隐通道存在的最小条件及其应用*)

王昌达[1,2] 鞠时光[1] 杨 珍[1] 郭殿春[1]
(江苏大学计算机科学与通信工程学院 镇江212013)[1]
(卡尔顿大学计算机科学学院 加拿大 渥太华 K1S 5B6)[2]

摘 要 隐通道能在安全机制的监控之下将保密信息外泄,因而对系统安全的威胁极大。通过研究隐通道的工作原理,形式化地证明了隐通道存在的最小条件。在此基础上,对现有的隐通道搜索与消除方法进行了分类,并从理论上说明了各种方法的正确性及其不足。这些工作不仅为隐通道的搜索与消除工作提供了可信的理论依据,而且为寻找新的隐通道搜索与消除方法提供了一个研究框架。

关键词 隐通道,安全模型,安全策略

The Minimum Criteria of Covert Channels' Existence and its Application

WANG Chang-Da[1,2] JU Shi-Guang[1] YANG Zhen[1] GUO Dian-Chun[1]
(School of Computer Science and Telecommunications, Jiangsu University1, Zhengjiang, Jiangsu 212013)[1]
(School of Computer Science, Carleton University2, Ottawa, Ontario, Canada K1S 5B6)[2]

Abstract Covert channels can leak confidential information under the supervision of security mechanism, so its threat is very serious. By research on the working principle of covert channels, the minimum criteria of its existence had been formally proved. Based on it, the taxonomy for the methods of search and elimination in covert channels was given. Furthermore, each method's correctness and deficiency were represented theoretically. These were not only offered the theory bedrock for the work of search and eliminate covert channels, but also given a frame for develop new search and elimination methods in covert channels.

Keywords Covert channel, Security model, Security policy

1 引言

1973年,B. W. Lampson 首次提出了隐通道问题[1]。隐通道是指安全系统中的高安全级用户,通过违反系统安全策略的方式向系统的低安全级用户传送信息的一种机制[2]。因为隐通道利用了系统原本不是用于数据传送的资源来传送数据,所以它能在系统安全机制的监控之下将保密信息外泄。一般地,隐通道的类型分为存储隐通道(Storage Channel)、时间隐通道(Timing Channel)和兼具两种特征的混合型隐通道(Storage and Timing Channel)[3]。存储隐通道和时间隐通道的区分的标志是看在整个通信进程中是否使用了外部时钟[4]。

隐通道在最初的20年里,研究非常活跃,针对特定的问题,人们提出了一些有效的隐通道搜索与消除防方法。在隐通道搜索方面,影响较大的有信息流分析法[5]、共享资源矩阵法[6]、隐蔽流树法[7]、无干扰分析法[8]和源代码分析法[9]等;在隐通道消除方面,影响较大的有存储转发法(SAFP)[10]、泵协议法[11]、混沌时间法[12]和操作隔离法[13]等。其后,隐通道的研究曾一度跌入低谷。进入21世纪后,伴随着计算机网络的飞速发展,隐通道的研究再次繁荣起来,并且国外这方面的研究多数具有政府和军方的背景,见参考文[1~17]。这是因为在单机环境下,一台计算机上的信息容量有限,用户必须要接触到计算机才可能触及其上存储的保密信息。所以与其花大量的时间精力去搜索和消除隐通道,还不如花钱雇用忠实的守卫、建造牢固的机房,来加强对计算机的管理。但在网络高度发达的环境下,情况就不同了。一台联网的计算机可能在其主人毫不知情的情况下,就被看不见的远程用户恶意窃取了保密信息。统计表明,多数木马程序都是利用隐通道来工作的[2]。与暴力入侵易于被安全管理人员发现不同,因为隐通道是在安全机制的监控之下将保密信息外泄,所以如果不借助其它手段,依靠系统固有的安全机制是不能检测出隐通道的[14]。在我国,对隐通道的研究已被列入863支持项目。

2 隐通道存在的最小条件

依据目前的认识,隐通道的工作原理是安全系统中具有较高安全级别的主体,使用事先约定好的编码方式,通过更改共享客体的属性并使低安全级别的主体观察到这种变化,来传送违反系统安全策略的信息的[14],见图1。存储隐通道中的共享客体是文件或变量等非时间性资源,时间隐通道的共享客体则是系统的响应时间。

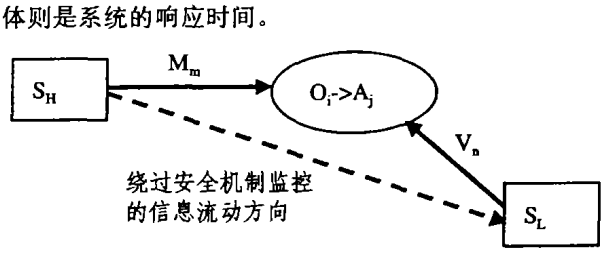

图1 隐通道的工作原理

需要指出的是,图1中的实线箭头所标识的操作及其信息

*)国家自然科学基金(No. 60373069)和江苏省自然科学基金(No. BK200204)资助项目。王昌达 讲师,博士研究生,加拿大 Carleton University 访问学者,主要研究方向为信息系统安全。鞠时光 教授,博导,主要研究方向为信息系统安全、空间数据库技术。杨 珍 硕士研究生。郭殿春 硕士生研究生。

流动都是合法的，但两次合法的操作却导致了一次非法的信息流动，如图1中虚线箭头所示。

约定1 S 是主体的集合，O 是客体的集合。

约定2 $O_i \to A_j$ 表示 A_j 是客体 O_i 的第 j 个属性；$S_H \to M_m$ 表示 M_m 是主体 S_H 的第 m 个方法，且该方法用于改变该主体可接触客体的某一个属性；$S_L \to V_n$ 表示 V_n 是主体 S_L 的第 n 个方法，且该方法用于观察该主体可接触客体的某一个属性的变化。其中，$O_i \in O$；$S_H, S_L \in S$。

约定3 $SL(X)$ 表示 X 的安全级，其中 $X \in S \cup O$，“$>$”是该安全级上的偏序关系。

约定4 $S_H \to M_m(O_i \to A_j, T_p)$，$S_L \to V_n(O_i \to A_j, T_q)$，$SL(S_H) > SL(S_L)$，$T_p < T_q$ 是四个布尔函数。其中，当且仅当在 T_p 时刻，$S_H \to M_m$ 成功改变 $O_i \to A_j$，$S_H \to M_m(O_i \to A_j, T_p)$ 值为真，否则为假；当且仅当在 T_q 时刻，$S_L \to V_n$ 成功观察到 $O_i \to A_j$ 的变化，$S_L \to V_n(O_i \to A_j, T_q)$ 值为真，否则为假；当且仅当 S_H 的安全级高于 S_L，$S_L(S_H) > S_L(S_L)$ 值为真，否则为假；当且仅当 T_p 早于 T_q，$T_p < T_q$ 值为真，否则为假。

定理1 隐通道存在的最小条件是：$\exists\ i, j, m, n$，使得 $S_H \to M_m(O_i \to A_j, T_p) \wedge S_L \to V_n(O_i \to A_j, T_q) \wedge (S_L(S_H) > S_L(S_L)) \wedge (T_p < T_q)$ 的值为真。

证明：由通道的工作原理可知，$S_H \to M_m(O_i \to A_j, T_p) \wedge S_L \to V_n(O_i \to A_j, T_q) \wedge (S_L(S_H) > S_L(S_L)) \wedge (T_p < T_q)$ 的值为真是隐通道存在的条件，现假设其不是隐通道存在的最小条件，设 C 是隐通道存在的最小条件，则必有：

$C \subseteq \{ S_H \to M_m(O_i \to A_j, T_p), S_L \to V_n(O_i \to A_j, T_q), S_L(S_H) > S_L(S_L), T_p < T_q \}$，且 $\{S_H \to M_m(O_i \to A_j, T_p), SL \to V_n(O_i \to A_j, T_q), S_L(S_H) > S_L(S_L), T_p < T_q\} \backslash C \neq \varphi$ 成立。

不妨设 $S_H \to M_m(O_i \to A_j, T_p) \notin C$，即隐通道中没有发送信息的主体，显然无法构成隐通道，矛盾，所以 $S_H \to M_m(O_i \to A_j, T_p) \in C$。同理可证 $S_L \to V_n(O_i \to A_j, T_q) \in C$，$(SL(S_H) > SL(S_L)) \in C$，$(T_p < T_q) \in C$，即：

$C \supseteq \{S_H \to M_m(O_i \to A_j, T_p), S_L \to V_n(O_i \to A_j, T_q), SL(S_H) > SL(S_L), T_p < T_q\}$，所以

$C = \{S_H \to M_m(O_i \to A_j, T_p), S_L \to V_n(O_i \to A_j, T_q), SL(S_H) > SL(S_L), T_p < T_q\}$

证毕。

定理1说明了，一个系统中如果存在隐通道，那么至少应同时满足以下四个条件：

① 发送方和接收方必须能对共享资源的同一属性进行存取；

② 必须存在一种方法，借之高安全级发送方能够改变该共享属性；

③ 必须存在一种方法，借之低安全级的接收方能够察觉这一改变；

④ 必须保证发送方和接收方之间的通讯以正确的顺序进行。

3 确立隐通道存在最小条件的意义

现有的隐通道搜索与消除方法，都是针对某一问题而提出的比较具体的可操作算法，但在这些算法中，尚无一种能证明自身的正确性，见文[5～13]。所以，在使用这些方法搜索或消除隐通道时，以下两个问题是无法回答的。第一，我们找到了一些隐通道，但是否我们找到了全部的隐通道？第二，我们消除了一些隐通道，但是否我们消除了全部的隐通道？

隐通道存在最小条件的确立，为我们研究隐通道的搜索与消除方法，提供了一个理论基础。根据定理1，一个正确的隐通道搜索算法，应该能按照某种次序检测定理1的四个条件，如果少检测条件，就可能导致误报，反之，如果多检测条件，就可能导致漏报。同理，一个正确的隐通道消除算法，应该能至少打破定理1的四个条件之一。以此为基础，我们对现有的隐通道搜索与消除方法进行了分类研究，进而说明这些方法的正确性与可行性。

4 隐通道的搜索方法

定理1要求在安全系统中搜索隐通道，应该寻找同时满足四个条件的情况。但事实上，如果同时检测四个条件的成立与否，不仅工作量大、复杂性高，而且效率低下，只要稍有不慎，就难免会出现漏报的情况。所以，现存的隐通道搜索方法，一般是仅搜索定理1四个条中的一个或几个。这样做一方面提高了效率，另一方面降低了方法的复杂程度，漏报的情况也较少。但随之而来的问题是，由于没有遍历定理1要求的最小条件的全部，因此会出现误报的情况。即被这样方法搜索到的仅仅可能是隐通道，要最终确认，还需要辅助以人工分析。而辅助分析的方法是明确的，即搜索时没用到定理1的哪个条件，就需要用哪个条件作进一步的检验，直到每一个候选者都被确认或排除是隐通道为止。

一般地，现有的隐通道搜索方法可以分成以下三类。

4.1 成对检测发送方和接收方的搜索方法

Richard A. Kemmerer 等提出的“共享资源矩阵法”[6]和“隐蔽流树法”[7]属于这种方法。它的核心思想是通过成对地搜索信息的发送方和接收方来寻找隐通道。

因为共享资源矩阵法着眼于发送方和接收方，即定理1中的 $S_H \to M_m(O_i \to A_j, T_p)$ 和 $S_L \to V_n(O_i \to A_j, T_q)$ 两个条件，所以，它找到的候选隐通道还需要辅之以 $SL(S_H) > SL(S_L)$ 和 $T_p < T_q$ 两项检测，才能被最终却认或排除是隐通道。

隐蔽流树法是对共享资源矩阵法的改进，其工作原理基本相同。但因为在“树”的遍历过程中，包含了对发送方和接收方工作时序的考虑，所以与共享资源矩阵法比，对找到的候选隐通道，只需要辅之以检测发送方的安全级是否高于接收方，即检测 $SL(S_H) > SL(S_L)$。

4.2 检测共享资源的搜索方法

CHII-REN TSAI 等[8]提出的“无干扰分析法”和 C. R. Tsai 等[9]提出的“源代码分析法”属于这种方法。它的核心思想是通过寻找高安全级主体与低安全级主体的共享资源来搜索隐通道。如果共享资源不存在，则可以说明隐通道一定不存在，否则需要按照定理1的要求对四个条件逐一进行分析。因此，这两种方法的操作复杂性很高，所以不能适用于大型安全系统的隐通道搜索，但这两种方法却能有效地证明安全系统中不存在隐通道[8,9]。

4.3 检测信息流向的搜索方法

Jingsha He 等[5]提出的“信息流分析法”是建立在 D. E. Denning 等提出的信息流格模型(Lattice Model)基础之上的一种隐通道搜索方法。在图1中可以看出，与本节4.1，4.2的方法不同，它的检测目标不是集中在两端的主体或中间的客体上，它要检测的是信息流动的方向。信息流分析法的核心思想是，任何对系统安全策略的违反，当然包含隐通道，都将体现为对“格(Lattice)”定义的破坏。有关信息流格模型的细节请参考文[15]。

这种方法兼顾了定理1的四个条件，而且容易用自动化的信息流分析工具加以实现。不足之处在于，它对于信息流的语义识别功能较弱。在分析过程中会产生隐蔽流(implicit flow)[10]和形式流(formal flow)[16]两种缺陷。隐蔽流是指安

全系统中的一些特定数据流能避开系统安全机制的监控，从而造成信息泄漏。形式流则是一种无法通过系统安全机制检查的安全信息流动，即尽管信息流向是符合安全策略的，但却不能通过系统安全机制的检查，因而造成误报。

5 隐通道的消除方法

根据定理1的要求，四个条件只要打破其中之一，就可以保证消除隐通道。但事实上，为了保证系统能正确运行，完全打破任何一个条件，几乎都是不可行的[2]。通常做法是，对隐通道赖以存在的最小条件施加某些限制，直至安全系统中某一类型的隐通道被消除，或是其带宽降低到了可以接受的程度。根据 TCSEC 的规定，带宽在100bits/s 以下的隐通道可以不作处理。

一般地，现有的隐通道消除方法可以分成以下两类。

5.1 打破时间同步消除隐通道的方法

存储转发法(SAFP)[10]、泵协议法[11]、混沌时间法[12]属于这种方法。它的核心思想是，让低安全级的接收方不能正确感知高安级发送方传递来的有害系统安全的信息，即打破定理1的条件④。

存储转发法和泵协议法的基本作法是，让从高安全级到低安全级的通信信号，经过一个可信的代理中转后才被发往低安全级。而在此中转过程中，一些可能有害系统安全的信息将被过滤掉。根据具体的算法不同，泵协议法又分为简单泵、量化泵和网络泵等。存储转发法和泵协议法，在处理存储隐通道方面是有效的，但在一些极限情况下，如缓冲区满，这两种方法都无法消除时间隐通道。关于这个问题的直观解释是，这两种方法控制的客体都是可以加载到系统内存中的变量，而时间也是一种客体，但它并不在存储转发协议和泵协议的控制之下。

"混沌时间法"控制的共享客体是时间，因而它是用来消除系统中的时间隐通道的。混沌时间法的基本做法是，首先构造一个混沌函数 $Fuzz(t_i)$，t_i 是种子，当高安全级的主体执行了某一个操作后，系统需要在间隔 $Fuzz(t_i)$ 之后再响应。这样，低安全级的主体就不能通过自己等待响应的时间，来感知高安全级主体发送来的信息，因而时间隐通道被消除。但这种方法的缺点是，因为人为地添加了等待时间 $Fuzz(t_i)$，所以会导致系统性能的显著下降。

5.2 取消共享资源消除隐通道的方法

P. M. Melliar-Smith 等提出的"操作隔离法"[13]属于这种方法，其核心思想是，通过取消共享资源来隔断高安全级主体和低安全级主体之间的通信，即打破定理1的条件①。这种方法取消的共享资源，包含了"时间"，所以这种方法可以同时消除时间隐通道和存储隐通道。但这种方法的缺点是比较保守，可能会排除一些完全无害的程序，另外，在精度高时它会变得相当复杂，因而导致慢速度和大空间开销。

结束语 本文的主要贡献有以下几点：第一，在隐通道工作原理的基础上，形式化地证明了隐通道存在的最小条件。国外也有人试图给出隐通道存在的最小条件，但他们给出的结论仅仅是一种猜测，没有理论证明，而且与本文的结果相比，其结论是不完整的，见参考文[2]。第二，我们应用这个结果对已有的隐通道搜索和消除方法进行了分类，指出了每种方法的不足以及各种方法间的内在联系，并在理论上说明了这些方法的正确性和可行性，从而为隐通道的搜索与消除工作提供了可信的理论依据。

此外，定理1还为寻找新的隐通道搜索与消除方法，建立了一个可研究的框架。亦即，任何一种新的搜索算法都必须兼顾定理1的四个条件；任何一种新的消除算法也都至少要打破定理1的四个条件之一。在这种思想的指导下，我们课题组注意到尚无一种以打破定理1的条件②和条件③为基础的隐通道消除方法，据此我们率先提出了一种新的隐通道消除算法，它能有效地同时消除安全系统中的存储隐通道和时间隐通道。

本文关于隐通道搜索、消除方法的分类不是绝对的，有些方法兼具多种特征。根据 TCSEC 标准，在达到 B2级要求的安全系统中需要进行存储隐通道的分析。所以，安全系统中对于隐通道的搜索和消除工作，可能需要多种方法的联合使用。

参 考 文 献

1 Lampson B W. A note on the confinement problem. CACM, 1973, 16(10): 613～615

2 McHugh J. Covert Channel Analysis: A Chapter of the Handbook for the Computer Security Certification of Trusted Systems, Portland State University, Dec. 1995

3 Scheafer M, Gold B, Linde R, Scheid J. Program Confinement in KVM/370. In: Proc. of the 1977 ACM Annual Conference, Seattel, WA, USA, Oct. 1977. 404～401

4 Karger P A, Wray J C. Storage Channels in Disk Arm Optimization, IEEE 1991

5 He Jingsha, Gligor V D. Information-Flow Analysis for Covert-Channel Identification in Multilevel Secure Operating Systems, IEEE 1990

6 Kemmerer R A. Shared resource matrix methodology: A practical approach to indetifying covert channels. ACM Transactions on Computer Systems, 1983, 1(3): 256～277

7 Kemmerer R A. Covert Flow Trees: A Visual Approach to Analyzing Covert Storage Channels. IEEE Transactions on Software Engineering, 1991, 17(11)

8 TSAI Chii-Ren, et al. On the identification of covert storage channels in secure systems. IEEE Transactions on Software Engineering, 1990, 16(6): 569～580

9 Tsai C R, Gligor V D, Chandersekaran C S. A formal method for the identification of covert storage channels in source code. In: 1987 IEEE Symposium on Security and Privacy, Oakland, CA, IEEE Computer Society, Computer Society Press, April 1987. 74～86

10 Ogurtsov N, Orman H, Schroeppel R, et al. Experimental Results of Covert Channel Limitation in One-Way Communication Systems, IEEE 1997

11 Kang M H, Moskowitz I S. A pump for rapid, reliable, secure communication. In: 1st ACM Conf on Computer and Communications Security, Fairfax, Virginia, Nov. 1993. 119～29

12 Hu Wei-Ming. Reducing timing channels with fuzzy time. IEEE, 1991

13 Melliar-Smith P M, Moser L E. Protection against covert storage and timing channels. IEEE, 1991

14 Wang Chang-da, Ju Shi-guang, Yang Zhen, et al. Research on the Methods of Search and Elimination in Covert Channels. In: The Second Intl. Workshop on Gridand Cooperative Computering, Lecture Notes in Computer Science, 2003. 988～991

15 Denning D E. A Lattice Model of Secure Information Flow. Communications of the ACM, 1976, 19(5): 236～243

16 Eckmann S T. Eliminating Formal Flows in Automated Information Flow Analysis. IEEE, 1994

17 Kemmerer R A. A Practical Approach to Identifying Storage and Timing Channels: Twenty Years Later. In: Proc. of the 18th Annual Computer Security Applications Conf. IEEE, 2002

18 Wang Changda, Ju Shiguang, Guo Dianchun, et al. Research on the methods of search and elimination in covert channels. In: The Proc. of Second Intl. Workshop on Grid and Cooperative Computing (GCC2003), Dec. 2003, Shanghai, China, To appear in Lecture Notes in Computer Science, Springer-verlag, 2004