网络传输中采用隐蔽通道实现秘密通信

李丽萍 王建华
(哈尔滨师范大学计算机科学与信息工程学院 哈尔滨 150025)

摘 要 秘密通信是指要隐藏通信的实际存在。在网络传输中利用隐蔽通道实现秘密通信,涉及到网络安全和采用数据隐藏技术实现网络隐私。主要讨论隐蔽通道的研究框架、分类、评估,以及秘密通信协议的设计问题。隐蔽通道可以分为结构模式、行为模式和内容模式,比较各种不同通道例证,阐明结构模式和行为模式通道更容易被消除,而内容模式则更为可靠并且具有较高的带宽。多种通道模式混用将更适合于秘密通信协议的开发。

关键词 秘密通信,数据隐藏,隐蔽通道
中图法分类号 TN915.08 **文献标识码** A

Implementation of Secret Communication with Covert Channels in Network Traffic

LI Li-ping WANG Jian-hua
(College of Computer Science and Information Engineering, Harbin Normal University, Harbin 150025, China)

Abstract Secret communication is to hide the existence of communication. This work relates network security and privacy with data hiding techniques, focusing on secret communication using covert channels in network traffic. The framework, classification and evaluation of covert channels and design issues in secret communication protocols were investigated. Covert channels were divided into structure-mode, behavior-mode and content-mode. The comparison of different channels illustrates that channels in structure-mode and behavior-mode are generally more apt to be eliminated while those in content-mode are more reliable and of high-bandwidth. A combination of different kinds of channels should be appropriate for developing secret communication protocols.

Keywords Secret communication, Data hiding, Covert channel

1 简介

随着互联网的发展,通过全球网络共享世界范围的信息已逐渐变为现实,与此同时网络安全和隐私正成为越来越严重的问题。传统的做法是在通信中采用加密技术来隐藏通信内容,以加强安全及保护隐私。然而,某些时候简单隐藏通信内容本身还不够,还需要隐藏通信的存在,这正是秘密通信遇到的实际问题。

本文从数据隐藏角度讨论了秘密通信,着重于如何利用网络传输中的隐蔽通道来达到掩盖进行彼此间通信事实的目的。

如文献[1]所定义的那样,隐蔽通道是一种机制,该机制是一种由某个系统使用者利用系统开发目的以外的形式,来实现彼此之间的信息传输。一个好的隐蔽通道应该不能被轻易地检测到,并且能提供更强的隐私保护和安全性。网络传输中的隐蔽通道实际是利用网络中的数据包流作掩护进行秘密信息的传输。

本文第2节介绍秘密通信模式,即囚犯问题;第3节讨论相关的工作;第4节介绍在网络传输中利用隐蔽通道实现秘密通信的研究框架,重点考虑非理想网络通道的影响和防御控制。隐蔽通道根据信息植入的方法可分为3种模式:结构模式、行为模式和内容模式;第5节提出了网络传输中的隐蔽通道的评估因素,基于这些因素给出了具体的对比情况;第6节讨论有关秘密通信协议中的设计和实现问题;最后是对未来的展望。

2 囚犯问题

囚犯问题被认为是最容易想到的秘密通信模式[2],它第一次由 Simmons 于 1983 年提出。在这个问题中,监狱中的两个犯人 Alice 和 Bob,试图计划一次越狱行动。但他们之间所有的联系都要经过看守人(Warden)Wendy 的监管,如果 Wendy 发现两人计划越狱甚至秘密沟通都将会把俩人分别单独监禁起来,所以 Alice 和 Bob 必须交换不引人注意的信号来传递隐藏的信息,而不被 Wendy 发现。

表面上似乎正常的数据经常用来隐藏真实的信息,这些数据称为"掩体",在掩体中被隐藏的信息叫做"植入信息",这些构成了 Stego-Object。这样,Alice 和 Bob 的目标就是传递 Stego-Object 而并不引起 Wendy 注意。

到稿日期:2008-11-20 本文受黑龙江省教育厅科学研究项目(No. 11511119),黑龙江省重点学科(No. 081203),黑龙江省智能教育重点实验室资助。

李丽萍(1956-),女,副教授,主要研究方向为计算机网络等,E-mail:lipingliw@126.com;王建华(1956-),女,教授,CCF 会员,主要研究方向为计算机网络等。

这里考虑到对两个囚犯传递信息改变的权力，将看守人分为两类。

被动 Warden：什么也不能做，只检测通信信道；

主动 Warden：可以轻微修改囚犯间传递的消息，但不能修改得太多以免正常信息无法被传递。

Warden 的权力不同影响了囚犯问题的困难等级，在设计秘密通信方法时必须首先考虑到。网络传输中使用隐蔽通道进行安全通信时，Warden 像防火墙一样，可以动态地修改信息，也可能被动监测网络传输并指出异常处的入侵检测系统。第 4 节将讨论这些 Warden 的实际影响力。

3 相关工作

隐蔽通道对于设计一个安全系统来说一直是一个值得注意的问题。文献[1]第一次从违反系统安全协议的意义上介绍了隐蔽通道的概念。隐蔽通道可以分为隐蔽存储通道和隐蔽定时通道。前者通过修改共享资源进行彼此间的存储信息传输，后者通过调整系统时序进行信号传输。文献[3]对隐蔽系统进行了详细分析。

网络传输中隐藏数据的观点在文献[4]中首次提到，之后在 OSI 模式下进行了实现[5]。主要观点是：通过数据包头部中的保留字节或未被使用的字节存储需要植入的数据。在文献[6]中，Rowland 描述了在 IP 字节的身份识别字段、初始序列号(ISN)字段和 TCP 授权顺序号字段中植入数据的技术，并且还给出了一个验证此概念的代码演示。相关的其他工作还包括用 TCP 时间戳[7]、IP 核对号码[8]等进行数据的隐藏技术。除了用修改数据包头部来隐藏数据的方法之外，文献[9]提出用分组报文目的地隐藏数据的可能性，这也是第一篇关于如何利用网络行为来实现数据隐藏的论文。

到目前为止，网络秘密通信已经有很多使用隐蔽通道的应用实例。Loki[10]于 1996 年发表的是第一个用来暗中传输 shell 命令的实用程序，主要通过 ICMP echo/ICMP echo-reply 和 DNS 名称查询和回复。另一种比较知名的是 Ncvert[11]的实现，通过使用 ISN 来隐藏数据，并且使用伪造的源地址使数据包被弹回来发送信息，并以此来隐藏发送方的地址。在上述研究基础之上，进一步讨论隐蔽通道的研究框架、分类、评估、设计和实现。论文的其他部分将详述这些研究。

4 框架

网络中隐蔽通道研究框架如图 1 所示。这里在吸收了密码系统的观点基础之上，扩展了研究工作。通讯双方是 Alice 和 Bob，他们试图通过隐蔽通道在网络通路中进行秘密通讯。Stego 函数 E 作为输入包括了植入信息 M、网络通路 T 和可能的编码键 K，从而形成一个 Stego 通路 T'，T' 穿过网络到达 Bob 处，并通过解码函数 E-1 进行解压。

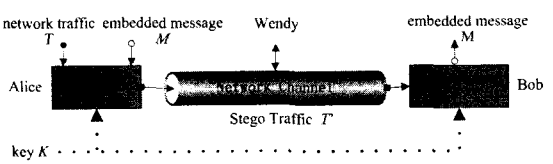

图 1 网络传输中隐蔽通道研究框架

对于研究框架的主要观点如下：

1)植入过程可按植入方式的不同分为 3 种模式。

结构模式：通过修改数据包格式字段在网络传输中植入数据。例如修改头部字段或者填充 TCP/IP 数据包部分以及修改 HTTP 请求部分等。行为模式：通过修改网络行为在网络传输中植入数据。例如延时发送数据包影响到达时间，发送数据包时用不同的速率代表不同的意思等等。内容模式：通过修改内容在网络传输中植入数据。这可以与传统的如在文本、音频、视频中隐藏数据的方式相结合。

2)Alice 与 Bob 可以使用秘钥 K 来保证只有 Bob 能知道秘密通信中的内容。这要求当被看守人 Wendy 侦测到时保证信息不被泄露。

3)Alice 和 Bob 之间的网络信道并不是理想的情况，数据包可能被延迟，或者因为意外原因被改动。这种情况在结构模式和行为模式中可能影响隐蔽通道，但在内容模式中影响很小。

另一方面，隐蔽通道必须保证 Stego 通路不能妨碍中间网络通路中的正常解释过程，不能因为 Stego 通路与正常的数据包明显不同而使中间网络通路不工作。

4)与实际情况类似，网络中的 Wendy 是研究框架中的一个非常重要的组成部分。像罪犯问题里所涉及到的一样，网络周边上的控制机构，诸如防火墙、代理、应用网关都会像一个活动的 Wendy 一样活动，改变 Stego 通路的传递，而 IDS 仅能被动监视通路并不从根本上改变通路。因为 Warden 的存在，必须要考虑可能的检测或消除隐蔽通道的可能性，这些也是评价的重要因素。

研究框架说明植入过程、网络设定及网络通路中的威胁模式。下边内容将讨论关于框架方面的评价方式。

5 评价

5.1 评价因素

通常意义上讲，一个隐蔽通道应该具有表面合理性和安全性。目前，网络传输中的隐蔽通道面临着更加复杂的环境，在传输过程中还将遇到更多的检测和查询。为了更全面地理解通道的控制机制，需要从多个层面上对其进行评价。

1) 带宽：带宽是指通过通道可以传输多少信息，这是一个很重要的评价因素。结构模式中通道带宽通常容易估算出来。例如，当修改 IPV4 头部中的 DF 部分时带宽为 1 比特/数据包，当修改 TCP 头部的 ISN 部分时为 32 比特/每连接。行为模式与内容模式中，带宽必须分类分析。这个因素会影响评价通道的效率。

2)约束：指当使用通道时，在规范和实现过程中是否有多余的因素存在。例如，时间标志字段通常会增加等等。

3)影响：这个因素用来评价植入数据是否会影响到标准网络的作用。例如数据包头部的 TOS 或 DF 部分。

4) 可检测性：这个因素表明，当被动的 Warden 通过时信道被侦测到的可能性。信道的被侦测能力范围从易到难直到无法被侦测到。若信道使用常用的比特设置，如用填充字段的方式来植入隐藏信息，则检测系统能通过相应的监测轻易地检测到。如果信道用 TCP 时间戳或 ISN 字段存储隐藏信息，检测系统必须使用统计方法来判断侦测观察到的数据流是否可疑，这比较困难。在一些比较极端的情况下，隐蔽通道可能根本无法被检测到。

5) 可被消除性：这个因素用来衡量被动态的检测系统修

改的可容忍度。动态 Warden 可能会修改数据包的头部，延迟数据包时间或者重安排数据包的顺序。然而，内容模式下植入的隐藏数据的可被消除性非常小。

6) 容许性：比较隐蔽通道的可被消除性，这个因素更着重于安全协议下通道的可被接受性。例如，一些网络管理员可能认为是 TFTP 恶意数据包，因为病毒等问题不会让数据通过，但却不会阻止 HTTP 数据通过，因为这是常用的协议。

7) 通用性：这个因素同容许性有些类似，只是有一些扩展。这个因素更注重于通道是否频繁出现。就隐藏体而言通道不应该频繁地出现在协议中，否则会引起注意并被检测端发现。不然的话，无所不在的协议就成了隐藏数据比较不错的植入场所。

以上的 7 个评价因素中，前 3 个因素表述了通道的内在特性，并可在不同情况下进行选用，后 4 个因素描述了实际环境中的通道的生存能力。

5.2 通道比较

基于以上因素，网络传输中可比较的隐蔽通道如表 1 所列。此处“模式”的含义指 3 种植入模式：S 表示结构模式，B 表示行为模式，C 表示内容模式。

表 1 网络传输中隐蔽通道比较

模式	通道描述 协议	方法	评价因素 带宽	约束	影响	被检测	被消除	容许性	通用性
S	All	padding bits	变化	有	无	经常	经常	不经常	不经常
S	All	reserved bits	变化	有	无	经常	经常	不经常	不经常
S	IP	identification bits	16bits/pkt	有	无	不经常	不经常	总是	总是
S	IP	源地址部分	32bits/pkt	无	有	经常	经常	有时	经常
S	IP	DF bit	1bit/pkt	无	有	不经常	不经常	总是	总是
S	IP	TOS bits	6bits/pkt	有	有	有时	有时	总是	总是
S	IP	option fields	变化	变化	变化	不经常	不经常	有时	有时
S	TCP	ISN bits	32bits/con	有	无	很少	很少	总是	
S	TCP	URG pointer without URG bit set	16bits/pkt	有	无	经常	经常	总是	总是
S	TCP	data bits with RST set	变化	无	无	经常	经常	不经常	不经常
S	TCP	source port field	16bits/pkt	无	Yes	不经常	不经常	总是	总是
S	ICMP	echo optional data	变化	无	无	有时	有时	有时	不经常
B	-	packet reach time	变化	无	无	不经常	经常	-	-
B	-	packet sort	变化	有	无	不经常	经常	-	-
B	-	packet rate	变化	无	有	不经常	经常	-	-
C	DNS	回应	变化	无	无	不经常	不经常	总是	总是
C	HTTP	upper or lower case of html tags	变化	无	无	经常	不经常	总是	总是

通过比较，不同的通道有不同的优点和缺点。一般来说，结构模式和行为模式面对动态 Warden 和非理想网络环境下更易于被消除。而内容模式的可靠性更好一些，通信中的内容被 Warden 修改的可能性很小。对于带宽，内容模式比前两者更高，且有更多的存储空间用来植入信息。

6 设计与实现

为网络传输中用隐蔽通道进行秘密通信设计和实现一个实际的协议，首先应该考虑的问题有：

1)通道选择。基于以上的比较，不同通道有不同的特性。因此不同类型的通道组合，将是一种比较适合秘密通信协议的开发方式。

例如，可以使用结构方式来传输少量的控制信息，用内容模式来传输大量的数据信息，这样也可以增进协议的可伸缩性，通信双方在开始时便进行通道的选择，不同类型的通道像插件一样插入协议当中。

2)同步。这个问题对于结构模式的通道非常重要。这些通道简单地修改了数据包头部的一部分，而打乱数据包顺序或数据包的重发可能会影响接收端对这些植入信息的解压。使用一个“magic flag”来提示数据传输的开始和结束，或者为收到的数据包正确的顺序加上索引都是一个很好的措施，并且这也是保护协议不受回应攻击的一种方法。

3)数据完整性。为了保护数据不被 Warden 或者网络信道修改，应该采用校验方式检测数据是否被篡改。

4)信息加密。当信道协议被 Warden 探知时，隐蔽通道应该使用较好的加密模式来保护信息。

5)鉴别与授权。这个问题是用来设计防止滥用通道协议的。

简而言之，在网络通路中采用隐蔽通道设计秘密通信的协议，应该考虑非理想环境下和不确定的中间网络频道。集中不同模式通道的优点是开发新协议的最佳方式。同样，高效的实现使协议不影响正常网络行为，这一点也是很重要的。

结束语 本文回顾了网络传输中用隐蔽通道实现秘密通信的控制机构研究框架、评价与设计问题。将隐蔽通道划分为 3 个模式：结构模式、行为模式、内容模式。评价的因素有：带宽、限制、影响、被侦测能力、被清除能力、容许性、通用性，以及现存通道的详细评价。

根据上述研究，讨论如下：

1)网络传输中采用隐蔽通道是实现秘密通讯的一种比较好的手段。

2)非理想状态和不确定的中间网络通道，以及中间检测端的存在，都是隐蔽通道的主要威胁。

3)不同的通道在带宽、实现难度等方面有不同的优点和缺点。一个混合的通道是一种较好的协议设计方案。

未来研究的重点方向主要是设计与实现秘密通讯使用的协议，其次是开发更新的通道，尤其是 IPV6 环境下。最后，我们应该结合 Internet 下匿名与不可见性的研究，并以此增进私人隐私的保护，这也应是非常值得注意的研究项目。

参 考 文 献

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

(下转第 176 页)

评分规则为:各测试子项(情感词和情景词)的召回率、精确率的平均值取和、简单求平均值、乘以(100+20)。其中,20用于抵消由于人工获取关键词产生的误差。由表2看来,得分为:(53.64%+32.75%+41.49%+44.5%)/4*(100+2)=52分,因此原有情感词和情景词的准确率尚未达到商用标准。

而由表3的对比测试结果可以看出,改进型情感分类比原始情感分类结果在召回率以及精确率上都有了显著提高,满足商用要求,一定程度上实现了以文字为基础的情感化检索要求。

参 考 文 献

[1] The Bulldog Group Research Report[OL]. http://www.bulldog.com

[2] Wood E, et al. Content based classification, search, and retrieval of audio[J]. IEEE Multimedia, 1996

[3] 王小凤,周明全,耿国华,等.一个使用歌谱信息进行哼唱检索的系统[J].计算机辅助设计与图形学学报,2007:941-946

[4] Park Kyu-Sik, Yoon Won-Jung, et al. A robust content-based music retrieval and browsing[J]. IEEE Transactions on Consumer Electronics, 2005

[5] Zhu Yongwei, Kankanhalli, Mohan S. Melody alignment and similarity metric for content-based music retrieval[C]// Proceedings of SPIE-The International Society for Optical Engineering. 2003

[6] Hevner K. Expression in music: a discussion of experimental studies and theories[J]. Psychological Review, 1935, 42:186-204

[7] Hevner K. Experimental studies of the elements of expression in music[J]. American Journal of Psychology, 1936, 48:246-268

[8] Thayer R. The biopsychology of mood and arousal[M]. Oxford University Press, 1989

[9] Katayose H, Imai M, Inokuchi S. Sentiment extraction in music. Rome, Italy: IEEE, Piscataway, NJ, USA, 1988

[10] Katayose H, et al. Expression extraction in virtuoso music performances. Atlantic City, NJ, USA: IEEE, Piscataway, 1990

[11] Liu T, Sun S, Pan Y. Emotional recognition for chime bell music. The Hague, Netherlands: Institute of Electrical and Electronics Engineers Inc., New York, NY 10016-5997, United States, 2004

[12] Liu T, et al. Music's Affective Computing Model based on Fuzry logic[C]// WCICA2006. 2006

[13] Liu D, Zhang N, Zhu H. Form and mood recognition of Johann Strauss's waltz centos[J]. Chinese Journal of Electronics, 2003, 12(4):587-593

[14] Liu D, Zhang N, Zhu H. CAD system of music animation based on form and moodrecognition[J]. Moshi Shibie yu Rengong Zhineng/Pattern Recognition and Artificial Intelligence, 2003, 16(3):283

[15] Liu D, Zhang N, Zhu H. Automatic Mood Detection from Acoustic Music Data[C]// Proceedings of 4rd International Conference on Music Information Retrieval, ISMIR 2003. 2003

[16] Wang M, Zhang N, Zhu H. User-adaptive music emotion recognition. Beijing, China: Institute of Electrical and Electronics Engineers Inc., New York, NY 10016-5997, United States, 2004

[17] Li T, Ogihara M. Content-based music similarity search and emotion detection. Montreal, Que, Canada: Institute of Electrical and Electronics Engineers Inc., Piscataway, NJ 08855-1331, United States, 2004

[18] Feng Y Z, Zhuang Y T, Pan Y H. Query similar music correlation degree[C]// Advances in Mutlimedia Information Processing—Pcm 2001, Proceedings. 2001, 2195:885-890

[19] 陈若涵.以音乐内容为基础的情绪分析及辨识[C]//2006 International Workshop on Computer Music and Audio Technology. 台湾,2006

[20] Tang Yongchuan. Linguistic modeling based on semantic similarity relation among linguistic labels. Fuzzy Sets and Systems, 2006

[21] Lawry J. Aframework for linguistic modelling. Artificial Intelligence, 2004

(上接第117页)

[2] Simmons G J. The prisoners' problem and the subliminal channel [C]// Chaum D, ed. A dvances in Cryp to logy: Proceedings of CRYPTO'88. New York: Plenum Press, 1984:51-67

[3] Gligor V. A guide to understanding covert channel analysis of trusted systems [M]. NCSC-TG-030. National Computer Security Center. Version 1, Nov. 1993

[4] Wolf M. Covert channels in LAN protocols [C]// Lecture Notes in Computer Science. New York, 1989:91-101

[5] Handel T G, Sandford M T. Hiding data in the OSI network model[C]// Proceedings of Information Hiding, first international workshop. Cambridge, UK, Berlin, Springer-Verlag, 1996:23-38

[6] Rowland C H. Covert channels in the TCP / IP protocol suite [EB/OL]. URL: http://www.psionic.com/papers/covert/covert.tcp.txt. 1996-11-14

[7] Giffin J, Greenstadt R, Litwack P, et al. Covert messaging in TCP[M]// Dingledine R, Syverson P, eds. Privacy Enhancing Technologies. Lecture Notes in Computer Science. Volume 2482, Springer-Verlag, 2002:194-208

[8] Abad C. IP Checksum Covert channels and selected Hash Collision[EB/OL]. http://www.gravitino.net/~aempirei/papers/pccc.pdf, 2001

[9] Ahsan K, Kundur D. Practical Data Hiding in TCP / IP[C]// Workshop Multimedia and Security at ACM Multimedia'02. December 2002

[10] Project Loki[EB/OL]. ICMP Tunneling. http://www.phrack.org/show.php? p=49&a=6

[11] Project Ncovert[EB/OL]. http://sourceforge.net/projects ncovert/