软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2020,31(1):228−245 [doi: 10.13328/j.cnki.jos.005878]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

隐蔽信道新型分类方法与威胁限制策略*

王 翀[1,2,3], 王秀利[4], 吕荫润[1,2,3], 张常有[3], 吴敬征[1,3], 关 贝[5], 王永吉[1,3]

[1](中国科学院 软件研究所 协同创新中心,北京 100190)

[2](中国科学院大学,北京 100049)

[3](计算机科学国家重点实验室(中国科学院 软件研究所),北京 100190)

[4](中央财经大学,北京 100081)

[5](Qatar Computing Research Institute, HBKU, Doha 999043, Qatar)

通讯作者: 王翀, E-mail: wangchong@nfs.iscas.ac.cn; 王永吉, E-mail: ywang@itechs.iscas.ac.cn

摘 要: 隐蔽信道是指恶意通信双方通过修改共享资源的数值、特性或状态等属性,来编码和传递信息的信道.共享资源的选取,由隐蔽信道的类型与具体通信场景所决定.早期,存储隐蔽信道和时间隐蔽信道主要存在于传统操作系统、网络和数据库等信息系统中.近年来,研究重点逐渐拓展到了 3 类新型隐蔽信道,分别为混合隐蔽信道、行为隐蔽信道和气隙隐蔽信道.对近年来国内外隐蔽信道研究工作进行了系统的梳理、分析和总结.首先,阐述隐蔽信道的相关定义、发展历史、关键要素和分析工作.然后,根据隐蔽信道共享资源的类型以及信道特征,提出新的隐蔽信道分类体系.首次从发送方、接收方、共享资源、编码机制、同步机制、评价指标和限制方法这 7 个方面,对近年来新型隐蔽信道攻击技术进行系统的分析和归纳,旨在为后续隐蔽信道分析和限制等研究工作提供有益的参考.进而,讨论了面向隐蔽信道类型的威胁限制技术,为设计面向一类隐蔽信道的限制策略提供研究思路.最后,总结了隐蔽信道中存在的问题和挑战.

关键词: 隐蔽通信;隐蔽信道;隐蔽信道分类;信息隐藏;行为隐蔽信道

中图法分类号: TP393

中文引用格式: 王翀,王秀利,吕荫润,张常有,吴敬征,关贝,王永吉.隐蔽信道新型分类方法与威胁限制策略.软件学报,2020,31(1):228−245. http://www.jos.org.cn/1000-9825/5878.htm

英文引用格式: Wang C, Wang XL, Lü YR, Zhang CY, Wu JZ, Guan B, Wang YJ. Categorization of covert channels and its application in threat restriction techniques. Ruan Jian Xue Bao/Journal of Software, 2020,31(1):228−245 (in Chinese). http://www.jos.org.cn/1000-9825/5878.htm

Categorization of Covert Channels and Its Application in Threat Restriction Techniques

WANG Chong[1,2,3], WANG Xiu-Li[4], LÜ Yin-Run[1,2,3], ZHANG Chang-You[3], WU Jing-Zheng[1,3], GUAN Bei[5], WANG Yong-Ji[1,3]

[1](Cooperative Innovation Center, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China)

[2](University of Chinese Academy of Sciences, Beijing 100049, China)

[3](State Key Laboratory of Computer Science (Institute of Software, Chinese Academy of Sciences), Beijing 100190, China)

[4](Central University of Finance and Economics, Beijing 100081, China)

[5](Qatar Computing Research Institute, HBKU, Doha 999043, Qatar)

* 基金项目: 国家自然科学基金(U1636213, 61772507, 61672508); 国家重点研发计划(2017YFB1002300)

Foundation item: National Natural Science Foundation of China (U1636213, 61772507, 61672508); National Key Research and Development Program of China (2017YFB1002300)

收稿时间: 2018-04-05; 修改时间: 2018-12-19; 采用时间: 2019-08-07; jos 在线出版时间: 2019-11-06

CNKI 网络优先出版: 2019-11-06 11:49:14, http://kns.cnki.net/kcms/detail/11.2560.TP.20191106.1148.005.html

Abstract: Covert channels are communication channels that allow secret transfer of information between two malicious processes by modifying the value or modulating the timing behavior of shared resources. Shared resources in covert communications vary according to the underlying covert channels. Initially, covert storage channels and covert timing channels are widely existed in information systems. More recently, the focus has shifted towards three new kinds of covert channels, namely, covert hybrid channels, covert behavior channels, and air-gap covert channels. This study surveys existing techniques for constructing covert channels that have been reported in literature, especially the covert channels that are presented in recent years. First, the definition, history, and key elements of covert channels are introduced. Covert channel analysis is also included. Second, a categorization technique is proposed for these covert channels based on the shared resources and channel characteristics. The traditional and new covert channel attack techniques are systematically analyzed based on the seven key elements of the covert channels. Third, the countermeasures for covert channels aforementioned are also demonstrated to restrict the threat brought by covert channels and to provide guidelines for future works. Finally, the challenges and problems on covert channels are provided.

Key words: covert communication; covert channel; covert channel categorization; information hiding; covert behavior channel

随着信息安全技术的不断发展,信息的安全传输越来越受到人们的重视.当信息以明文的形式传输时,很容易遭到拦截和篡改,无法保证信息的安全性和完整性.通常利用加密(cryptography)算法对信息进行编码形成密文,没有秘钥的其他接收者无法理解通信内容.然而随着计算机软件和硬件的不断发展,很多加密算法的破解时间日益缩短[1],加密技术受到了严重的挑战,甚至目前使用较为广泛的区块链技术也面临着潜在的安全威胁[2].此外,加密信息通常是一系列乱码,容易引起恶意拦截者的注意,即使拦截者无法破解加密算法,也可以进行破坏或干扰等操作,影响信息的正常传输.在此情况下,信息隐藏(information hiding)技术引起了研究者们的注意.信息隐藏将秘密信息以一种特定方式隐藏在公开的宿主信息载体上,使人们难于察觉到秘密信息的存在.

隐蔽信道(covert channel,简称 CC)是实现信息隐藏(information hiding)的重要技术[3],其概念最初由 Lampson[4]在 1973 年提出,主要关注的是单片机系统(monolithic system)中的安全机制问题.隐蔽信道利用隐蔽信息发送方和接收方所共享的资源(共享资源)编码隐蔽信息,并借助本意不是用来传输信息的信道传递隐蔽信息[4].隐蔽信道与加密技术的区别在于:加密仅仅使得通信内容不被恶意观测者所理解;而隐蔽信道在保护通信内容的同时注重隐藏通信自身的存在,使得非接收者无法察觉到通信的发生,增强了通信的隐蔽性和安全性.

随着编码理论、移动通信和云计算的飞速发展,隐蔽信道已经从一个概念思想转变为具有实践性的信息泄露技术[5].许多研究表明,隐蔽信道是多级安全系统的重要威胁,例如传统桌面操作系统、数据库系统和网络系统等[6−8].基于隐蔽信道机制的恶意信息泄露对信息安全构成了严重威胁,例如,违反操作系统的安全策略、泄露机密信息、破坏云环境中的隔离性等[9−12].不同类型隐蔽信道的应用场景、威胁程度和分析方法各不相同,因此,分析隐蔽信道的构成要素,提出信道分类方法,进而为限制各类隐蔽信道威胁提供具有通用性的策略和参考,对于研究和发展隐蔽信道限制技术是十分必要的.

根据现有研究工作和大量文献来看,隐蔽信道主要分为 5 种:早期出现的存储隐蔽信道(covert storage channel,简称 CSC)[13]和时间隐蔽信道(covert timing channel,简称 CTC)[14],以及后续新出现的混合隐蔽信道(covert hybrid channel,简称 CHC)[15]、行为隐蔽信道(covert behavior channel,简称 CBC)[16,17]和气隙隐蔽信道(air-gap covert channel,简称 ACC)[18].CSC 的发送方通过修改共享资源的数值(例如,数据包中字段的数值)来编码隐蔽信息,接收方读取共享资源的数值并解码隐蔽信息;CTC 发送方通过调节共享资源的时间特性(例如,包间隔时延[19])来编码隐蔽信息,接收方通过观察共享资源的变化解码隐蔽信息;CHC 是存储隐蔽信道和时间隐蔽信道的结合体,目标是提高信道容量或增强隐蔽性;CBC 基于共享资源的行为、状态等具有可改变性的属性编码隐蔽信息,共享资源可以是网络、计算机系统和通信中的现象或者事件;ACC 旨在于打破气隙系统(air-gapped system)的隔离性以及突破系统的访问控制策略.

目前,国内外学者在隐蔽信道的相关领域有了大量的研究成果,但是现有隐蔽信道分类方法[9,10,20]大多是针对某一类隐蔽信道进行分类,其中以基于网络的隐蔽信道(存储隐蔽信道和时间隐蔽信道)居多,并且分类粒度较粗.此外,近些年来,新型隐蔽信道(混合隐蔽信道、行为隐蔽信道和气隙隐蔽信道)技术也得到了快速发展.然而,目前国内很少有对于新型隐蔽信道的分类和分析工作;国外已有工作包含新型隐蔽信道的构建、检测和

限制等分析工作,但是缺乏对此类隐蔽信道的分类和总结.本文的分类工作不仅涵盖了存储和时间隐蔽信道,还包括了混合、行为和气隙这 3 类新型隐蔽信道,弥补了现有工作[9,10]的不足;同时,针对存储隐蔽信道和时间隐蔽信道提出了更细粒度的信道分类方法.此外,本文还分析和归纳了最近 5 年新提出的隐蔽信道技术.

本文从分析隐蔽信道的发展历史、通信模型和信道分析工作开始,讨论了构成隐蔽信道的 5 个关键要素.通过分析隐蔽信道的构建机理和关键要素,本文将现有隐蔽信道分为 CSC、CTC、CHC、CBC 和 ACC 这 5 大类信道.然后,根据每类隐蔽信道的实际情况,提出较为全面的、细粒度的隐蔽信道分类体系及分类依据,同时说明不同类别隐蔽信道之间的区别.然后,本文从发送方、接收方、共享资源、编码机制、同步机制、评价指标和限制方法这 7 个方面,详细地分析和归纳了近 5 年关键的隐蔽信道技术.最后讨论了该领域面临的主要问题和今后的发展方向.通过对隐蔽信道的分类、分析和归纳,本文希望为后续设计高效的、通用性强的隐蔽信道限制技术提供有益的参考和研究思路.

1 背景知识

1.1 信息隐藏

随着相关研究工作的不断发展,信息隐藏已成为一门包含许多分支技术的学科.较为常用的信息隐藏技术的分类方法是由 Petitcolas 等人[3]提出的,将信息隐藏技术分为隐写术、匿名通信、版权标识和隐蔽信道这 4 类.隐写术是一种研究如何利用多媒体信息的冗余性和人类感知的局限性将秘密信息隐藏在载体数据中的技术.匿名通信则注重于对通信关系的隐藏,使得除了秘密信息的发送者和接收者之外的第三方无法获取通信参与者的身份等信息,主要目的是隐匿秘密信息的来源,通常应用于合法用户在线选举投票、保护网络自由发言以及电子邮件匿名举报等方面.版权标识则与隐写术有所差别,强调对主动攻击的识别能力和抵抗攻击的鲁棒性[3],主要功能在于利用数字水印等技术完成数字作品的身份认证和版权保护工作,防止作品侵权.隐蔽信道是指不是被设计或本意不是用来传输信息的通信信道.相比于其他 3 种信息隐藏技术,隐蔽信道更注重于隐藏信道自身的存在,大大增强了通信过程的隐蔽性,从而保证了秘密消息的安全传输[4,7].此外,随着隐蔽信道编码和解码机制的日益完善,即使隐蔽信道自身的存在被发现,经过编码后的机密信息也很难被第三方所解读.总而言之,隐蔽信道被认为是信息系统的重要威胁之一[7,10].本文将在之后的章节对隐蔽信道进行详细的讨论.

1.2 隐蔽信道发展历史

1973 年,Lampson[4]首次给出了隐蔽信道的定义.1984 年,Simmons[21]提出的囚犯问题描述了隐蔽信道的通信场景.其中,Alice 和 Bob 被关在监狱的不同房间中并试图越狱.两人需要商定逃跑计划,但是所有通信信息都被看守人 Wendy 所监视[22,23].一旦 Wendy 发现有异常信息,就会更加严格地看管两人,彻底杜绝越狱的可能性.因此,Alice 和 Bob 需要使用 Wendy 无法察觉的通信手段完成越狱,例如隐蔽信道.Craver[24]拓展了上述问题并引入了 3 个新类型的看守人:(1) 消极的看守人可以发现隐蔽通信的存在,但不能修改隐蔽信息;(2) 积极的看守人可以稍微修改隐蔽信息,但要保持全文大意不变;(3) 恶意的看守人可以任意修改隐蔽信息.Alice 和 Bob 相当于隐蔽信道中的发送方和接收方,Wendy 是系统安全策略的设计者.隐蔽信道的目的是在发送方和接收方之间构建隐蔽信息流的传输通道,避免被安全策略所检测到.早期,研究人员关注本地存储时间隐蔽信道,例如,操作系统隐蔽信道.随着计算机网络的发展,研究重点逐渐转移到了网络隐蔽信道[9,14].此类信道利用网络协议内容或数据包间隔时延(inter-packet delay,简称 IPD)等资源编码隐蔽信息.新型隐蔽信道,例如,混合隐蔽信道、行为隐蔽信道和气隙隐蔽信道成为了最近几年的研究热点.这些隐蔽信道利用共享资源的不同特性达到提高信道容量或者增强隐蔽性等目的.

1.3 隐蔽信道的关键要素

根据隐蔽信道发展现状和已有研究工作成果,本文认为,一个隐蔽信道通常含有 5 个关键要素:发送方、接收方、编码机制(解码机制)、同步机制以及共享资源.发送方通过更改共享资源的特定属性编码隐蔽信息.接收方通过读取或观察共享资源的数值、状态等属性值的变化来解码隐蔽信息.同步机制和编码机制保证了信息传

输的正确性.以前,传统隐蔽信道研究将隐蔽信道表示为可信计算基三元组(trusted computing base,简称 TCB)[7]:⟨*variable*,PA_h,PV_i⟩,其中,*variable* 表示系统中的变量,PA_h 和 PV_i 分别是修改此变量的高安全级别 TCB 原语和低安全级别 TCB 原语.由于当时隐蔽信道研究关注于本地隐蔽信道(例如,操作系统隐蔽信道),定义中的 *variable* 特指系统中的共享变量.随着隐蔽信道的发展,研究和定义已经拓展到了行为隐蔽信道、气隙隐蔽信道以及混合隐蔽信道,而这些信道使用电磁信号、热信号和 Wi-Fi 强度等共享资源编码隐蔽信息,而不仅仅局限于系统中的共享变量.因此,结合目前隐蔽信道研究现状,本文将共享变量这个概念拓展为共享资源,即发送方和接收方所能修改和感知的资源,双方能够利用此资源编码和传递隐蔽信息.共享资源的选取方式与隐蔽信道的类型和实际通信场景有关,例如,网络中的 IPD、云计算环境中的指令缓存和内存总线[25]、微内核中的 IPC 机制[26]和操作系统中的临时文件等.

1.4 隐蔽信道分析工作内容

根据现有研究工作以及《可信计算机系统评估准则》(trusted computer system evaluation criteria,简称 TCSEC)的要求,隐蔽信道分析工作主要包含以下 4 个方面.

(1) 隐蔽信道标识.通过全面地扫描和分析目标系统,发现系统中的隐蔽信道和可能被用于构建隐蔽信道的共享资源,例如 Denning[27]提出的信息流分析方法、Tasi 等人[28]提出的语义信息流标识方法、Shrestha 等人[29]使用的基于支持向量机的框架以及 Yan 等人[26]使用的 ReplayConfusion 方法;

(2) 隐蔽信道构建.该项工作是实现真实隐蔽信道通信场景和模拟攻击者行为的方法.例如:基于模型的构建方法[11]忽略具体实现场景的特性,而更关注信道本身;基于共享资源的构建方法[25,30,31]注重具体通信场景中共享资源的特性;

(3) 隐蔽信道威胁度量.威胁度量的目标是评估隐蔽信道威胁程度,为隐蔽信道限制工作提供指导和判定依据.目前,隐蔽信道威胁度量指标主要包含[7]:信道容量(传输速率),即隐蔽信道能够取得的最大传输速度;准确率,即隐蔽信道传输信息的保真能力;短消息,即隐蔽信道传输机密而又短小的隐蔽信息的能力,弥补信道容量指标的不足.还有研究人员提出抗检测能力指标[6]量化隐蔽信道的隐蔽性,作为对现有威胁度量体系的补充;

(4) 隐蔽信道限制.目的是限制或消除隐蔽信道带来的威胁,包含审计、限制和消除这 3 项工作.但是近些年的隐蔽信道研究指出:隐蔽信道的威胁是无法完全消除的[9,32,33],彻底消除隐蔽信道需要消耗大量系统资源,会严重影响系统可用性.审计只能做到事后追责,而非事前预防,无法及时阻止信息泄露.因此,隐蔽信道限制是目前所普遍采用的方法.经典隐蔽信道限制技术是向信道中添加噪音(干扰)[34,35]和添加时延[36],达到干扰隐蔽信息传输以及降低信道容量、准确率的目的.例如,Kang 等人[37]提出了 Pump 限制算法,美国海军研究实验室(naval research laboratory)的 Network Pump[38]以及 Wu 等人[36]提出了 Xenpump.

隐蔽信道分析工作为清晰地了解隐蔽信道构成、度量信道威胁程度和设计相应的限制策略提供了准则.因此在本文第 2 节中,将以隐蔽信道分析包含的 4 个工作为指导,从隐蔽信道的 5 个关键要素、度量指标和限制方法这 7 个方面,对近年来的重要隐蔽信道技术进行分析和归纳,从而为信道分类方法提供依据和指导,同时也为设计面向隐蔽信道类型的威胁限制技术提供依据.其中,发送方、接收方、共享变量、编码机制和同步机制这 5 个要素属于隐蔽信道标识工作的目标,基于这 5 个要素在实际场景中构建信道则属于隐蔽信道构建工作的范畴.度量指标对应于隐蔽信道威胁度量工作,是研究人员量化隐蔽信道威胁性的依据.限制方法对应于隐蔽信道限制工作,即利用信道设计者提出的技术或者现有研究工作中的方法限制隐蔽信道的威胁.

2 隐蔽信道分类

本节将隐蔽信道分为存储、时间、混合、行为和气隙这五大类.根据隐蔽信道分析工作和现有研究工作,分别从发送方、接收方、共享资源、编码机制、同步机制、评价指标和限制方法这 7 个方面详细地分析和归纳每类隐蔽信道.此外,相比于混合、行为和气隙这 3 类新型隐蔽信道,存储隐蔽信道和时间隐蔽信道发展历史

悠久,相关研究工作数量较多.为了使研究问题更加清晰,本节根据共享资源的使用方式等因素提出细粒度分类方法,将存储和时间隐蔽信道细化为多个小类.

2.1 存储隐蔽信道

存储隐蔽信道以共享资源的内容为隐蔽信息的载体,主要可以分为网络存储隐蔽信道和本地存储隐蔽信道.网络存储隐蔽信道主要面向实时通信和网络系统,例如分布式计算网络中的隐蔽数据传输[39],很多研究工作都将隐蔽信息嵌入到数据包的字段中.本地信道主要面向单机和主机系统,利用系统中的软件和硬件资源的内容作为隐蔽信息的载体,例如,共享存储区域和共享变量等.

2.1.1 网络存储隐蔽信道

(1) 字段长度

此类隐蔽信道通过填充内容等方式更改整体数据包的长度或者某一包头字段的长度来编码隐蔽信息,例如:当字段长度小于(或大于)某一个预设阈值时,表示发送比特 0(或比特 1).

Epishkina 等人[40]提出了利用数据包长度编码隐蔽信息的方法,根据长度将数据包分为两个集合 L_0 和 L_1.发送比特 0 时,则从 L_0 中选取数据包并发送;反之,则发送 L_1 中的数据包.Epishkina 等人还借助多个数据包长度同时表示多位隐蔽信息.Girling[41]提出了通过调节链路层中帧的长度编码隐蔽信息的方法,此方法也可以应用于 IP、UDP 以及 TCP 数据包[42].Rios 等人[43]通过调节 DHCP(dynamic host configuration protocol)包中可选项的数量控制包的长度,从而构建隐蔽信道.还有一些研究将 IPSec 消息[44]、IP 分片[45,46]和 IEEE 802.3 帧填充字段等数据单元(data units)的长度[47]作为隐蔽信息的载体.

(2) 字段位置

此类隐蔽信道会通过更改数据包中某一个或多个元素/包头字段的位置或排列顺序编码隐蔽信息.

Rios 等人[43]借助 DHCP 协议中可选项的位置编码隐蔽信息.例如,预先选取 DHCP 的 4 个可选项,其顺序的排列组合可以表示不同的 4 位二进制数.同时,Rios 等人[43]还利用 DHCP 单个可选项在整体可选项中的位置编码隐蔽信息,每次只能传输一个比特.Zou 等人[48]利用 FTP 协议中命令的顺序来编码隐蔽信息.研究人员还利用 IPv4 中的字段、IPv6 扩展包头字段以及 HTTP 协议中头部字段的顺序构建隐蔽信道[10].

(3) 冗余字段

此类隐蔽信道根据具体的通信协议,扩展和填充协议中的未使用字段和保留字段,利用正常数据包额外的空间作为隐蔽信息的载体.

在 IPSec 连接中,Sadeghi 等人[44]利用 IP 数据包中的 ECN(explicit congestion notification)字段和 DS (differentiated services)作为隐蔽信息的载体.Muchene 等人[49]以小于以太网帧中所规定 IP 数据包的尺寸封装 IP 数据包,然后在 IP 数据包和以太网帧的间隙中嵌入隐蔽数据.Rios 等人[43]使用 DHCP 协议中的 sname 和 file 字段作为载体,在字符串结束符中嵌入隐蔽数据.此外,如果 hlen 字段的数值大于网络地址的大小,则启用未使用字段 chaddr 传递隐蔽信息.还有一些研究人员利用 IEEE 802.3 协议中的未使用域、IP 协议中路由记录字段、IP 包头中的校验字段和 TCP 协议中的未使用位等字段作为隐蔽信息的载体[9,10].

(4) 字段数值修改

此类隐蔽信道通过修改头部字段的数值编码隐蔽信息.网络协议中的某些包头字段数值是随机的或者仅提供有限个备选的数值,发送方利用这些数值来表示不同的隐蔽信息.一些头部字段中数值的大小写和最低有效位(least significant bit,简称 LSB)也可以用来编码隐蔽信息.

Classen 等人[50]基于 WARP(wireless open-access research platform)和 Wi-Fi 协议提出了 4 种隐蔽信道.第 1 个信道利用 Wi-Fi 帧中的 STF(short training field)的数值作为隐蔽信息的载体,结合 PSK(phase shift keying)编码比特 0 和比特 1.第 2 个信道使用 OFDM(orthogonal frequency-division multiplexing)的数值来修正 Wi-Fi 帧中的 CFO(carrier frequency offset),并利用 CFO 表示隐蔽信息.第 3 个 CS(camouflage subcarriers)和第 4 个 CPR(cyclic prefix replacement)信道是对已有信道的改进工作[51,52].CS 信道基于 802.11a/g 协议使用子载波作为隐蔽信息的载体.CPR 信道则利用 802.11a/g 协议中的 CP(cyclic prefix)隐藏信息.Vines 等人[53]采集游戏程序在通信过程中

的真实数据包并分类.当发送隐蔽信息时,依据编码规则选取相应类别的数据包,并用其内容替换正常数据包的内容.Tuptuk 等人[54]在温度传感器测量值的误差允许范围内,通过修改传感器数据包的 LSB 编码隐蔽信息,并利用预定义 16 比特前导码(preamble)作为同步机制.研究人员还利用 BACnet(building automation and control networking)的消息类型[55]、IP 地址等数值[44,56]和 DHCP 协议中的 xid[43]的数值构建隐蔽信道.

(5) 隐蔽信息直接嵌入

此类隐蔽信道直接将隐蔽信息嵌入到网络数据包中.

Daneault 等人[57]提出了一种使用中继构建网络隐蔽信道的方法,该方法在 HTTP 协议的 GET 请求的 URL 中添加隐蔽信息,以 Google 图片搜索为中继传输信息,利用 Google 的公信力增加信道隐蔽性.然后,Google 图片搜索会访问含有隐蔽信息的网址,完成隐蔽信息的传送.Ameri 等人[58]将隐蔽信息嵌入到 NTP 协议中,并将隐蔽信息与时间戳做 XOR 操作,增加隐蔽性.发送和接收双方分别有类似 TCP 三步响应的同步机制.Johnson 等人[59]在 HTTPS 的数据域中添加隐蔽信息,利用 MitM(man-in-the-middle)攻击更改信息流,如果没有原本 HTTPS 请求或者加密秘钥做对比,则这个隐蔽信道是无法被检测到的.Khader 等人[60]使用端口试探技术(port knocking)构建隐蔽信道,发送方会将隐蔽信息嵌入至图像的最低有效位中,利用与接收方事先约定的端口传输隐蔽信息.Rezaei 等人[61]讨论了在 Long Term Evolution-Advanced 协议的头部字段中嵌入隐蔽信息的可行性.

2.1.2 本地存储隐蔽信道

(1) 共享变量数值

此类隐蔽信道通过修改共享变量的数值编码隐蔽信息.发送方按编码规则修改共享变量的属性值,接收方不断或周期性地扫描共享变量以解码隐蔽信息,共享变量的选取影响此类信道的传输速率、准确率和隐蔽性.

Lin 等人[30]提出了 3 种隐蔽通信协议,分别为 BP(basic protocol)、TCTP(two-channel transmission protocol)和 SAP(self-adaptive protocol),并构建了相应的隐蔽信道.3 种信道的共享资源都是 Linux 操作系统中的 *last_pid*,通过给 *last_pid* 增加不同的数值来表示比特 0 和比特 1.BP 信道是一个基础信道,缺乏同步机制和抗干扰能力.TCTP 信道对 BP 信道进行了改进,利用临时文件实现了同步机制.SAP 信道则进一步利用校验位实现了隐蔽信息的重传机制.Luo 等人[13]基于 Docker 和 Linux 系统设计了 GUM(globally used memory)信道和 inode 节点信道.GUM 信道通过增加不同程度的内存使用量编码比特 0 和 1,接收方则通过读取/proc/meminfo 文件获取隐蔽信息.inode 信道以 inode 节点的数值作为隐蔽信息载体,是一种资源耗尽型的信道[13].Fern 等人[62]利用 SoC 空闲状态下未定义的总线信号,在 SoC 组件之间构造了隐蔽信道.还有研究人员[63]向 DNA(deoxyribonucleic acid)中插入含有隐蔽信息的人工合成核苷酸序列,利用该序列与宿主 DNA 的相似性验证信道的抗检测能力.

(2) 共享组件内容

共享组件通常会为发送方和接收方提供一块共享存储区域.与共享变量信道相比,此类信道可以一次性发送多位编码后的比特信息,甚至直接将信息写入共享存储区域,信道容量通常较高.

Hussein 等人[64]基于动态分配的共享物理内存(dynamically-allocated shared physical memory)传递隐蔽信息,发送进程将隐蔽信息装载到指定存储页,然后协同接收进程迫使 VMM(virtual machine monitor)强制回收该存储页,并将其分配给接收 VM(virtual machine)作为额外的存储空间.Luo 等人[13]利用系统中的内核消息缓冲区(kernel message buffer,简称 KMB)作为共享资源构建了 KMB 信道.由于向 KMB 中写入隐蔽信息需要拥有特殊权限,而读取 KMB 却不需要,利用这个特性可以通过 KMB 泄露一些权限相关的机密信息.

2.1.3 存储隐蔽信道分析和归纳

由于文章篇幅所限以及关注点等因素,本节从隐蔽信道分析的角度对近 5 年存储隐蔽信道的关键研究进行分析和归纳,见表 1.其中,存储隐蔽信道的限制方法有很多,例如,在隐蔽信道中添加干扰/噪音(add noise,简称 AN)[65]、为信道的特定操作添加时延(add delay,简称 AD)[36]以及利用通信量规范化(traffic normalization,简称 TN)[10]等.可以看出:近 5 年来,研究人员利用未被发现的协议字段作为网络信道的隐蔽信息载体,同时借助虚拟机、Docker 等新技术构建本地隐蔽信道.存储信道的传输速率一般较高,而添加噪音的方法也可以将本地信道的传输速率降到一个很低的范畴.利用 TN 方法可以降低甚至是消除大部分存储网络信道的威胁.

Table 1 Summary of key covert storage channels in recent five years

表 1 近 5 年关键存储隐蔽信道总结

隐蔽信道名称	发送方	接收方	共享资源	编码机制	同步机制	评价指标	限制方法
VMM memory reclamation CC[64]	虚拟机	虚拟机	共享内存	嵌入信息至内存页	–	–	添加噪音
Client-initiated HTTP CC[57]	客户端 PC	Web 服务器	HTTP 请求(GET)	嵌入信息至 HTTP	–	传输速率	TN
Normal traffic imitating CC[56]	PC	PC	IP 地址和 UDP 包长	更改 IP 地址和 UDP 包长	–	传输速率	TN
Sensor data CC[54]	Orisen 设备	Eve 设备	温度传感器	更改温度的数值	预定义前导码	传输速率; 准确率	添加噪音
Network time protocol CC[58]	PC	PC	NTP 协议帧	嵌入信息至数据域	预定义的 timestamp	传输速率	TN
MITM CC[59]	PC	服务器	HTTPS 数据域	嵌入信息至 HTTPS	预定义数据包内容	–	TN
Port knocking[60]	客户端 PC	服务器	图片	嵌入加密信息至图片	预定义端口	传输速率; 峰值信噪比	添加噪音
DNA CC[63]	研究人员	研究人员	人工合成 DNA	嵌入核苷酸序列至 DNA	预定义核苷酸序列	–	–
Basic; inode; KMB CC[13]	容器 (container)	容器 (container)	共享文件;内核消息队列	更改共享变量数值	固定时间 T	传输速率; 准确率	添加噪音; 添加时延
Covert trojan channel[62]	程序	程序	总线信号	更改总线信号	预定义总线信号	性能影响	规范化总线行为
WiFi-STF PSK; WiFi-CFO FSK; WiFi-CS WiFi-CPR[50]	WARP	PC	WiFi 帧 ST 域; OFDM 域; 子载波;CP	更改相位偏移和 OFDM; 嵌入信息至子载波和 CP	接收方持续监听; HT-LTF 同步机制	传输速率; 准确率	隐蔽信道审计;TN
Binary; Multi-symbol[40]	–	–	数据包	调节数据包长表示 0/1	SOF 包	传输速率; 准确率	TN
Rook[53]	游戏客户端	游戏服务器	数据包	修改数据域	预定义数据包	传输速率; 准确率	TN; 添加噪音

2.2 时间隐蔽信道

时间隐蔽信道主要分为网络信道和本地信道,利用网络或本地系统中共享资源的时间特性作为隐蔽信息的载体,例如缓存的访问时延(access latency)和包间隔时延等.

2.2.1 网络时间隐蔽信道

(1) 包间隔时延

包间隔时延是时间隐蔽信道中较为常用的共享资源,大小由数据包的发送时间决定.编码机制通常会设定一个阈值,当 IPD 大于此阈值时表示隐蔽信息比特 1(比特 0),当 IPD 小于此阈值时表示隐蔽信息比特 0(比特 1).

Tahir 等人[33]提出了跨虚拟网络的时间隐蔽通道,借助数据中心的共享网络资源在逻辑上隔离的虚拟网络中传输机密信息.发送方通过调整正常数据包的 IPD 控制数据包达到接收方的时间.如果在预定的周期 T 内接收方未收到数据包,则所传输的隐蔽信息是比特 0,反之则是比特 1.Tahir 等人还评估了信道的最大传输速率并提出了一个优化的编码机制.实验结果表明,此信道可以破坏商业云服务 EC2 和 Azure 中的安全机制.Archibald 等人[66]认为:视频实时通信场景通常要求较高的数据包传输速率,致使单一 IPD 过短,接收方很难根据单个 IPD 长短区分比特 0 和比特 1.因此,Archibald 等人在 Skype 中基于多个 IPD 的累加构建时间隐蔽信道,使得接收方能够明确地区分和解码隐蔽信息;同时还引入喷泉码[66]编码隐蔽信息,提高了信道容量.Liu 等人[67]提出了模拟喷泉码(analog fountain codes)以及通用模型拟合代码框架(general model-fitting coding framework),进一步提高隐蔽信道在 IP 网络电话通信场景中的可用性.Liguori 等人[68]基于 IPD 实现了 3 种开源时间隐蔽信道(open-source covert timing channel,简称 OSCTC),验证 MILS(multi independent levels of security/safety)架构的有效性,并讨论了同步机制和纠错机制的重要性和必要性.第 1 种 OSCTC 信道利用一个固定的模式保证发送方和接收方之间的信息同步.第 2 种 OSCTC 信道利用 Manchester Coding 作为同步机制,在此基础上,第 3 种同步 OSCTC

信道借助 Hamming Code 保证隐蔽通信的正确性.还有一类基于数据包传输速率的隐蔽信道[9,69],此类信道通过控制固定周期 T 内数据包发送的速率来编码不同的隐蔽信息,实质上类似于前文提到的借助多个 IPD 累加所构建的时间隐蔽信道[66].

(2) 数据包到达时间

此类信道通过控制多个数据包发送时间或达到时间编码隐蔽信息.例如,可以通过调制数据包发送顺序来控制数据包到达接收方的时间.

El-Atawy 等人[35]提出了利用无序数据包(out-of-order packets)构建时间信道的方法,该方法每次选取 k 个正常数据包,根据待发送信息移动其中某几个包的顺序,利用移动前后数据包顺序的变化计算 codeword[70]并编码隐蔽信息.同时,该信道还借用二进制反射格雷码(binary reflected Gray codes)纠正隐蔽信息中的错误.Herzberg 等人[71]在两个 VPN 站点之间的公共网络中构建了隐蔽信道.信道发送方是一个处在公共网络中的 MitM 攻击者,接收方是分别处于两个 VPN 站点上的 MitE(man-in-the-end)攻击者.两个 MitE 攻击者通过网络正常通信,而 MitM 攻击者通过修改其中数据包的顺序控制数据包到达接收方的时间,从而编码隐蔽信息.

(3) 网络缓存访问时延

此类隐蔽信道利用系统中各类缓存的访问时延作为隐蔽信息的载体,例如一级缓存和二级缓存等.基于缓存的隐蔽信道较为常见,但设计的方法各式各样,因此单独归为一类.

Liu 等人[72]借助 LLC(last-level cache)访问时延长短构建了跨虚拟机的隐蔽信道,该信道采用 PRIME+PROBE 算法确保了信息的传输正确率和速率.在 PRIME 阶段,发送方会根据待发送信息填充 LLC,之后进入等待状态.在 PROBE 阶段,接收方会持续地从 LLC 中尝试读取数据并测量访问时延,并根据时延长短解码隐蔽信息.该信道不依赖于虚拟机中的操作系统、虚拟机监控器和共享内存的缺陷,具有高度的实用价值.Yossef 等人[73]将上述 PRIME+PROBE 算法扩展到了 JavaScript,同样基于 LLC 的访问时延设计了微架构下的隐蔽信道攻击方法.该方法不要求目标机器(发送方)预先安装恶意软件,而是需要通过浏览器访问一个攻击者预先设计好的网页,攻击者会向 LLC 中装载网页中的特定内容,并执行 PRIME 步骤记录访问时延.然后,攻击者引导目标机器做出特定的动作,例如,目标机器浏览或开关网页,这些动作会使得 LLC 中的内容发生变化.之后,攻击者再执行 PROBE 步骤,通过访问时延可以推测出 LLC 中内容的变化,从而解码隐蔽信息.同时,在记录了大量 LLC 的访问时延的基础上,利用聚类方法在用户行为和 LLC 的不同访问时延之间构建映射关系,可以令攻击者远程地推测用户行为.该工作在实际部署中具有较好的可用性.

Yao 等人[74]基于非统一内存访问的体系结构在服务器上的两个套接字(socket)之间构建了时间隐蔽信道.每个套接字都有本地 L1 缓存和 LLC.当一个套接字的访问内容不在本地缓存中时,称为本地未命中(local miss,简称 LM),会使用其他套接字的缓存作为更低一层级的 LLC.若此时命中,则称为远程命中(remote hit,简称 RH).显然,RH 的时间要长于本地命中的时间.发送方首先借助木马程序,利用系统命令清除所有套接字的缓存内容,然后将特定内容装入自己的缓存中.此时接收方的缓存为空,产生 LM,需要访问发送方的缓存并产生 RH.该信道编码机制如下:发送比特 1 时,令接收方产生 4 个 RH;发送比特 0 时,令接收方产生两个 RH.Irazoqui 等人[75]指出:目前大部分时间隐蔽信道都是面向 Intel 处理器的,其缓存是包含式(inclusive)的,缺乏面向独立式(exclusive)缓存的时间信道,因此提出了基于 LLC 的时间隐蔽信道.与之前方法不同的是,该信道并不关心访问不同层级 cache 的时间差别,而是利用访问缓存时间和访问内存时间的差别来编码隐蔽信息.实验结果表明:缓存和 DRAM(dynamic random access memory)两者的访问时间区别较大,接收方可以根据时延明确解码隐蔽信息.

(4) 网络共享组件访问时延

此类隐蔽信道利用系统中的组件作为隐蔽信息的载体,例如云服务中的共享存储区域以及用户之间所共享的 CPU 等硬件或软件资源.

Hovhannisyan 等人[76]提出了云服务中基于重复数据(deduplication-based,简称 DB)的隐蔽信道,通过设计编码机制一次性传输多位隐蔽信息,克服了同类信道只能传输 1 比特的不足.其核心思想是:对于含有相同哈希码

的文件,服务器只存储一份原始数据,致使用户上传一个新文件的时间明显大于上传一个服务器中已有文件的时间.接收方根据上传时间的长短解码隐蔽信息.Block 等人[77]在高度虚拟化的数据中心上实现了基于干扰机制的时间隐蔽信道,该信道利用发送方的特定 HTTP 请求 GET 和 OK 之间的时间间隔长短编码隐蔽信息.当发送比特 1 时,发送方会产生大量请求,使服务器响应请求的速度变慢,造成 GET 和 OK 之间的时间间隔长于预设阈值;当发送比特 0 时,发送方则保持静默.该信道利用预先定义好的标记信息进行同步工作.

Wu 等人[12]认为,现有研究无法证明虚拟 x86 系统中的隐蔽信道是实际可用的,因此提出了两个具有高带宽和高可靠性的隐蔽信道:第 1 个信道借助 CLines(cache lines)作为隐蔽信息的传输介质,发送方通过访问一系列的 CLines 映射内存地址将这些缓存置于刷新状态,接收方测量访问这些 CLines 映射内存地址的时延,根据延长短解码隐蔽信息;第 2 种信道将第 1 种信道中的 CLines 替换为内存总线,利用总线的竞争态和空闲态分别编码比特 0 和比特 1,该信道使用 FEC(forward error correction)码保证信道的传输正确率,并采用差分曼切斯特编码(differential Manchester encoding)解决发送方和接收方的同步问题.

2.2.2 本地时间隐蔽信道

(1) 缓存访问时延(本地)

此类隐蔽信道与基于缓存的网络时间隐蔽信道相似,不同之处在于该信道主要利用本地系统中各类缓存的访问时延编码隐蔽信息,也包含一级缓存、二级缓存和三级缓存等.

Naghibijouybari 等人[78]利用 GPGPU(general purpose graphics processing units)在两个无法直接通信的进程之间搭建隐蔽信道.该研究首先针对处于相同 SM(streaming multiprocessor)上的应用构建了基于 L_1 缓存的隐蔽信道,然后提出了基于 L_2 缓存的隐蔽信道,使得不同 SM 上两个应用的隐蔽通信成为可能.两种隐蔽信道的核心思想都是通过创造竞争改变缓存的内容,利用缓存是否命中带来的访问时延不同来表示比特 0 和 1.实验结果表明:发生竞争时,时延为 112 个时钟周期,无竞争时时延为 49 个时钟周期,使得此信道具有实用性.但是该信道并没有同步机制以保证隐蔽通信的正常进行.Lin 等人[11]将 L_2 缓存分为两个子集 A 和 B,发送方会根据待发送信息将接收方 L_2 缓存中的某一个子集清空,并保持另一个子集内容不变.然后,接收方访问 L_2 缓存,如果子集 A 的访问时延比子集 B 的长,则收到的隐蔽信息为比特 1,反之则为 0.基于这种方法,该作者设计了 BP、SAP 和 TCTP 信道,并分别在 Linux、Xen 和 Fiasco.OC 这 3 种操作系统中予以实现.同时,还利用 HLPN(high-level petri nets)对 3 个信道进行建模,预估 3 个信道的传输速率.

(2) 共享组件访问时延(本地)

此类隐蔽信道与网络共享组件时间隐蔽信道类似,但主要利用本地系统中的组件作为隐蔽信息的载体,例如,共享存储区域、总线和分支预测器(branch predictor,简称 BP)等程序之间所共享的硬件或软件资源.发送方通常会利用这些组件的访问时延的长短编码隐蔽信息.

Evtyushkin 等人[79]借助处理器分支预测器在两个恶意进程之间构建隐蔽信道.当进程的某一分支跳转地址在分支预测器中“命中”时,此地址的跳转时间要小于“不命中”的时间,因此可以根据跳转时间编码隐蔽信息.两个恶意进程事先商定好一个分支跳转地址 address.当发送比特 0 时,发送方重复执行不含有 address 的代码,使得 BP 中不含有 address,使得接收方含有 address 的代码的执行时间变长,成功接收比特 0.反之,则为 1.Evtyushkin 等人[31]还利用 Intel CPU 处理器(基于 Skylake 架构)中的随机数生成器(random number generation,简称 RNG)作为隐蔽信息载体.该信道通过操纵一段时间内 rdseed 指令的执行次数,控制 CB(conditioner buffer)中随机数的数量,造成 CB 的资源竞争.其中,CB 资源耗尽时称为高竞争态,表示比特 1;反之,则称为低竞争态,表示比特 0.该信道采用 Simultaneous Scheduling Intervals 作为同步机制,并使用 RS(Reed-Solomon)纠错码保证信道的可靠性.

2.2.3 时间隐蔽信道分析和归纳

如表 2 所示,本节对近 5 年来和时间隐蔽信道紧密相关的重要研究工作进行分析和总结.与存储隐蔽信道不同,时间隐蔽信道会制造资源竞争,导致缓存等共享资源的访问时延发生变化发送隐蔽信息,接收方通过感知这些变化解码信息.因此,一般会采取消除竞争的方式使接收方难以区别不同的访问时延,或者采取添加时延、

添加噪音等方式降低信道的准确率,通过传输速率和准确率度量时间隐蔽信道的威胁.由表 2 可知,近 5 年的研究工作主要以基于缓存和 IPD 的时间信道为主.在本地信道中,研究者也利用 RNG、BP 等常见共享组件传递隐蔽信息.时间隐蔽信道抗检测能力强,通过添加噪音和时延的方法可以限制此类信道的威胁.

Table 2 Summary of key covert timing channels in recent five years

表 2 近 5 年关键时间隐蔽信道总结

隐蔽信道名称	发送方	接收方	共享资源	编码机制	同步机制	评价指标	限制方法
Deduplication-Based CC[76]	PC	PC	共享文件	共享文件的不同组合	预定义共享文件	传输速率	隐蔽信道审计
Packet reordering CC[35]	客户端	服务器	数据包	更改数据包顺序;纠错码	传输约定数据包	传输速率;准确率	添加噪音
PRIME+PROBE[72]	虚拟机	虚拟机	缓存	访问时延长/短	并发执行	传输速率;准确率	消除竞争;添加时延
Sneak-Peek[33]	PC	PC	数据包到达的时间	更改包到达时间;纠错码	固定时间 T	传输速率;准确率	添加噪音;添加时延
Random number generation CC[31]	程序	程序	随机数生成器	RNG 竞争/空闲态;纠错码	保证双方同步运行	传输速率;准确率	消除竞争
BP;TCTP;SAP[11]	程序	程序	L_2 缓存	访问时延长/短	共享资源状态	传输速率;准确率	消除竞争;添加时延
Data center CC[77]	客户端 PC	服务器	检索(查询请求)时间	检索时间长/短	服务器的同步信息	传输速率;准确率	消除竞争
Spy in the sandbox[73]	浏览器	服务器	L_3 缓存	访问时延长/短	–	传输速率	更改地址映射方式
Timing-based memory bus[12]	虚拟机	虚拟机	内存总线	总线竞争/空闲态;纠错码	曼彻斯特码	传输速率;准确率	添加噪音;消除竞争
GPGPU CC[78]	程序	程序	L_1 和 L_2 缓存	访问时延长/短	同步执行	传输速率	消除竞争;添加时延
Branch predictors CC[79]	程序	程序	分支预测器	分支执行时间长/短	同步执行	传输速率	控制预测器访问权限
NUMA-based CC[74]	程序	程序	Last level 缓存(LLC)	访问时延	–	传输速率;准确率	添加噪音;添加时延
Cross processor cache CC[75]	程序	程序	缓存与 DRAM	访问时延	预定义文本	准确率	添加噪音;添加时延
Open-source CC[68]	PC	PC	IPD	IPD 长短	曼彻斯特码;纠错码	准确率	添加噪音;添加时延
Skype traffic[66]	PC	PC	IPD	多重 IPD 的长短;喷泉码	通信软件保证同步	传输速率;准确率	添加噪音;添加时延

2.3 混合隐蔽信道

混合隐蔽信道是存储隐蔽信道和时间隐蔽信道相结合而产生的隐蔽通信技术.与存储隐蔽信道或时间隐蔽信道相比,此类隐蔽信道在共享资源的内容和时间特性中都嵌入了隐蔽信息,提升了信道容量,仅仅检测共享资源的某一个方面,在大多数情况下是无法发现全部隐蔽信息的,从而提高了信道的抗检测能力[6].

Wu 等人[80]在 Android 手机和服务器之间构建了双向通信的 biTheft 隐蔽信道,使用 URL 内容和 IPD 作为共享资源.biTheft 收集和分析手机中未受保护的用户隐私信息,然后将这些信息直接嵌入到 URL 请求中并发送到服务器.根据收到的内容,服务器将相应指令嵌入到 IPD 中并返回至手机,用以进一步收集用户的信息.Mazurczyk 等人[81]将隐蔽信息嵌入到实时传输协议中,利用公开信道中的 VoIP(voice-over-IP)[82]传输信息.发送方延迟发送含有隐蔽信息的数据包以增大 IPD.公开信道接收方会自动丢弃延迟数据包,而处于同侧的隐蔽信道接收方可以识别并提取这些数据包中的隐蔽信息.该信道为延迟数据包的数量设定了一个阈值以保证抗检测性,但却限制了传输速率.Zhao 等人[83]基于类似的技术提出了以 MPEG 4 数据流为隐蔽信息载体的信道.

Tahmasbi 等人[15]基于 EMD(exploiting modification direction)方法和 802.11 DCF 协议提出了一种构建 CB(code-based)信道的方法.DCF 协议通过监听信道内的通信状态检测信道是否繁忙,调节数据包的发送间隔避免发生碰撞.CB 通过调制此间隔编码一部分隐蔽信息,并将剩余信息通过 EMD 技术直接嵌入待传输的 JPEG 图

像中.相比于 DCF 隐蔽信道[15],CB 信道的容量有明显的提升.

本节对近 5 年混合隐蔽信道的关键研究进行分析和总结,见表 3.与前两类隐蔽信道不同,此类信道通常含有多种编码机制,以适应不同的隐蔽信息载体.同时,混合隐蔽信道将共享资源的数值和时间特性的优势相结合,使得隐蔽信道的传输速率和隐蔽性都有较为可观的提升.

Table 3 Summary of key covert hybrid channels in recent five years

表 3 近 5 年关键混合隐蔽信道总结

隐蔽信道名称	发送方	接收方	共享变量	编码机制	同步机制	评价指标	限制方法
biTheft[80]	手机浏览器(CSC)	服务器(CTC)	HTTP URL; IPD	URL 内容; IPD 长/短	–	–	TN; 添加时延
Code-based CC[15]	PC	PC	JPEG; IPD	图片内容; IPD 长/短	接收方持续监听	传输速率; 准确率	添加噪音; 添加时延

2.4 行为隐蔽信道

行为隐蔽信道主要借助共享资源的状态、表现和事件等行为特征编码隐蔽信息.共享资源通常是计算机系统、网络或通信中的事件、现象和特性,能够被控制、修改和感知.隐蔽信息潜伏于共享变量的状态转换和行为变化之中,提高了信道的隐蔽性.

Kohls 等人[84]借助 VoIP 中通常会含有噪音这一现象,利用 DSSS(direct-sequence spread spectrum)技术设计了 SkypeLine 隐蔽信道.SkypeLine 利用语音信号作为隐蔽信息的载体,将比特 0 和比特 1 映射至不同长度、不同内容的噪音序列,然后调制噪音序列与输入的语音,控制序列的熵和长度,最后通过 VoIP 传输给信道接收方.SkypeLine 使用 RS 和 GC(Golay codes)作为纠错码,并利用 VSD(virtual sound device)作为调制模块和输入语音之间的接口,SkypeLine 可以部署在任意的 VoIP 客户端.Hovhannisyan 等人[85]认为,现有基于 IPD 的时间隐蔽信道传输率低下且抗检测性低,因此提出了基于路由器的行为隐蔽信道.发送方通过控制数据包在传输过程中所经过的路由器编码隐蔽信息.接收方根据数据包达到的顺序及路由器编号解码信息,例如,从 Route0 收到的数据包表示比特 0.信道针对 TCP 和 UDP 数据包分别设计了相应的同步机制,确保隐蔽通信的正确率.

Tuptuk 等人[54]采用 Orisen 设备的信号作为隐蔽信息的载体,通过 RSSI(received signal strength indication)感知和量化信号的强弱程度.信道发送方通过调制数据包的发射功率编码隐蔽信息,利用约定好的 16 比特前导码(preamble)表示隐蔽信息传输的开始.该信道使用 Hamming Code 保证传输正确率.Ambrosin 等人[86]借助命名数据网络中短暂消息的有效状态编码隐蔽信息,该短暂消息在存活期内是有效的.该信道工作原理如下:发送方请求一个类型为短暂消息的内容包 C;该请求被系统响应,内容包 C 会被存储在缓存或 PIT(pending interest table)中;然后,接收方同样请求内容包 C,若 C 处于有效状态,认为收到比特 1;如果 C 已失效,则认为收到比特 0.

Shen 等人[16]利用浏览器对 HTTP 协议的响应行为构建隐蔽信道 LiHB.浏览器每次访问时会发送 N 个 HTTP 请求,并根据调度算法将 N 个请求分配到 M 个 HTTP 流中.LiHB 的发送方位于浏览器端,通过控制调度算法调节每个 HTTP 流中所包含的请求,并借此编码隐蔽信息.接收方在网关处解码隐蔽信息.双方通过 TCP 的 3 次握手协议进行同步.Shen 等人[87]对 LiHB 信道进行改进,提出 HBCC(HTTP behavior-based covert channel),克服了 LiHB 重复访问相同网页的缺点,利用 FTS(frequent traversal sequence)提升了信道容量和抗检测性.

Mohamed 等人[88]提出的 PSCAN 信道是基于端口开关的行为隐蔽信道.发送方利用给定主机中一系列端口的开关状态编码隐蔽信息,其中,“开”状态的端口表示比特 1,“关”状态的端口表示比特 0.接收方会向目标主机端口发送请求并等待响应,根据响应内容决定端口的状态,从而解码隐蔽信息.Qi 等人[17]发现,用户在玩手机游戏时的一些特定行为和动作会改变传感器的数值或状态,进而利用这些不同的行为编码隐蔽信息.

表 4 分析和归纳了近 5 年关键的行为隐蔽信道研究工作.行为信道的信息传输基于共享资源的变化,因此需要接收方较为频繁地监测共享资源才能成功地解码隐蔽信息,或者是根据编码机制提取共享资源的特定属性值.此类隐蔽信道的传输速率相较于前 3 类信道较低,通过规范化共享变量的行为或者人为地向信道中添加噪音等方法可以降低信道容量,能够有效地降低信道威胁.但是近 5 年,行为隐蔽信道利用互联网中或计算机系

统中的常见且正常的现象作为隐蔽信息的载体,此类通信行为很难引起监察者的注意,即使被发现,也很难区分是正常行为还是隐蔽通信行为,因此,此类信道的抗检测性较高.

Table 4 Summary of key covert behavior channels in recent five years

表 4 近 5 年关键行为隐蔽信道总结

隐蔽信道名称	发送方	接收方	共享变量	编码机制	同步机制	评价指标	限制方法
IP-timing CC[85]	程序	程序	路由器编号	更改路由器编号	预定义数据包顺序	传输速率;准确率	添加噪音;添加时延
RSSI/LQI CC[54]	Orisen 设备	Eve 接收器	接收信号	更改接收信号强度	预定义前导码	传输速率;准确率	添加噪音
LiHB[16]	PC	网关	http 流和数据对象	更改 http 流中的对象数	TCP 协议保证同步	传输速率;准确率	规范化浏览器行为
PSCAN[88]	程序	程序	网络端口	更改端口开/关状态	预先通信	传输速率;准确率	添加噪音
SkypeLine[84]	程序	程序	网络电话的 IP 数据包	更改噪音序列;纠错码	预定义噪音序列	传输速率;准确率	TN
User-behavior CC[17]	手机	互联网	用户行为	更改传感器状态/内容	预定义用户行为	传输速率;准确率	添加噪音;
Ephemeral messages CC[86]	程序	程序	短暂消息	更改消息的有效状态	用 NTP 服务器同步	准确率	添加噪音;
HBCC[87]	PC	网关	http 流和数据对象	更改 http 流内容;FTS	TCP 协议保证同步	传输速率;准确率	规范化浏览器行为

2.5 气隙隐蔽信道

气隙隐蔽信道针对网络上或空间上完全隔绝的发送方和接收方,通过电磁、声、热或光等信号编码隐蔽信息.例如,相邻两台机器的散热情况,这种热信号可以被内置的热传感器所感知.

Guri 等人[89]设计了 VisiSploit 气隙隐蔽信道,从网络上完全隔离的计算机中窃取机密数据.VisiSploit 会首先收集系统中的机密信息,然后将该信息嵌入对比度很低的图像或快速闪烁的图像里,并投影到计算机屏幕上.由于人类视觉的感知局限性,监察者无法发现隐蔽信息的存在,而该信息却可以被照相机所识别和接收.Guri 等人[18]还通过热信号在两台空间相邻的但网络隔离的计算机之间构建了 BitWhisper 气隙隐蔽信道.BitWhisper 利用机器的热排放控制周围环境的温度,利用温度的差异表示不同的隐蔽信息.接收方则通过自身内置的热传感器获取环境温度并解码隐蔽信息.BitWhispe 在预先定义好的时间周期内进行通信同步工作,其传输速率最高能达到每秒 8 比特.Masti 等人[90]借助温度传感器打破了多核平台的隔离性.该信道发送比特 1 时会执行 RSA 破解算法,产生大量的 CPU 密集型任务,使得温度传感器的测量值升高;发送比特 0 时,信道则保持静默,令温度传感器的测量值变低.该信道利用固定的前导码作为同步机制.

表 5 归纳了近 5 年的气隙隐蔽信道的关键研究工作,可以看出:气隙隐蔽信道的威胁限制方法与编码机制紧密相连,大多都是有针对性的防御方法,缺乏类似时间隐蔽信道的通用防御方法.并且,此类信道旨在打破系统间的空间或网络隔离性,因而信道容量与其他类型信道相比较低.

Table 5 Summary of key air-gap channels in recent five years

表 5 近 5 年关键气隙隐蔽信道总结

隐蔽信道名称	发送方	接收方	共享变量	编码机制	同步机制	评价指标	限制方法
VisiSploit[89]	计算机 LCD 屏幕	人/照相机	图片	图片颜色和播放速度	人为同步	–	实时扫描可疑行为
BitWhisper[18]	PC	PC	热信号	更改周围环境温度	预定义热信号序列	传输速率	实时监测温度变化
Thermal covert channels[90]	程序	程序	温度传感器	处理器温度高/低	预定义热信号序列	传输速率;准确率	传感器的访问控制

3 面向隐蔽信道类型的威胁限制技术

隐蔽信道限制是一项具有挑战性的工作[7,10],其目的主要是使隐蔽信道的传输速率、正确率或者隐蔽性降低到一个可接受的范围之内.由于大量的隐蔽信道构建技术的存在,在实际中很难设计一种能有效限制所有隐蔽信道威胁的方法.一些研究可以限制部分隐蔽信道的威胁,例如基于缓存的信道和基于共享变量的信道等.另一些研究只注重于隐蔽信道的检测,例如,KS(Kolmogorov-Smirnov)和 KL(Kullback Leibler)时间隐蔽信道检测方法.现有限制方法大多都是针对应用场景中某一具体隐蔽信道而提出的,缺乏通用性.而本文所提出的隐蔽信道分类方法根据共享变量的使用方式将具有共性的信道归为一类,使得设计针对一类隐蔽信道的(而非单一隐蔽信道)、通用的限制方法成为可能.下面基于前文所提及的隐蔽信道分类工作,从通用化的角度对各类隐蔽信道的威胁限制方法进行讨论,见表 6.

Table 6 Covert channel restriction methods based on the channel categorization

表 6 面向隐蔽信道类型的威胁限制策略

隐蔽信道类型		限制策略
存储隐蔽信道	网络	TN 方法;添加噪音
	本地	添加噪音
时间隐蔽信道	网络	添加时延
	本地	添加噪音;添加时延
混合隐蔽信道		TN 方法;添加噪音;添加时延
行为隐蔽信道		类似 TN 方法;规范化通信行为
气隙隐蔽信道		隔离发送方和接收方

(1) 存储隐蔽信道和时间隐蔽信道.

网络存储隐蔽信道主要利用协议中字段的各种属性传递隐蔽信息.TN 方法能够有效地规范化各类协议中的字段,达到近乎消除隐蔽信息载体的目的,通过添加噪音的方法也能有效降低此类信道的传输速率.而对于本地存储隐蔽信道而言,其准确性依赖于共享变量或共享组件的可靠性.利用添加噪音的方式随机修改共享变量(组件)的数值可以降低其可靠性,从而有效地降低信道的准确率.网络时间隐蔽信道以 IPD 或者访问非本地系统中缓存和共享组件的时延作为隐蔽信息的载体,通过添加时延的方式,可以更改 IPD 或访问时延的长短,从而降低信道接收方解码隐蔽信息的准确率.基于缓存和共享组件的本地时间隐蔽信道主要借助访问时延编码隐蔽信息,也可利用添加噪音和添加时延的方式降低信道的威胁程度.值得注意的是:在前文所归纳的本地和网络时间隐蔽信道中,共享组件信道通常利用组件本身在竞争态和空闲态的访问时延不同来编码隐蔽信息,因而消除竞争是降低此类信道威胁的另一有效方法.

(2) 3 种新型隐蔽信道.

混合隐蔽信道是存储隐蔽信道和时间隐蔽信道的融合产物,因此需要同时考虑两类信道的共享资源特性,结合 TN 方法、添加噪音和添加时延等方法限制信道威胁.相比于存储隐蔽信道,行为隐蔽信道更为侧重隐蔽性,但其信道容量通常较低.针对这个特性,利用添加噪音的方法可以将此类信道的容量限制到很低的地步,大大降低了信道的可用性.其中,部分信道会利用未明确规范的共享资源或者正常通信中的某些行为编码隐蔽信息,例如,浏览器调度 HTTP 请求.因此类比 TN 方法,明确并规范化这些行为也是限制信道威胁的方法之一.气隙隐蔽信道的目的主要在于打破空间上的隔离性,其隐蔽性较高.通过计算机技术防御此类信道的可行性较低[89].例如,基于热信号的信道要求发送方和接收方之间的距离很近才能相互感知温度,从而解码信息.因此在物理(空间)上隔离发送和接收双方,可以很容易地限制此类信道威胁.VisiSploit 信道构建的前提是接收方有权访问存有机密信息的机器,因此通过隔离双方或者适当的访问控制策略即可消除威胁.

4 挑战性问题和未来研究方向

隐蔽信道研究已经取得了众多的进展.从攻击者的角度来看,作为一种隐蔽通信的手段,由于共享资源的使用方式以及信道的具体应用场景不同,隐蔽信道很难同时具有很高的传输速率、正确率和抗检测性;从防御者

的角度来看,随着大量新型的隐蔽技术的不断提出,设计通用的、有效的隐蔽信道限制方法成为了研究的重点.因此,该领域仍然存在许多亟待解决的挑战性问题和未来的研究方向.

(1) 网络存储隐蔽信道的信道容量较高,但是抗检测性能力和对不同协议的适应性较差,可以利用通信量规范化消除或降低此类信道的威胁,例如,删除协议头部元素中的未使用位或者规范化头部元素的格式、顺序和长度等.因此,更有效地选取协议和数据包中的字段作为隐蔽信息的载体的方法,以及提升此类信道的抗检测能力和适应性,是值得关注的研究方向;

(2) 气隙隐蔽信道的信道容量普遍较低,尤其是基于热信号的隐蔽信道.目前研究的重点在于打破信道发送方和接收方之间的隔离性,忽略了信道容量,因而此类信道传输隐蔽信息的速率较低.关于选取合适的共享资源和编码机制用以提升气隙信道的传输速率是未来一个可能的研究方向,值得深入研究;

(3) 利用添加干扰和添加时延的方法可以限制网络时间隐蔽信道的威胁.此限制方法的思想源于 Pump 限制技术[37]及后续发展的相关技术[36,38].在含有干扰和噪音等信道限制机制的环境下,保证隐蔽信道的传输速率和传输质量的技术还有待探索;

(4) 隐蔽信道限制技术的目的是限制信道容量或传输正确率等方面.由于存在大量不同类型的隐蔽信道构建技术,现有的限制技术缺乏通用性,很难适用于所有隐蔽信道.在拓展隐蔽信道限制技术的通用性这一方面,基于模型的方法[11]和基于 PLML(pattern language markup language)语言[10]的方法值得借鉴;

(5) 基于 IPD 的时间隐蔽信道通过模拟正常通信中的 IPD 分布以提高信道的隐蔽性.但是目前已有很多检测方法,例如,熵检测、KS 检测和 KL 检测等.现有的 IPD 隐蔽信道只能避免被其中某一种或某几种方法所检测.针对现有检测方法,设计更好的 IPD 分布模式及信道编码机制,避免信道自身的存在被发现,是增强此类隐蔽信道抗检测性工作所面临的挑战.

5 总 结

目前,基于隐蔽信道机制的隐蔽通信技术对信息安全造成了威胁,但是隐蔽通信技术本身并没有恶意和善意之分,而是取决于具体的应用场景.针对恶意的隐蔽通信场景,就需要设计有效的信道威胁限制技术,而信道分类可以为威胁限制提供关键依据.本文对近年来的隐蔽信道研究工作进行了详细的综述和归纳.通过囚犯模型介绍了隐蔽信道的发展起源,简述了发展历史.提出并讨论了发送方、接收方、共享资源、同步机制和编码机制这 5 个构成隐蔽信道的关键要素.本文论述了隐蔽信道的威胁,根据安全标准和目前研究工作总结了隐蔽信道分析所包含的 4 个内容.本文主要关注于近 5 年隐蔽信道的关键研究工作,将隐蔽信道分为存储隐蔽信道、时间隐蔽信道、混合隐蔽信道、行为隐蔽信道和气隙隐蔽信道这 5 类,并对每个类别进行了详细的讨论和分析,归纳了各个信道的威胁限制方法.同时,分类工作可以为后续信道威胁限制工作提供参考和研究思路.最后,本文基于现有研究工作对隐蔽信道存在的问题和未来可能的研究方向做出预测和展望.总之,隐蔽信道技术仍然存在许多关键问题需要深入地讨论和细致地研究.

References:

[1] Chen K. Roles and limitations of cryptographic techniques in information security. Journal of China Institute of Communications, 2001,22(8):93−99 (in Chinese with English abstract).

[2] Fedorov AK, Kiktenko EO, Lvovsky AI. Quantum computers put blockchain security at risk. Nature, 2018,563:465−467.

[3] Petitcolas FAP, Anderson RJ, Kuhn MG. Information hiding-a survey. Proc. of the IEEE, 1999,87(7):1062−1078.

[4] Lampson BW. A note on the confinement problem. Communications of the ACM, 1973,16(10):613−615.

[5] Biswas AK, Ghosal D, Nagaraja S. A survey of timing channels and countermeasures. ACM Computing Surveys, 2017,50(1):1−39.

[6] Wang C, Zhang CY, Bin W, YuAn T, Wang YJ. A novel anti-detection criterion for covert storage channel threat estimation. SCIENTIA SINICA Informationis, 2018,61(4):048101:1−048101:3.

[7] Wang YJ, Wu JZ, Zeng HT, Ding LP, Liao XF. Covert channel research. Ruan Jian Xue Bao/Journal of Software, 2010,21(9): 2262−2288 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3880.htm [doi: 10.3724/SP.J.1001.2010.03880]

[8] Wu JZ, Ding LP, Wu Y, Min-Allah N, Khan SU, Wang YJ. C2detector: A covert channel detection framework in cloud computing. Security and Communication Networks, 2014,7(3):544−557.

[9] Zander S, Armitage G, Branch P. A survey of covert channels and countermeasures in computer network protocols. IEEE Communications Surveys Tutorials, 2007,9(3):44−57.

[10] Wendzel S, Zander S, Fechner B, Herdin C. Pattern-based survey and categorization of network covert channel techniques. ACM Computing Surveys, 2015,47(3):50:1−50:26.

[11] Lin YQ, Malik SUR, Bilal K, Yang Q, Wang YJ, Khan SU. Designing and modeling of covert channels in operating systems. IEEE Trans. on Computers, 2016,65(6):1706−1719.

[12] Wu Z, Xu Z, Wang H. Whispers in the hyper-space: High-bandwidth and reliable covert channel attacks inside the cloud. IEEE/ACM Trans. on Networking, 2015,23(2):603−615.

[13] Luo Y, Luo W, Sun X, Shen Q, Ruan A, Wu Z. Whispers between the containers: High-capacity covert channel attacks in Docker. In: Proc. of the 2016 IEEE Trustcom/BigDataSE/ISPA. 2016. 630−637.

[14] Kadloor S, Kiyavash N, Venkitasubramaniam P. Mitigating timing side channel in shared schedulers. IEEE/ACM Trans. on Networking, 2016,24(3):1562−1573.

[15] Tahmasbi F, Moghim N, Mahdavi M. Code-based timing covert channel in IEEE 802.11. In: Proc. of the 5th Int'l Conf. on Computer and Knowledge Engineering (ICCKE). IEEE, 2015. 12−17.

[16] Shen Y, Huang L, Wang F, Lu X, Yang W, Li L. LiHB: Lost in HTTP behaviors—A behavior-based covert channel in HTTP. In: Proc. of the 3rd ACM Workshop on Information Hiding and Multimedia Security. New York: ACM Press, 2015. 55−64.

[17] Qi W, Ding W, Wang X, Jiang Y, Xu Y, Wang J, Lu K. Construction and mitigation of user-behavior-based covert channels on smartphones. IEEE Trans. on Mobile Computing, 2018,17(1):44−57.

[18] Guri M, Monitz M, Mirski Y, Elovici Y. Bitwhisper: Covert signaling channel between air-gapped computers using thermal manipulations. In: Proc. of the 28th IEEE Computer Security Foundations Symp. Washington: IEEE Computer Society, 2015. 276−289.

[19] Wu P, Liu K, Zheng K, Ding Z, Tan Y. A road network modeling method for map matching on lightweight mobile devices. Distributed and Parallel Databases, 2015,33(2):145−164.

[20] Zhiyong C, Yong Z. Entropy based taxonomy of network convert channels. In: Proc. of the 2nd Int'l Conf. on Power Electronics and Intelligent Transportation System (PEITS). Piscataway: IEEE, 2009. 451−455.

[21] Simmons GJ. The prisoners' problem and the subliminal channel. In: Proc. of the Advances in Cryptology. New York: Spinger-Verlag, 1984. 51−67.

[22] Liu Y, Zhong ZM. Design and implementation of network covert channel based on multi−protocol. Modern Electronics Technique, 2017,40(8):19−21, 24 (in Chinese with English abstract).

[23] Dong LP, Yuan CX, Jie YY, Wang S. Implementation and detection of network covert channel. Computer Science, 2015,42(7): 216−221(in Chinese with English abstract).

[24] Craver S. On public-key steganography in the presence of an active warden. In: Proc. of the Int'l Workshop on Information Hiding. Berlin, Heidelberg: Springer-Verlag, 1998. 355−368.

[25] Millen J. 20 years of covert channel modeling and analysis. In: Proc. of the '99 IEEE Symp. on Security and Privacy (Cat. No.99CB36344). Piscataway: IEEE, 1999. 113−114.

[26] Yan M, Shalabi Y, Torrellas J. ReplayConfusion: Detecting cache-based covert channel attacks using record and replay. In: Proc. of the 49th Annual IEEE/ACM Int'l Symp. on Microarchitecture (MICRO). IEEE, 2016. 1−14.

[27] Denning DE. A lattice model of secure information flow. Communications of the ACM, 1976,19(5):236−243.

[28] Tsai CR, Gligor VD, Chandersekaran CS. A formal method for the identification of covert storage channels in source code. In: Proc. of the '87 IEEE Symp. on Security and Privacy. Piscataway: IEEE, 1987. 74.

[29] Shrestha PL, Hempel M, Rezaei F, Sharif H. A support vector machine-based framework for detection of covert timing channels. IEEE Trans. on Dependable and Secure Computing, 2016,13(2):274−283.

[30] Lin Y, Ding L, Wu J, Xie Y, Wang Y. Robust and efficient covert channel communications in operating systems: Design, implementation and evaluation. In: Proc. of the 7th IEEE Int'l Conf. on Software Security and Reliability Companion. Washington: IEEE, 2013. 45−52.

[31] Evtyushkin D, Ponomarev D. Covert channels through random number generator: Mechanisms, capacity estimation and mitigations. In: Proc. of the 2016 ACM SIGSAC Conf. on Computer and Communications Security. New York: ACM Press, 2016. 843−857.

[32] Zhang D, Askarov A, Myers AC. Predictive mitigation of timing channels in interactive systems. In: Proc. of the 18th ACM Conf. on Computer and Communications Security. New York: ACM Press, 2011. 563−574.

[33] Tahir R, Khan MT, Gong X, Ahmed A, Ghassami A, Kazmi H, Caesar M, Zaffar F, Kiyavash N. Sneak-Peek: High speed covert channels in data center networks. In: Proc. of the 35th Annual IEEE Int'l Conf. on Computer Communications. Piscataway: IEEE, 2016. 1–9.

[34] Gray JW. On introducing noise into the bus-contention channel. In: Proc. of the '93 IEEE Computer Society Symp. on Research in Security and Privacy. Washington, 1993. 90–98.

[35] El-Atawy A, Duan Q, Al-Shaer E. A novel class of robust covert channels using out-of-order packets. IEEE Trans. on Dependable and Secure Computing, 2017,14(2):116–129.

[36] Wu J, Ding L, Lin Y, Min-Allah N, Wang Y. XenPump: A new method to mitigate timing channel in cloud computing. In: Proc. of the 5th IEEE Int'l Conf. on Cloud Computing. Washington: IEEE Computer Society, 2012. 678–685.

[37] Kang MH, Moskowitz IS. A pump for rapid, reliable, secure communication. In: Proc. of the 1st ACM Conf. on Computer and Communications Security. New York: ACM Press, 1993. 119–129.

[38] Kang MH, Moskowitz IS, Lee DC. A network pump. IEEE Trans. on Software Engineering, 1996,22(5):329–338.

[39] Konoplev AS, Busygin AG. Steganographic methods of communications in distributed computing networks. In: Proc. of the 8th Int'l Conf. on Security of Information and Networks. New York: ACM Press, 2015. 131–134.

[40] Epishkina A, Kogos K. Protection from binary and multi-symbol packet length covert channels. In: Proc. of the 8th Int'l Conf. on Security of Information and Networks. New York: ACM Press, 2015. 196–202.

[41] Girling CG. Covert channels in LAN's. IEEE Trans. on Software Engineering, 1987,13(2):292–296.

[42] Lucena NB, Lewandowski G, Chapin SJ. Covert channels in IPv6. In: Proc. of the 5th Int'l Conf. on Privacy Enhancing Technologies. Berlin, Heidelberg: Springer-Verlag, 2006. 147–166.

[43] Rios R, Onieva JA, Lopez J. HIDE_DHCP: Covert communications through network configuration messages. In: Proc. of the IFIP Int'l Information Security Conf. Berlin, Heidelberg: Springer-Verlag, 2012. 162–173.

[44] Schulz S, Varadharajan V, Sadeghi AR. The silence of the LANs: Efficient leakage resilience for IPsec VPNs. IEEE Trans. on Information Forensics and Security, 2014,9(2):221–232.

[45] Mazurczyk W, Szczypiorski K. Evaluation of steganographic methods for oversized IP packets. Telecommunication Systems, 2012,49(2):207–217.

[46] Murdoch SJ, Lewis S. Embedding covert channels into TCP/IP. In: Proc. of the 7th Int'l Conf. on Information Hiding. Berlin, Heidelberg: Springer-Verlag, 2005. 247–261.

[47] Wolf M. Covert channels in LAN protocols. In: Proc. of the Workshop for European Institute for System Security on Local Area Network Security. London: Springer-Verlag, 1989. 91–101.

[48] Zou XG, Li Q, Sun SH, Niu X. The research on information hiding based on command sequence of FTP protocol. In: Proc. of the 9th Int'l Conf. on Knowledge-Based Intelligent Information and Engineering Systems. Berlin, Heidelberg: Springer-Verlag, 2005. 1079–1085.

[49] Muchene DN, Luli K, Shue CA. Reporting insider threats via covert channels. In: Proc. of the 2013 IEEE Security and Privacy Workshops. Washington: IEEE Computer Society, 2013. 68–71.

[50] Classen J, Schulz M, Hollick M. Practical covert channels for WiFi systems. In: Proc. of the 2015 IEEE Conf. on Communications and Network Security (CNS). Piscataway: IEEE, 2015. 209–217.

[51] Hijaz Z, Frost VS. Exploiting OFDM systems for covert communication. In: Proc. of the 2010 Military Communications Conf. IEEE, 2010. 2149–2155.

[52] Grabski S, Szczypiorski K. Steganography in OFDM symbols of fast IEEE 802.11n networks. In: Proc. of the 2013 IEEE Security and Privacy Workshops. Washington: IEEE Computer Society, 2013. 158–164.

[53] Vines P, Kohno T. Rook: Using video games as a low-bandwidth censorship resistant communication platform. In: Proc. of the 14th ACM Workshop on Privacy in the Electronic Society. New York: ACM Press, 2015. 75–84.

[54] Tuptuk N, Hailes S. Covert channel attacks in pervasive computing. In: Proc. of the 2015 IEEE Int'l Conf. on Pervasive Computing and Communications (PerCom). IEEE, 2015. 236–242.

[55] Wendzel S, Kahler B, Rist T. Covert channels and their prevention in building automation protocols: A prototype exemplified using BACnet. In: Proc. of the 2012 IEEE Int'l Conf. on Green Computing and Communications. Washington: IEEE Computer Society, 2012. 731–736.

[56] Lu X, Huang L, Yang W, Shen Y. Concealed in the internet: A novel covert channel with normal traffic imitating. In: Proc. of the 2016 Int'l IEEE Conf. on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress. IEEE, 2016. 285–292.

[57] Daneault G, Johnson D. Client-initiated HTTP covert channels using relays. In: Proc. of the 4th Int'l Symp. on Digital Forensic and Security (ISDFS). IEEE, 2016. 32−37.

[58] Ameri A, Johnson D. Covert channel over network time protocol. In: Proc. of the 2017 Int'l Conf. on Cryptography, Security and Privacy. New York: ACM Press, 2017. 62−65.

[59] Johnson M, Lutz P, Johnson D. Covert channel using man-in-the-middle over HTTPS. In: Proc. of the 2016 Int'l Conf. on Computational Science and Computational Intelligence (CSCI). IEEE, 2016. 917−922.

[60] Khader M, Hadi A, Hudaib A. Covert communication using port knocking. In: Proc. of the 2016 Cybersecurity and Cyberforensics Conf. (CCC). IEEE, 2016. 22−27.

[61] Rezaei F, Hempel M, Dongming P, Yi Q, Sharif H. Analysis and evaluation of covert channels over LTE advanced. In: Proc. of the 2013 IEEE Wireless Communications and Networking Conf. (WCNC). IEEE, 2013. 1903−1908.

[62] Fern N, San I, Koç ÇK, Cheng KTT. Hiding hardware trojan communication channels in partially specified SoC bus functionality. IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems, 2017,36:1435−1444.

[63] Chun JY, Lee HL, Yoon JW. Passing go with DNA sequencing: Delivering messages in a covert transgenic channel. In: Proc. of the 2015 IEEE Security and Privacy Workshops. Washington: IEEE Computer Society, 2015. 17−26.

[64] Hussein O, Hamza N, Hefny H. A proposed covert channel based on memory reclamation. In: Proc. of the 7th IEEE Int'l Conf. on Intelligent Computing and Information Systems (ICICIS). Piscataway: IEEE, 2015. 343−347.

[65] Ainapure BS, Shah D, Rao AA. Understanding Perception of Cache-based Side-channel Attack on Cloud Environment. Singspore: Spinger-Verlag, 2018. 9−21.

[66] Archibald R, Ghosal D. Design and analysis of a model-based covert timing channel for skype traffic. In: Proc. of the 2015 IEEE Conf. on Communications and Network Security (CNS). IEEE, 2015. 236−244.

[67] Liu W, Liu G, Zhai J, Dai Y, Ghosal D. Designing analog fountain timing channels: Undetectability, robustness, and model-adaptation. IEEE Trans. on Information Forensics and Security, 2016,11:677−690.

[68] Liguori A, Benedetto F, Giunta G, Kopal N, Wacker A. Analysis and monitoring of hidden TCP traffic based on an open-source covert timing channel. In: Proc. of the 2015 IEEE Conf. on Communications and Network Security (CNS). IEEE, 2015. 667−674.

[69] Handel TG, Maxwell T, Sandford I. Hiding data in the OSI network model. In: Proc. of the 1st Int'l Workshop on Information Hiding. Berlin, Heidelberg: Springer-Verlag, 1996. 23−38.

[70] El-Atawy A, Al-Shaer E. Building covert channels over the packet reordering phenomenon. In: Proc. of the IEEE INFOCOM 2009. 2009. 2186−2194.

[71] Herzberg A, Shulman H. Limiting MitM to MitE covert-channels. In: Proc. of the 2013 Int'l Conf. on Availability, Reliability and Security. Washington: IEEE Computer Society, 2013. 236−241.

[72] Liu F, Yarom Y, Ge Q, Heiser G, Lee RB. Last-level cache side-channel attacks are practical. In: Proc. of the 2015 IEEE Symp. on Security and Privacy. Washington: IEEE Computer Society, 2015. 605−622.

[73] Oren Y, Kemerlis VP, Sethumadhavan S, Keromytis AD. The spy in the sandbox: Practical cache attacks in Javascript and their implications. In: Proc. of the 22nd ACM SIGSAC Conf. on Computer and Communications Security. New York: ACM Press, 2015. 1406−1418.

[74] Yao F, Venkataramani G, Doroslova M. Covert timing channels exploiting non-uniform memory access based architectures. In: Proc. of the Great Lakes Symp. on VLSI 2017. New York: ACM Press, 2017. 155−160.

[75] Irazoqui G, Eisenbarth T, Sunar B. Cross processor cache attacks. In: Proc. of the 11th ACM on Asia Conf. on Computer and Communications Security. New York: ACM Press, 2016. 353−364.

[76] Hovhannisyan H, Lu K, Yang R, Qi W, Wang J, Wen M. A novel deduplication-based covert channel in cloud storage service. In: Proc. of the 2015 IEEE Global Communications Conf. (GLOBECOM). IEEE, 2015. 1−6.

[77] Block K, Noubir G. Return of the covert channel, data center style. In: Proc. of the 2015 ACM Workshop on Cloud Computing Security Workshop. New York: ACM Press, 2015. 17−28.

[78] Naghibijouybari H, Abu-Ghazaleh N. Covert channels on GPGPUs. IEEE Computer Architecture Letters, 2017,16:22−25.

[79] Evtyushkin D, Ponomarev D, Abu-Ghazaleh N. Covert channels through branch predictors: A feasibility study. In: Proc. of the 4th Workshop on Hardware and Architectural Support for Security and Privacy. New York: ACM Press, 2015. 1−8.

[80] Wu J, Wu Y, Yang M, Wu Z, Luo T, Wang Y. POSTER: biTheft: Stealing your secrets by bidirectional covert channel communication with zero-permission android application. In: Proc. of the 22nd ACM SIGSAC Conf. on Computer and Communications Security. New York: ACM Press, 2015. 1690−1692.

[81] Mazurczyk W. Lost audio packets steganography: The first practical evaluation. Security and Communication Networks, 2012,5:1394−1403.

[82] Mazurczyk W, Lubacz J. LACK—A VoIP steganographic method. Telecommunication Systems, 2010,45:153−163.
[83] Zhao H, Shi YQ, Ansari N. Hiding data in multimedia streaming over networks. In: Proc. of the 8th Annual Communication Networks and Services Research Conf. Washington: IEEE Computer Society, 2010. 50−55.
[84] Kohls K, Holz T, Kolossa D, Pöpper C. Skypeline: Robust hidden data transmission for VoIP. In: Proc. of the 11th ACM on Asia Conf. on Computer and Communications Security. New York: ACM Press, 2016. 877−888.
[85] Hovhannisyan H, Lu K, Wang J. A novel high-speed IP-timing covert channel: Design and evaluation. In: Proc. of the 2015 IEEE Int'l Conf. on Communications (ICC). IEEE, 2015. 7198−7203.
[86] Ambrosin M, Conti M, Gasti P, Tsudik G. Covert ephemeral communication in named data networking. In: Proc. of the 9th ACM Symp. on Information, Computer and Communications Security. New York: ACM Press, 2014. 15−26.
[87] Shen Y, Yang W, Huang L. Concealed in Web surfing: Behavior-based covert channels in HTTP. Journal of Network and Computer Applications, 2018,101:83−95.
[88] Mohamed EE, Mnaouer AB, Barka E. PSCAN: A port scanning network covert channel. In: Proc. of the 41st IEEE Conf. on Local Computer Networks (LCN). Piscataway: IEEE, 2016. 631−634.
[89] Guri M, Hasson O, Kedma G, Elovici Y. An optical covert-channel to leak data through an air-gap. In: Proc. of the 14th Annual Conf. on Privacy, Security and Trust (PST). Berlin, Heidelberg: IEEE, 2016. 642−649.
[90] Masti RJ, Rai D, Ranganathan A, Müller C, Thiele L, Capkun S. Thermal covert channels on multi-core platforms. In: Proc. of the 24th USENIX Conf. on Security Symp. Berkeley: USENIX Association, 2015. 865−880.

附中文参考文献:

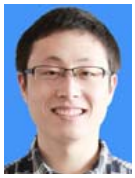
[1] 陈克非.信息安全——密码的作用与局限.通信学报,2001,22(8):93−99.
[7] 王永吉,吴敬征,曾海涛,丁丽萍,廖晓锋.隐蔽信道研究.软件学报,2010,21(9):2262−2288. http://www.jos.org.cn/1000-9825/3880.htm [doi: 10.3724/SP.J.1001.2010.03880]
[22] 刘娅,仲兆满.基于多重协议的网络隐蔽信道设计与实现.现代电子技术,2017,40(8):19−21.
[23] 董丽鹏,陈性元,杨英杰,等.网络隐蔽信道实现机制及检测技术研究.计算机科学,2015,42(7):216−221.

王翀(1991－),男,北京人,博士生,CCF 学生会员,主要研究领域为信息安全.

吴敬征(1982－),男,博士,高级工程师,CCF 专业会员,主要研究领域为漏洞挖掘,移动终端安全,操作系统安全.

王秀利(1977－),男,博士,副教授,CCF 高级会员,主要研究领域为金融科技,人工智能与安全.

关贝(1986－),男,博士,助理研究员,主要研究领域为虚拟化技术,虚拟化安全.



吕荫润(1991－),男,博士,主要研究领域为可满足性模理论,析取规划.

王永吉(1962－),男,博士,研究员,博士生导师,CCF 高级会员,主要研究领域为隐蔽信道,高可信网络技术,信息安全.

张常有(1970－),男,博士,研究员,博士生导师,CCF 高级会员,主要研究领域为并行与分布式软件与安全,软件工程.