doi :10.3969/j.issn.1671-1122.2012.08.047

网络时间隐蔽信道研究

汪婧，高能，林璟锵，管乐

（中国科学院信息工程研究所信息安全国家重点实验室，北京 100195）

摘 要：文章首先介绍隐蔽信道的基本概念以及网络隐蔽信道的研究现状，然后着重总结几种典型的网络时间隐蔽信道，最后综述网络时间隐蔽信道领域中经典的防御技术和方法。文章试图为该研究方向勾勒出一个较为全面的概貌，为该领域的研究人员提供有益的参考。

关键词：信息安全；隐蔽信道；网络时间隐蔽信道

中图分类号：TP393.08 文献标识码：A 文章编号：1671-1122（2012）08-0160-04

A Survey of Network-based Covert Timing Channels

WANG Jing, GAO Neng, LIN Jing-Qiang, GUAN Le

(*State Key Laboratory of Information Security, Institute of Information Engineering, The Chinese Academy of Sciences, Beijing* 100195, *China*)

Abstract: This paper firstly introduces the concept of covert channel, and then gives an overview of network-based covert channels. Next, it summarizes several typical network-based covert timing channels. Finally, it surveys the classic countermeasures in the field of network-based covert timing channels. This paper attempts to give a comprehensive outline for this research direction, and provides a useful reference for the researchers.

Key words: information security; covert channel; network-based covert timing channel

1 隐蔽信道基本概念

1.1 隐蔽信道定义

隐蔽信道的概念最初由 Lampson 在 1973 年提出[1]，其给出的隐蔽信道定义为本意不是用来传送信息的通信信道。在这篇开创性的文章中，Lampson 列举了 7 种泄露信息的方法，并建立了一套限制程序的规则以应对这些泄露方法。自 Lampson 首次提出隐蔽信道概念以来，研究人员针对隐蔽信道给出了多种不同的定义。TCSEC[2] 对隐蔽信道的定义是：允许进程以违背系统安全策略的形式传送信息的通信信道。Tsai 等人[3] 给出的隐蔽信道定义较为全面：给定一个强制安全策略模型 M 以及其在一个操作系统中的解释 I(M)，I(M) 中两个主体 I(Sh) 和 I(Si) 之间的潜在通信是隐蔽的，当且仅当模型 M 中主体 Sh 和 Si 之间的通信是非法的。

1.2 隐蔽信道分类

目前，隐蔽信道的分类方法有很多相关研究成果，其中在学术界认可度最高、使用频率最高的分类方法是根据共享资源属性划分，分为存储隐蔽信道和时间隐蔽信道。

存储隐蔽信道：发送者直接或间接写目标值，接收者直接或间接读目标值。

时间隐蔽信道：发送者通过时域上调制使用资源（例如 CPU）发送信息，接收者能够观测到并对信息进行解码。

与存储隐蔽信道相比，时间隐蔽信道又称为无记忆通道，它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，否则传送的信息就会消失。

1.3 隐蔽信道通信模型

1983 年，Simmons 通过研究囚犯问题引入了阈下信道的概念[4]。文中 Simmons 给出了经典的隐蔽通信实际模型：Alice 和 Bob 是两个被关押的囚犯，看守人 Wendy 监视着他们的一言一行。他们计划逃出监狱，必须秘密协商逃跑的计划，因为 Wendy 一旦发现有异常行为就会将他们单独囚禁，这会导致逃跑计划失败。图 1 描述了囚犯问题。

收稿时间：2012-07-12

基金项目：国家自然科学基金 [70890084、G021102]、中国科学院战略性先导专项子课题海云信息安全共性关键技术研究 [XDA06010702]

作者简介：汪婧（1986-），女，浙江，博士研究生，主要研究方向：网络与系统安全；高能（1976-），女，陕西，副教授，博士，主要研究方向：信息对抗理论与技术；林璟锵（1978-），男，福建，助理研究员，博士，主要研究方向：网络与系统安全；管乐（1987-），男，陕西，博士研究生，主要研究方向：网络与系统安全。

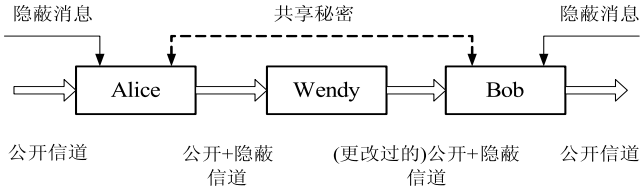

图1 囚犯问题

1996 年，Handel 将这一模型引入计算机网络中，Alice 和 Bob 使用了两台联网的计算机用于通信 [5]。他们之间可以建立一条看似无害的公开通信信道，但实际上在公开信道中隐藏了一条隐蔽信道，用于传递私密信息。Alice 和 Bob 共享着一套机制，用于确定隐蔽信道的编码参数以及加密和鉴别隐藏的信息。Alice 和 Bob 有可能是同一人，较为常见的一个情景是黑客控制已被攻破的主机给自己传递受限信息。Wendy 可以监控整个网络流量，甚至能够更改流量以消除或扰乱隐蔽信道。

2 网络隐蔽信道研究现状

起初，隐蔽信道被认为是单机系统的安全威胁，大部分有关于隐蔽信道的研究都是针对多级安全系统的。随着计算机网络的繁荣发展，隐蔽信道的焦点渐渐转移到计算机网络协议上。计算机网络公开信道，如网络协议，可用作隐蔽信道的载体。由于因特网拥有巨大的通信量以及多种通信协议，这使得它成为隐蔽信道理想的高带宽传输媒介。随着网络技术的高速发展，网络隐蔽信道的信道容量也随之大幅提升，而且这一趋势很有可能继续。

根据传统隐蔽信道的划分方法，网络隐蔽信道也包括存储隐蔽信道以及时间隐蔽信道。

2.1 网络存储隐蔽信道

网络存储隐蔽信道通常在网络协议的数据包中隐藏信息，例如 TCP/IP、HTTP 等协议。这些协议的数据包中可以用于传送隐蔽信息的字段包括：未使用或预留的 IP 头字段（包括 TOS 字段、DF 位和 URG 位），IP 头的扩展和填充段，IP 标识和碎片偏移量，IP 头的校验和字段，IP 头的存活时间字段，以及 IP 头的目的地址等；TCP 头的标志位字段，TCP 的重字段，TCP 的初始序列号字段，TCP 头的时间戳选项等；HTTP 头的值、顺序、可选字段的使用情况，HTTP 请求中的 URL 参数，以及 HTTP cookie 等。

2.2 网络时间隐蔽信道

网络时间隐蔽信道的媒介通常是数据包的传输时间间隔。信道的发送者通过巧妙地操控媒介数据包的发送时间，将隐蔽信息编码在数据包的时间特性中。信道的接收者通过观测媒介数据包的到达时间，推导出其发送时间，从而进一步将隐藏信息解码出来。

2004 年 Cabuk 等人首次提出 IP 时间隐蔽信道方案，简称为 IPCTC。IPCTC 使用了基于时间间隔的编码方案：在特定时间间隔内，发送一个数据包代表“1”，不发送数据包代表“0”。这种编码方案虽然简单，但却是启发式的。之后，Yao 等人具体分析了这种隐蔽信道，将其划分为两类：确定信道和非确定信道，并基于包延迟分布计算了非确定信道的最大传输率。Cabuk 在其博士论文中还提出了一种基于时间重放的时间隐蔽信道，简称为 TRCTC。Shah 等人于 2006 年设计并实现了键盘装置 Jitterbug，它能够泄露击键信息。Gianvecchio 等人于 2008 年提出了一种新型的时间隐蔽信道，它模拟了合法数据流的统计特性，具有较好的隐蔽性。Walls 等人以 Jitterbug 为基础设计了一种新的被动时间隐蔽信道，它可以抵抗现有的信道检测方法。

相比存储隐蔽信道，时间隐蔽信道构造更为复杂，隐蔽性更强，检测难度更大。近几年来网络时间隐蔽信道逐渐成为隐蔽信道的研究热点，下文将详尽且全面地介绍其构造方法及相应的防御技术。

3 几种典型的网络时间隐蔽信道

网络时间隐蔽信道可以分为“被动”和“主动”两种类型。“主动”是指构造信道的过程中产生了额外的通信流量用以传送信息，而“被动”是指只操控现有通信流量的时间特性用以传送信息。总体而言，主动时间隐蔽信道传递信息更加快速，但是被动时间隐蔽信道较难检测。从另一方面相比较，主动时间隐蔽信道通常需要攻破主机或操作系统，而被动时间隐蔽信道只需要把调制设备合理放置于计算机外围设备（例如放置在输入设备中，通过调制按键信息的时间特性，传送隐蔽消息）。

本章将介绍四种典型的被动和主动时间隐蔽信道，并具体分析和比较这四种信道的优缺点。

3.1 IPCTC

IPCTC 是 Cabuk 等人于 2004 年提出的第一个 IP 时间隐蔽信道方案。Cabuk 在构造 IPCTC 时，使用了基于时间间隔的编码方案：在时间间隔 t 内，发送一个数据包代表 1-bit，不发送数据包代表 0-bit。若发送一串二进制数据 01101001，则其编码结果如图 2 所示。显然，时间间隔 t 和两个 1-bit 之间的 0-bit 个数决定了包间隔 (IPD) 的分布。如果传送的比特序列符合均匀分布，IPD 的分布将接近几何分布。为了提高信道的隐蔽性，时间间隔 t 在某几个值之间循环。

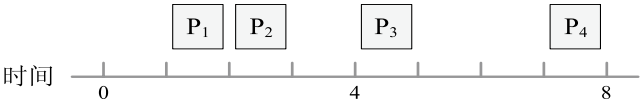

图2 IPCTC编码方案

IPCTC 的优点在于，即使中间丢失了某个包，只有 1 比特

信息发生跳变，而不影响收发双方的同步，不会影响后面数据的解码。它的弱点很明显，它需要接收者和发送者时刻保持同步，做到这一点需要牺牲一定的信道容量。

3.2 TRCTC

Cabuk 之后又设计了一种更加巧妙的时间隐蔽信道，其通过重放合法数据流来传送信息，简称为 TRCTC。TRCTC 将一组合法数据流的 IPD 记录在集合 S_{in} 中，用阈值 t_{cutoff} 将集合 S_{in} 分成集合 S_0 和 S_1。这种规则可以表示成：S_0=<0, t_{cutoff}, 0-bit>, S_1=< t_{cutoff}, t_{max}, 1-bit>。当 TRCTC 需要传送 1-bit 时，从集合 S_1 中随机选取一个 IPD，重放该 IPD；当 TRCTC 需要传送 0-bit 时，从集合 S_0 中随机选取一个 IPD，重放该 IPD。因为 S_{in} 由合法数据流的 IPD 构成，所以 TRCTC 的 IPD 分布近似于合法数据流的 IPD 分布。相比 IPCTC，TRCTC 具有更好的隐蔽性。

3.3 Jitterbug

Shah 等人于 2006 年提出了一种先进的被动时间隐蔽信道，其设计的键盘装置 Jitterbug 能够泄露击键信息。这篇启发式的文章描述了一种新颖的隐蔽信道构造方案：把 Jitterbug 放置在输入设备中，在键盘事件发送给主机之前，该设备通过对事件发送时间增加微小延迟将获得的口令泄露出去。由于没有产生额外的数据包，所以该信道是被动时间隐蔽信道。在 Jitterbug 的应用场景中，无需攻破主机，只要把 Jitterbug 放置在输入设备和主机的通信链路之间即可，如图 3 所示。

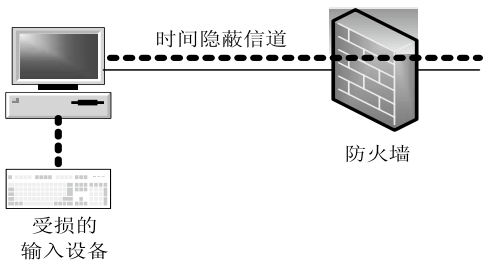

图3 Jitterbug应用场景

Shah 等人为 Jitterbug 设计的编码方案极为巧妙：令第 i 个击键事件发生的时间为 ti，对它增加微小延迟之后得到 Ti，相邻事件的时间间隔为 $\delta_i=T_i-T_{i-1}$。选定一个时间窗 w，当传送 0-bit 时，$\delta_i \bmod w=0$；当传送 1-bit 时，$\delta_i \bmod w=w/2$。为了避免传送的 IPD 是 w/2 的整数倍，在 δ_i 做模运算之前先减去随机数 S_i。

由于 Jitterbug 只对合法流量的 IPD 增加了微小的延迟，所以它具有很好的隐蔽性。此外，Jitterbug 不需要收发双方保持时间同步，只需要收发双方各自的时钟是精准的。

3.4 MBCTC

Gianvecchio 等人于 2008 年提出了一种新型的时间隐蔽信道，其模拟合法数据流的统计特性以逃避检测，是基于模型的时间隐蔽信道，简称 MBCTC。Gianvecchio 等人设计并实现了一套自动模拟框架，主要包括四个部分：过滤工具，分析工具，编码工具和传输工具。过滤工具的功能是把合法数据流的时间特性提取出来；然后分析工具将这些时间数据与一些分布模型进行拟合，如指数分布和韦伯分布等，均方根误差最小的模型被选为最佳拟合模型；编码工具使用所选模型的反向分布函数和累积分布函数作为编码函数和解码函数；最后，利用变量生成的反变换方法将消息隐藏在伪随机化的 IPD 中，传输工具将隐蔽信息传送出去。

伪随机化的 IPD 的分布由合法数据流拟合的分布模型所决定，因此，MBCTC 产生的 IPD 非常接近合法数据流的 IPD，MBCTC 可以较为有效地逃过隐蔽信道检测。

4 网络时间隐蔽信道防御技术和方法

为了防御时间隐蔽信道，研究人员提出了很多不同的解决方案，大致上可分为两类：信道限制和信道检测。信道限制通过在数据流中增加随机延迟，减小信道容量，但同时会降低系统性能。信道检测则利用统计方法将隐蔽信道从合法通信中分辨出来，据此找出发送隐蔽信息的主机，其极有可能已被黑客攻破。近几年来，信道检测方向的相关研究比较突出，本文将给予重点介绍。

4.1 信道限制

早期，研究人员把防御时间信道的焦点放在信道限制方向，并提出了多种限制隐蔽信道的方法。其中一种可行的限制途径是在信道中加入争夺噪声，扰乱发送者和接收者的系统时钟。Hu 等人提出了使用模糊时间的方案。在这个方案中，随机中断造成了随机时钟偏移，从而扰乱不同安全级别的系统时钟。因此，隐蔽信道的发送者和接收者不再共享同一个参考时钟。Giles 等人讨论了使用干扰设备以扰乱系统事件时间的方法。他们还从博弈论角度分析了被干扰信道的容量以及干扰设备的有效性。

另一种限制途径则是在降低信道传输速率的同时，也能够一定程度地保证系统性能。Kang 等人设计了一种设备，名为“Pump”，它主要用来解决不同安全级别主机之间的可靠且安全通信问题。在多级安全系统的通信中，如果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)，则传输是不可靠的；但是如果允许发送确认信息，则可以利用它来构造隐蔽信道，该通信是不安全的。Pump 的设计目的正是用于管理高安全级别主机的确认信息。

Pump 可以说是目前发展最为完善的时间隐蔽信道限制设备，已经被美国海军定型，并获得了相应的专利。Kang 等人在推出基础版 Pump 之后又设计并实现了网络版的 Pump。在实际应用中，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。

4.2 信道检测

网络时间隐蔽信道的检测方法可以分为两大类：形态检测和规律性检测。数据流的形态可以由一阶统计特性进行描述，如平均值、方差等。数据流的规律性可以由二阶或多阶统计特性进行描述，如相关性等。

4.2.1 Kolmogorov-Smirnov检测

在统计学中，Kolmogorov-Smirnov 测试是一种常用于测试连续的一维概率分布是否相等的非参数测试，简称 K-S 测试。它可以用于比较某个样本与参考概率分布（单样本 K-S 测试），也可以比较两个样本（双样本 K-S 测试）。双样本 K-S 测试可以用于确定这两个样本是否来自同个分布。K-S 测试的测试方法是对两个先验分布函数的最大距离进行测量：

$$KSTEST = \max|F_1(x) - F_2(x)| \quad (1)$$

F_1 和 F_2 是两个样本的先验分布函数。

K-S 测试可以用于检测时间信道的形态。Peng 等人在中表明 K-S 测试可以有效检测水印 IPD，其是时间信道的一种形式。该水印 IPD 的分布是正态分布和均匀分布的叠加。而在中，实验表明 K-S 测试可以成功检测出 IPCTC 的存在。

4.2.2 规律性检测

Cabuk 等人提出了一种基于规律性的时间隐蔽信道检测方法。该方法把数据流分成大小为 w 个包的子集。先对每个子集的 IPD 计算标准差 σ；对每一对子集 i<j，计算 σ_i 与 σ_j 的差值；最后，为了得到综合统计值，计算差值的标准差。公式 2 总结了上述计算过程：

$$regularity = STDEV(\frac{|\sigma_i - \sigma_j|}{\sigma_i}, i < j, \forall i, j) \quad (2)$$

该检测方法的依据在于：由于合法数据流的 IPD 是随着时间而变化的，而有些时间信道的 IPD 与发送的消息（符合均匀分布）有关，所以合法数据流两两子集的差值较大，最后得到的规律检测值也较大。在文献 [7] 中，实验数据显示合法数据流的规律检测值远大于 IPCTC 的值，但其同时也显示合法数据流的规律检测值有很大的标准差值，这说明该检测方法对合法数据流的波动非常敏感。

4.2.3 熵值检测

Gianvecchio 等人 [7] 首次把熵的概念引入信道检测中。基于观察到时间隐蔽信道的建立会一定程度的影响到原始过程的熵，Gianvecchio 认为熵的变化能够为时间隐蔽信道的检测提供重要线索。这篇文章提出了熵和条件熵两个参数，分别用于检测形态和规律性。

在信息论中，熵率（entropy rate）代表一个随机变量的平均熵，可以作为复杂性或者规律性的度量值。令随机过程 $X=\{X_i\}$ 为编了索引的随机变量序列，随机过程的熵率可以定义如下：

$$\bar{H}(X) = \lim_{m\to\infty} H(X_m \mid X_1, \cdots, X_{m-1}) \quad (3)$$

熵率可以使用无限序列的条件熵进行度量，然而，如果样本空间有限，需要修正其条件熵，从而实现对熵率的估计。经修正的条件熵 (corrected conditional entropy，简称 CCE) 定义如下：

$$CCE(X_m \mid X_1, \cdots, X_{m-1}) = CE(X_m \mid X_1, \cdots, X_{m-1}) + perc(X_m) * EN(X_1) \quad (4)$$

其中 $perc(X_m)$ 是长度为 m 的序列中只出现一次的样式的概率，$EN(X_1)$ 是长度为 1 时的熵，即一阶熵。

该检测方法把合法数据流的 IPD 划分到等概率的 Q 个分区中，即每个分区中的 IPD 个数相等。由此，界定每个分区的 IPD 范围。若 Q 个分区是等概率的，则一阶熵值达到最大。当时间隐蔽信道建立之后，每个分区中出现的 IPD 个数将会不等，计算得到的熵值将会变小，即数据流的形态发生变化。从规律性而言，合法数据流有较高的规律性，其熵率较小；时间隐蔽信道则更加随机，其熵率较大。

这一先进的检测方法能成功检测出上述四种经典的时间隐蔽信道，相比 K-S 测试和规律性测试更加有效，且应用范围更加广泛。

5 结束语

本文首先介绍了隐蔽信道的定义、分类以及通信模型。通过将通信模型扩展至计算机网络场景，把研究的焦点引入网络隐蔽信道中。然后，针对存储和时间两类网络隐蔽信道的研究现状分别做了总结。本文重点介绍了几种典型的时间隐蔽信道，并总结了经典的防御技术和方法。本文试图为该研究方向勾勒出一个较为全面的概貌，为该领域的研究人员提供有益的参考。（责编 杨晨）

参考文献：

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

[2] National Computer Security Center, Department of Defense Trusted Computer System Evaluation Criteria[R]. DoD 5200.28-STD, December 1985.

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

[4] Simmons GJ. The prisoners' problem and the subliminal channel[C]. In: Proc. of the CRYPTO ’83— Advances in Cryptology. 1984.51-67.

[5] T. Handel, M. Sandford. Hiding Data in the OSI Network Model[C]. Proc. 1st Int' l. Wksp, Information Hiding, 1996. 23-38.

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

[7]S. Gianvecchio, H. Wang, Detecting covert timing channels: an entropy-based approach[C]. In: CCS' 07: Proceedings of the 14th ACM Conference on Computer and Communications Security, ACM, New York, NY, USA, 2007. 307-316