ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.21, No.9, September 2010, pp.2262−2288
doi: 10.3724/SP.J.1001.2010.03880
© by *Institute of Software*, *the Chinese Academy of Sciences*. All rights reserved.
E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

隐蔽信道研究*

王永吉[1,2,3+], 吴敬征[1,4], 曾海涛[5], 丁丽萍[1], 廖晓锋[1,4]

[1](中国科学院 软件研究所 基础软件国家工程研究中心,北京 100190)
[2](中国科学院 软件研究所 互联网软件技术实验室,北京 100190)
[3](中国科学院 软件研究所 计算机科学国家重点实验室,北京 100190)
[4](中国科学院 研究生院,北京 100049)
[5](中国移动通信研究院,北京 100053)

Covert Channel Research

WANG Yong-Ji[1,2,3+], WU Jing-Zheng[1,4], ZENG Hai-Tao[5], DING Li-Ping[1], LIAO Xiao-Feng[1,4]

[1](National Engineering Research Center for Fundamental Software, Institute of Software, The Chinese Academy of Sciences, Beijing 100190, China)
[2](Laboratory for Internet Software Technologies, Institute of Software, The Chinese Academy of Sciences, Beijing 100190, China)
[3](State Key Laboratory of Computer Science, Institute of Software, The Chinese Academy of Sciences, Beijing 100190, China)
[4](Graduate University, The Chinese Academy of Sciences, Beijing 100049, China)
[5](China Mobile Research Institute, Beijing 100053, China)
+ Corresponding author: E-mail: ywang@itechs.iscas.ac.cn

Wang YJ, Wu JZ, Zeng HT, Ding LP, Liao XF. Covert channel research. *Journal of Software*, 2010,21(9):2262−2288. http://www.jos.org.cn/1000-9825/3880.htm

Abstract: Covert channel is the communication channel that allows a process to transfer information in a manner that violates the system's security policy. It is a major threat to the secure information systems and widely exists in secure operation systems, secure networks and secure database. Covert channel analysis is generally required by secure information systems's secure criterion, such as TCSEC. This paper firstly analysis the covert channel concept, field, techniques and classification. Next, it surveys the classic techniques and methods from the following aspects: covert channel identification, measurement, elimination, limitation, auditing, and detection. The research achievements in the past 30 years are systematically concluded, especially the new techniques of covert channel measurements and handlings in recent years. This paper attempts to give a comprehensive and clear outline for this research direction, and provides a useful reference for the researchers of this field.

Key words: covert channel; covert channel identification; covert channel measurement; covert channel elimination; covert channel limitation; covert channel auditing; covert channel detection

* Supported by the National Natural Science Foundation of China under Grant No.60673022 (国家自然科学基金); the National High-Tech Research and Development Plan of China under Grant No.2007AA010601 (国家高技术研究发展计划(863)); the Knowledge Innovation Key Directional Program of the Chinese Academy of Sciences under Grant No.KGCX2-YW-125 (中国科学院重要方向项目)
Received 2009-07-27; Accepted 2010-05-05

© 中国科学院软件研究所 http://www.jos.org.cn

摘 要: 隐蔽信道是指允许进程以危害系统安全策略的方式传输信息的通信信道,是对安全信息系统的重要威胁,并普遍存在于安全操作系统、安全网络、安全数据库系统中.国内外的安全标准都要求对高等级的安全信息系统进行隐蔽信道分析.首先分析隐蔽信道的基本概念,研究领域、技术组成及分类,然后从信道识别、度量、消除、限制、审计和检测几个技术层面综述隐蔽信道研究中经典的技术和方法,系统地总结隐蔽信道领域 30 多年来的研究成果,尤其对近年来隐蔽信道度量和处置新技术作了较为详尽的介绍.试图为该研究方向勾画出一个较为全面和清晰的概貌,为隐蔽信道分析领域的研究者提供有益的参考.

关键词: 隐蔽信道;隐蔽信道识别;隐蔽信道度量;隐蔽信道消除;隐蔽信道限制;隐蔽信道审计;隐蔽信道检测

中图法分类号: TP393 **文献标识码**: A

隐蔽信道是指允许进程以危害系统安全策略的方式传输信息的通信信道[1].我国的《计算机信息系统安全保护等级划分准则》(GB17859-1999)[2]、美国的《可信计算机系统评估准则》(TCSEC)[1]以及国际标准化组织 ISO 在 1999 年发布的《信息技术安全评估通用准则》(ISO/IEC 15408,简称 CC 标准)[3]都对隐蔽信道分析提出了明确的规定.要求高等级信息系统(GB17859-1999 第四级,TCSEC 中 B2 级以上)必须进行隐蔽信道分析,在识别隐蔽信道的基础上,对隐蔽信道进行度量和处置.

隐蔽信道的概念最初是由 Lampson 在 1973 年提出[4],其给出的隐蔽信道定义为:不是被设计或本意不是用来传输信息的通信信道.在这篇开创性的文章里,Lampson 关注于程序的限制问题,即如何在程序的执行过程中进行限制,使其不能向其他未授权的程序传输信息.他列举了恶意或行为不当的程序绕过限制措施,泄露数据的 6 种方法和相应的处理措施,并把这些方法归纳为 3 种类型:存储信道,合法信道和“隐蔽信道”.后续的研究将隐蔽信道重新划分为两种类型:存储隐蔽信道和时间隐蔽信道[5],统称隐蔽信道.其中:时间隐蔽信道对应于 Lampson 所指的“隐蔽信道”;合法信道则是一种阈下信道(subliminal channel)[6],是公开信道中所建立的一种实现隐蔽通信的方式.信道中公开的、有意义的信息仅仅充当了秘密信息的载体,秘密信息通过它进行传输.这种隐蔽传输信息的方式后来逐渐淡出了隐蔽信道研究的中心,形成了相对独立的研究领域.

对隐蔽信道的分析和研究,文献[7]给出了详细的解释.隐蔽信道分析工作包括信道识别、度量和处置.信道识别是对系统的静态分析,强调对设计和代码进行分析发现所有潜在的隐蔽信道.信道度量是对信道传输能力和威胁程度的评价.信道处置措施包括信道消除、限制和审计.隐蔽信道消除措施包括修改系统、排除产生隐蔽信道的源头、破坏信道的存在条件.限制措施要求将信道危害降低到系统能够容忍的范围内.但是,并非所有的潜在隐蔽信道都能被入侵者实际利用,如果对所有的潜在隐蔽信道进行度量和处置会产生不必要的性能消耗,降低系统效率.隐蔽信道检测则强调对潜在隐蔽信道的相关操作进行监测和记录,通过分析记录,检测出入侵者对信道的实际使用操作,为信道度量和处置提供依据.

本文综述了隐蔽信道分析技术的研究历史、目前面临的主要问题以及今后的发展方向,试图为该研究方向勾画出一个较为全面和清晰的概貌,为隐蔽信道相关领域的研究者提供有益参考.本文首先介绍隐蔽信道基本概念、分类、研究背景和相关研究领域.从第 2 节逐步展开论述隐蔽信道识别、度量、消除、限制、审计和检测技术中的典型方法,阐述隐蔽信道概念提出 30 多年来在各个技术层面的研究成果.最后总结全文,指出隐蔽信道技术的发展方向.

1 隐蔽信道基本概念

1.1 隐蔽信道表示

在隐蔽信道研究过程中,研究人员给出了多种不同的定义.其中,Tsai 等人给出的隐蔽信道定义较为全面[8]:给定一个强制安全策略模型 M 及其在一个操作系统中的解释 $I(M)$.$I(M)$中的两个主体 $I(S_h)$和 $I(S_l)$之间的通信是隐蔽的,当且仅当模型 M 中的对应主体 S_h 和 S_l 之间的任何通信都是非法的.该定义指出,隐蔽信道只与系统的强制访问控制策略模型相关.隐蔽信道广泛存在于部署了强制访问控制机制的安全操作系统、安全网络和安全

© 中国科学院软件研究所 http://www.jos.org.cn

数据库中.

1973 年,Bell 和 LaPadula 提出了著名的 Bell-LaPadula 多级安全强制访问控制模型(BLP 模型)[9].该模型描述如下:

系统包含主体集 S 和客体集 O,S 中的每一个主体 s 和 O 中的每一个客体 o 都分别具有一个固定的安全标记 $C(s)$和 $C(o)$(表示信任和敏感等级).BLP 模型在安全标记之间建立了一种称为“支配”的偏序格关系,用“≥”表示.BLP 模型要求安全系统内主体操作客体的安全信息流具有简单安全特性和*-特性:

- 简单安全特性:仅当 $C(s)\geqslant C(o)$时,主体 s 才可以对客体 o 有“读”访问权限;
- *-特性:仅当 $C(p)\geqslant C(o)$时,对客体 o 有“读”访问权限的主体才可以对客体 p 有“写”访问权限.

简单安全特性表明,信息接收者的信任等级不得低于信息的敏感等级.*-特性表明,将一个敏感对象的内容写入另一个敏感对象,要求后者的敏感等级至少不低于前者.这两个特性可以简单地概括为“不上读,不下写”.BLP 模型既可以阻止低级别的主体访问高密级的信息,同时也阻止高安全级别主体通过“写”操作向低级别主体泄漏信息.

即使在强制访问控制模型下,恶意用户仍然能够通过构建隐蔽信道实现从高安全级主体向低安全级主体的信息传输,实现方式如图 1 所示.高安全级和低安全级用户之间通过修改和感知共享变量的值或者属性传递信息.TCSEC 标准使用 TCB(trusted computing base,可信计算基)表示计算机系统中所有保护机制的总和(包括硬件、固件和软件),负责执行安全策略.因此,隐蔽信道可以表示为 TCB 三元组:

$$\langle variable, PA_h, PV_i\rangle \tag{1}$$

其中:$variable$ 是系统中的变量;PA_h 是修改这个变量的 TCB 原语且具有较高的安全级;PV_i 是感知、观察这个变量的 TCB 原语且安全级较低.从 PA_h 到 PV_i 的通信是系统安全策略所不允许的,则 PA_h 到 PV_i 的通信信道称为隐蔽信道.

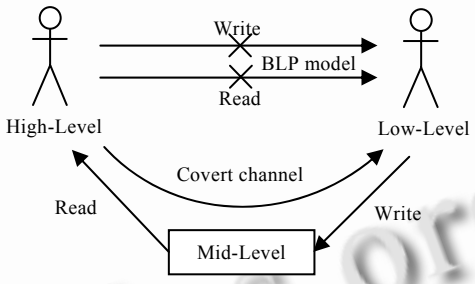

Fig.1 Example of covert channel

图 1 隐蔽信道示例

1.2 隐蔽信道分类

隐蔽信道三元组$\langle variable, PA_h, PV_i\rangle$中变量 $variable$ 可以表示系统中不同的属性,当 $variable$ 表示存储属性时,隐蔽信道为存储隐蔽信道.例如,在资源耗尽型信道中,$variable$ 表示收发双方能够修改和感知的共享资源.当 $variable$ 表示 CPU 时间或者响应时间等属性时,隐蔽信道为时间隐蔽信道.在对隐蔽信道识别方法的研究中,Kemmerer 给出了隐蔽信道存在的最小条件[10].

存储隐蔽信道存在最小条件:

(1) 信息的发送者和接收者必须能够访问某个共享资源的同一个属性;

(2) 信息的发送者能够以某种方式改变这个属性;

(3) 同时,信息的接收者必须能够检测这个属性的任何一个改变;

(4) 存在着某种机制初始化发送者和接收者,并且要保证发送和接收时间顺序的正确性,即建立好的同步机制以保证信息正确地发送与接收.

© 中国科学院软件研究所 http://www.jos.org.cn

时间隐蔽信道存在最小条件:

(1) 发送者和接收者必须对某个共享资源的同一个属性有访问权;

(2) 发送者和接收者必须有一个统一的时间参考,比如一个实际时钟;

(3) 发送者必须能够调制接收者的响应时间来表示一个属性的改变;

(4) 一定存在某个机制使得发送和接收双方能够同步发送事件.

与存储隐蔽信道相比,时间隐蔽信道又称为无记忆通道,不能长久地存储信息.发送者发送的信息接收者必须及时接收,否则要传递的信息就会消失,时效性较强.分析隐蔽信道存在条件及其表示$\langle variable,PA_h,PV_i\rangle$可知,存储隐蔽信道和时间隐蔽信道并没有本质的区别,只是 *variable* 变量代表的属性不同.在隐蔽信道分析中,时间隐蔽信道具有更大的复杂性,TCSEC 标准要求 B2 级安全系统进行彻底的存储隐蔽信道分析,而更高级别的 B3 级和 A1 级安全系统才要求必须同时进行时间隐蔽信道分析.

与其他的通信信道类似,隐蔽信道也可以分为噪音信道和无噪信道.对于$\langle variable,PA_h,PV_i\rangle$中的 *variable* 变量,如果该变量只能被PA_h原语修改,而且对于任意修改,PV_i原语都能够实现概率为 1 的正确解码,则该信道称为无噪信道;如果 *variable* 变量被PA_h原语修改的同时还可能被其他原语修改,PV_i不能正确解码,则该信道称为噪音信道.在隐蔽信道分析中,通常将信道抽象成无噪信道以度量信道最大容量.但是在实际场景中,信道多为噪音信道,影响隐蔽信道的传输效率.

隐蔽信道传输有固定的信息传输周期,如图 2 所示[11].一个完整的信息传输周期包括发送者/接收者同步阶段、信息传输阶段和反馈阶段.同步阶段中,发送者通知接收者准备发送信息,如果收发双方有事先的约定,例如每隔 t 个时间单元发送新的信息,则同步阶段可以省略;如果收发双方通信路径不可信,则反馈阶段必须存在,否则发送者无法确认接收方是否收到信息,也无法确认何时开启新的传输周期.

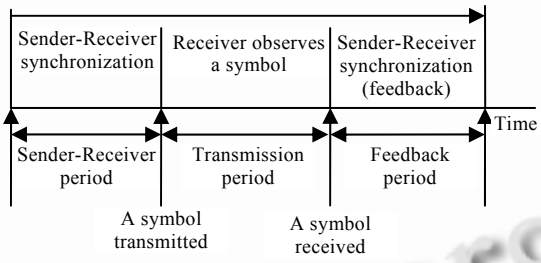

Fig.2 Covert channel cycle

图 2 隐蔽信道周期

1.3 隐蔽信道研究领域

Lampson 提出的隐蔽信道概念关注于程序的限制问题,但当前的隐蔽信道问题已经涉及到安全信息产品的多个领域,包括安全操作系统、安全数据库、安全网络等.此外,还存在一些倍受关注的、与隐蔽信道相关联的概念.下面分析隐蔽信道涉及到的研究领域以及相互之间的区别和联系,进一步加深对隐蔽信道的理解.

1.3.1 数据库隐蔽信道

数据库系统中的隐蔽信道主要包括以下 3 类[12]:

(1) 数据库存储资源引入的信道.信道可利用的数据库存储资源包括数据和数据字典,其主要原理是发送者修改数据/数据字典,接收者则通过完整性约束等方式间接感知数据/数据字典的修改,从而获得信息[13];

(2) 数据库管理资源引入的信道.主要是数据库系统变量或安全机制的资源耗尽型信道.资源包括游标、临时数据区等.另外,同时管理多个安全级别用户的系统安全机制也可能引入信道,如审计机制等[14];

(3) 事务并发控制引起的隐蔽信道.安全数据库系统中通常依据 BLP 模型[9]实施强制访问控制,约束用户的数据访问操作,以保证数据的安全性.同时,为了保证数据操作的实时性,系统还需要采用实时算法

© 中国科学院软件研究所 http://www.jos.org.cn

处理事务调度和并发控制[15].恶意主体可以利用不同安全级事务间的并发冲突构造隐蔽信道,称作数据冲突隐蔽信道(data conflict covert channel,简称 DC 信道)[16].

数据冲突隐蔽信道中,两个不同安全级别的用户发起的事务 tr_l,tr_h 共同访问同一数据项 d_x,其安全级别关系为 $SL(tr_h)\geqslant SL(d_x)\geqslant SL(tr_l)$.其中,低安全级别事务 tr_l 写访问 d_x,高安全级别事务 tr_h 读访问 d_x.在该场景下,可以构造多种具体的数据冲突隐蔽信道,实现高安全级用户向低级别用户传递信息.

例如,入侵者利用事务执行过程中是否发生冲突的事实表示希望传输的符号,如图 3 所示.首先,低安全级用户发起事务 tr_l,如果高安全级用户希望发出符号‘1’,则发起事务 tr_h.由于两个事务间存在冲突,系统放弃事务 tr_l;如果高安全级用户希望发出符号‘0’,则不发起事务 tr_h,tr_l 可以执行完成.在该场景下,处于不同安全级别的事务通过并发控制机制相互干扰传递信息.

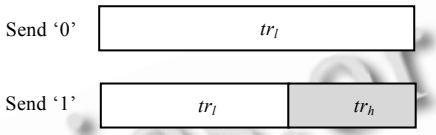

Fig.3 DC covert channel

图 3 数据冲突隐蔽信道

1.3.2 阈下信道

阈下信道是指在基于公钥密码技术的数字签名、认证等应用密码体制的输出密码数据中建立起来的一种隐蔽信道,除指定的接收者外,任何其他人均不知道密码数据中是否存在阈下消息[17].阈下信道又称潜信道,是一种信息隐藏方法.Simmons 于 1984 通过研究看守监狱中两个囚犯秘密协商逃跑计划的例子(如图 4 所示),引入了阈下信道的概念[6].图 4 中,Wendy 负责监视囚犯 Alice 和 Bob 的活动,一旦发现有异常行为就将其分开并更加严格地看管;Alice 和 Bob 必须采用某种约定协商越狱情况.

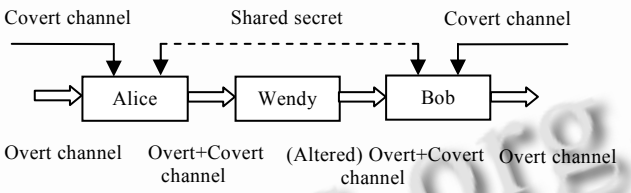

Fig.4 Prisoner problem

图 4 囚犯问题

虽然在 Simmons 的定义中阈下信道也被称作隐蔽信道,但是一般认为,阈下信道与 TCSEC 标准中所指的隐蔽信道有所差别[6,18]:

(1) 阈下信道是在公开信道中所建立的一种实现隐蔽通信的信道.由于传输信道本身的合法性,其更接近于信息隐藏研究的范畴,并且已经被认可为一种典型的信息隐藏方法;

(2) 阈下信道的宿主是密码系统,且只能是非对称密码体制.阈下信道的特点是,即使监视者知道要寻求的内容,也无法发现信道的使用并获取正在传送的阈下消息.因为阈下信道的加密特性,决定了其安全性要么是无条件的,要么是计算上不可破的.这不是普通隐蔽信道所能做到的而且也不是必需的.

1.3.3 网络信道

网络信道一般可以分为两种:一种是多级安全网络传输信道,另一种是普通网络传输信道.第 1 种网络信道中强调多级安全概念,这种信道存在于具有不同安全级别,需要进行隔离的主机之间.入侵者期望利用这种信道从高安全级别主机获得信息,并传递给低安全级别主机.第 2 种网络信道中并不局限于多级安全环境,普通网络中主机没有安全级别的定义.这种信道的两端主机甚至可能是被允许通信的,该信道只是期望在通信链路上再

© 中国科学院软件研究所 http://www.jos.org.cn

附加一层隐蔽通信.由于更贴近于日常应用,并且涉及更广泛的安全环境和安全策略,目前第 2 种网络信道的研究逐渐占据了主流地位.

1987 年,Girling 发现了 3 种局域网上的隐蔽信道,开启了对普通网络中隐蔽信道的研究[19].1996 年,Handel 对 OSI 网络模型进行了深入分析,提出了许多理论上的潜在隐蔽信道.同年,Rowland 在 TCP/IP 协议部分找到了许多隐蔽信道实例[20,21].之后,网络信道的威胁得到了广泛的认识.网络隐蔽信道的识别、度量和处置也逐渐成为隐蔽信道研究领域的热点之一[22−25].

网络隐蔽信道也包括存储隐蔽信道和时间隐蔽信道两种类型.网络存储隐蔽信道主要是在各种协议的数据包中加载信息.为了实现隐蔽传输,一般将信息附加在不常用的数据段中,包括未用的 IP 头字段(TOS 字段、DF 和 URG 位)、IP 头的扩展和填充段、IP 标识和碎片偏移等[19−21].也有的网络存储隐蔽信道将信息隐藏在应用层编码中[26].网络时间隐蔽信道则一般利用网络中传输数据包的时间特性来表示信息,这些时间特性包括数据包的发送/到达时刻、间隔时间等[27−29].

1.3.4 推理信道

推理信道一般存在数据库系统中,是指恶意用户利用历史访问记录查询信息,实现对敏感信息间接访问[30].在部分研究成果中,推理信道被归属于隐蔽信道领域.不过,这种信道与 TCSEC 标准中的隐蔽信道概念存在一些差距:

(1) 推理信道所针对的系统不只局限于多级安全系统,执行其他安全策略的系统中同样存在推理信道威胁.恶意用户可以利用推理信道以未授权的方式获取敏感信息;

(2) 推理信道中发送者并非是必须的,恶意用户可以独立构造查询来完成信息盗取.因此,推理信道并不需要植入木马.

2 隐蔽信道分析技术

隐蔽信道分析技术主要可以分为 4 个领域,其分别关注于隐蔽信道的建模、识别、度量和处置[31].其中,后三者被 TCSEC 标准规定为针对具体信道需要执行的工作[1,7].

信道建模关注于隐蔽信道产生原因的研究和信道的形式化模型表示,主要包括信息流模型[32]和无干扰模型[33].

信道识别(search/identify)强调对系统设计和代码进行分析,寻找可能被用来构建信道、进行隐蔽通信的共享资源、原语等设施,即搜索$\langle variable,PA_h,PV_i\rangle$中的 *variable* 变量和 PA_h,PV_i 原语.对系统执行信道识别操作,可以确定系统中是否存在隐蔽信道隐患.针对信道建模模型描述的隐蔽信道产生原因,分别形成了一系列隐蔽信道的识别方法,包括信息流分析方法[34−36]、无干扰分析方法[37,38]、共享资源矩阵方法[10]及其改进[39]、隐蔽流树方法[40]、Tsai 等人提出的代码级分析技术[41,42]、回溯搜索法[18]、逆向共享资源矩阵[43]等方法.

在识别出隐蔽信道之后,系统的安全保障人员就可以对信道的传输能力及危害程度进行度量,并采取处置措施来保障系统的安全性.对隐蔽信道威胁的度量结果可以用来评价信道对系统安全性的威胁程度,并指导对其采取适当的限制措施,以有限的代价来保障系统的安全服务.

TCSEC 标准中规定,使用信道容量作为信道威胁评价的指标.信道容量度量方法主要分为两种类型,分别是 Millen 提出的形式化方法[34]和 Tsai 与 Gligor 提出的非形式化方法[44].除了通过精确计算或实验来获得信道的容量数值以外,实际应用中也可能只需要通过数学分析获得信道容量值的取值范围[45−47].除了信道容量之外,用来对信道威胁度量的指标还包括短消息指标[48,49]、隐蔽信道因素[50]、相对容量[51]等.

信道的处置措施包括 3 类,分别是信道消除、限制、审计和检测.对隐蔽信道危害的消除措施包括修改系统、排除产生隐蔽信道的源头或者破坏信道的存在条件.但是信道消除的方法一般代价较高,不易实现.早在信息安全标准 TCSEC 中就已经承认了隐蔽信道难以消除的可能性,并认为,当安全系统对隐蔽信道施加有效干扰后能够限制信道传输能力,从而确保恶意用户即使通过信道盗取了机密信息,也会因为信息的准确度有限或者数据已经过时而无法对系统安全构成威胁.因此,TCSEC 标准允许系统放弃完全消除信道,而选择限制信道能力

© 中国科学院软件研究所 http://www.jos.org.cn

的处置措施,将隐蔽信道的传输能力限制在不能有效传递信息、侵害系统安全的范围内[1].隐蔽信道限制措施的目标是破坏隐蔽信道的传输能力,可采取的操作包括添加干扰[52,53]、添加延时[44]等.

信道审计强调对隐蔽信道相关操作的监测和记录,而信道检测则是指从审计到的操作记录中筛选出实际使用的隐蔽信道记录.审计方法的关键是确定哪些事件和数据必须被记录,检测方法的关键在于如何区分实际使用信道时产生的记录和系统正常使用产生的记录.对信道使用情况的审计操作可以用来对入侵者进行威慑,以降低入侵者使用信道威胁系统安全的可能性[54].

隐蔽信道的识别是审计和检测信道使用状况的基础,而被标识的信道则是审计和检测的对象.利用信道检测结果,防御方能够获得更加明确的信道使用信息.在这些信息基础上,可以度量信道的实际传输能力,从而能够对入侵行为采取针对性措施.另外,从检测结果中也能够获得入侵者的信息,增加系统对入侵者的威慑性.

3 隐蔽信道识别方法

隐蔽信道识别目的在于寻找可能被用来构建信道、进行隐蔽通信的共享资源及原语等设施.识别方法主要包括 3 种:信息流分析法、共享资源矩阵法和无干扰分析法.

3.1 隐蔽信道信息

隐蔽信道信息是信道分析操作的对象,其来源主要包括 3 个方面:

(1) 系统参考手册.系统参考手册中一般都会给出以下内容的描述,TCB 原语、CPU 和 I/O 处理器指令、原语对系统客体的影响、TCB 的参数、指令范围等;

(2) 系统设计,实现所依据的顶层规范.B2~A1 级系统要求使用描述性顶层规范(detailed top-level specification,简称 DTLS),A1 级系统要求使用形式化顶层规范(formal top-level specification,简称 FTLS);

(3) 源代码.TCB 的源代码和处理器代码(微代码).

系统参考手册是最容易获得的信息,但是由于其所提供的多为抽象和概括信息,缺乏系统实现细节.利用参考手册信息时,信息分析者将面对一个黑盒系统,参考手册信息一般在系统实现之后才能完全生成,此时已经错过了隐蔽信道处置的最佳时机.

由于以上原因,目前从参考手册出发识别信道的研究成果不多,绝大多数的识别方法都选择利用 FTLS 作为识别信息的来源,可以在设计早期就发现可能产生信道的设计缺陷,有利于利用最小代价修正这些缺陷.但是,完全依赖 FLTS 也存在不足:

(1) 无法保证 FTLS 和代码完全相符,无法发现代码阶段引入的隐蔽信道;

(2) FTLS 中缺少数据结构和代码的细节,无法指导非直接信息流的发现(这些信息流可能是由程序语言语义引起的).由于这些细节的缺乏,也不利于信道处置措施的实现,如审计位置和限制措施力度的确定.从代码层面进行隐蔽信道分析可以避免 FTLS 的缺陷,但是面临着工作量过大的问题,目前还缺乏可用的自动化工具.

3.2 信息流分析法

Denning 于 1976 年提出的信息流分析方法(system information-flow analysis)是最早也是最著名的隐蔽信道分析方法之一[32].Tsai,Gligor 等人于 1990 年对 Denning 的方法进行了重大改进,增加了语义分析[42].因此,可以进一步地将信息流分析法划分为以 Denning 方法为代表的语法信息流方法和以 Tsai 方法为代表的语义信息流方法[55].

Denning 首先对信息流模型进行了形式化描述,$FM=\langle N,P,SC,\oplus,\rightarrow\rangle$.其中:$N=\{a,b,\ldots\}$是逻辑存储单元的集合,即$\langle variable,PA_h,PV_i\rangle$中 *variable* 的集合;$P=\{p,q,\ldots\}$是进程的集合,包含信息流中的所有活动进程,即 PA_h,PV_i 原语的集合;$SC=\{A,B,\ldots\}$是不同信息的安全级的集合;$\oplus$是安全级别的上确界运算,$A\oplus B$ 取得安全级别 A 和 B 的最小公共上界;$\rightarrow$是一个偏序关系,表示安全级别之间的信息流关系,当且仅当 A 中的信息允许流向 B 时表示为 $A\rightarrow B$.通过形式化的描述,Denning 给出了语法信息流识别方法,方法的主要步骤是:

© 中国科学院软件研究所 http://www.jos.org.cn

(1) 从每个语句中抽象出信息流语义.例如,赋值语句代表变量之间的“明流”(显式信息流),从条件语句中能够抽象出变量之间的“暗流”(隐式信息流);
(2) 定义信息流策略.将信息流策略应用于系统的顶层规范或者代码上,能够生成信息流公式.例如,语句“$y:=x$”表示信息从变量 x 流向变量 y,则变量 y 的安全级别必须支配变量 x,表示成信息流公式为 $y\rightarrow x$;
(3) 利用定理证明器证明信息流公式的正确性.如果信息流公式不能被证明,则可能存在隐蔽信道,需要进一步分析:判断该信息流是真实的非法信息流还是误报;判断该信息流是否能构造真实的信道,而不只是潜在的隐蔽信道.

语法信息流识别方法的优点包括:
(1) 可以用相对简单的自动执行方式;
(2) 同时支持 FTLS 和源代码两个层次的信道识别;
(3) 可以采用增量式的分析方法逐个对函数和 TCB 原语进行检查;
(4) 搜索彻底,不会遗漏任何非法流.

同时,该方法也存在一定的缺点:
(1) 可能会标识出大量伪非法流,增加了人工分析的负担;
(2) 不能用于非形式化顶层规范;
(3) 不能从该方法中直接获得在 TCB 中放置隐蔽信道处置代码的位置.

语法信息流方法从语法分析角度出发,建立信息流公式,并判断信息流的合法性,会产生大量的伪随机流.Tsai 等人改进该方法,加入语义理解,提出语义信息流方法,该方法步骤如下:
(1) 分析编程语言的语义、内核代码中的数据结构,发现其中变量的可修改性(alterability)/可见性(visibility);
(2) 解析内核变量的别名,确定其是否具有间接可修改性;
(3) 利用信息流分析方法来判断内核变量的间接可见性[7,42].

语义信息流方法同样具有搜索彻底、能够发现所有的潜在隐蔽存储通道的优点.另外,Tsai 的方法优于语法信息流方法之处在于:
(1) 语义信息流方法可以发现大量伪非法流,减轻了人工分析这些伪随机流的负担;
(2) 可以找出内核共享变量被查看/修改的位置,有助于确定放置隐蔽信道处置代码的位置.

但是,语义信息流方法仍然存在着工作量大、缺少自动化工具的缺点.例如,对 Secure Xenix 系统进行语义信息流分析需要 2 人/年的额外工作量[7].为此,He 与 Gligor 研制了一种自动工具,该工具能够检查所有通过 TCB 接口可见的信息流,并且从中区分出非法信息流[56].但是,区分伪非法流和真实非法流的工作仍然依赖于人工分析.类似的信息流分析方法还包括文献[57]中提到的基于有限状态机的隐含信息流分析方法,该方法将安全系统及安全策略模型化为有限自动机,通过研究有限自动机的特性来分析安全系统的信息流特性,进而确定系统中是否存在隐蔽信道.

卿斯汉和朱继峰设计了一种代码层次的标识方法,称为回溯搜索法,该方法采用与 Tsai 的语义信息流法相同的识别共享变量规则、语义信息流规则和处理别名的规则.由于在回溯过程中引入“剪枝规则”,该方法执行过程中能够立即删除不能构成隐蔽信道的共享变量,从而显著地减少了进一步分析的工作量.该方法被应用于安胜 OS v4.0 系统的隐蔽信道识别中[55,58],成功地发现了 18 个真实隐蔽通道.其中,有些通道只能应用回溯分析法才能找到.

3.3 共享资源矩阵法

共享资源矩阵法(shared resource matrix,简称 SRM)是 Kemmerer 于 1983 年提出的,该方法曾成功应用于几个项目(如 Unix 2 和 DG/UX 等)[10,38].Kemmerer 指出,隐蔽信道的存在归根于系统中的共享资源,即$\langle variable, PA_h, PV_i\rangle$中 *variable* 变量.如果能够找出所有用于读/写的系统资源及其上操作,即 PA_h,PV_i,对这些资源进行分析就能够找到相应的隐蔽信道.利用 SRM 方法进行信道标识需要的几个步骤是:

© 中国科学院软件研究所 http://www.jos.org.cn

(1) 分析所有的TCB原语操作,构建共享资源矩阵.矩阵中用户可见的TCB原语作为列,可见的/可修改的共享资源属性作为行.矩阵项利用 R 和 M 分别表示操作原语对这些属性具有读能力和修改能力(包括间接读和间接修改).用来生成共享资源矩阵的原语信息可以来自形式化和非形式化顶层规范,也可以从源代码中获得;

(2) 对共享资源矩阵进行传递闭包操作,找到所有能够间接读共享资源属性的原语,并将“间接读”关系添加到共享资源矩阵中;

(3) 分析矩阵中的每一行,如果该行中同时包含 R 和 M,则一个进程可以通过读该变量感知另一个进程对该变量的修改,而修改变量进程的安全级别能够支配读变量进程的安全级别,就可能存在隐蔽信道.

以上分析产生的结果中,还可以排除以下类型的信道:两个进程间存在的合法信道、信道使用者无法从信道中获得有用信息的无用信道、信道的发送者和接收者是同一进程的伪信道.余下的信道才可以归为潜在隐蔽信道.

SRM 方法的优点包括:

(1) 具有广泛适用性,能够支持对形式化和非形式化顶层规范,以及源代码的分析;

(2) 不需要事先为 TCB 变量设置安全级别,因此避免了出现伪非法流.

同时它也存在一些缺点:

(1) 从源代码层次构建共享资源矩阵工作量巨大,且没有自动化构建工具;

(2) 不能证明单个的 TCB 原语或原语对的安全隔离性,不能增量分析新的原语;

(3) SRM 方法过于保守,利用信息流分析能够自动排除的信道可能被 SRM 认为是潜在隐蔽信道.

1996 年,McHugh 对 SRM 方法做出了改进,包括区分用户与系统之间的信息流和状态属性之间的信息流、区分信息流的流入属性、区分信息流产生的条件等,这些改进精化了共享资源矩阵对信息流的描述能力[39,55].

Kemmerer 提出的隐蔽流树(covert flow tree,简称 CFT)方法实质上是共享资源矩阵方法的一种变形,同样考察 TCB 原语与变量之间的修改和读取关系[40].不同的是,CFT 方法采用更加直观的树形结构表示信息流,并且支持图形化的分析工具.

沈建军的博士论文中提出了一种 SRM 的改良方案,逆向共享资源矩阵方法.其对 SRM 方法的改进包括:

(1) 扩展 SRM 矩阵,从而记录信息流路径;

(2) 采用逆向的 SRM 传递,获得 TCB 变量的间接修改关系;

(3) 采取传递控制措施,制约信息流在 SRM 传递闭包过程中的任意扩散;

(4) 利用前期元流分析结果初始化 SRM 矩阵,并依据元流承受的访问控制约束进一步细分矩阵列.

该方法应用在安胜 OS v4.0 系统中,结果显示,该方法有效地限制了信息流组合扩散,在组合过程中消除了大部分伪非法流[43].

3.4 无干扰分析法

无干扰模型是安全领域的一个经典模型,它首先由 Goguen 和 Meseguer 于 1982 年提出[33].无干扰模型从本质上形式化了一个原则:在安全系统中,一个用户不能意识到任何不由它所支配的用户的任何操作.无干扰模型中,TCB 被抽象成一个状态机,假设 X 和 Y 是两个用户进程,W 是状态机在初始状态时的输入序列,并且该输入的最后一个操作来自进程 Y.在初始状态下输入 W 后,进程 Y 观测到的输出为 $Y(W)$.另外,设 W/X 是从 W 中删除来自 X 的输入后得到的子序列.称进程 X 与进程 Y 之间无干扰,当且仅当对于所有可能的以 Y 的输入结尾的输入串 W,$Y(W)=Y(W/X)$,即进程 Y 所观测到的输出与从 W 中剔除 X 的输入后的观测结果一致.

可以证明,进程之间无干扰时将具有以下性质:如果一个进程的输入不能影响另一个进程的输出,则不可能从第 1 个进程向第 2 个进程传输信息.因此,如果多级安全系统中不存在隐蔽信道,则任何一个用户都应该与其支配的任何用户之间满足无干扰关系.

在利用无干扰方法(non-interference analysis)分析实际系统时,必须使用 Goguen 和 Meseguer[37]给出的展开定理(unwinding theorem).该定理指出,系统的状态可以按照某一个用户(如用户 Y)分成不同的等价类.两个 Y 等

© 中国科学院软件研究所 http://www.jos.org.cn

价类间满足:对于同一个 Y 的输入,Y 所获得的输出是相同的;对于任何输入,下一个状态也是 Y 等价的;进程 X 与进程 Y 无干扰,当且仅当对于 X 的任何输入,都使当前状态迁移到一个 Y 等价状态.展开定理对无干扰分析的实际可行性十分重要,因为它避免了分析无穷级的输入序列,使得用户能够分析单独的 TCB 函数和原语.

无干扰方法的优点包括:

(1) 同时支持 FTLS 和源代码两个层次的信道识别;

(2) 可以避免出现伪非法流;

(3) 可以采用增量式的分析方法,逐个对函数和 TCB 原语进行检查.

但是它同样也会存在一些缺点:

(1) 无法对无形式化顶层规范的系统进行分析;

(2) 无干扰方法是一种乐观方法.利用该方法分析系统的过程,是尝试证明 TCB 规范和代码中不存在干扰.因此,该方法适合分析可信进程隔离的 TCB 规范,不适于分析包含大量共享变量的 TCB 组件.

无干扰方法的相关研究还包括 Fine 在无干扰分析中构建等价关系的方法.该方法的创新性在于,可以被用来分析已完成开发的系统,而不是仅能应用于设计阶段[59].

朱继峰的博士论文中曾经提出一种语义推理法,该方法是一种 DTLS 级别的隐蔽信道标识方法[18].他认为,从无干扰的意义上来说,用户根本无须关注共享资源问题,而只需要了解哪些行为可以让系统发生状态的变迁.而系统出错是目前发现的唯一一种系统状态变迁的方式,因此对出错返回进行分析,如果一个用户进程能够造成系统状态变迁,而另一个用户进程通过出错返回能够感受到系统状态的这个变迁,则可以识别为隐蔽信道.这种隐蔽信道只包括能够导致系统状态变迁的资源耗尽型隐蔽信道,而不包括事件计数型隐蔽信道.

4 隐蔽信道度量方法

隐蔽信道度量是对信道传输能力和威胁程度的评价,度量结果可以用来指导限制措施的实施.因此,信道度量是整个信道分析过程中的关键环节.隐蔽信道的度量指标包括:

(1) 信道容量(channel capacity),信道能够取得的最大信息传输速率.容量的概念最早来源于信息理论,并被 TCSEC 采用作为信道威胁评价的指标,因此在信道度量领域应用最为广泛[1];

(2) 事务安全级别差.Ahmed 利用冲突事务的安全级别差作为信道威胁的度量,并命名为隐蔽信道因素(covert channel factor).信道两端的安全级别差别越大,其间隐蔽信息传输对系统的威胁就越大[50];

(3) 短消息指标(small message criterion).信道容量适合描述信道传输长文件的能力,但是并不适合度量信道的短消息传输能力.针对信道容量指标的缺陷,Moskwitz 提出了短消息指标的概念,利用消息长度参数 n、消息传输时间和消息保真度 ρ 共同描述信道的短消息传输能力[48].

4.1 容量指标

TCSEC 标准中使用的信道传输能力的概念是带宽(bandwidth),但是 Moskowitz 在 1994 年指出,带宽与信道容量(capacity)之间存在差距,度量信道传输能力时应该使用容量,而不是带宽或最大带宽.带宽在信号处理、通信领域的含义是对频率范围宽度的的度量,单位是 Hz.信道容量是通过一个通信信道能够可靠传输的信息量的上限值,单位是 bits/s,实际上是连续信道带宽的函数.隐蔽信道作为一种传输信道,容量反映了隐蔽信道的信息传输能力,因此在度量信道威胁时应该使用容量指标.在较晚制定的 CC 标准中就选择了容量指标.

目前,计算容量的方法中最为著名的是 Millen[34]提出的形式化方法和 Tsai 与 Gligor[44]提出的非形式化方法.这两种方法都得到了 TCSEC 标准的认可,分别适用于不同的场合.

4.1.1 形式化方法

Millen 的方法基于 Shannon 计算信道最大能力的目标,该方法假设隐蔽信道是无干扰信道,即信道工作过程中,系统中除发送和接收进程以外没有其他进程,信道的收、发者之间同步的时间和进程切换的时间消耗可忽略.

Millen 方法中将隐蔽信道模拟为有限状态机,如图 5 所示.其中,状态的转移都是确定性的.方法中采用的信

© 中国科学院软件研究所 http://www.jos.org.cn

道带宽计算公式为(Millen 提出该方法时,隐蔽信道研究领域仍在使用带宽概念来度量信道的传输能力,其实质即指信道容量):

$$C=\lim_{t\to\infty}\frac{\log_2 N_h(t)}{t} \tag{2}$$

其中,$N_h(t)$是从状态 h 开始在时间段 t 内所传输的符号数,且满足下式:

$$N_h(t)=\sum_i N_i(t-T_{hi}) \tag{3}$$

其中,T_{hi} 是状态机中从状态 h 迁移到状态 i 所需的时间.

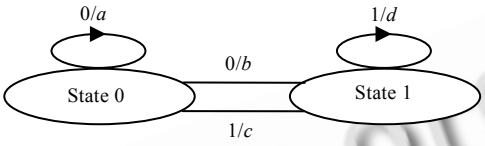

Fig.5 Two-State of covert channel

图 5 隐蔽信道两状态图

4.1.2 非形式化方法

Tsai 和 Gligor 提出的非形式化方法中同样假定隐蔽信道是无干扰信道,系统不存在能够延迟隐蔽信道传输的进程.其方法中采用式(4)计算信道的最大带宽:

$$B(0)=\frac{b}{T_r+T_s+2T_{cs}} \tag{4}$$

其中:b 表示编码系数,在大多数实际应用中都取值为 1;T_r 和 T_s 分别是信道完成上一次传输后,在进行新的传输过程中接收进程“读取”共享变量所需的平均时间以及发送进程“设置”共享变量所需的平均时间.T_r 和 T_s 中包括了发送和接收进程建立隐蔽通信环境所需的时间;T_{cs} 代表进程切换的时间消耗.

文献[7]中对两种方法进行了比较,指出相对于 Tsai 的方法,Millen 的形式化方法具有以下优点:

(1) Millen 方法可以度量信道能够实现的最大传输能力;

(2) Millen 方法的使用过程中需要定义隐蔽信道的实际使用场景,这个场景的定义能够避免在信道环境设置上存在的差别所可能导致的误解.

4.1.3 改进方法

1999 年,Shieh 对 Millen 的方法进行了改进[60].他指出:在资源耗尽型信道和事件计数型信道(两种主要的隐蔽存储信道)中,只有前者可以模拟为有限状态信道,利用有限状态机进行分析;而后者不能被模拟为有限状态信道.Shieh 将事件计数型信道称作无限状态信道,并给出计算有限状态信道和无限状态信道带宽的公式以及实现最大可达带宽的编码方法.

Millen 和 Tsai 的方法中都假定信道具有理想的传输环境,其中对信道特性和状态进行了许多假设和限制,在应用中往往需要根据信道的实际情况加以修改.这两种方法都假设信道中没有噪音存在,度量的结果是信道的最大传输能力.作为确定信道限制措施力度的指导依据,信道在限制措施作用下能力的度量同样重要.限制措施往往通过延长信道信号的传输时间、向信道中添加噪音的方法降低信道的传输能力.这些故意施加的干扰是信道无法避免的,属于受限信道的特有属性,不能作为一般噪音而忽略.

1991 年,Moskowitz 给出了简单时间信道(simple timing channel)在噪音干扰下的容量,这里的噪音是由系统中其他用户对 CPU 和 I/O 资源的竞争造成的[61,62].1993 年,Gray 提出利用概率分区法限制总线竞争信道的能力,并给出了限制下信道容量的计算方法.Moskowitz 于 1996 年给出了一种典型的含噪信道——Z 信道容量的计算方法,并且给出了这种信道容量的取值范围[63].

大多数容量度量方法中都假定目标信道为自同步信道,即存在信道传输同步机制,并且同步操作的消耗可以忽略.Wang 指出,实际系统中有很多信道并不是自同步的,同步操作的消耗不能忽略.Wang 给出了考虑克服

© 中国科学院软件研究所 http://www.jos.org.cn

非自同步状态的消耗时信道容量的计算方法,并证明非自同步信道同样能够提供可靠的传输[64,65].

容量度量研究成果还包括 Lanott 提出的概率模型检验器,支持对复杂系统中信道容量的度量[66].Son 分析了单调速率调度算法(rate-monotonic algorithm,一种典型的实时调度算法[67,68])对时间隐蔽信道的影响,提出了一种计算该调度算法下信道容量的数学框架[51].

4.2 短消息指标

Shannon 信息论中的容量指标是一个极限指标,反映的是传输时间趋于无穷时信道的性质.文献[48]等都证明,即使信道的容量为 0,信道仍然具有传输能力,使用者可以在有限时间内完成对一定信息的传输.Moskowitz 指出,容量描述的是信道花费漫长时间传输长文件的能力,而无法反映信道传输短消息的能力.为了克服容量指标的不足,Moskowitz 提出了描述信道传输短消息能力的指标——短消息指标(small message criterion).该指标包括 3 个要素(n,τ,ρ),分别是短消息的长度、信道传输该短消息的时间、消息传递的保真度.短消息指标表述为,安全系统所容忍的隐蔽信道短消息传输能力为在长度τ的时间内传递长度为 n 位的消息,而消息的保真度为ρ.Moskowitz 认为,短消息指标是对容量指标描述能力的必要补充,二者应该结合运用.

短消息指标被认为是信道容量的必要补充,但是 Moskowitz 的定义只列举了短消息指标的参数,并没有对这些参数进行深入分析,现有定义中还存在以下问题:

(1) 一般的安全信息系统如安全操作系统,用户掌握的数据类型多样,数据的长度跨度较大,无法确定参数 n;

(2) 对短消息传输能力的容忍程度表示为τ和ρ两个参数,二者缺乏关联,系统难以同时满足这两个约束;

(3) 该指标的定义只能描述信道的传输能力,无法反映传输信息的敏感程度.

针对这些问题,文献[49,69]引入了短消息传输价值的概念,短消息传输价值函数的具体形式为

$$V_i(\rho,\tau)=\rho^{\omega}U_i(\tau) \tag{5}$$

其中,$U_i(\tau)$为数据项 d_i 的准确信息的价值随时间变化的函数,由两部分确定:消息的初始价值 U_0 以及消息价值随时间变化的趋势.短消息的价值 V 同时还受到数据传输的保真度ρ制约,参数ω反映了保真度对消息价值的影响方式.当ω=0 时,数据价值不受保真度影响.参数ω越大,数据的价值随传输的保真度下降而衰减得越快.

引入短消息传输价值概念后,用户 u_{high} 与较低安全级别用户 u_{low} 之间隐蔽信道的短消息指标度量 SMM (small message measurement)记为

$$SMM=(ULabel(u_{high}),ULabel(u_{low}),ml,\tau,\rho,V_{high}) \tag{6}$$

在该定义中,$Ulable$ 为用户到安全级的映射,$ml=minlen(UD(u_{high}))$为较高安全级别用户 u_{high} 所拥有的长度最短的数据类型的数据长度.V_{high} 为用户 u_{high} 所拥有的长度最短的数据类型的价值时间函数.利用价值阈值统一表示系统对信道短消息传输能力的容忍程度,并且在所采用的价值函数中引入了消息的敏感度因素.基于该短消息指标的新定义,系统可以对隐蔽信道威胁实施全面的度量.

5 隐蔽信道消除方法

隐蔽信道消除要求从根本上消除隐蔽信道危害,包括修改系统、排除产生隐蔽信道的源头或者破坏信道的存在条件.完全切断信道威胁,是保护系统安全最终极的目标.对于隐蔽信道表示$\langle variable,PA_h,PV_i\rangle$来讲,信道消除即删除 $varaible$ 变量,或者保护该变量不被 PA_h,PV_i 原语修改,使 PA_h,PV_i 原语不能够通过 $variable$ 变量传递信息.

5.1 完全消除方法

能够完全消除隐蔽信道、避免隐蔽通信,自然是保护系统安全的最理想选择.只要有可能,就应该设法消除隐蔽通道.消除隐蔽信道需要对系统的设计和实现进行修改,这些修改包括:

(1) 预留最大资源,或者为每个安全级别划分并隔离资源,消除可能被用于隐蔽信道的共享资源;

(2) 消除可以导致隐蔽信道的接口、属性、机制.

© 中国科学院软件研究所 http://www.jos.org.cn

这两类修改方式分别是从系统中的可能被用于隐蔽信道的共享资源(*variable* 变量)以及能够感知和修改共享资源属性的操作(PA_h,PV_i 原语)角度出发消除信道.CPU、内存、磁盘、系统时钟等都是容易引发隐蔽信道的共享资源,很多研究关注于如何在不同安全级别用户之间划分资源、隔离用户,避免隐蔽信道[7].

1992 年,Proctor 和 Neumann 曾指出,不仅要从具体的共享资源和操作出发消除隐蔽信道,还应该从整个系统结构、框架的角度出发,寻找解决多级安全中隐蔽信道问题的方法[70].他们认为,单机系统并不是实现多级安全应用的唯一选择.在单机上实现多级安全应用时,不同安全级别间的共享资源众多,包括硬件资源(磁盘等)和软件资源(内核资源、可信进程资源等),需要解决复杂的资源分配问题,因此并不是最佳选择.他们认为,分布式的单级处理器多级安全系统(distributed single-level-processor multilevel-secure,简称 DSM)才是实现多级安全应用的最佳框架.这种框架避免了单机上的隐蔽信道,把问题聚焦在对可信网络接口的设计和实现上,这种方法的复杂性低于多级单机上的资源分配问题.虽然 Proctor 和 Neumann 的观点得到了广泛认可,但是目前可信网络接口的实现仍显复杂,DSM 方案还缺乏真实应用[31].

这类消除隐蔽信道的方案中都需要实施资源隔离措施,这种措施在保障系统安全的同时,也造成了使用不便和无法容忍的性能下降等一系列问题.因此,更多安全应用中放弃了完全消除隐蔽信道,而倾向于通过限制隐蔽信道的传输能力,将信道的威胁降低到系统可以容忍的范围,从而保障系统安全.

5.2 数据冲突隐蔽信道消除方法

数据冲突隐蔽信道是典型的数据库隐蔽信道,完全消除该隐蔽信道,需要利用安全并发控制协议实现不同安全级别事务间的无干扰.在绝对安全得到保障的条件下,需要采取其他措施减少安全并发控制带来的实时性能损失.

George 在 2000 年提出了一种安全实时数据库结构 GUARD[71],如图 6 所示.GUARD 结构要求必须保证事务处理的安全性,消除数据冲突隐蔽信道,因此需要利用安全并发控制协议处理不同安全级别的事务之间的数据冲突,而相同安全级别的事务间冲突则采用实时并发控制协议处理.这样,在 GUARD 结构中同时存在两种并发控制协议,被称作双并发控制方法(dual-CC).另外,GUARD 结构中还采用准入控制方法来保证系统的实时性能.为了弥补安全并发控制对高安全级别事务的不公平性,在准入控制方法中将限制低安全级别事务的准入率.

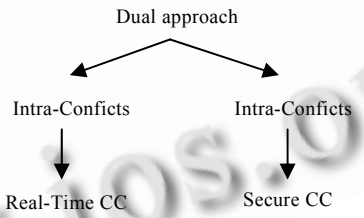

Fig.6 GUARD dual concurrency control

图 6 GUARD 双并发控制示意图

Kang 在 2002 年提出了一种安全实时数据库结构 STAR(security and timeliness assurance in real-time databases)[72].该结构中强调数据库的安全性,认为必须消除隐蔽信道.数据库中,在事务调度和并发控制时优先照顾安全级别低的事务,避免高安全级别事务操作对低安全级别事务的影响,实现了事务之间的无干扰,消除了数据冲突信道.STAR 结构中利用准入控制机制保证系统的实时性,另外还可以采用降低服务质量(quality of service,简称 QoS)的方式保证实时性能.在 STAR 结构中,每个事务都具有两个版本,对应不同的服务质量.两个版本中,当 QoS 级别为 1 时,事务执行需要更长时间,计算结果也更准确,服务质量更高.当系统负载过高时,系统可以降低一些事务的服务质量,从而减少事务的计算消耗,保证事务能够在截止期之前完成.因此,STAR 结构中不同属性要求的重要性排序如下:

安全性>实时性>服务质量,

© 中国科学院软件研究所 http://www.jos.org.cn

其中,只有安全性是严格保证的,实时性只是作为系统的性能指标,需要无条件的为系统安全性让步.

如果想要完全消除数据冲突隐蔽信道,实时性能必须向安全性能让步.TCSEC 安全评估标准中已经指出,如果隐蔽信道的传输能力较低,无法对系统安全构成威胁时,系统可以容忍这样的信道存在.同样,系统也可以采取限制措施约束信道的传输能力,将信道威胁降低到系统的容忍范围以内.因此,这种完全消除数据冲突隐蔽信道的策略并不是必须的,并且缺乏灵活性.

6 隐蔽信道限制方法

不消除隐蔽信道而只对其进行限制,使信道满足安全标准要求,也是信道处置措施的一种选择.Proctor 和 Neumann 曾指出,在如下两种情况下可以不进行隐蔽信道消除操作也能确保系统安全[70]:

(1) 如果系统中没有恶意用户和木马,那么即使隐蔽信道存在也不能被利用,所以系统可以容忍其存在;

(2) 当隐蔽信道的容量小于一定限度,而机密信息的有效时间又较短时,信息即使被泄漏,也不会对系统造成影响,这样的信道也是可以容忍的.

同时,还可以总结出另外一种情况:当隐蔽信道传输中的噪音大到一定程度,信道的信噪比很低.这时,即使入侵者完成了信息传输,但是由于信息的误差较大,可利用价值低,这样的信道也是可以容忍的.

当然,Proctor 和 Neumann 提出的第 1 种情况过于理想化,在实际系统中无法得到保证.只有对信道进行限制,使信道满足容忍条件,系统才能容忍隐蔽信道的存在.因此,限制信道的目标就是要降低信道的传输能力,把信道的威胁限制在系统能够容忍的范围内.

6.1 共享资源信道限制措施

CPU、总线、内存、磁盘、系统时钟等都是容易引发隐蔽信道的共享资源,降低共享资源信道传输能力的方法主要包括几种操作:向信道中添加噪音、在信道中添加延时、直接干扰信道的传输机制和同步机制.

当多个处理器共享总线时,这些处理器操作总线的请求之间存在竞争关系.如果处理器能够确定自己的总线请求的执行速率,则高安全级别用户可以利用总线请求间的竞争关系,影响低安全级别应用所在处理器的请求速率,从而向低安全级别用户传输信息.这种信道称作总线竞争信道.Hu 在 1991 年指出,在当时的系统运算能力下,该信道已经能够达到 1 000bits/s 的速度[52].总线竞争信道属于时间隐蔽信道.在时间信道中,信道使用者依赖参考时钟,以便完成同步、计时等操作.针对总线竞争信道对参考时钟的依赖性,Hu 提出利用“模糊时间”来限制这种信道的方法.模糊时间方法的核心思想是要求避免低安全级别进程访问准确的参考时钟,这里的时钟不仅包括时钟中断,还包括所有能被用来作为时间参考的消息、事件等,特别是异步控制器产生的事件.系统中的这些事件将被安全内核缓存,并在一段随机时间间隔之后再统一发送给接收进程.这样,信道进程的参考时钟被随机打乱,只能获得“模糊”的时间信息.模糊时间方法既增加了信道传输的延时,又通过破坏通信者的同步向信道中添加了噪音,能够有效地降低时间隐蔽信道的容量.但是同时它也具有一些缺点和局限性:

(1) 进程无法获得准确的时间信息,因此,该方法不能用于进程的执行依赖于时间信息的系统,如实时系统等;

(2) 模糊时间方法中,对事件的缓存会放慢不同级别的进程间的同步操作,其中也包括由低级别到高级别的同步操作(即使这种同步是安全的);

(3) 该方法会降低系统的吞吐量,延长系统响应时间,大量的随机数生成操作也会增加额外的性能损失.

Gray 指出,如果系统按照固定时间片(fixed-time-slice)轮换(round robin)执行每个处理器的总线请求,就能够避免处理器间的竞争,以防止其影响总线请求的执行速度,从而消除隐蔽信道.但是在这种隔离方法下,如果某个时间片内对应的处理器没有总线请求,即使别的处理器有正在等待的总线请求,系统仍然将被闲置,造成系统性能的浪费.为了降低这种性能浪费,同时限制信道的威胁,Gray 提出了概率分区隔离法.系统按照一定的概率在安全模式(分区隔离方式)或非安全模式(非分区隔离方式)下工作,系统管理者可以调节概率值,求取系统安全和性能间的均衡[53].与模糊时间方法相比,Gray 的方法具有在限制信道的同时保证进程能够访问准确时钟的优点,节省了大量随机数计算,信道的实际容量计算较容易.该方法也存在一定的缺点,包括只对总线竞争信道

© 中国科学院软件研究所 http://www.jos.org.cn

有效而不能同时限制其他时间隐蔽信道,而且依赖于特殊的硬件(总线接口控制器).

Tsai 和 Gligor 针对操作系统中的几种隐蔽信道分别提出了相应的信道限制方法[44]:

(1) 对于资源耗尽型信道,在资源耗尽的异常报告发送之前插入延迟;

(2) 对于监测动态存储资源分配数的信道,利用随机产生的资源分配请求来向信道中加入噪音;

(3) 对于策略冲突信道,可以在状态报告原语中添加延迟.不过,由于在正常应用中也经常产生状态报告,因此这种添加延迟的方法也会降低系统的性能.可以利用容量计算结果对这些限制措施进行指导.

6.2 Network Pump信道限制设备

美国海军研究实验室(Naval Reserch Laboratory,简称 NRL)的 Network Pump 可以说是目前发展最为完善的隐蔽信道限制设备,该产品经历了 10 多年的发展,现已经被美国海军定型,且获得了相应的专利[73−75].该设备主要用来解决在安全级别不同的机器间的可靠和安全通信问题.在网络中,当具有不同安全级别的主机需要通信时,按照 BLP 模型的要求,只能进行“下读”和“盲上写”两种操作.由于不允许高安全级别主机向低安全级别主机发送确认信息(ACK/NAK),因此传输是低效率的(下读方式)或者不可靠的(盲上写方式).在 TCSEC 标准对隐蔽信道容量允许的范围内发送少量的确认信息,是一种可靠传输的解决方案,但是该方案中连接仍然是低效率的.NRL 的方案中采用特殊的网络设备 Pump 来管理高安全级别主机的确认信息.Pump 基本结构如图 7 所示.

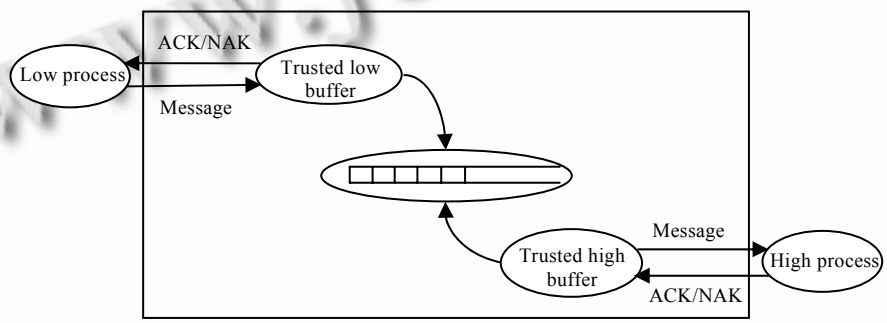

Fig.7 Structure of pump

图 7 Pump 基本结构

在 Pump 中,低级别端的缓存(trusted low buffer,简称 TLF)负责向高级别端发送数据,并向低级别主机/进程发送确认信息.Pump 避免了高级别主机向低级别主机直接发送确认,但是入侵者仍然可以利用 TLF 的反馈信息发送时间来构建时间隐蔽信道.Pump 中通过随机修改 TLF 对低安全级别主机确认的发送时间,向隐蔽信道中添加噪音.利用 Pump 能够提供可靠、快速的通信.通过对噪音干扰下隐蔽信道容量的分析可以证明:Pump 能够将隐蔽信道的传输能力限制到普通传输机制的 $1/n$ 以下,其中,n 是 Pump 中通信缓存(communication buffer)的长度[73].实际应用中,Pump 可以被实现为工作站之间的交换机,或者局域网之间的路由器等.

6.3 阈值模型限制方法

对于安全信息系统而言,隐蔽信道限制措施允许系统制定自己的折衷策略,在系统安全性能与实时性能之间求取均衡.所采取的数据冲突隐蔽信道处置方法中并不要求完全消除信道,而是制定更灵活的安全需求,利用安全并发控制协议处理一部分事务竞争,将信道威胁限制在安全需求允许的范围内;利用实时并发控制协议处理其他的事务竞争,保证实时性能.

为了满足安全性和实时性的要求,数据冲突隐蔽信道限制方法中,需要根据安全需求选择并发控制协议.基于阈值的策略(threshold based protocol selection policy,简称 TBPSP)在已有的限制方法中采用的典型的协议选择策略.

图 8 给出了基于阈值的并发控制协议选择策略的示意图.系统中,安全标准表示为所能容忍的信道威胁阈

© 中国科学院软件研究所 http://www.jos.org.cn

值(danger threshold).TBPSP 中并发控制器将信道的威胁度量结果与标准中的阈值相比较:当信道威胁超过阈值时,控制器将选择安全协议处理事务冲突;否则选择实时协议.文献[50,76]中的信道限制方法就采用了 TBPSP 策略.

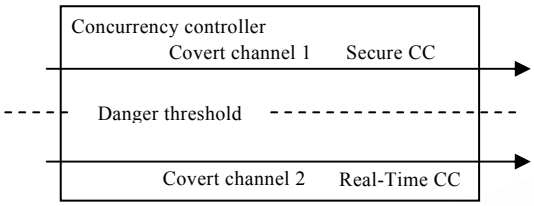

Fig.8 Threshold based protocol selection policy

图 8 基于阈值的并发控制协议选择策略(TBPSP)

6.4 概率模型限制方法

Son 曾提出一种基于概率的 PBPSP 策略(probability based protocol selection policy,简称 PBPSP),如图 9 所示.该策略中,并发控制器不再直接依据威胁阈值选择协议,而是先根据阈值为安全和实时协议设定不同的概率值.当事务发生冲突时,再按照概率选择并发控制协议.系统按照 q 的概率执行安全协议切断信道.另外,用 $p=1-q$ 的概率选择实时协议.概率值 q 的选取必须使系统中所有信道都满足利用信道威胁阈值指定的安全标准[15].

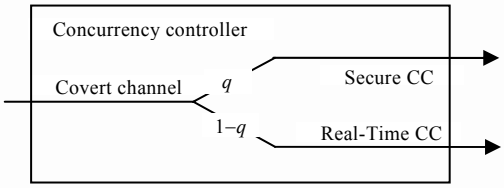

Fig.9 Probability based protocol selection policy

图 9 基于概率的并发控制协议选择策略(PBPSP)

与绝对安全的数据冲突隐蔽信道消除方法对比,TBPSP 和 PBPSP 两个策略有如下优点:

(1) 放宽了完全消除隐蔽信道的要求,只对部分潜在隐蔽信道执行了安全并发控制协议,其余并发控制中选择了有利于实时性能的协议,增加了对实时性能的保护;

(2) 两个策略中的阈值和概率都可以调节,因此安全和实时性能的折衷也是可调节的,策略更加灵活.

对比 TBPSP 和 PBPSP 策略可以认为,TBPSP 只是无信道限制和完全消除信道这两种方式的简单组合.信道度量结果在该策略中只被用来对信道进行区分,并没有起到指导并发协议选择、适度实施信道限制的作用.而 PBPSP 策略不仅能够保证信道的威胁满足阈值限制,还实现了对信道干扰的量化控制.系统不是完全阻止超过威胁阈值的信道,而只是依据概率选择安全协议将信道威胁限制在阈值之下.因此,PBPSP 比 TBPSP 进一步减少了信道限制操作对系统实时性能的影响.

6.5 多概率模型限制方法

分析表明,PBPSP 在限制信道威胁的同时,对实时性能的影响更小.不过,Son 提出的 PBPSP 策略中利用互信息量 I 作为信道威胁度量指标,其度量结果与信道实例的参数无关.因此,其整个系统中只根据单一概率值来指导协议选取[15].与 Son 的方法不同,文献[77]借鉴 PBPSP 策略的思路,提出了基于多概率的并发控制协议选择策略.该协议使用的容量指标 C_t 包含每个信道的时间特性,针对特定信道,并发控制器能够根据容量阈值为信道计算相应的概率值,指导并发控制协议的选择,其结构如图 10 所示.具体实现为,将系统的安全标准用能够容忍的信道容量阈值表示,当不同安全级别事务间发生冲突时,系统采集潜在隐蔽信道的参数,并根据容量阈值计算信道相应的概率值 q_i.概率 q_i 决定了安全协议对信道的干扰程度,称为干扰概率.并发控制器依据概率 q_i 选择安全

© 中国科学院软件研究所 http://www.jos.org.cn

协议,而选择实时协议的概率则是 $1-q_i$.该方法称为基于多概率的并发控制协议选择策略(multiple probabilities based protocol selection policy,简称 MPBPSP).

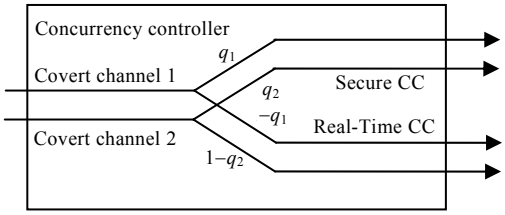

Fig.10 Multi probabi protocol selection policy

图 10 基于多概率的 协议选择策略(MPBPSP)

在使用单一概率值的 PBPSP 策略中,为了确 都能够满足信道威胁阈值的要求,必然按照最坏的情况选取干扰概率.依据这样的概率限制信道威胁 实时性能的浪费.而根据 MPBPSP 选择并发控制协议,信道受到的干扰程度只需要确保其自身指标 标准要求,没有额外的实时性能浪费.因此,较之 PBPSP 策略,MPBPSP 对实时性能的影响更小.另一方面,从入侵者角度看,系统信道限制操作的不确定性增加了,因此该策略还可以提高入侵者绕过系统安全机制的难度.

对比 TBPSP 和 PBPSP,基于多概率并发控制协议选择策略(MPBPSP)中为每一个信道选择相应的干扰概率.利用该策略,安全信息系统能够根据安全标准对信道施加适当的干扰,减少了不必要的性能损失.

6.6 短消息指标限制方法

文献[49]提出了一种新的短消息指标限制策略 SMMP(small message mitigation policy).该策略首先定义了短消息指标约束 SMR(small message restriction):

$$SMR=(N,V_{thres}) \tag{7}$$

其中:

- $N=\{n_1,n_2,...,n_i,...\}$,处于安全级别 i 的用户拥有长度小于 n_i 的数据时适用该约束.N 是这些长度限制的集合;
- V_{thres} 为对用户利用信道传递短消息可以获取的价值的限制阈值;
- SMR 表示系统所容忍的信道威胁.

利用 $SMM(SMM=(ULabel(u_{high}),ULabel(u_{low}),ml,\tau,\rho,V_{high}))$度量用户 u_{high} 与用户 u_{low} 之间隐蔽信道的短消息传输能力.根据 SMR 的要求,当 $ml<N_{high}$ 时,系统需要采取隐蔽信道限制措施,将信道可能传输的短消息价值限制在容忍的范围内,即要求确保

$$V_{high}(\tau,\rho)\leqslant V_{thres} \tag{8}$$

该策略考虑了消息长度参数,将对消息传输时间和保真度的约束归结为对传输消息价值的单一限制.通过将消息价值的初值设定为信道两端的安全级别差别,在指标中引入了消息的敏感程度因素,同时引入短消息传输价值的概念,利用价值阈值统一表示系统对信道短消息传输能力的容忍程度.

同时,文献[49]提出了融合短消息指标和信道容量的并发控制机制 CoCCM(comprehensive concurrency control mechanism).CoCCM 中以执行安全并发控制协议的概率 q 作为限制短消息传输价值 V 和信道容量 C 的参量,如图 11 所示.在该机制中,按照 q 选择安全控制协议和实时控制协议,可以同时兼顾系统的实时性和安全性需求.

CoCCM 机制中的安全标准包括:信道容量标准 C_{thres} 以及系统短消息指标限制策略 SMMP.SMMP 策略中,SMM 指定了不同数据项 d_i 的短消息传输价值函数 $V_i(\rho,\tau)$,SMR 部分包括短消息价值的限制阈值 V_{thres} 以及约束实施条件集合 N.同步控制机制中的实时标准为期望的截止期错失率 $DDMP$.系统中将根据实际情况动态调节 C_{thres},V_{thres} 和 $DDMP$ 这 3 个标准,并按照这些标准确定采用安全控制协议的概率 q.

© 中国科学院软件研究所 http://www.jos.org.cn

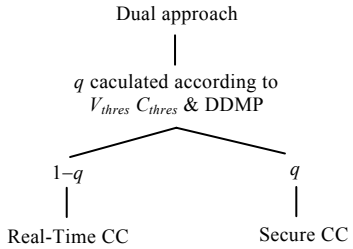

Fig.11 Concurrency control protocol in CoCCM

图 11 CoCCM 中并发控制策略

7 隐蔽信道审计和检测方法

信道审计的目标是威慑已知信道的使用者.它的目的是从系统的众多操作中准确检测隐蔽信道的使用,从而能够明确的对信道使用者进行威慑.审计操作一般需要 3 个步骤:

(1) 确定能够用来检测隐蔽信道使用状况所需的信息,包括共享资源属性信息、针对资源的操作信息等;

(2) 采集并记录系统运行时的这些信息为信道检测服务,并要求信息采集不被旁路,保证采集到完整的信息;

(3) 从记录的信息中检测出每次隐蔽信道使用事件,包括具体的信道使用操作、信道类型、信息的收发双方.

7.1 信道审计方法

Shieh 和 Gligor 在文献[54]中给出了一种存储隐蔽信道的审计方法,隐蔽信道用三元组$\langle variable,PA_h,PV_i\rangle$表示.准确地检测出这种信道的使用需要解决 4 个问题:确定隐蔽信道使用的变量,即 *variable* 变量;区分发送者和接受者;确定某个 TCB 原语是否修改/感知了某个信道变量,即确定 PA_h,PV_i 原语;排除信道审计机制被旁路的可能性.为了解决这些问题,检测隐蔽信道,一切涉及$\langle PA_h,variable\rangle$和$\langle PV_i,variable\rangle$的事件都应该被记录下来.在完备的数据基础上给出了信道的用户检测、组合事件处理、记录中噪音的排除等问题的解决方案,并完成了用于 Secure Xenix 系统的信道审计工具.实验显示,该工具能够检测存储隐蔽信道的使用,并且避免了误报.

文献[78]提出了一种信道审计标准并指出,目前的信道审计标准中只利用信道的容量来描述信道威胁,而忽略了许多其他因素,如安全级别差、带宽敏感参数、发送者安全级、信道的时刻和时段信息等,这些因素都制约着信道的威胁程度.作为对实际信道使用情况的评价,审计信息中应该记录这些因素.

7.2 网络信道检测

最近几年中,网络信道研究领域中对隐蔽信道的检测产生了一系列新的研究成果.网络隐蔽信道同样也包括存储隐蔽信道和时间隐蔽信道这两种类型.

7.2.1 网络存储隐蔽信道检测方法

为了实现隐蔽传输,网络存储隐蔽信道主要利用网络数据包的协议控制部分(一般在包头)或扩展数据部分加载信息,而不是直接利用协议的常规数据部分保存隐蔽信息.附加信息一般保存在包头的保留字段、未用字段和填充字段中.例如:IP 头的 TOS(type of service)[20],DF(don’t fragment)[79]或 TCP 头的标志[20]、RST 字段[80]等等.检测这种类型的信道比较容易,只要对每个数据包的特殊位进行监视,一旦发现这些数据位取值或取异常值,则可确定有利用这些数据位传输信息的隐蔽信道,或至少可以确定该数据包异常[81].

也有的存储隐蔽信道采用包头中的常用字段保存隐蔽信道,如 IP 头中的标识(ID)、生存时间(time to live)字段[82]和 TCP 的初始化序列号(ISN)、时间戳[83]等等.例如:Ahsan 使用 IP 标识的高字节传输,同时随机生成标识的低字段[79];Rowland 将隐蔽信道的每个字节乘以 256^3,并作为 ISN 传输[21].针对这类信道的检测方法,一般通过检验字段值的概率分布是否与自然生成的字段间存在差异,从而判断这些字段值是否被蓄意控制以便传输

© 中国科学院软件研究所 http://www.jos.org.cn

数据[84,85].

NUSHU 就是一种利用 TCP 头部序列号(SEQ)表示隐蔽数据的方法.NUSHU 被实现为 Linux 系统的内核模块,可以在数据包发出之前设置数据包序号.为了增加数据传输的隐蔽性,数据在被放置到 SEQ 字段之前将被加密,以便使观察到的 SEQ 字段接近伪随机过程.检测 NUSHU 信道,需要判断连接中 SEQ 字段是否符合普通系统中序号的产生规律.在普通系统中,为了避免序列号冲突,一般采用较复杂的方式随机生成序列号的初始值 ISN.为了学习这种复杂的序列号产生规律,Tumoian 在其设计的 NUSHU 信道检测器中使用了神经网络技术[86].首先利用普通系统的正常序列号对神经网络中的参数进行训练,在检测过程中,神经网络将对 ISN 进行预测,根据实际 ISN 值和预测结果的相似性度量结果判断是否存在异常.此外,针对使用 IP 标识和 TCP 序列号的网络隐蔽信道,Sohn 也曾提出一种利用支持向量机(support vector machine)技术的检测方法[87].

由于协议头部字段的位数有限,因此,使用协议头部字段保存隐蔽信息的效率也就相对较低.如果能够利用协议的常规数据部分保存隐蔽信息,将有利于提高传输效率.这就需要解决如何在常规数据中隐藏秘密信息的问题.Patel 指出,恶意用户可以采用隐写术(steganography)在网络图片数据上附加隐蔽信息以便进行通信.由于该方法构成了不同用户间隐蔽通信的信道,因此也是一种隐蔽信道[88],并且属于存储隐蔽信道.针对这种信道,Patel 提出了一种网络搜索引擎 STEALTH.该引擎根据一组启发式规则收集网络上可疑的 Web 地址,之后利用信息隐藏分析单元对这些 Web 上的内容进行分析,判断是否有隐藏信息存在.

7.2.2 网络时间隐蔽信道检测方法

网络时间隐蔽信道中,一般使用数据包的发送时刻、发送间隔等特性来表示数据.因此,针对这些信道的检测方法也主要采用针对数据包的这些时间数据进行分析,计算检测指标,并根据指标值判断是否有人使用了隐蔽信道.这些检测指标包括 Cabuk 的数据包间隔方差指标[27]、Berk 的数据包间隔概率分布相似度指标[28]、Gianvecchio 的数据包间隔熵率指标等[29].

2004 年,Cabuk 提出了一种 IP 时间隐蔽信道[27],这种信道被称作 IPCTC(IP covert timing channel).在该信道中,发送者和接收者约定一定的时间段(timing interval).在传输过程中的每个时间段内,发送者向接收者发送一个数据包,或者保持静默,这两种动作分别代表符号 0 和 1,这样就构成了一条二元隐蔽信道.由于这种信道依赖于时钟计时,因此为时间隐蔽信道.如图 12 所示:当发送者希望发出符号 1 时,其将在时间段内发出数据包;如果希望发出符号 0,则不发出数据包.而接收者如果接收到该数据包,则识别符号 1,否则识别符号 0.

Cabuk 认为网络中正常通信中的数据包间隔具有不确定性,而 IPCPC 信道中对数据包发送的时间的蓄意控制,将提高数据包间隔的规律性.基于此结论,Cabuk 设计了标准差度量指标(旨在度量包间隔数据的波动程度)和ε-相似度(ε-Similarity 表示数据中相似数据的比例)度量指标来分析数据包间隔的规律性.

Berk 于 2005 年设计了另外一种网络时间隐蔽信道,这种隐蔽信道利用网络包间的间隔时间(packet interarrival times)表示要传输的数据[28].在如图 13 所示的信道中,发送端使用单位间隔时间 it 表示符号 0,而当需要发送符号 1 时,则确保相邻的两个数据包之间的间隔时间为单位时间的 2 倍,即 $2it$.接收端从收到第 1 次数据包后开始计时,到收到下一个数据包,利用两个数据包之间的间隔时间来判断发送端所发送的数据.

Berk 分析信道的使用者一般经验丰富,能够选择最佳方式,充分利用信道能力发送信息.根据该结论,Berk 提出了一种时间信道检测方法,其中同样使用包间隔数据作为检测依据:

(1) 网络监视器采集每个连接正常使用状态下的包间隔概率分布;

(2) 利用 Arimoto-Blauth 算法计算正常概率分布条件下传输能力最优的输入包间隔概率分布;

(3) 用相似度比较算法检查最优包间隔概率分布和实测包间隔概率分布的相似性,作为信道检测依据.

Berk 还提出了另外一种信道检测方法,他指出,正常传输中包间隔数据的概率密度通常为单峰值,平均值附近概率密度高.而采用偶数个符号的隐蔽信道中其包间隔时间概率密度为偶数个峰值,因此其平均值附近概率密度低.Berk 利用实测的包间隔时间平均值处数据包数 C_μ 与概率密度峰值处数据包数的差距 $1-C_\mu/C_{\max}$ 作为判定隐蔽信道存在的依据.

© 中国科学院软件研究所 http://www.jos.org.cn

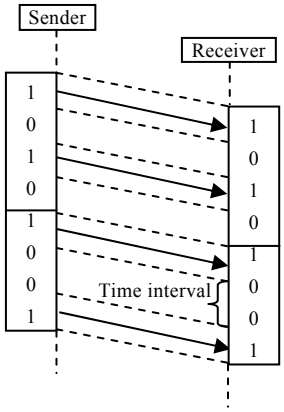

Fig.12 IP covert timing channel of Cabuk's

图 12 Cabuk 的 IP 时间隐蔽信道

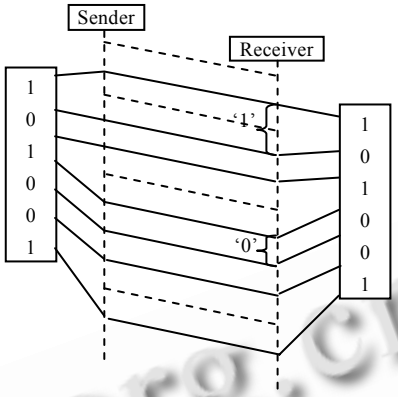

Fig.13 Packets interarrival covert channel of Berk's

图 13 Berk 的 IP 包间隔时间隐蔽信道

Peng 提出使用 Kolmogorov-Smirnov 方法检验一种时间隐蔽信道,称为包间隔水印方法(watermarked inter-packet delays).Kolmogorov-Smirnov 方法能够分析采样数据的概率分布,用来判断两个采样是否一致,或者采样是否符合某种概率分布.Peng 指出,利用包间隔水印方法传输数据时,数据包间隔将呈现出正态分布和平均分布的叠加.其中,正态分布为正常网络传输的效果,而平均分布是水印传输的结果.利用 Kolmogorov-Smirnov 判断实际网络包间隔是否符合以上分布规律,能够检测水印传输.

Gianvecchio 与 Cabuk 的观点相同,认为网络连接中存在时间隐蔽信道时,数据包间隔的规律性将提高.Gianvecchio 提出利用熵率指标度量数据包间隔的规律性,并且提出利用修正条件熵(corrected conditional entropy)克服统计数据不足的缺点,提高熵率计算的准确性[29].

现有的网络时间隐蔽信道检测方法可以归纳为两种类型:形状参数检验(shape)和规律性检验(regularity)[29].其中:形状参数检验主要是分析数据的一阶统计参数,包括平均值、方差以及概率分布;而规律性检验则一般分析数据间相关性,采用二阶或高阶统计量,度量数据的概率分布规律性.具体划分如图 14 所示,其中,Regularity test 指 Cabuk 所采用的规律性检验方法.

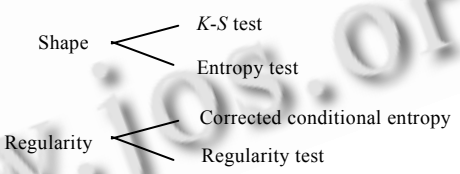

Fig.14 Classification of network covert timing channel detection approach

图 14 网络时间隐蔽信道检测方法分类

7.3 基于冲突间隔检测方法

目前,对数据库中数据冲突隐蔽信道检测方法的研究还比较匮乏.文献[12]提出一种基于隐马尔可夫模型的数据库隐蔽信道检测方法,该方法利用隐马尔可夫模型学习数据库中正常用户的 SQL 操作序列,在运行过程中根据正常用户与隐蔽信道用户行为模式的区别来检测隐蔽信道.该方法主要适用于检测安全数据库中的存储资源信道和管理资源信道,并没有挖掘数据冲突隐蔽信道的特征,不适合对数据冲突隐蔽信道进行检测.

文献[69]提出一种数据冲突隐蔽信道的检测方法,基于冲突间隔时间的信道检测方法(confliction time interval based detection approach,简称 CTIBDA),该方法中使用数据冲突的间隔时间记录作为信道检测的依据.按照主体客体两个不同角度分析数据冲突特征,提高入侵者逃避检测的难度.当根据单一角度组织冲突记录、

© 中国科学院软件研究所 http://www.jos.org.cn

分析冲突特征时,入侵者能够利用分散冲突的方法来逃避检测.由于 CTIBDA 检测方法中没有复杂的学习和运算过程,因此方法具有实施代价低、适用范围广等优点.

在数据库系统中,正常用户的操作往往具有随意性和突发性,事务的发起时间以及事务冲突的间隔时间规律性较差.而在 DC 信道中,入侵者对事务冲突的蓄意控制会影响事务冲突的时间特征,造成冲突间隔时间的规律性增强.因此,可以通过监测事务冲突间隔时间的规律性特征来判断是否发生数据冲突隐蔽信道.

该方法定义了衡量事务冲突规律性的两个指标:冲突间隔分布特征(conflict interval distribution criterion,简称 CIDC)和冲突间隔序列特征(conflict interval sequence criterion,简称 CISC).利用系统运行过程中的事务冲突记录,为每个用户、每个数据计算这些指标,从而判断与用户、与数据有关的事务冲突是否由隐蔽信道引起.

Cabuk 利用标准差构造了一个度量变量随机性的指标[27],CTIBDA 采用同样的指标来度量冲突间隔时间的分布特征.标准差是度量随机变量取值离散程度的指标,标准差值越大,说明变量随机性越强;反之,随机性越弱.给定一组随机过程,X 表示为随机变量的取值序列 $X=\{X_i\}$,其标准差 STDEV 定义为

$$\sigma = STDEV(X) = \sqrt{\frac{\sum_{i=1}^{n}(X_i - \overline{X})^2}{n}} \tag{9}$$

$$CIDC = STDEV\left(\frac{|\sigma_i - \sigma_j|}{\sigma_i}, i < j < sw, \forall i, j\right) \tag{10}$$

CIDC 表示冲突间隔分布指标,为了提高度量的敏感度,该指标首先将 CIT 数据分割大小为 w 的 sw 个不重叠窗口(共包括 $w\times sw$ 条冲突记录),并计算每个窗口内部数据的标准差 σ_n.不同窗口标准差的相对差距(σ_i,σ_j 是两个检测窗口的标准差,二者的相对差距为 $|\sigma_i-\sigma_j|/\sigma_i$)指示相邻窗口间随机分布的差异程度.最后,CIDC 指标取值为这些相对差距的标准差.该指标值越小,说明事务冲突的随机性越弱,规律性越强,发生数据冲突隐蔽信道的可能性越大.

CTIBDA 采用熵率值作为冲突间隔的序列指标来表示冲突间隔规律性.该指标值越低,说明冲突间隔的随机性越弱、规律性越强、系统中发生数据冲突隐蔽信道的可能性越高.

$$CISC = \overline{ER} = \min_{i=1,m}(CCE(X_i \mid X_{i-1})) \tag{11}$$

其中,CCE 是 Porta 等人提出利用修正条件熵(corrected conditional entropy,简称 CCE)[89]

$$CCE(X_m \mid X_{m-1}) = CE(X_m \mid X_{m-1}) + perc(X_m)\cdot EN(X_1) \tag{12}$$

熵率是一个极限概念,是无穷序列的条件熵,表示无穷序列的不确定性.当熵率很小时,说明随机事件前后之间规律性强;当熵率过大时,又说明随机事件之间缺乏关联,事件复杂性高.在实际应用中,只能通过有限的采样数据进行估计[17].由于利用有限数据估计的熵率无法真实反映随机事件的性质,修正条件熵用来解决有限数据采样的问题.其中,$CE(X_m|X_1,\ldots,X_{m-1})$为经验概率密度条件熵,$perc(X_m)$为采样中长度为 m 的序列只出现一次的比例.$EN(X_1)$是序列长度 $m=1$ 时的熵,即一阶熵.

这两个指标的指示作用分别为:

(1) 冲突间隔分布指标 CIDC 越小,事务冲突随机性越弱、规律性越强、发生隐蔽信道的可能性越大;

(2) 冲突间隔序列指标 CISC 越小,事务冲突随机性越弱、规律性越强、发生隐蔽信道的可能性越大.

利用这两个指标检测信道时,首先需要对系统正常状态下的指标值进行计算,确定指标检测阈值.以指标 CIDC 为例,利用大量系统正常状态下的冲突记录确定指标值的取值范围,可获得正常状态下指标值的下限为 $ThreshCIDC$,即系统正常时指标值满足 $CIDC\geqslant ThreshCIDC$.当系统的检测窗口中计算的指标值低于该阈值时,说明系统中可能发生了隐蔽信道.利用 CISC 检测隐蔽信道时也需要确定相应的阈值 $ThreshCISC$.

为了同时利用两个指标检测信道,该方法还设计了两个指标融合的策略,融合规则是只要有一个或一个以上指标指示系统异常时,就认为系统中可能发生了隐蔽信道.

CTIBDA 方法采用的指标结构简单,不需要复杂的学习过程,检测过程中也不需要复杂的运算,适合在线实施.基于 CTIBDA,系统可以获得准确的隐蔽信道使用者和中间数据信息,从而能主动针对隐蔽信道施加限制,避

© 中国科学院软件研究所 http://www.jos.org.cn

免了对潜在隐蔽信道采用普遍消除和限制带来的性能消耗.CTIBDA 方法中没有依赖于安全数据库系统的专有属性,对于检测并发冲突产生的隐蔽信道具有广泛适用性.

7.4 其他检测方法

文献[90]提出一种检测时间隐蔽信道的方法,称为时域恶意主体检测法(identify malicious subjects in the time domain,简称 IMS).IMS 方法中首先需要枚举可能引用或修改客体的主体,以及可能被修改和引用的客体,并将这些主客体记录于矩阵,然后进行关键的一步:对每个客体进行检查,看其是否被用于从高安全级别向低安全级别传输信息.最后,利用这些矩阵记录的结果计算信道的容量.该方法形式简单,在完成信道检测的同时能够获得相应的容量结果.不过,该方法存在构建矩阵工作量大、检测分析准确性难以保证的缺点.

8 总 结

对于安全信息系统来说,机密信息的泄漏将会造成无法挽回的损失.对于隐蔽信道这种危害性极强的信息泄漏途径,必须做到提前预防、尽早发现、及时处理,以保证信息的安全.随着对隐蔽信道研究的逐步深入,隐蔽信道分析技术也逐渐成熟.为了保证系统安全,降低隐蔽信道的危害,未来的系统开发应该更注重设计阶段的形式化描述,从源头上减小隐蔽信道发生的可能性.同时,要规范系统实现过程,严格按照形式化描述,尽最大可能消除代码中引入的潜在隐蔽信道.对于形式化描述中已发现但是无法彻底消除的潜在隐蔽信道,必须加入审计机制,并尽可能将其限制在系统能够容忍的范围内.对于已经存在的系统,例如安全网络系统中,隐蔽信道研究应该更注重对现有系统的审计与检测,发现被应用的隐蔽信道并及时反馈以采取进一步的消除和限制措施.

隐蔽信道本质上是一种通信信道,可以用$\langle variable,PA_h,PV_i\rangle$三元组表示.虽然隐蔽信道的识别、度量、处置的具体实现有各种不同的方法,但实质上是对该三元组的分析与刻画.信道识别是搜索 *variable* 变量和 PA_h,PV_i 原语的过程,从不同的研究角度出发,产生了一系列的识别方法.信道度量评估 PA_h,PV_i 之间的通信能力,度量结果作为信道处置的参考.处置措施根据度量的结果决定采取消除措施或者限制措施,当有能力破坏 *variable* 变量和 PA_h,PV_i 原语的存在条件时,则要不遗余力地消除信道.当无法彻底消除时则要采取限制措施,将信道的传输能力限制在系统能够容忍的范围内.信道审计和检测要求记录所有$\langle variable,PA_h,PV_i\rangle$信息,从中发现入侵者实际使用的信道,并反馈给度量和处置作为参考,以采取进一步的措施威慑入侵者.

自从 Lampson 的开创性工作以来,隐蔽信道的研究已经实现了从程序到单机、从单机到网络的飞跃,即使在云计算平台中,仍然存在着隐蔽信道的威胁[91].网络隐蔽信道已经成为当前信息安全的热点研究领域[92,93].相比传统的单机隐蔽信道,网络隐蔽信道更容易受到网络延迟、网络抖动等噪音的影响.因此,网络隐蔽信道的编码、传输和解码技术以及同步机制将会是未来一段时期的研究重点[94,95].

本文从隐蔽信道的研究历史、研究领域和技术组成出发,根据存储隐蔽信道和时间隐蔽信道分类,从信道识别、度量、消除、限制、审计和检测几个技术层面综述了隐蔽信道研究中经典的技术和方法,总结了隐蔽信道 30 多年来的研究成果.本文试图为该研究方向勾画出一个较为全面和清晰的概貌,为隐蔽信道分析领域的研究者提供有益的参考.

References:

[1] U.S.Department of Defense. Trusted computer system evaluation criteria. DoD 5200.28-STD, 1985.

[2] GB 17859-1999. Classified oriteria for security protection of computer information system. 2001 (in Chinese).

[3] ISO/IEC 15408. Information technology-security techniques-evaluation criteria for IT security. 1999.

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

[5] Lipner SB. A comment on the confinement problem. Operating Systems Review, 1975,9(5):192−196. [doi:10.1145/1067629.806537]

[6] Simmons GJ. The prisoners' problem and the subliminal channel. In: Proc. of the CRYPTO'83—Advances in Cryptology. 1984. 51−67. http://www.cs.nccu.edu.tw/~raylin/.../Spring2009/ThePrisonerProblem.pdf

[7] National Computer Security Center. A guide to understanding covert channel analysis of trusted systems. NCSC-TG-30, 1993.

© 中国科学院软件研究所 http://www.jos.org.cn

[8] Tsai CR, Gligor VD, Chandersekaran CS. A formal method for the identification of covert storage channels in source code. In: Proc. of the IEEE Symp. on Security and Privacy. 1987. 74−87. http://www.computer.org/portal/web/csdl/doi/10.1109/SP.1987.10014

[9] Bell DE, Lapadula LJ. Secure computer systems: Mathematical foundations. Vol.1: Hanscom AFB, Bedford, FSD-TR-73-278, ESD/AFSC, 1973. 1−33.

[10] Kemmerer RA. Shared resource matrix methodology: An approach to identifying storage and timing channels. ACM Trans. on Computer System, 1983,1(3):256−277. [doi: 10.1145/357369.357374]

[11] Joon S, Jim AF. A formal framework for real-time information flow analysis. Computers & Security, 2009,28(6):421−432.

[12] Cui BG. Research on covert channel analysis and related techniques in secure database system [Ph.D. Thesis]. Harbin: Harbin Engineering University, 2006 (in Chinese with English abstract).

[13] Jensen NR. Implications of multilevel systems on the data dictionary of a secure relational DBMS. In: Proc. of the 4th Aerospace Computer Security Applications Conf. 1988. 58−65. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=113418

[14] He YZ, Li L, Feng DG. A generic audit policy model on multilevel secure DBMS. Journal of Software, 2005,16(10):1774−1783 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/16/1774.htm [doi: 10.1360/jos161774]

[15] Son SH, Mukkamala R, David R. Integrating security and real-time requirements using covert channel capacity. IEEE Trans. on Knowledge and Data Engineering, 2000,12(6):865−879. [doi: 10.1109/69.895799]

[16] Keefe TF, Tsai WT, Srivastava J. Database concurrency control in multilevel secure database management systems. IEEE Trans. on Knowledge and Data Engineering, 1993,5(6):1039−1055. [doi: 10.1109/69.250090]

[17] Dong QK. Study on subliminal channels [Ph.D. Thesis]. Xi'an: Xidian University, 2003 (in Chinese with English abstract).

[18] Zhu JF. Study on covert channel analyhsis in high-level secure operating system [Ph.D. Thesis]. Beijing: Graduate School, the Chinese Academy of Sciences, 2006 (in Chinese with English abstract).

[19] Girling CG. Covert channels in LAN's. IEEE Trans. on Software Engineering, 1987,SE-13(2):292−296. [doi: 10.1109/TSE.1987.233153]

[20] Handel TG, Sandford MT. Hiding data in the OSI network model. Information Hiding, 1996,1174:23−38.

[21] Rowland CH. Covert channels in the TCP/IP protocol suite. Peer Reviewed Journal on the Internet, 1997,2(5):1.

[22] Gianvecchio S, Wang H, Wijesekera D, Jajodia S. Model-Based covert timing channels: Automated modeling and evasion. Recent Advances in Intrusion Detection, 2008,5230:211−230. [doi: 10.1007/978-3-540-87403-4_12]

[23] Luo XP, Chan EWW, Chang RKC. TCP covert timing channels: Design and detection. In: Proc. of the Int'l Conf. on Dependable Systems & Networks. 2008. 420−429. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4630112

[24] Zander S, Armitage G, Branch P. Covert channels and countermeasures in computer network protocols. IEEE Communications Magazine, 2007,45(12):136−142. [doi: 10.1109/MCOM.2007.4395378]

[25] Zander S, Armitage G, Branch P. Covert channels in multiplayer first person shooter online games. In: Proc. of the 33rd IEEE Conf. on Local Computer Networks. 2008. 215−222. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4664172

[26] Sun XM, Huang HJ, Wang BW, Sun G, Huang JW. An algorithm of webpage information hiding based on equal tag. Journal of Computer Research and Development, 2007,44(5):756−760 (in Chinese with English abstract).

[27] Cabuk S, Brodley CE, Shields C. IP covert timing channels: Design and detection. In: Proc. of the 11th ACM Conf. on Computer and Communications Security. 2004. 178−187. http://portal.acm.org/citation.cfm?id=1030083.1030108

[28] Berk V, Giani A, Cybenko G. Detection of covert channel encoding in network packet delays. Technical Report, TR2005536, Department of Computer Science, Dartmouth College, 2005. 1−11.

[29] Gianvecchio S, Wang HN. Detecting covert timing channels: An entropy-based approach. In: Proc. of the 14th ACM Conf. on Computer and Communications Security. 2007. 307−316. http://www.cs.wm.edu/~hnw/paper/ccs07.pdf

[30] Qian XL, Stickel ME, Karp PD, Lunt TF, Garvey TD. Detection and elimination of inference channels in multilevel relational database systems. In: Proc. of the IEEE Symp. on Security and Privacy. Oakland, 1993. 196−205. http://www.computer.org/portal/web/csdl/doi/10.1109/RISP.1993.287632

[31] Millen J. 20 years of covert channel modeling and analysis. In: Proc. of the IEEE Symp. on Security and Privacy. Oakland, 1999. 113−114. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=766906

© 中国科学院软件研究所 http://www.jos.org.cn

[32] Denning DE. A lattice model of secure information flow. Communications of the ACM, 1976,19(5):236−243. [doi:10.1145/360051.360056]

[33] Goguen JA, Meseguer J. Security policies and security models. In: Proc. of the IEEE Symp. on Security and Privacy. 1982. 11−20. http://www.cs.ucsb.edu/~kemm/courses/cs177/noninter.pdf

[34] Millen JK. Finite-State noiseless covert channels. In: Proc. of the Computer Security Foundations Workshop II. 1989. 81−86. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=40590

[35] Eckmann ST. Eliminating formal flows in automated information flow analysis. In: Proc. of the IEEE Symp. on Security and Privacy. 1994. 30−38. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=296594

[36] Volpano D, Smith G, Irvine C. A sound type system for secure flow analysis. Journal of Computer Security, 1996,4(2):167−187.

[37] Goguen JA, Meseguer J. Unwinding and inference control. In: Proc. of the IEEE Symp. on Security and Privacy. 1984. 75−87. http://www.computer.org/portal/web/csdl/doi/10.1109/SP.1984.10019

[38] Haigh JT, Kemmerer RA, Mchugh J, Young WD. An experience using two covert channel analysis techniques on a real system design. IEEE Trans. on Software Engineering, 1987,13(2):157−168. [doi: 10.1109/TSE.1987.226479]

[39] Mchugh J. Covert channel analysis: A chapter of the handbook for the computer security certification of trusted systems. Department of Computer Science, Portland State University, 1996. 1−78. http://chacsnrlnavymil/publications/handbook

[40] Kemmerer RA, Porras PA. Covert flow trees: A visual approach to analyzing covert storage channels. IEEE Trans. on Software Engineering, 1991,17(11):1166−1185. [doi: 10.1109/32.106972]

[41] Tsai CR. Covert channel analysis in secure computer systems [Ph.D. Thesis]. Maryland: University of Maryland-College Park (MD), 1987.

[42] Tsai CR, Gligor VD, Chandersekaran CS. On the identification of covert storage channels in secure systems. IEEE Trans. on Software Engineering, 1990,16(6):569−580. [doi: 10.1109/32.55086]

[43] Shen JJ. Research on information flow technologies and security architecture of secure operating system [Ph.D. Thesis]. Beijing: Graduate University, the Chinese Academy of Sciences, 2008 (in Chinese with English abstract).

[44] Tsai CR, Gligor VD. A bandwidth computation model for covert storage channels and its applications. In: Proc. of the IEEE Symp. on Security and Privacy. 1988. 108−121. http://www.computer.org/portal/web/csdl/doi/10.1109/SECPRI.1988.8103

[45] Diggavi SN, Grossglauser M. Bounds on the capacity of deletion channels. In: Proc. of the IEEE Int'l Symp. on Information Theory. 2002. 421−421. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1023693

[46] Tallini LG. Bounds on the capacity of the unidirectional channels. IEEE Trans. on Computers, 2005,54(2):232−235. [doi: 10.1109/TC.2005.18]

[47] Zeng W, Tokas J, Motwani R, Motwani R, Kavcic A. Bounds on mutual information rates of noisy channels with timing errors. In: Proc. of the Int'l Symp. on Information Theory. 2005. 709−713. http://www-ee.eng.hawaii.edu/~alek/Archive/2005/isit05.pdf

[48] Moskowitz IS, Kang MH. Covert channels—Here to stay? In: Proc. of the 9th Annual Conf. on Computer Assurance (COMPASS 1994) 'Safety, Reliability, Fault Tolerance, Concurrency and Real Time, Security'. 1994. 235−243. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=318449

[49] Zeng HT, Wang YJ, Zu W, Cai JY, Ruan L. New definition of small message criterion and its application in transaction covert channel mitigating. Journal of Software, 2009,20(4):985−996 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3246.htm [doi: 10.3724/SP.J.1001.2009.03246]

[50] Ahmed QN, Vrbsky SV. Maintaining security and timeliness in real-time database system. Journal of Systems and Software, 2002, 61(1):15−29. [doi: 10.1016/S0164-1212(01)00111-X]

[51] Joon S, Jim AF. Covert timing channel analysis of rate monotonic real-time scheduling algorithm in MLS systems. In: Proc. of the IEEE Workshop on Information Assurance United States Military Academy. 2006. 361−368. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1652117

[52] Hu WM. Reducing timing channels with fuzzy time. In: Proc. of the IEEE Computer Society Symp. on Research in Security and Privacy. 1991. 8−20. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=130768

[53] Gray JW. On introducing noise into the bus-contention channel. In: Proc. of the IEEE Symp. on Security and Privacy. Oakland, 1993. 90−98. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=287640

© 中国科学院软件研究所 http://www.jos.org.cn

[54] Shieh SPW, Gligor VD. Auditing the use of covert storage channels in secure systems. In: Proc. of the IEEE Computer Society Symp. on Research in Security and Privacy. 1990. 285−295. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=63858

[55] Qing SH. Covert channel analysis in secure operating systems with high security levels. Journal of Software, 2004,15(12): 1837−1849 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/15/1837.htm

[56] He JS, Gligor VD. Information-Flow analysis for covert-channel identification in multilevel secure operating systems. In: Proc. of the Computer Security Foundations Workshop III. 1990. 139−148. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=128194

[57] Zi XC, Yao LH, Li L. A state-based approach to information flow analysis. Chinese Journal of Computers, 2006,29(8):1460−1467 (in Chinese with English abstract).

[58] Qing SH, Zhu JF. Covet channel analysis on ANSHENG secure operating system. Journal of Software, 2004,15(9):1385−1392 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/15/1385.htm

[59] Fine T. Constructively using noninterference to analyze systems. In: Proc. of the IEEE Computer Society Symp. on Research in Security and Privacy. 1990. 162−169. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=63847

[60] Shieh SP. Estimating and measuring covert channel bandwidth in multilevel secure operating systems. Journal of Information Science and Engineering, 1999,15(1):91−106.

[61] Moskowitz IS. Variable noise effects upon a simple timing channel. In: Proc. of the IEEE Computer Society Symp. on Research in Security and Privacy. 1991. 362−372. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=130803

[62] Moskowitz IS, Miller AR. The channel capacity of a certain noisy timing channel. IEEE Trans. on Information Theory, 1992,38(4): 1339−1344. [doi: 10.1109/18.144712]

[63] Moskowitz IS, Greenwald SJ, Kang MH. An analysis of the timed Z-channel. In: Proc. of the IEEE Symp. on Security and Privacy. 1996. 2−11. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=502664

[64] Wang ZH, Lee RB. Capacity estimation of non-synchronous covert channels. In: Proc. of the 25th IEEE Int'l Conf. on Distributed Computing Systems Workshops. 2005. 170−176. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1437172

[65] Wang ZH, Lee RB. New constructive approach to covert channel modeling and channel capacity estimation. In: Proc. of the 8th Information Security Conf. 2005. 498−505. http://palms.ee.princeton.edu/PALMSopen/ISC05_w_cit.pdf

[66] Lanotte R, Maggiolo-Schettini A, Tini S, Troina A, Tronci E. Automatic covert channel analysis of a multilevel secure component. In: Proc. of the Information and Communications Security. 2004. 249−261. http://www.springerlink.com/content/r8fkgckuew0l9mgr/

[67] Liu CL, Layland JW. Scheduling algorithms for multiprogramming in a hard-real-time environment. Journal of the Association for Computing Machinery, 1973,20(1):46−61.

[68] Wang YJ, Chen QP. On schedulability test of rate monotonic and its extendible algorithms. Journal of Software, 2004,15(6): 799−814 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/15/799.htm

[69] Zeng HT. Research on covert channel measurement and handling in secure real-time database [Ph.D. Thesis]. Beijing: Graduate University, the Chinese Academy of Sciences, 2008 (in Chinese with English abstract).

[70] Proctor NE, Neumann PG. Architectural implications of covert channels. In: Proc. of of the 15th National Computer Security Conf. 1992. 28−43. http://www.csl.sri.com/users/neumann/ncs92.html

[71] George B, Haritsa JR. Secure concurrency control in firm real-time database systems. Distributed and Parallel Databases, 2000,8(1): 41−83. [doi: 10.1023/A:1008783216944]

[72] Kang KD, Son SH, Stankovic JA. STAR: Secure real-time transaction processing with timeliness guarantees. In: Proc. of the 23rd IEEE Real-Time Systems Symp. (RTSS 2002). 2002. 303−314. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1181584

[73] Kang MH, Moskowitz IS. A pump for rapid, reliable, secure communication. In: Proc. of the 1st ACM Conf. on Computer and Communications Security. 1993. 119−129. http://portal.acm.org/citation.cfm?id=168604

[74] Kang MH, Moskowitz IS, Lee DC. A network pump. IEEE Trans. on Software Engineering, 1996,22(5):329−338. [doi: 10.1109/32.502225]

[75] Kang MH, Moskowitz IS, Chincheck S. The pump: A decade of covert fun. In: Proc. of the 21st Annual Computer Security Applications Conf. (ACSAC 2005). 2005. 352−360. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1565262

© 中国科学院软件研究所 http://www.jos.org.cn

[76] Son SH, David R, Thuraisingham B. Improving timeliness in real-time secure database systems. SIGMOD Record, 1996,25(1): 29−33.

[77] Zeng HT, Wang YJ, Ruan L, Zu W, Cai JY. Covert channel mitigation method for secure real-time database using capacity metric. Journal on Communications, 2008,20(8):46−56 (in Chinese with English abstract).

[78] Wang CD, Ju SG. Integrated criteria for covert channel auditing. Journal of Zhejiang University—Science A, 2008,9(6):737−743. [doi: 10.1631/jzus.A071510]

[79] Ahsan K, Kundur D. Practical data hiding in TCP/IP. In: Proc. of the ACM Wksp. Multimedia Security, 2002. 1−8.

[80] Fisk G, Fisk M, Papadopoulos C, Neil J. Eliminating steganography in Internet traffic with active wardens. In: Proc. of the Revised Papers from the 5th Int'l Workshop on Information Hiding. 2002. 18−35. http://portal.acm.org/citation.cfm?id=732023

[81] Kwecka Z. Application layer covert channel analysis and detection. Edinburgh: Napier University, 2006. http://www.buchananweb.co.uk/zk.pdf

[82] Zander S, Armitage G, Branch P. Covert channels in the IP time to live field. In: Proc. of the Australian Telecommunication Networks and Application Conf. (ATNAC 2006). 2006. 298−302. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.85.1442&rep=rep1&type=pdf

[83] Giffin J, Greenstadt R, Litwack P, Tibbetts R. Covert messaging through TCP timestamps. In: Proc. of the Privacy Enhancing Technologies. 2003. 189−193. http://www.springerlink.com/content/4d5jy0ewplea12d4/

[84] Eraser SA. An exploit-specific monitor to prevent malicious communication channel. Technical Report, GIT-CERCS-04-28, Georgia Institute of Technology, 2004. 1−12.

[85] Murdoch SJ, Lewis S. Embedding covert channels into TCP/IP. In: Proc. of the Information Hiding. 2005. 247−261. http://www.cl.cam.ac.uk/~sjm217/papers/ih05coverttcp.pdf

[86] Tumoian E, Anikeev M. Network based detection of passive covert channels in TCP/IP. In: Proc. of the 30th IEEE Conf. on Local Computer Networks Anniversary (LCN 2005). 2005. 802−809. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber= 1550966

[87] Sohn T, Seo JT, Moon J. A study on the covert channel detection of TCP/IP header using support vector machine. Information and Communications Security, 2003,2836:313−324. [DOI: 10.1007/978-3-540-39927-8_29]

[88] Patel A, Shah M, Chandramouli R, Subbalakshmi KP. Covert channel forensics on the Internet: Issues, approaches, and experiences. Int'l Journal of Network Security, 2007,5(1):41−50.

[89] Porta A, Baselli G, Liberati D, Montano N, Cogliati C, Gnecchi-Ruscone T, Malliani A, Cerutti S. Measuring regularity by means of a corrected conditional entropy in sympathetic outflow. Biological Cybernetics, 1998,78(1):71−78. [doi: 10.1007/ s004220050414]

[90] Wang CD, Ju SG. Searching covert channels by identifying malicious subjects in the time domain. In: Proc. of the IEEE Wksp. on Information Assurance United States Military Academy. 2004. 68−73. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1437799

[91] Ristenpart T, Tromer E, Shacham H, Savage S. Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds. In: Proc. of the 16th ACM Conf. on Computer and Communications Security. 2009. 199−212. http://portal.acm.org/citation.cfm?id=1653662.1653687

[92] Sellke SH, Wang CC, Bagchi S, Shroff N. TCP/IP timing channels: Theory to implementation. In: Proc. of the 28th Conf. on Computer Communications (INFOCOM). 2009. 2204−2212. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5062145

[93] Cabuk S, Brodley CE, Shields C. IP covert channel detection. ACM Trans. on Information and System Security, 2009,12(4):1−29. [doi: 10.1145/1513601.1513604]

[94] Kiyavash N, Coleman T. Covert timing channels codes for communication over interactive traffic. In: Proc. of the IEEE Int'l Conf. on Acoustics, Speech, and Signal Processing. 2009. 1485−1488. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4959876

[95] Ji LP, Jiang WH, Dai BY, Niu XM. A novel covert channel based on length of messages. In: Proc. of the Int'l Symp. on Information Engineering and Electronic Commerce. 2009. 551−554. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5175179

© 中国科学院软件研究所 http://www.jos.org.cn

附中文参考文献:

[2] GB17859-1999.计算机信息系统安全保护等级划分准则.2001.

[12] 崔宾阁.安全数据库系统隐通道分析及相关技术研究[博士学位论文].哈尔滨:哈尔滨工程大学,2006.

[14] 何永忠,李斓,冯登国.多级安全DBMS的通用审计策略模型.软件学报,2005,16(10):1774−1783. http://www.jos.org.cn/1000-9825/16/1774.htm [doi: 10.1360/jos161774]

[17] 董庆宽.阈下信道技术研究[博士学位论文].西安:西安电子科技大学,2003.

[18] 朱继峰.高安全级操作系统隐蔽信道分析技术研究[博士学位论文].北京:中国科学院研究生院,2006.

[26] 孙星明,黄华军,王保卫,孙光黄,俊伟.一种基于等价标记的网页信息隐藏算法.计算机研究与发展,2007,44(5):756−760.

[43] 沈建军.安全操作系统信息流技术与安全架构研究[博士学位论文].北京:中国科学院研究生院,2008.

[49] 曾海涛,王永吉,祖伟,蔡嘉勇,阮利.短消息指标新定义及在事务信道限制中的应用.软件学报,2009,20(4):985−996. http://www.jos.org.cn/1000-9825/3246.htm [doi:10.3724/SP.J.1001.2009.03246]

[55] 卿斯汉.高安全等级安全操作系统的隐蔽通道分析.软件学报,2004,15(12):1837−1849. http://www.jos.org.cn/1000-9825/15/1837.htm

[57] 訾小超,姚立红,李斓.一种基于有限状态机的隐含信息流分析方法.计算机学报,2006,29(8):1460−1467.

[58] 卿斯汉,朱继锋.安胜操作系统的隐蔽信道分析.软件学报,2004,15(9):1385−1392. http://www.jos.org.cn/1000-9825/15/1385.htm

[68] 王永吉,陈秋萍.单调速率及其扩展算法的可调度性判定.软件学报,2004,15(6):799−814. http://www.jos.org.cn/1000-9825/15/799.htm

[69] 曾海涛.安全实时数据库隐蔽信道度量和处理技术研究[博士学位论文].北京:中国科学院研究生院,2008.

[77] 曾海涛,王永吉,阮利,祖伟,蔡嘉勇.使用容量指标的安全实时数据库信道限制方法.通信学报,2008,29(8):46−56.

王永吉(1962－),男,辽宁营口人,博士,研究员,博士生导师,CCF 高级会员,主要研究领域为实时系统,网络优化,智能软件工程,优化理论,信息系统安全,控制理论.

丁丽萍(1965－),女,博士,研究员,主要研究领域为信息安全,操作系统,计算机取证,软件工程.

吴敬征(1982－),男,博士生,主要研究领域为隐蔽信道分析,网络信息安全,安全操作系统.

廖晓锋(1981－),男,博士生,主要研究领域为信息检索,机器学习,统计学习,图像理解.

曾海涛(1979－),男,博士,主要研究领域为操作系统安全,数据库安全,实时系统.

© 中国科学院软件研究所 http://www.jos.org.cn