欺骗或控制敌方防空预警网络。强电磁照射的隐蔽植入方式最大特点是不直接接触目标电子设备, 这是区别于物理介质感染、供应链污染等隐蔽植入方式的地方。基于以上特点, 该隐蔽植入方式可以作为未来的物理隔离网络对抗技术研究的重要发展方向。

另一种非接触式隐蔽植入方式是激光注入[19]。Shamir 等人利用一束含有二进制代码的激光照射在一体式打印机上, 然后通过连接一体式打印机的计算机上的恶意软件控制一体式打印机中的扫描仪传感器接收和解调该激光信号, 实现物理隔离网络入侵的目的。激光注入与强电磁照射相同点是, 两者都属于非接触式隐蔽植入方式; 不同点是激光注入的隐蔽植入方式需要预先植入到目标电子设备的恶意软件的配合, 才能实现隐蔽植入。

从物理介质感染、供应链污染、强电磁照射、激光注入等 4 种针对物理隔离网络的隐蔽植入方式以及将来由于技术发展导致可能出现的隐蔽植入方式来看, 可分成接触式(物理介质感染和供应链污染)和非接触式(强电磁照射和激光注入)两类隐蔽植入方式。接触式隐蔽植入技术的优点是可实现软件和硬件的植入, 缺点是由于需要接触目标电子设备导致其安全性性能较差; 而非接触式隐蔽植入的优点是因其不必直接接触目标电子设备, 所以安全性较高, 缺点却是只能实现软件的植入。根据目前物理隔离网络对抗技术的发展趋势来看, 在目标电子设备中植入恶意软件成为主流[20], 因此高安全性的非接触式隐蔽植入将会成为未来隐蔽植入技术的重点发展方向。

阶段 4. 行为执行

行为执行阶段是指敌对方选择目标电子设备的某个组成部分作为作用点, 利用预先植入的软硬件对目标电子设备实施行为的阶段。从行为执行阶段来看, 物理隔离网络对抗技术与传统网络对抗技术的目的类似, 都是针对目标电子设备实施控制、窃取、监视、干扰、破坏、摧毁等行为; 不同的是, 物理隔离网络对抗技术可以根据实际的应用场景, 采用软件(固件)或者硬件(芯片), 甚至软硬件结合的方式实施以上行为。

在实际的应用案例中, 物理隔离网络对抗技术的行为执行阶段多数是采用高级持续威胁(APT)技术实施破坏行为。例如在 2009 年, 美国利用“震网”蠕虫病毒入侵伊朗的铀浓缩设备, 造成伊朗核电站

推迟发电[21]。另一个案例是 2015 年的乌克兰停电事件, 俄罗斯黑客组织利用黑色能量(BlackEnergy)病毒入侵乌克兰的电厂, 致使部分用户供电被迫中断[22]。而最近发生的委内瑞拉停电事件(2019 年), 也被推测可能是 APT 技术实施的破坏行为[23]。

阶段 5. 隐蔽通信

隐蔽通信阶段是指敌对方在目标电子设备与中继设备之间建立隐蔽信道的阶段。在隐蔽通信阶段, 中继设备指的是在目标电子设备和远程操控中心建立通信的设备, 它可以是通用设备(例如计算机、手机等), 也可以是特制的专用设备, 而中继设备设置的主要原因是物理隔离网络不与公共通信网络连接, 利用中继设备就可以在物理隔离网络和公共通信网络之间建立连接, 便于将物理隔离网络内的敏感信息传输到公共网络内或通过公共网络远程控制物理隔离网络内的电子设备。

隐蔽通信阶段是由物理隔离网络特性决定的, 而传统网络对抗技术分析模型不具有这个阶段。隐蔽通信的建立过程是主要包括信道生成、调制/解调和信息传输三个步骤。

信道生成是隐蔽通信阶段的主要步骤, 前期隐蔽植入阶段植入的软硬件负责在目标电子设备与中继设备之间建立隐蔽信道。由于没有公共通信网络可以利用, 物理隔离网络对抗技术会利用目标计算机组件(CPU、显卡、风扇、键盘等)或者外部专用硬件(在隐蔽植入阶段植入的恶意硬件)与中继设备形成隐蔽信道, 涉及的隐蔽信道的种类包括电磁、光、声、热等信道。

调制/解调步骤负责调制目标电子设备的敏感信息或者解调中继设备的控制信号。调制/解调方式包括调幅(AM)、二进制频移键控(BFSK)、正交频分复用(OFDM)等。敌对方将根据实际应用情况选择调制/解调方式, 如果数据量小、传输速率要求不高的情况下, 可以选择二进制频移键控调制/解调方式; 如果数据量大、传输速率要求高的情况下, 可以选择正交频分复用调制/解调方式。

信息传输步骤主要将目标电子设备中调制后的敏感信息传输给中继设备或者将中继设备的控制信号传输给目标电子设备。为了保证信息传输的隐蔽性和完整性, 通常会在拟传输信息的前面加上前导码, 保证信息传输的隐蔽性; 在拟传输信息的后面加上纠错码, 保证信息的完整性。

与隐写术(Steganography)[24]、阈下信道(Subliminal Channel)[25]、匿名通信(Anonymity)[26]、数字水印(Digital Watermark)[27]一样, 隐蔽通信属于信息隐藏技术之一[28]。在 2015 年之前[29], 隐蔽通信技术分为单机隐蔽通信(Single-Host Covert Communication)[30]和网络隐蔽通信(Network Covert Communication)[31], 但是随着针对物理隔离网络对抗技术的迅速发展, 物理隔离网络隐蔽通信(也称为带外隐蔽通信: Out-of-Band Covert Communication[32])技术也成为隐蔽通信技术的分支之一。

单机隐蔽通信建立在单个宿主系统上, 从而实现单个宿主系统内的非自主(即强制)访问控制策略。物理隔离网络隐蔽通信技术与单机隐蔽通信都是在没有通信意愿的进程之间建立通信链路, 但是不同于单机隐蔽通信的信道生成、调制/解调、信息传输等步骤都是单个宿主系统内完成, 物理隔离网络隐蔽通信是在目标电子设备与中继设备之间建立通信链路, 即信道生成、调制/解调、信息传输等步骤发生在目标电子设备和中继设备之间。此外, 单机隐蔽通信是为了规避强制访问控制系统的安全性而设计的, 而物理隔离网络隐蔽通信则是在进程之间建立的, 而不管它们运行主机的访问控制策略如何[32]。

传统网络对抗技术的隐蔽通信技术, 即网络隐蔽通信技术是在公共通信网络受正式或非正式网络安全策略约束的进程之间建立的。传统网络隐蔽隐蔽通信和物理隔离网络隐蔽通信的相似之处在于它们都是在不同主机上执行的进程之间建立通信链路。物理隔离网络隐蔽通信和传统网络隐蔽通信的主要区别在于, 传统网络隐蔽通信利用主机之间已经建立的信道进行隐蔽通信, 而物理隔离网络隐蔽通信需要自己建立信道进行隐蔽通信。另一方面, 传统网络隐蔽通信被设计成在公共通信网络协议中隐藏信息, 物理隔离网络隐蔽通信关心的是如何通过自己建立的隐蔽信道隐藏传输信息, 从隐蔽信道和信息隐藏两个方面考虑隐蔽通信的建立[32]。

阶段 6. 命令与控制

命令与控制阶段是指敌对方建立与目标电子设备远程对抗路径的阶段。该阶段是在中继设备与远程操控中心之间实现命令与控制, 这是由于隐蔽通信阶段的隐蔽信道性能无法满足远距离(大于 100 米)和高速率(大于 100M 位/秒)的通信性能要求, 因此命令与控制阶段与隐蔽通信阶段共同担负着目标电子设备与远程操控中心之间通信链路的建立。当这种远程通信链路建立之后, 就可以将远程操控中心发送的指令传输给物理隔离网络内的目标电子设备, 对该目标电子设备实施控制、窃取、监视、干扰、破坏、摧毁等行为; 同时可以将从目标电子设备中获取的敏感信息传输给远程操控中心, 以便在远程操

控中心内设立的数据分析中心对这些敏感信息进行还原和分析。

命令与控制阶段的主要任务之一就是建立远程网络隐蔽通信, 这与传统的网络隐蔽通信具有相似的建立过程。这种远程网络隐蔽通信不论利用公共通信网络, 还是专用通信网络, 都会针对通信内容和通信链路的安全性进行研究, 保证远程网络通信不被发现和破译。

阶段 7. 目标达成

目标达成阶段是指敌对方达到预期目标的阶段。针对物理隔离网络的目标达成的成果可呈现多样化, 具体来讲有电子设备侦察、敏感情报收集、控制信号干扰、基础设施破坏、重要系统摧毁等。结合目前物理隔离网络对抗技术发展现状和实际应用, 基础设施破坏成为敌对方期望的重要目标和成果[21-23]。

此外, 物理隔离网络对抗技术达成目标的程度和效果需要进行评估, 网络空间靶场[33]是一个比较好的选择。网络空间靶场是针对网络攻防演练和网络新技术评测的重要基础设施, 主要供政府和军队部门使用, 用来提高网络和信息系统的稳定性、安全性和性能, 而网络攻防武器评测验证是网络空间靶场的主要功能之一。利用物理隔离网络对抗技术构建的武器也可通过网络空间靶场对其进行评测验证, 以此评估该武器是否达到预期目标和成果。

2.3 小结

通过对物理隔离网络对抗技术工作原理和分析模型的论述, 本章将物理隔离网络对抗技术和传统网络对抗技术进行了全面对比, 进一步阐述了隐蔽植入和隐蔽通信是物理隔离网络对抗技术区别于传统网络对抗技术的重要特征。同时, 物理隔离网络对抗技术的研究工作离不开传统网络对抗技术的支持, 这种支持重点体现在物理隔离网络对抗技术分析模型中的行为执行阶段和命令与控制阶段。从以上结论来看, 物理隔离网络对抗技术和传统网络对抗技术是密不可分的关系。

此外, 本章提出了物理隔离网络对抗技术分析模型的七个阶段, 全面了分析了物理隔离网络对抗技术的对抗流程。在实际应用过程中, 敌对方会灵活地掌握物理隔离网络对抗技术分析模型的七个阶段的使用情况, 比如, 根据应用场景可使用分析模型的某几个阶段, 而不是使用全部阶段达成目标。

3 隐蔽信道

物理隔离网络对抗技术分析模型中的隐蔽植入和隐蔽通信是比较重要的两个阶段, 从某种程度来讲, 隐蔽植入是物理隔离网络对抗的手段,隐蔽通信则是实现物理隔离网络对抗的目的。而相比于隐蔽植入阶段, 隐蔽通信阶段的研究工作更具有挑战性[20]。其中, 隐蔽信道的建立是隐蔽通信的关键技术。下面, 将从电磁、光、声、热等几个方面介绍隐蔽信道建立的过程。

3.1 电磁

电磁是目前物理隔离网络对抗技术中比较常用的隐蔽信道。按照电磁隐蔽信道产生的方式, 可分为电磁辐射、传导发射、无线收发等。

电磁辐射是指电子设备本身产生的电磁波向空间辐射引起的信息泄漏。这种不同波长和强度的电磁波一般是由电子设备的各个组成部件(例如显示器、显卡、接口、CPU 等)产生的, 任何处于工作状态的电子设备(如计算机)都或多或少存在电磁辐射与泄漏的问题。电磁辐射最早源于上世纪 60 年代末 70 年代初由美国国家安全局提出的 TEMPEST (Transient Electromagnetic Pulse Emanation Surveillance Technology)技术, 是用于防止电磁信息设备潜在的安全威胁以及反向的用以获取和还原其他信息发射源的技术。当前, 随着计算机的日益普及, 利用低成本的电磁信号接收设备就可以截获并还原这些因电磁辐射造成的敏感信息, 从而引起各种政治、军事、经济情报的泄漏, 造成日趋严重的信息安全问题[34]。

1985 年荷兰的学者 Wim Van Eck 利用电磁辐射技术, 在物理隔离网络内部和外部建立了隐蔽信道[6]。这种电磁辐射属于无意的泄漏方式, 只能获取 CRT 显示器的显示内容。相对于这种无意泄漏方式, 1998 年 Kuhn 和 Anderson 提出一种 SOFT-TEMPEST 技术[35]。该技术的工作原理是通过目标计算机显卡的电磁辐射方式, 有意地在物理隔离网络内部和外部建立隐蔽信道。这种隐蔽信道是利用预先植入的恶意软件控制目标计算机显卡的电磁辐射频率和强度而实现的, 可以获取目标计算机硬盘存储的信息。2014 年, Guri 等人采用了与 SOFT-TEMPEST 的类似技术提出了 AirHopper 技术, 通过电磁辐射方式实现了目标计算机与手机之间隐蔽信道的建立[36-37]。2018 年, Guri 等人更进一步地实现了以带有 LCD 显示屏的现代计算机为目标的通信链路的建立[34]。这种被称为 LCD-TEMPEST 可以实现物理隔离网络内的密钥、键盘记录、电子文档等信息的获取, 在 8 米的距离能够达到 640 位/秒的传输速率。此外, Thiele[39]、Bellard[40]等人也利用计算

机显卡的电磁辐射方式, 开发出了可以针对物理隔离网络的信息获取程序。

与计算机显卡或显示屏一样, GPIO[41]、UART[41]、USB[42]、电源[43]、CPU[44-46]等计算机组件也可以作为隐蔽信道的发射源, 无意地或有意地进行电磁辐射。值得注意的是, 文献[44]提出的 SAVAT 技术也是一种侧信道技术, 因此从无意的电磁辐射方面讲, 侧信道与物理隔离网络的隐蔽信道具有一定相关性[47]。

如果使用磁接收器接收电磁辐射产生的电磁波时, 就只会产生磁隐蔽信道。当电流通过导线时, 导线周围就会产生磁场。利用这种磁场产生特性, 人们发展了磁通信技术。其中透地应急无线通信技术[48]和近场磁通信技术[49]是比较典型的磁通信技术。但这些典型的通信方式通常需要体积较大的磁发射器和接收器, 不适合用于隐蔽通信中。近几年, 利用计算机组件(硬盘[50]和 CPU[51-52])的磁信号泄漏现象建立隐蔽信道, 可以进行相应的隐蔽通信。

2016 年, Matyunin 等人[50]将笔记本电脑的硬盘磁头作为发射源, 提出了一种基于磁的隐蔽信道设计方案。该方案的工作原理是利用笔记本电脑的 CPU 核满载程度的不同在硬盘上产生不同的低频磁场辐射, 实现敏感数据的获取。 这种设计方案是在笔记本和手机之间建立了磁隐蔽信道, 即笔记本硬盘作为发射端, 而手机作为接收端。它利用磁信道进行隐蔽通信时, 包括信号生成、数据调制和传输协议制定 3 个步骤。其中, 在数据调制时, 两种调制方案被应用, 一种是幅度调制, 另一种是周期调制。从试验结果来看, 在误码率相同情况下, 磁隐蔽信道采用幅度调制时将会获得更高的传输速率; 而采用周期调制时将会获得更远的传输距离。目前, 该设计方案能够达到的最大工作距离为 0.12 米, 最大工作速率为 2 位/秒。

文献[51]提出并设计了一款针对处于物理隔离网络的电子设备的恶意软件——ODINI。不同于利用硬盘的磁场辐射进行数据获取, 该软件的工作原理是利用电子设备中的 CPU 核的满载工作使电源线上产生的低频磁场辐射, 实现敏感数据的获取。ODINI 可应用在任何含有 CPU 的电子设备, 如计算机、服务器、IoT(Internet of Things)等, 具有不受法拉第笼屏蔽的影响, 木马查杀软件难以检测, 可以在独立的虚拟机运行等优点。ODINI 利用磁信道进行隐蔽通信时, 包括信号生成、数据调制和传输协议制定 3 个步骤。其中, 在信号生成时, ODINI 提出的算法可任意控制 CPU 核的工作个数和载荷利用率, 这不仅可以灵活地控制 CPU 核是否工作及工作强度, 还具有一定的隐蔽性。ODINI 能够达到的最大工作距离为 1.2 米, 最大工作速率为 40 位/秒。

由于 ODINI 采用了专用的磁接收设备, 便携性和隐蔽性方面的不足限制了 ODINI 的应用场景, 因此为了增加可用性, 另一款恶意软件——MAGENETO[52]采用了通用设备(例如手机)进行磁信号的采集和处理。除了具有 ODINI 的隐蔽通信特性之外, MAGENETO 提出并设计了一种安卓应用。利用普通手机内的磁传感器和安卓系统内的函数(android.hardware.Sensor), MAGENETO 可以采样和解调磁信号。MAGENETO 能够达到的最大工作距离为 0.12 米, 最大工作速率为 5 位/秒。

相比于其他电磁接收设备, 建立磁隐蔽信道的磁传感器(磁力计)主要用于定位, 与蜂窝, Wi-Fi, 蓝牙和 NFC 区别之处在于, 磁传感器无需考虑通信接口的问题, 因此, 即使在飞行模式下, 通信接口被禁用, 仍然可以使用基本权限建立磁隐蔽信道; 同时低频磁场具有绕过法拉第笼和金属屏蔽的特点, 即使在操作环境布置长时电磁监测设备的情况下, 磁隐蔽信道也不会被发现。然而, 由于计算机组件产生磁辐射的频率较低, 导致磁信号最快只有几十位/秒的传输速度, 这将会影响磁信号的传输速度; 此外, 由于磁信号在传输过程中, 其衰减的程度较大, 导致传输距离较近, 这是限制其应用的瓶颈。

传导发射是指利用与电子设备连接的导线作为隐蔽信道产生的信息泄漏[53]。与有意的电磁辐射方式类似, 电力线传输需要预先植入恶意软件; 不同的是, 电力线传输不是利用辐射发送方式, 而是利用传导发送方式进行信息泄漏。

目前电力线是传导发射中比较常见的传输介质[54-62]。2019 年, Zhao 等人提出了一种 Powermitter 技术[54], 该技术的工作原理是利用预先植入的恶意软件控制与目标计算机相连接的电力线电流工作状态的方式, 有意地在物理隔离网络内部和外部建立隐蔽信道。这种隐蔽信道的发送端是目标计算机, 接收端是一个虚拟的示波器, 其信道的通信过程是: 首先将目标计算机硬盘中的敏感信息调制成二进制信号; 然后将二进制信号映射在 CPU 利用率的变化上; 其次通过 CPU 利用率的变化影响与目标计算机相连接的电力线电流工作状态的方式, 用电力线将二进制信号发送出去; 最后使用虚拟示波器接收和还原这些敏感信息。PowerHammer[64]技术采用了与 Powermitter 技术类似的方法, 通过 CPU 多内核调制方式和小型电流钳接收信号, 实现了更高的传输性

能, 实验数据证明该技术的传输速率最大为 3000 位/秒, 传输距离最长为 110 米。

无线收发是指利用恶意硬件产生的无线信道引起的信息泄漏。通过定义来看, 无线收发不像电磁辐射和传导发射通过恶意软件, 而是通过恶意硬件实现目标电子设备敏感信息接收功能。而且, 无线收发不仅可以与电磁辐射和传导发射一样实现目标电子设备敏感信息接收功能, 而且可以反向地将数据注入到目标电子设备内。

RAGEMASTER[65]是一款美国国家安全局的无线发射器, 该无线发射器被串联在目标计算机的 VGA 视频线缆中, 与物理隔离网络之外的连续波照射和信息接收设备建立了隐蔽通道, 可以实时获取目标计算机显示屏的显示信息。RAGEMASTER 的通信过程是 : 首先将目标计算机显示屏的敏感信息进行调制; 然后利用 RAGEMASTER 的天线部分将调制信号发送到物理隔离网络之外; 最后通过连续波照射和信息接收设备接收和还原这些敏感信息。RAGEMASTER 的主要优点是具有静默功能, 平时不工作时保持静默状态, 当工作时, 连续波照射和信息接收设备向发射连续波并激活 RAGEMASTER 进入工作状态, 这个优点可以有效躲避电磁监测设备的监测。RAGEMASTER 与 ANGRYNEIGHBOR 系列 (LOUDAUTO[66] 、 TAWDRYYARD[67] 、 SURLYSPAWN[68]等)都属于逆向反射器(Retro Reflectors)[69], 工作原理也相同, 能够达到的最大工作距离为 15 米[66]。

与 RAGEMASTER 类似, COTTONMOUTH 产品系列[7-9]和 FIREWALK[70]也是建立电磁隐蔽信道的恶意硬件。但是不同点是, 它们可以建立无线发射和接收的信道, 即双向隐蔽信道。COTTONMOUTH 产品系列通过目标计算机的 USB 接口被动地接收硬盘的敏感信息, 同时主动地将恶意软件植入到同一目标计算机内。FIREWALK 能够通过目标计算机的网络接口被动地收集千兆位以太网网络流量, 并主动将以太网数据包注入到同一目标计算机网络中。

下表从电磁辐射、传导发射、无线收发等电磁隐蔽信道产生方式中各选择了一种比较有代表性的技术进行电磁隐蔽信道的性能对比:

表 1 典型的电磁隐蔽信道性能对比

Table 1 Performance Comparison of Typical Electromagnetic Covert Channels

	发送端	接收端	传输距离	传输速率
文献[34]	视频线	软件无线电	8 米	640 位/秒
文献[64]	电力线	小型电流钳	110 米	3000 位/秒
文献[65]	专用硬件	专用设备	15 米	实时传输

电磁隐蔽信道具有穿越障碍物和传输性能较好的优点, 已经具备了实战化的条件, 因此是物理隔离网络对抗技术的重要研究方向。目前, 物理隔离网络对抗技术的电磁隐蔽信道研究方向正朝着软件化方面发展, 这可以降低电磁隐蔽信道被发现的风险, 同时结合传统网络对抗技术中的高级持续威胁(APT), 可以丰富物理隔离网络对抗的应用场景。

3.2 光

电子设备的一些应用使其具有光源, 比如显示器、计算机指示灯等, 使得光可以作为隐蔽信道应用于物理隔离网络对抗技术中。

早在 2002 年, Loughry 和 Umphress[71]就讨论了利用计算机键盘上的状态指示灯的 LED 光源进行敏感信息泄漏的风险。文献[72]在此基础上, 提出了一种具有高级持续威胁(APT)特性的恶意软件。该软件的工作原理是利用计算机键盘上的 Caps-Lock、Num-Lock 和 Scroll-Lock 状态指示灯的 LED 光源进行光传输, 实现敏感数据的获取。该软件在计算机和光接收设备(包括光传感器、摄像机、手机等)之间建立了光隐蔽通道, 即计算机键盘上的状态指示灯作为光信号的发射端, 光接收设备作为光的接收端。这种恶意软件的对抗过程是: 首先将目标计算机中的敏感数据调制成光信号; 然后通过该计算机键盘的 Caps-Lock、Num-Lock 和 Scroll-Lock 状态指示灯将调制后的敏感数据发送出去; 最后通过光传感器、摄像机或手机等接收并进行解调光信息, 从而实现数据隐蔽传输的功能。其中, 将敏感信息调制成光信号的过程是通过控制计算机键盘上的状态指示灯开关实现的。这个恶意软件能够实现 3000 位/秒的传输速率。

与计算机键盘状态指示灯的 LED 光源调制方式类似, 通过控制和调制计算机硬盘指示灯[73]、交换机和路由器指示灯[74]、红外摄像头[75]、一体式打印机[19]的 LED 光源, 也可以建立光隐蔽信道并实现物理隔离网络内敏感信息的获取。然而, 当通过控制电子设备 LED 光源构建隐蔽信道时, 其 LED 闪烁现象容易

被发现, 从而造成光隐蔽信道的不安全性。

利用液晶显示屏(LCD)建立隐蔽信道是另一种光信道的构建方法。2013 年, Brassup[77]演示了通过修改液晶显示屏进而实现图像隐藏的方法, 该方法需要去掉液晶屏中的偏振滤波器, 这使得它在实际的对抗场景中不太可行。文献[78]和文献[79]讨论了肩窥的概念, 肩窥是指当合法用户输入数据时, 恶意的内部人员或访客(或被利用的监控摄像头)获取机密数据, 如密码或 PIN 码[80]。结合以上方法, 文献[81-83]改进并提出了一种能够从物理隔离网络泄漏敏感数据的恶意软件。该软件的工作原理是利用人类裸眼视觉在亮度感知方面的局限性, 将含有敏感信息的图像以低对比度形式显示在计算机液晶显示屏中, 实现光隐蔽信道的建立及敏感信息的获取。这种软件是在计算机液晶显示屏与光接收设备(包括谷歌眼镜、摄像机、手机等)之间建立了光隐蔽通道, 即计算机液晶显示屏作为光信号的发射端, 光接收设备作为光的接收端。这种恶意软件的对抗过程是: 首先将目标计算机中的敏感数据隐藏在低对比度的图像中; 然后通过该计算机液晶显示屏将调制后的敏感数据发送出去; 最后通过谷歌眼镜、摄像机或手机等接收并进行解调光信息, 从而实现数据隐蔽传输的功能。该恶意软件建立的光隐蔽信道可以达到的最远传输距离为 9 米, 最高传输速率为 10 位/秒[83]。

Shamir 等人[19]在 2014 年提出了一种利用激光作为隐蔽信道的恶意软件。该恶意软件的工作原理是利用扫描仪传感器进行光信号接收和发射, 实现目标设备的远程控制及敏感信息的获取。这种软件的主要特点是能够建立双向隐蔽信道: 一种隐蔽通道是利用一束含有二进制代码的激光照射在一体式打印机上, 然后通过连接一体式打印机的计算机上的恶意软件控制一体式打印机中的扫描仪传感器接收激光信号; 另一种隐蔽通道是利用该恶意软件控制与其连接的一体式打印机中的扫描仪指示灯发送敏感信息, 然后通过远端的摄像机实现敏感信息的接收。因此, 利用这种双向隐蔽通道, 敌对方不仅可以获取目标计算机的敏感信息, 而且可以达到控制目标计算机的目的。这种恶意软件能够达到的最远工作距离为 1200 米, 最大传输速率为 20 位/秒。

下表从电子设备指示灯、液晶显示屏、激光产生的光隐蔽信道中各选择了一种比较有代表性的技术进行光隐蔽信道的性能对比:

表 2　典型的光隐蔽信道性能对比

Table 2　Performance Comparison of Typical Optical Covert Channels

	发送端	接收端	传输距离	传输速率
文献[72]	计算机键盘状态指示灯	光传感器、摄像机或手机	可见光范围	3000 位/秒
文献[82]	液晶显示屏	谷歌眼镜、摄像机或手机	9 米	10 位/秒
文献[19]	激光器	一体式打印机	1200 米	20 位/秒

光隐蔽信道的传输距离一般较远, 传输速率也较快, 而且部分技术可以实现双向隐蔽信道的建立, 这使得光隐蔽信道具有了较好的应用前景。

3.3　声

声通信是一种具有所需通信设备简单, 实现成本低, 不受电磁信号干扰的近距离通信技术。在物理隔离网络中, 敌对方可以在计算机与计算机、计算机与手机、手机与手机之间建立声隐蔽信道, 从而进行数据通信。由于声信道传输的隐蔽性, 它正逐渐成为信息安全领域里重点关注技术之一。

2014 年德国研究人员提出并设计了一种可以在计算机之间进行声隐蔽通信的恶意软件[83]。该软件的工作原理是利用笔记本电脑的扬声器和麦克风进行人耳不可听闻声的传输, 实现敏感数据的获取。该软件是在笔记本和笔记本之间建立了声隐蔽信道, 即一台笔记本的扬声器作为人耳不可听闻声的发射端, 另一台笔记本的麦克风作为人耳不可听闻声的接收端。这种恶意软件的对抗过程是: 首先将目标笔记本电脑中的敏感数据调制到 17KHz-19KHz 的高频波段上; 然后通过该笔记本电脑的扬声器将调制后的敏感数据发送出去; 最后通过另一台笔记本电脑的麦克风进行实时录音并进行解调, 从而实现数据隐蔽传输的功能。在物理隔离网络中, 人耳不可听闻声可以实现高效的短距离通信, 在没有误码率的情况下, 人耳不可听闻声的最远传输距离可以达到 19.7 米, 最高传输速率能达到 20 位/秒。特别地, 这种恶意软件还可以通过自组网技术实现多台计算机之间的声隐蔽通信。该研究团队利用水下声协议 GUWMANET 将多台笔记本电脑组成声隐蔽传输网络, 并通过连接互联网的笔记本电脑将敏感信息传输到物理隔离网络之外。这种多级传输解决了传输距离过短的限制, 有效增加了利用声信道进行信息传输的距离。在 2014 年, Carrara 等人[84]同样利用人耳不可听闻声建立了声隐蔽信道, 不同的地方是该

研究采用了正交频分复用(OFDM)调制方式, 这极大地促进了传输速率, 在误码率为 2%的情况下, 达到了 230 位/秒的传输速率, 传输距离也可以达到 11 米。

2016 年, 文献[85]提出并设计了一种名为“Fansmitter”的恶意软件。该软件的工作原理是利用计算机风扇引起的噪声, 实现敏感数据的获取。这种恶意软件是在计算机和手机之间建立了声隐蔽信道, 即计算机 CPU 或机箱的风扇作为声信道的发射端, 手机麦克风作为声信道的接收端。该恶意软件的对抗过程是: 首先将目标计算机中的敏感数据调制到 CPU 或机箱风扇的转速上; 然后通过 CPU 或机箱风扇产生的噪声将调制后的敏感数据发送出去; 最后通过手机的麦克风进行实时录音并进行解调, 从而实现数据隐蔽传输的功能。Fansmitter 的突破点是利用计算机主板上的风扇控制端口实现计算机 CPU 或机箱风扇的转速大小的控制, 从而可以达到的最远传输距离为 8 米, 最高传输速率为 0.3 位/秒。

与 Fansmitter 的工作原理类似, 另一种名为“DiskFiltration”的恶意软件[87]则是利用计算机机械硬盘的噪声, 实现敏感数据的获取。这种恶意软件是在计算机和手机之间建立了声隐蔽信道, 即计算机机械硬盘作为声信道的发射端, 手机麦克风作为声信道的接收端。该恶意软件的对抗过程是: 首先将目标计算机中的敏感数据调制到机械硬盘的转速上; 然后通过机械硬盘产生的噪声将调制后的敏感数据发送出去; 最后通过手机的麦克风进行实时录音并进行解调, 从而实现数据隐蔽传输的功能。DiskFiltration 实际上是通过机械硬盘的机械臂杆寻道操作实现计算机机械硬盘的转速大小的控制, 从而可以达到的最远传输距离可以达到 2 米, 最高传输速率为 3 位/秒。

2018 年, 文献[88]提出了“Mosquito”技术, 该技术的工作原理是利用计算机声卡从扬声器功能转换成麦克风功能以及人耳部可听闻声的传输功能, 实现敏感数据的获取。这种技术是在计算机扬声器之间建立了声隐蔽信道, 即一台计算机的扬声器作为人耳不可听闻声的发射端, 另一台计算机的扬声器作为人耳不可听闻声的接收端。该技术的对抗过程是: 首先将一台计算机中的敏感数据调制到 18KHz-24KHz 的高频波段上; 然后通过该计算机的扬声器将调制后的敏感数据发送出去; 最后通过另一台计算机的扬声器进行实时录音并进行解调, 从而实现数据隐蔽传输的功能。Mosquito 的工作重点是利用“Jack Retasking”端口特性, 将计算机的扬声器功能转换成麦克风功能, 建立了从扬声器到扬声器的声隐蔽信道, 其最远传输距离可以达到 8 米, 最高传输速率为 166 位/秒。

下表总结了利用声信道建立隐蔽通信的技术。

表 3 声隐蔽信道性能对比

Table 3 Performance Comparison of Acoustic Covert Channels

	发送端	接收端	传输距离	传输速率
文献[84]	笔记本扬声器	笔记本麦克风	19.7 米	20 位/秒
文献[85]	笔记本扬声器	笔记本麦克风	11 米	230 位/秒
文献[86]	计算机风扇	手机麦克风	8 米	0.3 位/秒
文献[87]	计算机机械硬盘	手机麦克风	2 米	3 位/秒
文献[88]	计算机扬声器	计算机扬声器	8 米	166 位/秒

声隐蔽信道的优势在于能够躲避电磁监测设备的监测, 然而较短的传输距离和较低的传输速率限制了其应用前景。目前, 基于声音的自组网技术在一定程度上增加了声隐蔽信道的传输距离, 但是声隐蔽信道的传输速率仍然有待提高, 可以作为将来的研究重点, 例如基于声的调制方式研究。

3.4 热

热隐蔽信道是物理隔离网络对抗技术近几年发展起来的。

2015 年, 文献[89]提出并设计了一种名为“BitWhisper”的恶意软件。该软件的工作原理是利用计算机 CPU 产生的热量建立热隐蔽信道, 实现敏感数据的获取。这种恶意软件是在计算机和计算机之间建立了热隐蔽信道, 即一台计算机的 CPU 作为热信道的发射端, 另一台计算机主板上的温度传感器作为热信道的接收端。该恶意软件的对抗过程是: 首先将目标计算机中的敏感数据调制到 CPU 计算量上; 然后通过 CPU 计算量产生的热量将调制后的敏感数据发送出去; 最后通过另一台计算机主板上的温度传感器实时接收并进行解调, 从而实现数据隐蔽传输的功能。BitWhisper 的突破点是利用 CPU 不同时间的计算量控制CPU产生不同时间的温度变化,

从而可以达到的最远传输距离为 0.04 米, 最高传输速率为 0.13 位/秒。

2015 年, 文献[90]提出并设计了一种名为“HVACKer”的恶意软件。该软件的工作原理是利用空调温度变化建立热隐蔽信道, 实现敏感数据的获取。这种恶意软件是在空调和计算机之间建立了热隐蔽信道, 即空调作为热信道的发射端, 计算机主板上的温度传感器作为热信道的接收端。该恶意软件的对抗过程是: 首先将利用恶意软件将信息与空调温度之间建立调制关系; 然后通过空调将调制后的信息发送出去; 最后通过与空调同一房间的计算机实时接收并进行解调, 从而实现信息发送的功能。HVACKer 的突破点是恶意硬件可以控制空调的温度变化, 从而可以达到0.83位/秒的最高信息传输速率。

2016 年, 文献[91]提出并设计了另一种热隐蔽信道技术。该技术的工作原理是利用计算机 CPU 核的温度变化建立热隐蔽信道, 实现敏感数据的获取。这种恶意软件是在计算机 CPU 核之间建立了热隐蔽信道, 即一台计算机的一个 CPU 核作为热信道的发射端, 同一台计算机的另一个 CPU 核作为热信道的接收端。该恶意软件的对抗过程是: 首先将目标计算机中的敏感数据调制到一个 CPU 核的计算量上; 然后通过该 CPU 核计算量产生的热量将调制后的敏感数据发送出去; 最后通过另一台 CPU 核实时接收并进行解调, 从而实现数据隐蔽传输的功能。该技术的突破点是利用CPU核不同时间的计算量控制CPU核产生不同时间的温度变化, 从而可以达到的最高传输速率为 12.5 位/秒。Long 等人[92]在此基础之上采用了一种新的调制方式, 极大地促进了信息的传输速率, 最高传输速率可达到 160 位/秒。

下表总结了利用热信道建立隐蔽通信的技术。

表 4 热隐蔽信道性能对比

Table 4 Performance Comparison of Thermal Covert Channels

	发送端	接收端	传输距离	传输速率
文献[89]	CPU	主板温度传感器	0.04 米	0.13 位/秒
文献[90]	CPU	主板温度传感器	未知	0.83 位/秒
文献[91]	CPU 核	CPU 核	未知	12.5 位/秒
文献[92]	CPU 核	CPU 核	未知	160 位/秒

从热隐蔽信道性能来看, 无论传输距离, 还是传输速率, 热隐蔽性能都比其他隐蔽信道技术有着不小的差距。但是随着热隐蔽信道技术的发展, 其性能也会逐步提高。

3.5 小结

为了横向比较电磁、光、声、热等物理隔离网络隐蔽信道的性能, 表 5 给出了各个隐蔽信道的横向对比情况。

表 5 隐蔽信道性能对比

Table 5 Performance Comparison of Covert Channels

隐蔽信道	隐蔽性	传输距离	传输速率
电磁	高	高	高
光	中	高	高
声	高	中	中
热	中	低	低

目前物理隔离网络隐蔽信道面临实用化的挑战, 只有解决了隐蔽性和传输性能(传输距离和传输速率)问题, 才能被真正地应用。从表 5 可以看出, 电磁隐蔽信道在隐蔽性和传输性能方面都具有优势, 是物理隔离网络隐蔽信道中较好的选择, 其中以无线收发形式产生的电磁隐蔽信道已经实用化。光隐蔽信道在传输性能方面有较好的表现, 但是在该信道传输过程中, 容易被人眼发现, 导致其只能在无人的情况下使用。声隐蔽信道与光隐蔽信道正好相反, 它可利用人耳不可听闻声躲避监测, 然而声隐蔽信道较弱的传输性能限制了其向实用化方面的发展。热隐蔽信道是近几年发展起来的新技术, 它的隐蔽性和传输性能尚不能实用化, 还需要进一步的提高。

4 应对措施

为了应对物理隔离网络对抗技术带来的威胁, 目前各个国家从标准制定、检测和防护技术研究、供应链安全管理等方面入手, 初步建立了物理隔离网络安全防护体系。

(1) 物理隔离网络安全标准

在针对物理隔离网络安全的标准制定上, 西方国家制定了一系列专门针对物理隔离网络安全的标准, 北约的 SDIP 系列标准[93]中明确规定了物理隔离网络内的电磁环境检测规程、等级划分准则及安全防护设备设计生产测评标准, 强调了现场防护、区域

防护是物理隔离网络安全防护的发展趋势。美国ICD/ICS705 系列[94-97], JAFAN6/9[98]明确规定了处理敏感信息场所(SCIF)的建设规范, 其中针对物理隔离网络防护的要求涵盖了电磁、声 、光等隐蔽信道及涉密载体管控几个方面。我国也不断推动物理隔离网络安全的标准体系建设 , 近几年来相继制定了保密会议室、保密要害部门部位、涉密场所检查等方向的多项国家标准, 并对电磁泄漏发射标准体系进行了复审修订, 确保涉密信息系统建设中物理隔离网络安全防护与传统网络安全防护的并行推进。

(2) 物理隔离网络检测防护技术

在物理隔离网络检测和防护技术研究方面, 针对物理隔离网络对抗技术的应对措施可从目标电子设备外部和内部入手解决。金属屏蔽是目前比较常见的防护技术之一[99], 该技术是在目标电子设备外部罩上一层金属材料, 可以有效阻止电磁信号的泄漏。信号滤波是另一种防护技术, 这种技术是将滤波器连接在目标电子设备的通信线路上, 能够将特定频率范围的信号滤除, 有效防止不期望的电磁辐射。信号干扰也是一种防护技术, 这种技术通过发射特定频率的随机性电磁或声信号, 能够干扰工作在该频率下的其它电磁或声信号, 保证有效阻拦异常信号的通信。在物理隔离对抗技术分析模型的隐蔽植入、行为执行和隐蔽通信阶段, 恶意软硬件已经进入目标电子设备内部实施恶意行为, 在这种情况下, 可利用行为分析、机器学习[98][100]、异常检测等反病毒和行为检测技术[20], 在目标电子设备内部进行检测防护。

(3) 供应链安全管理

对于供应链安全管理方面, 美国政府从 2008 年开始就制定了供应链安全战略, 并且相继制定了 SP 800-161[103]、IR7622、IR7622-2[102]等政策, 将供应链安全提升至保障网络空间安全的高度。欧盟《供应链完整性》 报告指出, 供应链完整性是国家经济发展的关键因素, 提高供应链完整度对公共和私营部门意义重大[103]。中国联合其他国家共同提交联合国的《信息安全国际行为准则》强调, 应当努力确保信息技术产品和服务供应链的安全, 防止他国利用自身资源、关键设施、核心技术及其他优势, 削弱落后国家对信息技术的自主控制权, 或威胁落后国家的政治、经济和社会安全[104]。在具体的供应链安全管理方法上, 分为硬件供应链安全管理方法和软件供应链安全管理方法。硬件供应链安全管理方法主要是风险管理, 该方法主要针对硬件木马、恶意固件、硬件伪造等进行风险管理。软件供应链安全管理的重要方法是软件供应链风险评估, 常用的是基于卡内基梅隆大学软件工程研究所的风险评估方法。

5 未来的发展方向

按照物理隔离网络对抗和物理隔离网络防护两个方面介绍未来的发展方向。

(1) 物理隔离网络对抗

当前, 大多数的物理隔离网络对抗技术是由学术界提出并在实验室验证, 因此在继续研究物理隔离网络对抗技术的理论基础之外, 还需要解决现有技术能否实用化的问题。隐蔽植入是物理隔离网络对抗技术比较薄弱的环节, 目前可利用的方法比较少, 较多的实际案例都是利用物理介质感染、供应链污染等接触式方法实施针对物理隔离网络的隐蔽植入。为了保证保隐蔽植入的安全性, 非接触式的软件隐蔽植入技术将是未来的发展趋势, 因此针对物理隔离网络内的目标电子设备, 可远程植入软件的漏洞利用技术成为隐蔽植入的研究重点。虽然隐蔽通信是当前物理隔离网络对抗技术的研究热点, 电磁、光、声、热等隐蔽信道构建技术相继被提出, 但是这些隐蔽信道依然存在隐蔽性能差和信道性能弱的缺点, 这两个问题限制了隐蔽通信向实用化的发展。为了促进隐蔽通信的实用化, 提高隐蔽信道的隐蔽性和信道性能成为将来的研究方向。所以, 具有较好隐蔽性和信道性能的电磁、声、光等隐蔽信道可成为重要的研究对象。除了重点关注物理隔离网络对抗技术本身的隐蔽植入和隐蔽通信两个重要支柱之外, 未来的物理隔离网络对抗技术还可以借鉴传统网络对抗技术的模块化设计思想。模块化设计是指根据不同功能, 将恶意软件划分成不同模块的设计。模块化设计的核心要点是将完整的恶意软件分割成多个部分, 从而既可以为任务分发提供良好的灵活性, 又可以提高恶意软件各个组成部分的生存性。为了提升物理隔离网络对抗技术的灵活性和生存性, 将模块化设计思想融入到物理隔离网络对抗技术成为今后的主流方向。因而, 依据物理隔离网络对抗技术实施的控制、窃取、监视、干扰、破坏、摧毁等行为并结合物理隔离网络对抗技术的对抗流程进行功能划分和模块设计, 成为主要的研究领域。

(2) 物理隔离网络防护

在物理隔离网络对抗技术的应对措施上, 要构建“关口前移, 防患于未然”的物理隔离网络安全体系。“关口前移”是对落实物理隔离网络安全防护方法提出的重要要求, 而“防患于未然”则形成了鲜明地以防护效果为导向的指引要求, 这是对如何解决

当前面临问题的深刻回答, 在此思想的指导下, 完善物理隔离网络防护标准, 研究针对物理隔离网络对抗技术有效的态势感知或认知技术(例如恶意软硬件识别、信道长时监测、计算机接口异常行为检测防护等), 建全供应链安全管理政策和方法, 最终形成完整的物理隔离网络安全防护体系。

6 总结

近十年以来, 针对军事设施、政府设施、基础设施等内部的物理隔离网络发生的对抗案例, 使人们不再相信物理隔离网络是安全的, 敌对方是可以利用物理隔离网络对抗技术实施控制、窃取、监视、干扰、破坏、摧毁等行为。本文通过分析工作原理及提出分析模型, 能够深刻理解物理隔离网络对抗技术是如何工作的, 同时通过与传统网络对抗技术的对比, 能够深入了解两种网络对抗技术之间既有区别, 又有相同的关系, 从而得出隐蔽植入和隐蔽通信是物理隔离网络对抗技术的两个重要支柱。隐蔽信道构建技术是物理隔离网络对抗技术重要支柱之一—隐蔽通信的关键技术, 其研究工作也是当前学术界的研究热点, 结合近期隐蔽信道构建技术的发展状况, 对电磁、光、声、热等物理隔离网络隐蔽信道的构建流程作了透彻地认识。为了应对物理隔离网络对抗技术, 国内外政府和学者也提出了一些应对措施, 可对物理隔离网络对抗技术施以一定的抑制。总之, 对于物理隔离网络, 攻与防的技术将会继续研究, 矛与盾的对抗将会持续博弈。

致 谢 本课题得到国家重点研发计划项目 2018YFF01014303 资助。

参考文献

[1] Mansfield-Devine S. Security through Isolation[J]. *Computer Fraud & Security*, 2010, 2010(5): 8-11.

[2] Christopher R. Bridging the air gap: an information assurance perspective[D]. University of Southampton, 2012.

[3] Lindqvist U, Jonsson E. A Map of Security Risks Associated with Using COTS[J]. *Computer*, 1998, 31(6): 60-66.

[4] Classified United States Website. https://en.wikipedia.org/wiki/Classified_United_States_website. May 2018.

[5] Byres E. The Air Gap[J]. *Communications of the ACM*, 2013, 56(8): 29-31.

[6] Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk. https://cryptome.org/emr.pdf. 1985.

[7] COTTONMOUTH-I: NSA Exploit of the Day. https://www.schneier.com/blog/archives/2014/03/cottonmouth-i_n.html. Mar. 2014.

[8] COTTONMOUTH-II: NSA Exploit of the Day. https://www.schneier.com/blog/archives/2014/03/cottonmouth-ii.html. Mar. 2014.

[9] COTTONMOUTH-III: NSA Exploit of the Day. https://www.schneier.com/blog/archives/2014/03/cottonmouth-iii.html. Mar. 2014.

[10] Vault 7: Projects. https://wikileaks.org/vault7/?#Brutal%20 Kangaroo. Apr. 2018.

[11] Hammerdrill v2.0. https://wikileaks.org/ciav7p1/cms/page_17072172.html. Apr. 2018.

[12] Revealed: How a secret Dutch mole aided the U.S.-Israeli Stuxnet cyberattack on Iran. https://news.yahoo.com/revealed-how-a- secret-dutch-mole-aided-the-us-israeli-stuxnet-cyber-attack-on-iran-160026018.html. Sept. 2019.

[13] Wang Q. Network attack and defense technology[M]. Beijing: Tsinghua University Press, 2019.
(王群. 网络攻击与防御技术[M]. 北京: 清华大学出版社, 2019.)

[14] Hutchins E, Cloppert M, Amin R. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains[J]. *6th International Conference on Information Warfare and Security*, ICIW 2011, 2011: 113-125.

[15] Glenn G. No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State[M]. Metropolitan Books, 2014: 1-10.

[16] Network Centric Warfare: Appendix. http://www.dodccrp.org/files/ncw_report/report/ncw_appendix.pdf. Jul. 2001.

[17] ACCOMPLISHMENTS. http://www.selectinnovation.com/SI- accomplishments.htm. Oct. 2009.

[18] INFORMATION WAR. https://www.afio.com/sections/wins/2002/2002-42.html. Nov. 2002.

[19] Light-based printer attack overcomes air-gapped computer security. https://www.scmagazineuk.com/light-based-printer-attack-overcomes-air-gapped-computer-security/article/1480640. Oct. 2014.

[20] Guri M, Elovici Y. Bridgeware[J]. *Communications of the ACM*, 2018, 61(4): 74-82.

[21] Iran says nuclear plant unaffected by virus as industrial computers struck. https://www.latimes.com/archives/la-xpm-2010-sep-26-la-fgw-iran-computer-virus-20100927-story.html. Sep. 2010.

[22] BlackEnergy by the SSHBearDoor: attacks against Ukrainian news media and electric industry. https://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry. Jan. 2016.

[23] Venezuelan Gov't Denounces Latest Attack on Electric System. https://www.telesurenglish.net/news/Venezuela-Denounces-US-Participation-in-Electric-Sabotage-20190308-0021.html. Mar. 2019.

[24] Petitcolas F A P, Anderson R J, Kuhn M G, et al. Information hiding-a survey[C]. *The IEEE*, 2002: 1062-1078.

[25] Gustavus J S. Advances in Cryptology: The Prisoners Problem and the Subliminal Channel[M]. Springer, 1984:51-67.

[26] Pfitzmann A, Waidner M. Networks without User Observability[J]. *Computers & Security*, 1987, 6(2): 158-166.

[27] Andrew T. Electronic Watermark[C]. *Digital Image Computing: Techniques and Applications*, 1993: 666-673.

[28] Huang Y F, Li S B. *Network covert communication and its detec-*

tion technology[M]. Beijing: Tsinghua University Press, 2016.
(黄永峰, 李松斌. 网络隐蔽通信及其检测技术[M]. 北京: 清华大学出版社, 2016.)

[29] Wendzel S, Zander S, Fechner B, et al. Pattern-Based Survey and Categorization of Network Covert Channel Techniques[J]. *ACM Computing Surveys*, 2015, 47(3): 50.

[30] Lipner S B. A comment on the confinement problem[C]. *The fifth symposium on Operating systems principles - SOSP '75*, 1975: 192-196.

[31] Girling C G. Covert Channels in LAN's[J]. *IEEE Transactions on Software Engineering*, 1987, SE-13(2): 292-296.

[32] Carrara B, Adams C. Out-of-Band Covert Channels—A Survey[J]. *ACM Computing Surveys*, 2017, 49(2): 23.

[33] Cyber Range. https://www.techopedia.com/definition/28613/cyber-range. Feb. 2020.

[34] Guri M, Monitz M, Bioengineering, et al. LCD TEMPEST air-gap attack reloaded[C]. *2018 IEEE International Conference on the Science of Electrical Engineering in Israel*, 2019: 1-5.

[35] Kuhn M G, Anderson R J. Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations[M]. Information Hiding. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998: 124-142.

[36] Guri M, Kedma G, Kachlon A, et al. AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies[C]. *2014 9th International Conference on Malicious and Unwanted Software*: *The Americas*, 2015: 58-67.

[37] Guri M, Monitz M, Elovici Y. Bridging the Air Gap between Isolated Networks and Mobile Phones in a Practical Cyber-Attack[J]. *ACM Transactions on Intelligent Systems and Technology*, 2017, 8(4): 50.

[38] Tempest for Eliza. http://www.erikyyy.de/tempest/. Jan. 2001.

[39] Analog and Digital TV (DVB-T) Signal Generation. http://bellard.org/dvbt/. Jun. 2005.

[40] Emanate like a boss: Generalized covert data exfiltration with Funtenna. https://www.blackhat.com/us-15/briefings.html# emanate-like-a-boss-generalized-covert-data-exfiltration-with-funtenna. Aug. 2015.

[41] Guri M, Monitz M, Elovici Y, et al. USBee: Air-gap covert-channel via electromagnetic emission from USB[C]. *2016 14th Annual Conference on Privacy*, *Security and Trust*, 2017: 264-268.

[42] Degauque P, Laly P, Degardin V, et al. Power line communication and compromising radiated emission[C]. *SoftCOM 2010*, *18th International Conference on Software*, *Telecommunications and Computer Networks*, 2010: 88-91.

[43] Callan R, Zajic A, Prvulovic M, et al. A practical methodology for measuring the side-channel signal available to the attacker for instruction-level events[C]. *2014 47th Annual IEEE/ACM International Symposium on Microarchitecture*, 2015: 242-254.

[44] Guri M, Kachlon A, Hasson O, et al. GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies[C]. *The 24th USENIX Conference on Security Symposium*, 2015: 849-864.

[45] Guri M, Communication N A B T, Processing C A. BeatCoin: leaking private keys from air-gapped cryptocurrency wallets[C]. *2018 IEEE International Conference on Internet of Things and IEEE Green Computing and Communications and IEEE Cyber*, *Physical and Social Computing and IEEE Smart Data*, 2019: 1308-1316.

[46] Fan J F, Guo X, de Mulder E, et al. State-of-the-art of secure ECC implementations: a survey on known side-channel attacks and countermeasures[C]. *2010 IEEE International Symposium on Hardware-Oriented Security and Trust*, 2010: 76-87.

[47] Through-the-earth two-way emergency wireless communications for mine industry safety. http://www.teslasociety.ch/info/ magnet-link/2.pdf. Mar. 2017.

[48] Bansal R. Near-Field Magnetic Communication[J]. *IEEE Antennas and Propagation Magazine*, 2004, 46(2): 114-115.

[49] Matyunin N, Szefer J, Biedermann S, et al. Covert channels using mobile device's magnetic field sensors[C]. *2016 21st Asia and South Pacific Design Automation Conference*, 2016: 525-532.

[50] Guri M, Zadov B, Elovici Y. ODINI: Escaping Sensitive Data from Faraday-Caged, Air-Gapped Computers via Magnetic Fields[J]. *IEEE Transactions on Information Forensics and Security*, 15: 1190-1203.

[51] MAGNETO: Covert Channel between Air-Gapped Systems and Nearby Smartphones via CPU-Generated Magnetic Fields. https://arxiv.org/ftp/arxiv/papers/1802/1802.02317.pdf. Feb. 2018.

[52] Fiori F, Musolino F. Comparison of IC Conducted Emission Measurement Methods[J]. *IEEE Transactions on Instrumentation and Measurement*, 2003, 52(3): 839-845.

[53] Kocher P, Jaffe J, Jun B. Differential Power Analysis[M]. Advances in Cryptology — CRYPTO\u2019 99. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999: 388-397.

[54] Islam M A, Ren S L. Ohm's Law in Data Centers: A Voltage Side Channel for Timing Power Attacks[C]. *The 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2018: 146-162.

[55] Clark T. Software-based data ex-filtration via simple power analysis[D]. USA: Naval Post Graduate School, 2009.

[56] Khatamifard S K, Wang L F, Das A, et al. POWERT channels: A novel class of covert CommunicationExploiting power management vulnerabilities[C]. *2019 IEEE International Symposium on High Performance Computer Architecture*, 2019: 291-303.

[57] Data Exfiltration From Air Gapped Systems Using Power Line Communication. https://pushstack.wordpress.com/2017/07/24/data- exfiltration-from-air-gapped-systems-using-power-line-communication/. Jul. 2017.

[58] Billings K H, Morey T, Rinaldi W, et al. Switchmode power supply handbook[M]. 3rd ed. New York: McGraw-Hill, 2011.

[59] Ye S, Eberle W, Liu Y F. A Novel EMI Filter Design Method for Switching Power Supplies[J]. *IEEE Transactions on Power Electronics*, 2004, 19(6): 1668-1678.

[60] FCC Part 15B. https://cdn-shop.adafruit.com/datasheets/SIM800_FCC_Part15.pdf. Jul, 2013.

[61] Introduction to Conducted Emission. http://www.ee.cityu.edu.hk/~emc/20150418P1.pdf. Apr. 2015.

[62] Zhao B, Ni M T, Fan P R. Powermitter: Data Exfiltration from Air-Gapped Computer through Switching Power Supply[J]. *China Communications*, 2018, 15(2): 170-189.

[63] Guri M, Zadov B, Bykhovsky D, et al. PowerHammer: Exfiltrating Data from Air-Gapped Computers through Power Lines[J]. *IEEE*

Transactions on Information Forensics and Security, 2020, 15: 1879-1890.

[64] RAGEMASTER: NSA Exploit of the Day. https://www.schneier.com/blog/archives/2014/03/ragemaster_nsa.html. Mar. 2014.

[65] LOUDAUTO: NSA Exploit of the Day. https://www.schneier.com/blog/archives/2014/01/loudauto_nsa_ex.html. Jan. 2014.

[66] TAWDRYYARD: NSA Exploit of the Day. https://www.schneier.com/blog/archives/2014/01/tawdryyard_nsa.html. Jan. 2014.

[67] SURLYSPAWN: NSA Exploit of the Day. https://www.schneier.com/blog/archives/2014/02/surlyspawn_nsa.html. Feb. 2014.

[68] Building Retro Reflectors. https://www.schneier.com/blog/ archives/2014/06/building_retro_.html. Jun. 2016.

[69] FIREWALK: NSA Exploit of the Day. https://www.schneier.com/blog/archives/2014/03/firewalk_nsa_ex.html. Mar. 2014.

[70] Loughry J, Umphress D A. Information Leakage from Optical Emanations[J]. *ACM Transactions on Information and System Security*, 2002, 5(3): 262-289.

[71] Sepetnitsky V, Guri M, Elovici Y, et al. Exfiltration of information from air-gapped machines using monitor's LED indicator[C]. *2014 IEEE Joint Intelligence and Security Informatics Conference*, 2014: 264-267.

[72] Guri M, Zadov B, Elovici Y. LED-it-GO: Leaking (a Lot of) Data from Air-Gapped Computers via the (Small) Hard Drive LED[M]. Detection of Intrusions and Malware, and Vulnerability Assessment. Cham: Springer International Publishing, 2017: 161-184.

[73] Guri M, Zadov B, Daidakulov A, et al. xLED: covert data exfiltration from air-gapped networks via switch and router LEDs[C]. *2018 16th Annual Conference on Privacy*, *Security and Trust*, 2018: 1-12.

[74] Guri M, Bykhovsky D. AIR-Jumper: Covert Air-Gap Exfiltration/Infiltration via Security Cameras & Infrared (IR)[J]. *Computers & Security*, 2019, 82: 15-29.

[75] How to make a computer screen INVISIBLE. https://www. dailymail.co.uk/sciencetech/article-2480089/How-make-screen-INVISIBLE-Scientist-shows-make-monitor-blank-using-3D-glasses.html. Oct. 2013.

[76] Lashkari A H, Farmand S, Zakaria D O B, et al. Shoulder Surfing Attack in Graphical Password Authentication[J]. *International Journal of Computer Science and Information Security*, 2009, 6(2): 145.

[77] Manu K, Tal G, Dan B, et al. Reducing shoulder-surfing by using gaze-based password entry[C]. *Proceedings of the 3rd symposium on Usable privacy and security*, 2017: 13-19.

[78] Shoulder surfing (computer security). https://en.wikipedia.org/wiki/Shoulder_surfing_%28computer_security%29. Aug. 2019.

[79] Guri M, Hasson O, Kedma G, et al. An optical covert-channel to leak data through an air-gap[C]. *2016 14th Annual Conference on Privacy*, *Security and Trust*, 2017: 642-649.

[80] Guri M. Optical Air-Gap Exfiltration Attack via Invisible Images[J]. *Journal of Information Security and Applications*, 2019, 46: 222-230.

[81] Guri M, Bykhovsky D, Elovici Y, et al. Brightness: leaking sensitive data from air-gapped workstations via screen brightness[C]. *2019 12th CMI Conference on Cybersecurity and Privacy*, 2020: 1-6.

[82] Hanspach M, Goetz M. On Covert Acoustical Mesh Networks in Air[J]. *Journal of Communications*, 2013, 8(11): 758-767.

[83] Carrara B, Adams C. On Acoustic Covert Channels between Air-Gapped Systems[M]. Foundations and Practice of Security. Cham: Springer International Publishing, 2015: 3-16.

[84] Fansmitter: Acoustic Data Exfiltration from (Speakerless) Air-Gapped Computers. https://arxiv.org/ftp/arxiv/papers/1606/1606.05915.pdf. Jun. 2016.

[85] Guri M, Solewicz Y, Daidakulov A, et al. Acoustic Data Exfiltration from Speakerless Air-Gapped Computers via Covert Hard-Drive Noise ('DiskFiltration')[M]. Computer Security - ESORICS 2017. Cham: Springer International Publishing, 2017: 98-115.

[86] Guri M, Solewicz Y, Elovici Y, et al. MOSQUITO: covert ultrasonic transmissions between two air-gapped computers using speaker-to-speaker communication[C]. *2018 IEEE Conference on Dependable and Secure Computing*, 2019: 1-8.

[87] Guri M, Monitz M, Mirski Y, et al. BitWhisper: covert signaling channel between air-gapped computers using thermal manipulations[C]. *2015 IEEE 28th Computer Security Foundations Symposium*, 2015: 276-289.

[88] HVACKer: Bridging the Air-Gap by Manipulating the Environment Temperature. https://deepsec.net/docs/Slides/2015/Bridging_the_Air-Gap_Data_Exfiltration_from_Air-Gap_%20Networks_-_Yisroel_Mirsky.pdf. Jan. 2015.

[89] Bartolini D B, Miedl P, Thiele L. On the Capacity of Thermal Covert Channels in Multicores[C]. *The Eleventh European Conference on Computer Systems*, 2016: 1-16.

[90] Long Z J, Wang X H, Jiang Y T, et al. Improving the efficiency of thermal covert channels in multi-/ many-core systems[C]. *2018 Design*, *Automation & Test in Europe Conference & Exhibition*, 2018: 1459-1464.

[91] TEMPEST Equipment Selection Process. https://www.ia.nato.int/niapc/tempest/certification-scheme. Jan. 2010.

[92] INTELLIGENCE COMMUNITY DIRECTIVE NUMBER 705. https://www.dni.gov/files/documents/ICD/ICD_705_SCIFs.pdf. May, 2010.

[93] INTELLIGENCE COMMUNITY STANDARD NUMBER 705-1. https://www.dni.gov/files/NCSC/documents/Regulations/ICS-705-1.pdf. Sep. 2010.

[94] INTELLIGENCE COMMUNITY STANDARD NUMBER 705-2. https://www.dni.gov/files/NCSC/documents/Regulations/ICS_705-2_Standards_for_Accreditation_Reciprocal_Use_of_SCIFs.pdf. Dec. 2016.

[95] Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities. https://www.dni.gov/files/NCSC/documents/Regulations/Technical-Specifications-SCIF-Construction.pdf. Sep. 2017.

[96] JAFAN6/9. https://www.dni.gov/files/NCSC/documents/ Regulations/Technical-Specifications-SCIF-Construction.pdf. Sep. 2017.

[97] Ross Anderson. Emission security. Security Engineering, 2nd Ed[M]. Wiley Publishing, 2008:1-10.

[98] Zhu W J, Nie K, Ban S H, et al. A novel algorithm for detecting GSMem attacks[C]. *2017 8th IEEE International Conference on*

Software Engineering and Service Science, 2018: 855-858.

[99] Detecting Disk Filtration using the BT Algorithm. http://m. paper.edu.cn/paper/release_detail/4747369. Mar. 2019.

[100] Zhu W J, Liu Y C, Fan Y W, et al. If air-gap attacks encounter the mimic defense[C]. *2019 9th International Conference on Information Science and Technology*, 2019: 485-490.

[101] Supply Chain Risk Management Practices for Federal Information Systems and Organizations. https://csrc.nist.gov/publications/ detail/sp/800-161/final. Apr. 2015.

[102] Notional Supply Chain Risk Management Practices for Federal Information Systems. https://csrc.nist.gov/publications/detail/nistir/7622/final. Oct. 2012.

[103] Supply Chain Integrity: An overview of the ICT supply chain risks and challenges, and vision for the way forward (2015). https://www.enisa.europa.eu/publications/sci-2015. Sep. 2015.

[104] China, Russia and Other Countries Submit the Document of International Code of Conduct for Information Security to the United Nations. http://uk.chineseembassy.org/eng/zgyw/t858978.htm. Sep. 2011.

孙德刚 现任中国科学院信息工程研究所高级工程师, 博士生导师。研究领域为高安全等级系统防护技术、电磁泄漏与发射技术、无线通信安全技术等。Email: sundegang@iie.ac.cn

夏宇琦 于 2016 年在武汉科技大学电子信息工程专业获得学士学位。现在中国科学院大学通信与信息系统专业攻读硕士学位。研究领域为声音安全、跨网攻防。研究兴趣包括: 计算机网络、隐蔽通信。Email: xiayuqi@iie.ac.cn

吕志强 于 2007 年在哈尔滨工业大学微电子学与固体电子学专业获得博士学位。现任中国科学院信息工程研究所副研究员。研究领域为信号收发与分析、射频系统集成。Email: lvzhiqiang@iie.ac.cn

张宁 于 2013 年在哥伦比亚大学电气工程专业获得硕士学位。现在中国科学院信息工程研究所攻读博士学位, 任中国科学院信息工程研究所工程师。研究领域为信息安全。Email: zhangning@iie.ac.cn

孔庆善 于 2014 年在中国科学院大学微电子与固体电子学专业获得博士学位。现任中国科学院信息工程研究所助理研究员。研究领域为: 物理隔离网络光信息获取技术, 光纤网络信息检测防护技术。Email: kongqingshan@iie.ac.cn