

一种隐通道威胁审计的度量方法

王昌达 鞠时光 周从华 宋香梅

(江苏大学计算机科学与通信工程学院 江苏 镇江 212013)

摘 要 隐通道分析是高等级可信评估的重要指标,在 TCSEC、CC 和我国的 GB17859—1999 等标准中均有相关要求.隐通道的威胁审计是隐通道分析的重要组成部分,目前一般使用 TCSEC 的纯带宽标准,但它并不能全面反映出隐通道的威胁.通过形式化地定义隐通道,研究其可量化属性,分析其空间拓扑结构,建立了一个用于隐通道计算的代数系统.通过引入威胁度和威胁率两个概念给出了一种新的威胁审计度量方法,新方法已有的纯带宽方法兼容,能够从多个不同的角度对隐通道的威胁程度进行较为全面的度量.进一步,在隐通道代数系统的支持下给出了审计中有关问题的计算方法,形成了一套完整的隐通道威胁审计度量体系.

关键词 隐通道;威胁审计;度量;代数系统;可信评估

中图法分类号 TP309

DOI号: 10.3724/SP.J.1016.2009.00751

A Measurement of Covert Channels Threat

WANG Chang-Da JU Shi-Guang ZHOU Cong-Hua SONG Xiang-Mei

(School of Computer Science and Telecommunication Engineering, Jiangsu University, Zhenjiang, Jiangsu 212013)

Abstract Covert channel analysis is one of an important target of high level trusted system evaluation in TCSEC, CC and GB17859—1999. Covert channel audit is a critical part of covert channel analysis. Currently the pure bandwidth criterion of TCSEC are adopted, unfortunately that can't reflect the threat of covert channels thoroughly. Via researched on its quantified characteristics and topology change, an algebra system of covert channels is presented based on formally define covert channels. Threat degree and threat rate are introduced to make a new audit measurement method that can evaluate covert channel from many different aspects to get a comprehensive measurement, which also compatible with the pure bandwidth method. Moreover, calculating methods are discussed for the measurement issues under the support of an algebra system of covert channels to form a rounded threat measurement system infrastructure.

Keywords covert channel; threat audit; measurement; algebra system; trust evaluation

1 引 言

安全模型是安全策略的形式化表述,是计算机能理解、执行的安全策略.但由于技术的限制,多数安全模型都无法做到与其代表的安全策略完全一

致.所以在这种情况下,总可以找到一些能通过安全模型的验证但却是被安全策略所禁止的操作,隐通道(covert channel)就是利用这种场景来工作的^[1].隐通道是指可信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中具有较低或不可比安全级的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,所以这种通信方式一般不能被系统的固有安全机制所检测和控制^[1].例如,(1)一个高安全级用户,通过对某个文件的加、解锁来控制低安全级用户对该文件的写入是否成功,并以此向低安全级的用户传递信息;或是,(2)一个高安全级进程通过选择自己的 CPU 占用状态影响 CPU 对低安全级进程的响应,并以此向低安全级进程传递信息,都是典型的隐通道.隐通道可以分为存储隐通道和时间隐通道^[3-4].存储隐通道是指发送方通过改变某些共享资源的属性并使接收方感知到这种变化而实现的从高安全级主体到较低或具有不可比安全级主体的信息通道.特殊地,如果这种共享资源是系统的响应时间,则称其为时间隐通道^[5].在前面提到的例子中,(1)是存储隐通道,(2)是时间隐通道.有些隐通道兼具存储和时间两种特征,如磁臂隐通道^[4].

隐通道的潜在威胁是它可能被木马程序利用泄露系统中的保密信息^[2].根据 TCSEC 的要求,隐通道的搜索、审计与消除,是软件获得 B2 级及以上可信级认证的必备条件^[6];在信息技术安全评价通用准则(CC,ISO 15408)中规定软件获得 EAL5 级及以上可信级的认证需要通过对应强度的隐通道分析^[7];我国的 GB 17859—1999 第四级、第五级亦有相似的要求.

隐通道分析需要 3 个顺序步骤:(1)搜索隐通道;(2)审计评估被搜索到的隐通道的威胁程度;(3)消除隐通道^[2].经过 20 多年的研究,人们在隐通道的搜索与消除领域积累了丰富的方法.例如可以使用信息流分析法^[8]、共享资源矩阵法^[9]、隐蔽流树法^[10]、无干扰分析法^[11]、源代码分析法^[12]以及近年来由我国学者卿斯汉等提出的回溯法^[13]或刘文清等在文献^[14]中提出的隐通道标识方法来搜索隐通道;用混沌时间法^[15]、存储转发法^[16]、泵协议法^[17]或我们课题组提出的动态法^[18]等来消除隐通道.目前隐通道的威胁审计一般采用 TCSEC 的带宽标准,即隐通道带宽在 100bits/s 以上的必须要做消除处理;带宽在 1bit/s 以下的可以不做消除处理;而带宽介于 1bit/s~100bits/s 之间的将根据具体情况,由审计人员决定是否做消除处理.因此与隐通道审计相关的研究一般局限在如何有效地估算隐通道的带宽上^[19],且数量较少,见文献^[19-21].

但是仅仅使用带宽作为审计指标并不能全面地刻画出隐通道的威胁.例如,在一个多安全级的可信系统中,密级有公开、限制、秘密、机密和绝密等五

级,其上的偏序关系“ $<$ ”是:公开 $<$ 限制 $<$ 秘密 $<$ 机密 $<$ 绝密.在这样的系统中,如果两个隐通道 CC_1 和 CC_2 的带宽都是 90bits/s,那么根据 TCSEC 中的相关标准,将无法区分它们对系统安全威胁的差别.如果 CC_1 是将敏感信息从绝密级泄露到公开级,而 CC_2 仅仅是将敏感信息从绝密级泄露到机密级,那么明显地 CC_1 与 CC_2 对系统安全的威胁并不真正相同.类似的情况还有,如果 CC_1 仅工作了 1s,而 CC_2 却工作了 1h,那么又该如何评价它们的威胁?在 TCSEC 准则关于隐通道的审计标准中,没有回答这些问题.在实践中我们认识到,审计隐通道的威胁不仅需要带宽作为指标,隐通道的安全级跨度、工作时间的长短等,都是需要综合考虑的因素.此外,一个系统中如果存在多个隐通道,它们之间的空间拓扑结构不同对系统安全的威胁也不会相同,例如两个隐通道串联可能会得到更大的安全级跨度,并联则会得到更多的带宽.

为解决这些问题,本文的主要工作是:通过形式化地定义隐通道,研究隐通道的可量化属性,进而建立一个用于隐通道计算的代数系统,然后使用包括带宽在内的多个隐通道的量化参数建立一个与纯带宽标准兼容的新的威胁审计方法,并在隐通道代数系统的支持下,给出不同空间拓扑结构的隐通道威胁的度量方法.

2 隐通道的形式化定义

目前隐通道的描述性定义多达 5 种^[2],本质上它们都能使用图 1 解释其工作原理^[5],即一个高安全级的主体 S_S 和具有较低或不可比安全级的主体 S_R 共享客体 O 的某一个属性, S_S 在时刻 t_1 通过方法 β_1 修改 O 的一个属性值并以此支配(dominate) S_R 使用方法 β_2 对 O 这一属性值的操作结果, S_R 依据在 t_2 时刻 β_2 操作是否成功来感知 S_S 发送的信息 I ,其中 $\beta_1, \beta_2 \in TCB$ (Trusted Compute Base).尽管隐通道只能识别“0,1”,即操作成功与失败两种状态,但若

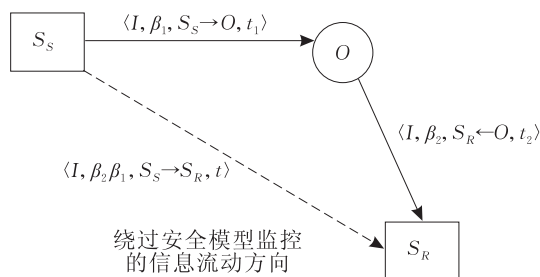


图 1 隐通道的工作原理

发送方和接收方预先约定了信息编码方式就能够通过隐通道传送任何可数字化的信息. 与信息隐藏相比, 隐通道的标志特征是每次只能传递 1 个 bit 的信息^[11].

2.1 隐通道元

定义 1. 隐通道元.

在信息传导过程中, 主体 S_S 利用传导方法 β 在 t 时刻将信息 I 通过客体 O 的某一属性传输到主体 S_R , 若这样的信息传导 $T = \langle I, \beta, S_S \rightarrow S_R, t \rangle \not\models P$, 即不满足安全策略 P 的要求, 则称其是隐通道元, 记为 ECC (Elementary Covert Channel), 隐通道元的集合记为 **ECC**.

一个隐通道元所表示的信息传导 $T = \langle I, \beta, S_S \rightarrow S_R, t \rangle$, 在时间维上可以分成 3 个有序的动作:

Action 1. $T = \langle I, \beta_1, S_S \rightarrow O, t_1 \rangle$, 即在 t_1 时刻, 主体 S_S 将信息 I 利用传导方法 β_1 送至客体 O ;

Action 2. $T = \langle I_1, \beta_2, S_R \leftarrow O, t \rangle$, 即在 t_2 时刻, 主体 S_R 从客体 O 利用传导方法 β_2 获得信息 I_1 , 这里 $I_1 \subseteq I$;

Action 3. $T = \langle I_2, \beta, S_R \leftarrow S_S, t_3 \rangle$, 即在 t_3 时刻, 主体 S_R 利用传导方法 β 从主体 S_S 获得信息 I_2 , $I_2 \subseteq I_1$. 其中, 传导方法 β 是 Action 1 和 Action 2 中两个传导方法 β_1, β_2 的累积, 记为 $\beta = \beta_2 \beta_1$.

上述 3 个动作不一定是连续发生的, 但它们发生的时刻必满足关系 $t_1 < t_2 \leq t_3$.

在一个多安全级可信系统中, 主体 S_S 将信息 I 发送至客体 O 以及主体 S_R 从客体 O 获得信息 I_1 是两个物理动作. 一般地, 传导方法 β_1, β_2 是读或写的类型, 它们必须通过系统安全机制的检查且满足安全模型才能被执行. Action 3 是一个逻辑动作, 并没有实在的物理操作发生, 所以不存在通过系统安全机制检查的过程. 传导方法 β 是 Action 1 和 Action 2 中两个传导方法 β_1, β_2 的效应累积, 故 β 通常是一个感知型的操作. 这就是说即使 β_1, β_2 满足某一安全模型 M , 也不能保证其累积效应 β 满足系统的安全策略 P .

设 $\beta \models M$ 表示某个信息传导 T 的传导方法 β 使得信息 I 的传输满足安全模型 M , 函数 $L(X)$ 表示实体 X 的安全级, “ $>$ ”和“ $<>$ ”分别表示安全级之间的支配和不可比关系, 则一个隐通道元 **ECC** 可以描述为 8 元组: $ECC = \{P, M, S_S, O, S_R, L(X), \beta_1, \beta_2\}$, 且

(1) $L(S_S) > L(S_R)$ 或 $L(S_S) <> L(S_R)$;

(2) 信息发送传导. $T_1 = \langle I_1, \beta_1, S_S \rightarrow O, t_1 \rangle \wedge$

$\beta_1 \models M, \beta_1 \in TCB$;

(3) 信息接收传导. $T_2 = \langle I_2, \beta_2, S_R \leftarrow O, t_2 \rangle \wedge \beta_2 \models M, \beta_2 \in TCB$;

(4) 信息感知传导. $T_3 = \langle I_3, \xi, S_S \rightarrow S_R, t_3 \rangle \wedge \xi \models M \wedge \xi \not\models P$, 其中 $\xi = \beta_2 \beta_1$, P 是安全策略;

(5) $I_3 \subseteq I_2 \subseteq I_1$;

(6) $t_3 \geq t_2 > t_1$.

2.2 隐通道元之间的依赖关系

定义 2. 依赖关系.

若相异的两个隐通道元代表的信息传导分别是 $T_1 = \langle I, \beta_1, S_S \rightarrow S, t_1 \rangle$ 和 $T_2 = \langle I, \beta_2, S \rightarrow S_R, t_2 \rangle$, 其中 S 为两个隐通道元的共享主体, 且 $t_2 > t_1$. 通过 T_1, T_2 两者的相继传导作用, 若能成功地将信息 I 从 T_1 所表示的隐通道元的起始端传送到 T_2 所表示的隐通道元的末端, 则称这两个隐通道元之间具有依赖关系, 记为 $T_1 \vdash T_2$. 其中 T_1 代表的隐通道元为该依赖关系的前元, T_2 代表的隐通道元为该依赖关系的后元.

依赖关系的性质如下.

性质 1. 时序性. 如果 $T_1 \vdash T_2$, 则 $t_2 > t_1$ 一定成立. 即在一个依赖关系中, 根据绝对时钟, 前元先发生, 后元后发生.

性质 2. 共享主体. 如果 $T_1 \vdash T_2$, 则存在某一主体 S , 它是前元、后元的共享主体, 即 $S \in T_1 \wedge S \in T_2$ 成立.

性质 3. 依赖的传递性. 如果 $T_1 \vdash T_2$ 且 $T_2 \vdash T_3$, 则 $T_1 \vdash T_3$.

性质 4. 作用效果累积. 如果 $T_1 \vdash T_2$, 则 β_1 发生的作用效果对 β_2 发生的结果有影响, 反之不然.

2.3 隐通道

设 **ECC** 是一个可信系统中全体隐通道元的非空集合, I 为所传导信息的集合, $\beta: ECC \times I \rightarrow I$ 是信息传导方法.

定义 3. 隐通道.

n 个隐通道元首尾相连 ($n \geq 1$), $T_1 = \langle I, \beta_1, S_1 \rightarrow S_2, t_1 \rangle, T_2 = \langle I, \beta_2, S_2 \rightarrow S_3, t_2 \rangle, \dots, T_n = \langle I, \beta_n, S_n \rightarrow S_{n+1}, t_n \rangle$ 分别表示这 n 个隐通道元所形成的信息传导, 若

(1) 对于任意的 $1 \leq i \leq n-1, i \in \mathbb{N}$, 则 $T_i \vdash T_{i+1}$ 成立;

(2) 对于任意的 $1 \leq j < k \leq N, j \in \mathbb{N}, k \in \mathbb{N}$, 则 $L(S_j) > L(S_k)$ 或 $L(S_j) <> L(S_k)$ 成立;

那么将这个隐通道元的依赖链 $(\dots(T_1 \vdash T_2) \vdash \dots) \vdash T_n$ 称为一个隐通道, 记为 **CC**, 隐通道的集合记

为 \mathbf{CC} .

条件(1)决定了隐通道元之间的序关系,条件(2)决定了隐通道具有唯一确定的隐通道元组成结构.

推论 1. 一个隐通道包含唯一确定的非空若干个有序隐通道元,其排列顺序由隐通道元在隐通道中的依赖关系决定.

定义 4. 隐通道的描述.

对任意的隐通道 $\mathbf{CC} \in \mathbf{CC}$, 定义记号 $\underline{\mathbf{CC}} = \{ECC_1, ECC_2, \dots, ECC_n\}$, 其中 $ECC_i \in \mathbf{ECC}$, $1 \leq i \leq n$, $n \in \mathbf{N}$, 是组成 \mathbf{CC} 的 n 个有序隐通道元, 则称 $\underline{\mathbf{CC}}$ 是隐通道 \mathbf{CC} 的描述.

推论 2. 在 $\underline{\mathbf{CC}}$ 中, 对于任意的 $1 \leq i \leq n$, $n \in \mathbf{N}$, 有 $ECC_i \vdash ECC_{i+1}$ 成立, 即 ECC_{i+1} 依赖 ECC_i .

推论 3. 一个隐通道元即是一个隐通道, 隐通道元是隐通道的最小组成单位.

3 隐通道的可量化属性

根据定义 3, 我们知道:

(1) 隐通道的发送方和接收方是主体, 且发送主体的安全级高于接收主体的安全级或两者之间不具有可比性.

(2) 隐通道是有向的, 其方向是信息从发送主体 S_s 流向接收主体 S_R .

(3) 通过隐通道传递的信息能够通过安全模型 M 的检验, 但却是违反安全策略 P 的.

在此基础上, 我们讨论隐通道的可量化属性.

定理 1. 若一个可信系统中主体集合 \mathbf{S} 和客体集合 \mathbf{O} 的基数分别是 m 和 n , 则隐通道元集合 \mathbf{ECC} 是有限集, 且 \mathbf{ECC} 的基数不超过 $P_m^2 \cdot n$.

证明. \mathbf{S} 的基数 $\text{card}(\mathbf{S}) = m$, \mathbf{O} 的基数 $\text{card}(\mathbf{O}) = n$, 其中 $m, n \in \mathbf{N}$. 根据定义 1, 并非任意一个三元组 (S_s, S_R, O) 都能用于构造隐通道元, 所以必有 \mathbf{ECC} 的基数 $\text{card}(\mathbf{ECC}) \leq m(m-1)n = P_m^2 \cdot n$, \mathbf{ECC} 是有限集. 证毕.

定理 2. 若隐通道元集合 \mathbf{ECC} 的基数 $\text{card}(\mathbf{ECC}) = k$, 则隐通道集合 \mathbf{CC} 的基数 $\text{card}(\mathbf{CC}) \leq 2^k - 1$.

证明. 设 $\text{Power}(\mathbf{ECC})$ 表示 \mathbf{ECC} 的幂集, 由定义 3 可知隐通道的集合 $\mathbf{CC} \subseteq \text{Power}(\mathbf{ECC}) - \Phi$, 而 $\text{Power}(\mathbf{ECC}) = 2^k$, 所以 $\text{card}(\mathbf{CC}) \leq 2^k - 1$.

证毕.

推论 4. 一个可信系统中的隐通道集合 \mathbf{CC} 是有限集.

定义 5. 隐通道的顶和尾.

对任意的隐通道 $\mathbf{CC} \in \mathbf{CC}$, 根据定义 4, $\underline{\mathbf{CC}} = \{ECC_1, ECC_2, \dots, ECC_n\}$, 其中 $ECC_i \in \mathbf{ECC}$, $1 \leq i \leq n$, 是组成 \mathbf{CC} 的 n 个有序隐通道元的集合. 则 ECC_1 的发送主体, 称为该隐通道 \mathbf{CC} 的顶, 记为 $\text{Head}(\mathbf{CC})$, ECC_n 的接收主体, 称为该隐通道 \mathbf{CC} 的尾, 记为 $\text{Rear}(\mathbf{CC})$. 即在一个隐通道中, $\text{Head}(\mathbf{CC})$ 是保密信息以违背系统安全策略方式流动的起点, $\text{Rear}(\mathbf{CC})$ 是其终点.

推论 5. 任意一个隐通道的 $\text{Head}(\mathbf{CC})$ 和 $\text{Rear}(\mathbf{CC})$ 是唯一的, 且 $\text{Head}(\mathbf{CC})$ 的安全级高于 $\text{Rear}(\mathbf{CC})$ 的安全级或两者之间不具有可比性.

定义 6. 隐通道相等.

对于任意隐通道 $\mathbf{CC}_1, \mathbf{CC}_2 \in \mathbf{CC}$, $\underline{\mathbf{CC}}_1 = \{ECC_{11}, ECC_{12}, \dots, ECC_{1M}\}$, $\underline{\mathbf{CC}}_2 = \{ECC_{21}, ECC_{22}, \dots, ECC_{2N}\}$, 若 $M=N$ 且对任意 $1 \leq i \leq M$, 有 $ECC_{1i} = ECC_{2i}$, 则称隐通道 \mathbf{CC}_1 与 \mathbf{CC}_2 相等, 记为 $\mathbf{CC}_1 = \mathbf{CC}_2$.

定义 6 表明, 相等的隐通道具有完全相同的隐通道元组成结构. 这里“结构”一词有两个含义: (1) 指隐通道元之间的序关系相同; (2) 指隐通道元之间的依赖关系相同.

我们知道在一个有 $n(n \geq 2, n \in \mathbf{N})$ 个安全级的多安全级可信系统中, 对于任意的 $X \in \mathbf{S} \cup \mathbf{O}$, 其安全级 $L(X) = \{(C, K) \mid C \in \mathbf{C} \wedge K \in \mathbf{K}\}$ 是一个二元组, 其中 \mathbf{C} 是等级分类集合, \mathbf{K} 是非等级类别集合. 等级分类集合 \mathbf{C} 中的元素是密级, 在 \mathbf{C} 中存在全序关系“ $<$ ”, 如公开 $<$ 限制 $<$ 秘密 $<$ 机密 $<$ 绝密. 非等级类别集合 \mathbf{K} 中的元素是部门集, 如部门 A、部门 B、部门 C 等, 在 \mathbf{K} 中无明显的序关系. 安全级之间的关系可以分为以下 3 种:

(1) 相等关系“ $=$ ”

对于任意的安全级 $L_1 = (C_1, K_1), L_2 = (C_2, K_2)$, 若 $C_1 = C_2 \wedge K_1 = K_2$, 则称 $L_1 = L_2$.

(2) 支配关系“ \geq ”

对于任意的安全级 $L_1 = (C_1, K_1), L_2 = (C_2, K_2)$, 若 $C_1 \geq C_2 \wedge K_1 \supseteq K_2$, 则称 $L_1 \geq L_2$.

(3) 不可比关系“ $<>$ ”

对于任意的安全级 $L_1 = (C_1, K_1), L_2 = (C_2, K_2)$, 若 $K_1 \not\subseteq K_2 \wedge K_2 \not\subseteq K_1$, 则称 $L_1 <> L_2$.

设 $\text{Class}(X), X \in \mathbf{S} \cup \mathbf{O}$, 是一个定义在等级分类集合 \mathbf{C} 上的函数, 若将 \mathbf{C} 中的所有密级, 按照从低到高的顺序排成一个数列 $\{a_i\}, 1 \leq i \leq n$, 对于任意的 X , 若其密级是 a_i , 则令 $\text{Class}(X) = i$.

定义 7. 隐通道的势差 U_{cc} .

对任意的隐通道 $CC \in \mathbf{CC}$, $L(\text{Head}(CC)) = \{(C1, K1) \mid C1 \in \mathbf{C} \wedge K1 \in \mathbf{K}\}$, $L(\text{Rear}(CC)) = \{(C2, K2) \mid C2 \in \mathbf{C} \wedge K2 \in \mathbf{K}\}$, 定义 $U_{CC} = |\text{Class}(C1) - \text{Class}(C2)| + \lambda$, 其中 λ 表示 $K1$ 与 $K2$ 之间的距离。

一般地, 集合之间的距离度量并不满足欧式空间距离的定义, 而是 Hausdorff 距离的推广^[22]. 我们知道在安全级的定义中, \mathbf{K} 的物理意义是由涉密的不同部门或机构所组成的集合. 用“ \subset ”表示部门或机构之间的隶属管理, 那么容易验证“ \subset ”在 \mathbf{K} 上满足以下 3 条性质:

对于任意的 $A, B, C \in \mathbf{K}$,

(1) 自反性: $A \subset A$;

(2) 反对称性: $A \subset B \Rightarrow B \not\subset A$;

(3) 传递性: $A \subset B \wedge B \subset C \Rightarrow A \subset C$.

所以序偶 $\langle \mathbf{K}, \subset \rangle$ 是一个偏序集. 在偏序集合 $\langle \mathbf{K}, \subset \rangle$ 中, 如果 $A, B \in \mathbf{K}$, $A \subset B$, $A \neq B$, 且没有其它元素 $C \in \mathbf{K}$ 满足 $A \subset C$, $C \subset B$, 则称元素 B 盖住元素 A . 对于给定的偏序集, 其盖住关系是唯一的, 所以可以用盖住关系画出偏序集合图, 即哈斯图^[23]. 对于任意的 $A, B \in \mathbf{K}$, 我们定义 A 与 B 之间的距离 λ 是哈斯图上 A 与 B 之间最短路径的长度。

λ 的数值可由其对应哈斯图的邻接矩阵计算得出, 其依据是图论中的一个重要定理: 若 $\mathbf{M}(G)$ 是图 G 的邻接矩阵, 则 $(\mathbf{M}(G))^n$ 中的 i 行 j 列元素 $m_{ij}^{(n)}$ 等于 G 中联结节点 v_i 与 v_j 长度为 n 的路的数目^[23]. 即可从 $n=1$ 开始, 通过对矩阵 $\mathbf{M}(G)$ 逐次进行乘法运算, 当首次出现 $m_{ij}^{(n)} \neq 0$ 时, 即可判定节点 v_i 与 v_j 之间的最短路径长度为 n .

在 U_{CC} 的定义中, $|\text{Class}(C1) - \text{Class}(C2)|$ 衡量了隐通道工作时所形成的密集跨度, λ 则衡量了泄密涉及的两个部门之间的接近程度. 在相同部门的内部 $\lambda=0$, 在具有直接隶属关系的部门之间 $\lambda=1$, 在不具有直接隶属关系的部门之间 $\lambda \geq 2$.

推论 6. $U_{CC} \geq 1$ 且 $U_{CC} \in \mathbf{N}$.

研究隐通道势差的意义在于, 为隐通道中流动的保密信息所能实现的安全级跨度提供了一个量化的指标。

定义 8. 隐通道的带宽 I_{CC} .

隐通道 CC 的带宽 I_{CC} , 是在单位时间内通过该隐通道泄漏信息的 bit 数, 其单位是 bits/s.

定义 9. 隐通道的长度 L_{CC} .

隐通道 CC 的长度 L_{CC} , 是 1 个 bit 的信息从隐通道的顶 $\text{Head}(CC)$ 流到隐通道的尾 $\text{Rear}(CC)$ 所

经历的隐通道元的个数。

推论 7. 隐通道元的长度为 1, 隐通道的最短长度为 1.

任何通信信道都可以分为有噪音通道和无噪音通道两大类. 在一个隐通道中, 如果对发送方传送的任意比特, 接收方都能以概率 1 正确地解码, 则称该通道为无噪音通道. 相反地, 在噪音通道中, 对发送方传送的任意比特, 接收方能够正确解码的概率小于 1. 所以隐通道工作的可靠性与接收方能够正确解码发送方传递信息的概率正相关, 即解码的概率越高, 工作的可靠性也越高. 因此一个隐通道的可靠性不仅取决于其自身的结构, 还取决于其工作时的系统环境. 这是在审计隐通道的威胁时需要综合考虑的因素。

定义 10. 隐通道的可靠性 P_{CC} .

隐通道 CC 的可靠性 P_{CC} , 是该隐通道能正确工作的概率, 其中 $P_{CC} \in (0, 1]$.

这里 P_{CC} 的值不取 0, 是因为若 $P_{CC}=0$, CC 将是一个不能工作的隐通道, 即无害通道, 因而没有理论研究和工程实践的意义。

推论 8. 隐通道的可靠性与其长度成反比, 即 $P_{CC} \propto 1/L_{CC}$.

定义 11. 隐通道的特征向量

对于任意的隐通道 $CC \in \mathbf{CC}$, 隐通道的特征向量 $\mathbf{F}(CC) = \{U_{CC}, I_{CC}, L_{CC}, P_{CC}\} \in \mathbf{R}^4$.

定义 11 的作用在于定量地描述隐通道, 它提供了从隐通道到实数集上四元组的一个映射。

4 隐通道的代数系统

隐通道的代数系统, 是由隐通道集合 \mathbf{CC} 与其上的若干个二元代数运算所构成的整体, 其主要内容是研究隐通道拓扑结构变化对部分可量化属性的影响, 并从中抽象出最基本的公共性质, 建立适用于隐通道威胁审计度量的数学工具。

4.1 隐通道集合上的二元关系

定义 12(“+”). 设隐通道 $CC_1, CC_2 \in \mathbf{CC}$, $\underline{CC}_1 = \{ECC_{11}, ECC_{12}, \dots, ECC_{1M}\}$, $\underline{CC}_2 = \{ECC_{21}, ECC_{22}, \dots, ECC_{2N}\}$, 其中 $ECC_{1i}, ECC_{2j} \in \mathbf{ECC}$, $1 \leq i \leq M, 1 \leq j \leq N$, 是组成 CC_1 和 CC_2 的若干个有序隐通道元. 若 $\text{Rear}(CC_1) = \text{Head}(CC_2)$, 且 $\{ECC_{11}, ECC_{12}, \dots, ECC_{1M}, ECC_{21}, ECC_{22}, \dots, ECC_{2N}\}$ 满足定义 3, 那么定义 $CC_1 + CC_2 = CC_3 \in \mathbf{CC}$, 且有 $\text{Head}(CC_3) = \text{Head}(CC_1)$, $\text{Rear}(CC_3) = \text{Rear}(CC_2)$,

$$\underline{CC}_3 = \{ECC_{11}, ECC_{12}, \dots, ECC_{1M}, ECC_{21}, ECC_{22}, \dots, ECC_{2N}\}.$$

“+”研究的是隐通道之间的串联关系. 在工程实践上, 对隐通道串连的需求是: 当两个不同安全级的主体之间无法借助一个隐通道实现违反系统安全策略的通信时, 那么就会考虑借助两个或更多个隐通道, 通过逐级串联的方式进行通信. 与所有串联的通信方式类似, 串联得到的隐通道要能够正常工作, 要求串联组成该隐通道的所有子隐通道都必须能正常工作, 因此串联会降低隐通道传递信息的可靠性 P_{CC} .

定义 13 (“-”). 设隐通道 $CC_1, CC_2 \in \mathbf{CC}$, 若 $CC_1 + CC_2 = CC_3 \in \mathbf{CC}$, 则定义 $CC_1 = CC_3 - CC_2$.

根据定义 12 显然有 $Head(CC_1) = Head(CC_3)$, $Rear(CC_1) = Rear(CC_2)$. 因为 $(CC_1 + CC_2) - CC_2 = CC_1$, 所以“-”是“+”的右逆运算. “-”的直观意义是, 如何在系统中逐级撤销由串联方式所构成的隐通道.

定义 14 (“ \vee ”). 设隐通道 $CC_1, CC_2 \in \mathbf{CC}$, $\underline{CC}_1 = \{ECC_{11}, ECC_{12}, \dots, ECC_{1M}\}$, $\underline{CC}_2 = \{ECC_{21}, ECC_{22}, \dots, ECC_{2N}\}$, 其中 $ECC_{1i}, ECC_{2j} \in \mathbf{ECC}$, $1 \leq i \leq M, 1 \leq j \leq N$, 是组成 CC_1 和 CC_2 的非空若干个有序隐通道元. 若 $Head(CC_1) = Head(CC_2)$, $Rear(CC_1) = Rear(CC_2)$, 且 $\underline{CC}_1 \cap \underline{CC}_2 = \emptyset$, 则定义 $CC_1 \vee CC_2 = CC_3 \in \mathbf{CC}$, 且 $Head(CC_3) = Head(CC_1) = Head(CC_2)$, $Rear(CC_3) = Rear(CC_1) = Rear(CC_2)$.

“ \vee ”运算研究的是隐通道之间的并联关系. 在工程实践上, 对隐通道并连的需求是: 当两个不同安全级的主体之间借助一个隐通道实现隐蔽通信时带宽过低, 那么就会考虑借助两个或更多个隐通道通过并联的方式, 即“ \vee ”运算, 来分担通信流量, 从而达到获取较高通信带宽的目的. 与所有并联的通信方式类似, 并联得到的隐通道要能够正常工作, 只要并联组成该隐通道中的任意一个子隐通道能够正常工作即可, 所以并联不仅会提高隐通道的带宽 I , 也会提高其可靠性 P_{CC} .

这里显然有, $CC_1 \vee CC_2 = CC_2 \vee CC_1$. 所以我们约定

$$\begin{aligned} \underline{CC}_3 &= \underline{CC}_1 \vee \underline{CC}_2 \\ &= \{ECC_{11}, ECC_{12}, \dots, ECC_{1M}\} \vee \\ &\quad \{ECC_{21}, ECC_{22}, \dots, ECC_{2N}\} \\ &= \left\{ \begin{array}{l} ECC_{11}, ECC_{12}, \dots, ECC_{1M} \\ ECC_{21}, ECC_{22}, \dots, ECC_{2N} \end{array} \right\} \end{aligned}$$

$$\begin{aligned} &= \left\{ \begin{array}{l} ECC_{21}, ECC_{22}, \dots, ECC_{2N} \\ ECC_{11}, ECC_{12}, \dots, ECC_{1M} \end{array} \right\} \\ &= \underline{CC}_2 \vee \underline{CC}_1. \end{aligned}$$

定义 15 (“ \wedge ”). 设隐通道 $CC_1, CC_2 \in \mathbf{CC}$, 若 $CC_1 \vee CC_2 = CC_3 \in \mathbf{CC}$, 则 $CC_1 = CC_3 \wedge CC_2$.

因为 $(CC_1 \vee CC_2) \wedge CC_2 = CC_1$ 且 $CC_1 \wedge (CC_1 \vee CC_2) = CC_2$, 所以“ \wedge ”是“ \vee ”的逆运算. “ \wedge ”运算的直观意义是, 如何在系统中逐级撤销由并联方式所构成的隐通道. 根据定义 14 显然有

$$Head(CC_1) = Head(CC_2) = Head(CC_3),$$

$$Rear(CC_1) = Rear(CC_2) = Rear(CC_3).$$

4.2 代数系统

定义 16. 隐通道的代数系统.

设 \mathbf{CC} 是一个多安全级可信系统中隐通道的非空集合, τ 为 \mathbf{CC}^2 到 \mathbf{CC} 的映射, 即 $\tau: \mathbf{CC}^2 \rightarrow \mathbf{CC}$, 其中 $\tau = \{+, -, \vee, \wedge\}$ 是 \mathbf{CC} 上二元代数运算关系的集合, 则集合 \mathbf{CC} 与 τ 一起构成了隐通道的代数系统.

隐通道的代数系统研究的是隐通道集合上的二元代数运算关系, 即隐通道的串联、并联、撤销串联、撤销并联等操作, 使用这些关系符能够描述隐通道的不同空间拓扑结构. 下面通过讨论隐通道代数系统的运算法则证明隐通道集合与其上的串联与并联运算构成半群.

4.3 隐通道代数系统的运算法则

(1) “+”和“ \wedge ”运算满足结合率

$$\textcircled{1} (CC_1 + CC_2) + CC_3 = CC_1 + (CC_2 + CC_3)$$

证明. 若 $(CC_1 + CC_2) + CC_3, CC_1 + (CC_2 + CC_3)$ 均有意义, 对隐通道 $CC_1, CC_2, CC_3 \in \mathbf{CC}$, 不妨设

$$\underline{CC}_1 = \{ECC_{11}, ECC_{12}, \dots, ECC_{1L}\},$$

$$\underline{CC}_2 = \{ECC_{21}, ECC_{22}, \dots, ECC_{2M}\},$$

$$\underline{CC}_3 = \{ECC_{31}, ECC_{32}, \dots, ECC_{3N}\},$$

则根据定义 12 有

$$\begin{aligned} \text{左边} &= \{ECC_{11}, ECC_{12}, \dots, ECC_{1L}, \\ &\quad ECC_{21}, ECC_{22}, \dots, ECC_{2M}\} + \\ &\quad \{ECC_{31}, ECC_{32}, \dots, ECC_{3N}\} \\ &= \{ECC_{11}, ECC_{12}, \dots, ECC_{1L}, \\ &\quad ECC_{21}, ECC_{22}, \dots, ECC_{2M}, \\ &\quad ECC_{31}, ECC_{32}, \dots, ECC_{3N}\}, \\ \text{右边} &= \{ECC_{11}, ECC_{12}, \dots, ECC_{1L}\} + \\ &\quad \{ECC_{21}, ECC_{22}, \dots, ECC_{2M}, \\ &\quad ECC_{31}, ECC_{32}, \dots, ECC_{3N}\} \\ &= \{ECC_{11}, ECC_{12}, \dots, ECC_{1L}, \\ &\quad ECC_{21}, ECC_{22}, \dots, ECC_{2M}, \end{aligned}$$

$$ECC_{31}, ECC_{32}, \dots, ECC_{3N}\},$$

其中

$$Rear(ECC_{1L}) = Head(ECC_{21}),$$

$$Rear(ECC_{2M}) = Head(ECC_{31}),$$

故由定义 6 可知,

$$(CC_1 + CC_2) + CC_3 = CC_1 + (CC_2 + CC_3).$$

$$\textcircled{2} (CC_1 \vee CC_2) \vee CC_3 = CC_1 \vee (CC_2 \vee CC_3)$$

证明. 若 $(CC_1 \vee CC_2) \vee CC_3, CC_1 \vee (CC_2 \vee CC_3)$

均有意义, 对隐通道 $CC_1, CC_2, CC_3 \in \mathbf{CC}$, 不妨设

$$\underline{CC}_1 = \{ECC_{11}, ECC_{12}, \dots, ECC_{1L}\},$$

$$\underline{CC}_2 = \{ECC_{21}, ECC_{22}, \dots, ECC_{2M}\},$$

$$\underline{CC}_3 = \{ECC_{31}, ECC_{32}, \dots, ECC_{3N}\},$$

则根据定义 14 有

$$\begin{aligned} \text{左边} &= \left\{ \begin{array}{l} ECC_{11}, ECC_{12}, \dots, ECC_{1L} \\ ECC_{21}, ECC_{22}, \dots, ECC_{2M} \\ ECC_{31}, ECC_{32}, \dots, ECC_{3N} \end{array} \right\} \vee \\ &= \left\{ \begin{array}{l} ECC_{11}, ECC_{12}, \dots, ECC_{1L} \\ ECC_{21}, ECC_{22}, \dots, ECC_{2M} \\ ECC_{31}, ECC_{32}, \dots, ECC_{3N} \end{array} \right\}, \\ \text{右边} &= \{ECC_{11}, ECC_{12}, \dots, ECC_{1L}\} \vee \\ &\quad \left\{ \begin{array}{l} ECC_{21}, ECC_{22}, \dots, ECC_{2M} \\ ECC_{31}, ECC_{32}, \dots, ECC_{3N} \end{array} \right\} \\ &= \left\{ \begin{array}{l} ECC_{11}, ECC_{12}, \dots, ECC_{1L} \\ ECC_{21}, ECC_{22}, \dots, ECC_{2M} \\ ECC_{31}, ECC_{32}, \dots, ECC_{3N} \end{array} \right\}. \end{aligned}$$

所以根据定义 6, 有

$$(CC_1 \vee CC_2) \vee CC_3 = CC_1 \vee (CC_2 \vee CC_3).$$

其中

$$Head(ECC_{11}) = Head(ECC_{21}) = Head(ECC_{31}),$$

$$Rear(ECC_{1L}) = Rear(ECC_{2M}) = Rear(ECC_{3N}).$$

(2) “ \vee ”运算满足交换律

证明. 若 $CC_1 \vee CC_2, CC_2 \vee CC_1$ 均有意义, 对隐通道 $CC_1, CC_2 \in \mathbf{CC}$, 不妨设

$$\underline{CC}_1 = \{ECC_{11}, ECC_{12}, \dots, ECC_{1L}\},$$

$$\underline{CC}_2 = \{ECC_{21}, ECC_{22}, \dots, ECC_{2M}\},$$

则根据定义 14 有

$$\begin{aligned} \text{左边} &= \left\{ \begin{array}{l} ECC_{11}, ECC_{12}, \dots, ECC_{1M} \\ ECC_{21}, ECC_{22}, \dots, ECC_{2N} \end{array} \right\} \\ &= \left\{ \begin{array}{l} ECC_{21}, ECC_{22}, \dots, ECC_{2N} \\ ECC_{11}, ECC_{12}, \dots, ECC_{1M} \end{array} \right\} \\ &= \text{右边}. \end{aligned}$$

所以根据定义 6, 有

$$CC_1 \vee CC_2 = CC_2 \vee CC_1.$$

因为 $+$, \vee 在集合 \mathbf{CC} 上具有封闭性且满足结合律, 所以有如下结论成立.

推论 9. $\langle \mathbf{CC}, + \rangle, \langle \mathbf{CC}, \vee \rangle$ 是半群.

5 隐通道威胁审计的量化指标

隐通道除了带宽 I 以外, 其势差 U 越高、工作时间 Δt 越长, 相应地对系统安全的威胁也越大, 势差高说明分级保密信息在泄漏的过程中安全级跨度大; 工作时间长, 说明通过隐通道向外泄漏的保密信息数量多. 为克服 TCSCE 中将带宽作为唯一审计指标的局限性, 本节在综合考虑隐通道带宽、势差和工作时间等参数的基础上, 引入两个新的指标来定量地刻画隐通道的威胁.

5.1 隐通道的威胁度和威胁率

定义 17. 隐通道的威胁度.

对任意 $CC \in \mathbf{CC}$, $W(U_{CC}, I_{CC}, \Delta t) = U_{CC} \cdot I_{CC} \cdot \Delta t$, 称为隐通道 CC 在工作时间段 $[t_s, t_e]$ 内的威胁度, 其中 $\Delta t = t_e - t_s > 0$.

一般地, 如果隐通道 CC 确定, 那么 U_{CC} 是确定的, 但 I_{CC} 往往会随着系统运行状态的不同而发生变化, 即 I_{CC} 是时间 t 的函数, 记为 $I_{CC}(t)$.

定义 18. 隐通道的威胁率.

对任意的 $CC \in \mathbf{CC}$, $WP(U_{CC}, I_{CC}(t_0)) = U_{CC} \cdot I_{CC}(t_0)$, 称为隐通道 CC 在 t_0 时刻的瞬时威胁率.

隐通道的威胁度 W 是评估在一段时间内, 隐通道对系统安全威胁程度的量化指标; 而隐通道的威胁率 WP 则是衡量在某一个瞬间时刻, 隐通道对系统安全威胁程度的量化指标.

5.2 等效隐通道

定义 19. 等效隐通道.

对任意 $CC_1, CC_2 \in \mathbf{CC}$, 若 $WP_{CC_1} = WP_{CC_2}$, 则称 CC_1 与 CC_2 是等效的隐通道.

推论 10. 具有相同势差和带宽的隐通道是等效的, 等效的隐通道不一定具有相同的势差和带宽.

推论 11. 对任意 $CC_1, CC_2 \in \mathbf{CC}$, CC_1 与 CC_2 是等效的充分非必要条件是 $F(CC_1) = F(CC_2)$, 其中 $F(CC) = \{U_{CC}, I_{CC}, L_{CC}, P_{CC}\}$ 是隐通道的特征向量.

推论 12. 对任意 $CC_1, CC_2 \in \mathbf{CC}$, 若 CC_1 与 CC_2 等效, 那么在相同的工作时间 $\Delta t > 0$ 内, CC_1 与 CC_2 的威胁度相同, 即 $W_{CC_1} = W_{CC_2}$.

6 隐通道审计的 IA(Integrated Audit) 标准

设 CC_1 和 CC_2 是同一多安全级可信系统中的两个隐通道,则

(1) 在工作时间 $\Delta t > 0$ 内, CC_1 的威胁大于 CC_2 当且仅当 $W_{CC_1} > W_{CC_2}$;

(2) 在 t_0 时刻, CC_1 的威胁大于 CC_2 当且仅当 $WP_{CC_1} > WP_{CC_2}$.

若 $W_{CC_1} = W_{CC_2}$ 或 $WP_{CC_1} = WP_{CC_2}$, 则具有较高工作可靠性 P_{CC} 的隐通道威胁也较大.

6.1 隐通道威胁率的计算

(1) $CC_1 + CC_2$ 威胁率的计算

若 $CC_1, CC_2 \in CC$, 且有 $CC_1 + CC_2 = CC_3 \in CC$, 那么根据定义 12 我们有 $Head(CC_3) = Head(CC_1)$, $Rear(CC_3) = Rear(CC_2)$, 所以 U_{CC_3} 的值可由定义 7 算出. 根据定义 12, CC_3 的带宽由 CC_1 和 CC_2 的最小带宽决定, 即 $I_{CC_3} = \min(I_{CC_1}, I_{CC_2})$. 因此有 $WP_{CC_1+CC_2} = U_{CC_3} \cdot \min(I_{CC_1}, I_{CC_2})$. 在这种情况下, CC_3 要正常工作, 必须 CC_1 和 CC_2 同时正常工作, 故 CC_3 的可靠性 $P_{CC_3} = P_{CC_1} P_{CC_2}$.

(2) $CC_1 - CC_2$ 威胁率的计算

若 $CC_1, CC_2 \in CC$, 且有 $CC_1 - CC_2 = CC_3 \in CC$, 那么根据定义 13 我们有 $Head(CC_3) = Head(CC_1)$, $Rear(CC_3) = Head(CC_2)$, 与上例相似, U_{CC_3} 可以根据定义 7 计算得出.

又因为 $CC_3 = CC_1 - CC_2$, 所以 $CC_1 = CC_3 + CC_2$, 由上例中的分析可知 $I_{CC_1} = \min(I_{CC_2}, I_{CC_3})$, 即有 $I_{CC_2} \geq I_{CC_1}$ 成立, 下面分两种情况进行讨论:

① $I_{CC_1} < I_{CC_2}$, 因为 $I_{CC_1} = \min(I_{CC_2}, I_{CC_3})$, 所以 $I_{CC_3} = I_{CC_1}$, 故 $WP_{CC_1-CC_2} = U_{CC_3} I_{CC_1}$.

② 若 $I_{CC_1} = I_{CC_2}$, 因为 $I_{CC_1} = \min(I_{CC_2}, I_{CC_3})$, 所以 $I_{CC_3} > I_{CC_1}$, 此时 I_{CC_3} 不能由 I_{CC_1}, I_{CC_2} 确定, 需要额外约束条件作进一步分析. 因此有, $WP_{CC_1-CC_2} = U_{CC_3} I_{CC_3}$.

在这种情况下, 因为 $CC_1 = CC_3 + CC_2$, 所以 $P_{CC_1} = P_{CC_2} P_{CC_3}$, 故 CC_3 的可靠性 $P_{CC_3} = P_{CC_1} / P_{CC_2}$.

(3) $CC_1 \vee CC_2$ 威胁率的计算

若 $CC_1, CC_2 \in CC$, 且有 $CC_1 \vee CC_2 = CC_3 \in CC$, 那么根据定义 14 有 $U_{CC_3} = U_{CC_1} = U_{CC_2}$, $I_{CC_3} = I_{CC_1} + I_{CC_2}$, 因此有 $WP_{CC_1 \vee CC_2} = U_{CC_1} (I_{CC_1} + I_{CC_2})$.

根据定义 14, CC_3 完全不可靠的条件是, 当且仅当 CC_1 与 CC_2 同时不可靠, 所以 CC_3 的可靠性为

$$P_{CC_3} = 1 - (1 - P_{CC_1})(1 - P_{CC_2}).$$

(4) $CC_1 \wedge CC_2$ 威胁率的计算

若 $CC_1, CC_2 \in CC$, 且有 $CC_1 \wedge CC_2 = CC_3 \in CC$, 那么根据定义 15 有 $U_{CC_3} = U_{CC_1} = U_{CC_2}$, 又因为 $CC_3 = CC_1 \wedge CC_2$, 所以 $CC_1 = CC_3 \vee CC_2$, 由上例可知 $I_{CC_1} = I_{CC_2} + I_{CC_3}$, 即有 $I_{CC_3} = I_{CC_1} - I_{CC_2}$, 因此有 $WP_{CC_1 \wedge CC_2} = U_{CC_1} (I_{CC_1} - I_{CC_2})$.

又因为 $CC_1 = CC_3 \vee CC_2$, 所以由上例可知: $P_{CC_1} = 1 - (1 - P_{CC_2})(1 - P_{CC_3})$, 从此式中可解出 CC_3 的可靠性为 $P_{CC_3} = (P_{CC_1} - P_{CC_2}) / (1 - P_{CC_2})$.

6.2 隐通道威胁度的计算

当隐通道的带宽 I 是一个常量时, 隐通道的威胁度 W 在 $\tau = \{+, -, \vee, \wedge\}$ 上的计算可以仿照 WP 的计算给出. 下面讨论当隐通道的带宽 I 是时间 t 的函数时, 隐通道威胁度 W 的计算方法.

对任意的隐通道 $CC \in CC$, 如果在时间 $[t_s, t_e]$ 内, I_{CC} 是常数, 那么 $W(U_{CC}, I_{CC}, \Delta t) = U_{CC} \cdot I_{CC} \cdot \Delta t$ 可以直接计算得出. 一般地, I_{CC} 是时间 t 的函数, 即 $I_{CC}(t)$. 在这种情况下, 我们首先在 CC 的工作时间 $[t_s, t_e]$ 内插入 $n+1$ 个分点, 其中 $t_s = t_0 < t_1 < \dots < t_{n-1} < t_n = t_e$, 那么整个区间被分成 n 个较小的闭区间 Δ_i , 其中 $\Delta_i = [t_{i-1}, t_i]$, $i = 1, 2, 3, \dots, n$. 因为在区间 Δ_i 内, $I_{CC}(t)$ 可以近似地认为是常数, 故隐通道 CC 的威胁度在 Δ_i 内的增量可以表示为 $\Delta_i W_{CC} \approx U_{CC} \cdot I_{CC}(\xi_i) \cdot \Delta t_i$, 其中 $\xi_i \in \Delta_i$, $\Delta t_i = t_i - t_{i-1}$. 又因为

$W_{CC} = \sum_{i=1}^n \Delta_i W_{CC}$, 所以 $W_{CC} = \lim_{\|\Delta t_i\| \rightarrow 0} \sum_{i=1}^n U_{CC} I_{CC}(\xi_i) \Delta t_i$, 其中 $\xi_i \in \Delta_i$, $\|\Delta t_i\| = \max_{1 \leq i \leq n} \{\Delta t_i\}$, 又因为在 CC 选定的情况下 U_{CC} 是一个常数, 所以有 $W_{CC} = U_{CC} \cdot$

$\lim_{\|\Delta t_i\| \rightarrow 0} \sum_{i=1}^n I_{CC}(\xi_i) \Delta t_i$, 即 $W_{CC} = U_{CC} \cdot \int_{t_s}^{t_e} I_{CC}(t) dt$, 该式即为在工作时间 $[t_s, t_e]$ 内给定 CC 的威胁度计算公式.

$\int_{t_s}^{t_e} I_{CC}(t) dt$ 的物理意义是, 在工作时间 $[t_s, t_e]$ 内, 经由隐通道 CC 泄漏的信息总量的 bit 数. 如果在工作时间 $[t_s, t_e]$ 内 $I_{CC}(t)$ 是常数, 即 I_{CC} , 那么有

$$\begin{aligned} W_{CC} &= U_{CC} \cdot \int_{t_s}^{t_e} I_{CC}(t) dt = U_{CC} \cdot I_{CC} \cdot \int_{t_s}^{t_e} dt \\ &= U_{CC} \cdot I_{CC} \cdot (t_e - t_s). \end{aligned}$$

这与定义 17 的表达式是一致的. 所以可以用 $W_{CC} = U_{CC} \cdot \int_{t_s}^{t_e} I_{CC}(t) dt$ 取代定义 17 中的表达式 $W(U_{CC}, I_{CC}, \Delta t) = U_{CC} \cdot I_{CC} \cdot \Delta t$. 故定义 17 可以改写为

定义 17'. 隐通道的威胁度.

对任意 $CC \in \mathbf{CC}$, $W_{CC} = U_{CC} \cdot \int_{t_s}^{t_e} I_{CC}(t) dt$, 称为隐通道 CC 在工作时间段 $[t_s, t_e]$ 内的威胁度, 其中 $\Delta t = t_e - t_s > 0$.

6.3 带有敏感参数 α 的威胁度与威胁率

在某些情况下审计度量隐通道的威胁, 我们发现有时隐通道对于势差 U 敏感, 而在另外一些情况下则对带宽 I 敏感. 例如保护用于加密或数字签名的密钥, 其长度可能只有 128 位或更短, 此时很高的带宽对于泄漏这样长度的保密信息并无实际意义, 人们更关心的是密钥被泄露到了哪一个安全级, 此时审计度量隐通道的威胁就对势差 U 敏感. 而在另外一些情况下, 如保密信息是国家档案馆中的影像资料或其它多媒体信息, 因为这类文件的数据量异常庞大, 若在有限的时间里使用较小的带宽向外泄漏, 隐通道的接收方可能得不到任何有价值的信息, 此时审计度量隐通道的威胁就对带宽 I 更为敏感. 所以我们考虑在隐通道威胁度和威胁率的计算中引入敏感参数.

定义 20. 带有敏感参数 α 的隐通道威胁度.

对任意 $CC \in \mathbf{CC}$, $W(U_{CC}, I_{CC}, \Delta t, \alpha) = U_{CC}^\alpha \cdot \int_{t_s}^{t_e} I_{CC}(t) dt$, 称为隐通道 CC 在工作时间段 $[t_s, t_e]$ 内的威胁度, 其中 $\Delta t = t_e - t_s > 0$.

定义 21. 带有敏感参数 α 的隐通道威胁率.

对任意的 $CC \in \mathbf{CC}$, $WP(U_{CC}, I_{CC}(t_0)) = U_{CC}^\alpha I_{CC}(t_0)$, 称为隐通道 CC 在 t_0 时刻的瞬时威胁率.

在上述两个定义中, $\alpha \in [0, +\infty)$ 称为势差敏感参数. 根据推论 6, 我们知道对于任意的隐通道 $CC \in \mathbf{CC}$, 有 $U_{CC} \geq 1$ 成立. 而在函数 $y = x^\alpha$ 中, 如果 $x_1 > x_2 \geq 1$, 那么有

$$\begin{cases} x_1^\alpha > x_2^\alpha, & \alpha > 0 \\ x_1^\alpha = x_2^\alpha, & \alpha = 0 \end{cases}.$$

可以证明, 随着 α 值的增大, $\lim_{\alpha \rightarrow +\infty} (x_1^\alpha - x_2^\alpha) = +\infty$, 而当 α 的值趋近于 0 时, $\lim_{\alpha \rightarrow 0} (x_1^\alpha - x_2^\alpha) = 0$. 这说明当 α 在区间 $[0, +\infty)$ 中选取不同的值时, 可以有效地放大或缩小隐通道的势差 U 对 W 和 WP 计算结果的影响.

下面通过实例来讨论敏感参数的作用. 对于任意的隐通道 $CC_1, CC_2 \in \mathbf{CC}$, 设势差 U_{CC_1} 和 U_{CC_2} 分别是 2 和 3, 带宽 I_{CC_1} 和 I_{CC_2} 分别是 150bits/s 和 110bits/s, 且 CC_1 和 CC_2 的工作时间域都是 $[t_1, t_2]$,

$$t_2 - t_1 > 0.$$

(1) 取 $\alpha = 1$, 那么有

$$W_{CC_1} = U_{CC_1} \cdot \int_{t_1}^{t_2} I_{CC_1}(t) dt = 2 \cdot \int_{t_1}^{t_2} 150 dt = 300(t_2 - t_1),$$

$$W_{CC_2} = U_{CC_2} \cdot \int_{t_1}^{t_2} I_{CC_2}(t) dt = 3 \cdot \int_{t_1}^{t_2} 110 dt = 330(t_2 - t_1).$$

因为 $t_2 - t_1 > 0$, 所以有 $W_{CC_1} < W_{CC_2}$, 根据 IA 标准我们判定在工作时间 $[t_1, t_2]$ 内, CC_2 的威胁大于 CC_1 .

(2) 取 $\alpha = 1/2$, 即通过 $U_{CC}^{1/2}$ 来弱化势差在隐通道威胁度计算中的影响, 那么有

$$W_{CC_1} = U_{CC_1}^\alpha \cdot \int_{t_1}^{t_2} I_{CC_1}(t) dt = 2^{\frac{1}{2}} \cdot \int_{t_1}^{t_2} 150 dt \approx 212(t_2 - t_1),$$

$$W_{CC_2} = U_{CC_2}^\alpha \cdot \int_{t_1}^{t_2} I_{CC_2}(t) dt = 3^{\frac{1}{2}} \cdot \int_{t_1}^{t_2} 110 dt \approx 191(t_2 - t_1).$$

因为 $t_2 - t_1 > 0$, 所以有 $W_{CC_1} > W_{CC_2}$, 根据 IA 标准我们判定在工作时间 $[t_1, t_2]$ 内, CC_1 的威胁大于 CC_2 .

根据函数 $y = x^\alpha, x \geq 1$ 的性质我们知道, 当 $\alpha \in (0, 1)$ 时, α 的作用是弱化势差在隐通道审计中的影响; 当 $\alpha \in (1, +\infty)$ 时, α 的作用是强化势差在隐通道审计中的影响. 这样通过一个参数 α , 就可以决定系统是对于势差 U 敏感 ($\alpha \in (1, +\infty)$)、还是对于带宽 I 敏感 ($\alpha \in [0, 1)$), 或是对于两者的敏感程度相同 ($\alpha = 1$). 在一些特殊情况下, 如当 $\alpha = 1$ 时, 带有敏感参数的 IA 审计方法就退化成了 IA 审计方法; 当 $\alpha = 0$ 时, 因为 $U_{CC}^0 = 1, U_{CC} \neq 0$, 此时如不考虑时间因素, 带有敏感参数的 IA 审计方法就退化成了 TCSEC 准则中的纯带宽审计方法. 此时在工作时间 $[t_s, t_e]$ 内, 隐通道平均带宽的计算公式可以表示为 W 与其工作时间 Δt 的商, 即

$$\bar{I} = \frac{\int_{t_s}^{t_e} I(t) dt}{t_e - t_s} = \frac{U_{CC}^0 \cdot \int_{t_s}^{t_e} I(t) dt}{t_e - t_s} = \frac{W}{\Delta t}.$$

7 相关工作比较

隐通道的定义经历了从自然语言描述到形式语言刻画的过程. 20 世纪 90 年代以前, 隐通道的定义主要有 Schaefer^[3], Lampson^[24], Huskamp^[25] 和 Kemmerer^[9] 等给出的基于描述其工作原理或特征的定义. 以后开始出现形式化定义, 如 Tsai 等^[12]: 给定一个强制安全策略模型 M 和它在一个操作系统中的解释 $I(M)$, $I(M)$ 中两个主体 $I(S_i)$ 和 $I(S_j)$ 之间的任何潜在通信都是隐蔽的, 当且仅当模

型 M 中的相应主体 S_i 和 S_j 之间的任何通信在 M 中都是非法的. Shieh 和 Gligor^[26] 将隐通道描述为三元组 $\langle variable, PA_i, PV_j \rangle$, 其中 $variable$ 表示系统的内部变量, $PA_i, PV_j \in TCB$ 分别表示对 $variable$ 的更改和观察操作. Tsai^[27] 定义了隐通道的单通道和复通道通信模式, 并研究了它们对带宽的影响. 2007 年我国学者卿斯汉和沈昌祥^[28] 给出了隐通道标识完备性的理论基础, 通过定义信息流基本单元 (s, op, vs_1, vs_2) 给出了直接通道 DCC 、原子通道 ACC 、单通道 SCC 、复通道 PCC 和只有一个发送操作的隐通道 SR^+CC 等具有不同信息流基本单元拓扑结构的隐通道定义, 并证明了有如下关系成立: $DCC \subseteq ACC \subseteq SCC \subseteq SR^+CC$, 其中 s 表示主体, op 表示 TCB 操作, vs_1, vs_2 表示共享变量.

在上述工作的基础上, 我们给出的隐通道形式化定义与文献[28]中的定义具有一致性, 其中隐通道元 ECC 等价于直接通道 DCC . 因为有 $DCC \subseteq ACC \subseteq SCC \subseteq SR^+CC$ 成立, 所以 ACC, SCC, SR^+CC 都可以在 ECC 的基础上进行扩展. 不同的是, 我们在 ECC 的定义中引入了时序性约束, 而且建立了一套代数系统对隐通道的拓扑结构进行计算, 使用这种方法能够描述具有任意空间拓扑结构的隐通道, 其逻辑表达能力更强. 我们还进行了不同拓扑结构的隐通道传输数据及其抗干扰性的实验, 见文献[29], 证实了隐通道代数系统中一些相关计算结果的正确性.

在隐通道威胁审计方面, 一般使用纯带宽标准进行度量, 所以相关文献一般局限在如何计算隐通道的带宽上, 如文献[19-21]等. 本文我们首先指出了使用纯带宽方法审计隐通道的局限性, 并通过定义隐通道的威胁度和威胁率给出了一种新的审计度量方法, 通过敏感参数 α 不同取值的调解, 新方法不仅与传统的带宽审计度量法兼容, 而且能够有效克服带宽审计度量法中存在的一些问题. 在隐通道代数系统的支持下, 还讨论了审计度量中涉及的一些具体问题的计算方法.

下面我们采用对比分析法, 进一步说明本文中提出的隐通道威胁审计的度量方法相比于传统的带宽审计度量方法的优越性. 假设在一个系统中发现两个隐通道 $C1$ 和 $C2$, 其带宽都是 60bits/s, 我们比

较传统带宽审计方法和本文中提出的方法在度量隐通道威胁方面的差别.

(1) 采用传统带宽标准的审计度量

① 因为 $C1$ 和 $C2$ 的带宽完全相同, 所以审计人员认为 $C1$ 和 $C2$ 对系统的威胁程度是一样的, 无法区分 $C1$ 和 $C2$ 对系统安全威胁的差别.

② 因为 $C1$ 和 $C2$ 的带宽均小于 100bits/s, 根据 TCSEC 的规定, 审计人员有可能会做出容忍 $C1$ 和 $C2$ 存在而不予消除的决定.

(2) 采用本文中所提出的标准的审计度量

① 尽管 $C1$ 和 $C2$ 带宽相同, 但可以通过其各自的势差 U 的高低和工作时间 T 的长短等因素, 进一步区分它们对系统安全的威胁程度, 具体计算过程可以参阅本文 6.3 节中的相关内容. 在此基础上, 可以决策如何分配有限的人力和物力资源对 $C1$ 和 $C2$ 进行消除.

② 尽管 $C1$ 和 $C2$ 的带宽均小于 100bits/s, 但需要进一步讨论 $C1$ 和 $C2$ 的空间拓扑结构对系统安全的影响. 若 $C1$ 和 $C2$ 采用串联结构, 根据定义 12 可计算出 $C1$ 和 $C2$ 至多等效于一个带宽为 60bits/s 的隐通道. 而采用并联结构, 根据定义 14 可计算出 $C1$ 和 $C2$ 等效于一个带宽为 120bits/s 的隐通道, 必须作消除处理.

③ 在兼容性方面, 可以通过势差敏感参数 α 的调节, 使得本文中提出的度量方法与传统的带宽度量方法完全兼容.

须要指出的是, 在隐通道代数系统的支撑下, 上述结论可以向 n 个隐通道 ($n > 2, n \in \mathbf{N}$) 的情况下推广.

从理论上来说, 传统的带宽审计度量采用的只是一个关于带宽的一元函数, 记为 $f(I)$, 而本文中所提出的方法则采用的是一个关于势差 U 、带宽 I 、时间 T 和势差敏感参数 α 的四元函数, 记为 $g(U, I, T, \alpha)$. 通过不同参数的取值调节, $f(I)$ 可以表示成 $g(U, I, T, \alpha)$ 在坐标轴 I 上的投影函数, 所以本文中提出的审计度量方法在度量空间上完全涵盖了传统的带宽审计度量法, 而且可以根据具体需求, 从多个角度使用不同的参数对隐通道的威胁进行度量. 表 1 列举了传统带宽法与本文中提出的方法在所支持的参数和兼容性等方面的对比.

表 1 传统带宽法与本文中提出的方法的对比

	带宽 I	势差 U	工作时间 T	势差敏感参数 α	隐通道拓扑结构计算	兼容性
传统带宽法	支持	不支持	不支持	不支持	不支持	未考虑
本文中提出的方法	支持	支持	支持	支持	支持	兼容带宽法

8 结 语

在隐通道形式化定义的基础上研究了隐通道的可量化属性, 主要包括势差 U 、带宽 I 、长度 L 和可靠性 P 等 4 种. 在此基础上, 通过讨论隐通道之间的二元运算关系建立了一个隐通道的代数系统. 隐通道的威胁度和威胁率两个概念的引入, 使得隐通道的威胁既可以从一个时间段去审计度量, 也可以从一个瞬间时刻去审计度量. 而且通过选择不同的敏感参数, 审计人员可以自行决定具体的隐通道是对势差敏感, 还是对带宽敏感, 或是对两者的敏感程度相同. 这种审计度量方法兼容于已有的带宽审计度量方法.

参 考 文 献

- [1] Wang Chang-Da, Ju Shi-Guang. The dilemma of covert channels searching//Proceedings of the 8th Annual International Conference on Information Security and Cryptology. LNCS 3935. Seoul, Korea, 2006: 169-174
- [2] McHugh J. Covert channel analysis: A chapter of the handbook for the computer security certification of trusted systems. Technical Report: 97207-0751, Portland State University, 1995
- [3] Schaefer M, Gold B, Linde R, Scheid J. Program confinement in KVM/370//Proceeding of the 1977 Annual ACM Conference. New York, USA, 1977: 404-410
- [4] Karger P A, Wray J C. Storage channels in disk arm optimization//Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy. Oakland, USA, 1991: 52-61
- [5] Wang Chang-Da, Ju Shi-Guang, Guo Dian-Chu, Yang Zhen, Zheng Wen-Wi. Research on the methods of search and elimination in covert channels//Proceedings of the Grid and Cooperative Computing. Shanghai, 2003. LNCS 3032. Springer, 2004: 988-991
- [6] Trusted computer system evaluation criteria. USA, DoD, December 26, 1985
- [7] Common criteria for information technology security evaluation, Part 3: Security assurance requirements. ISO, January 2004
- [8] He J, Gligor V D. Information-flow analysis for covert-channel identification in multilevel secure operating systems//Computer Security Foundations Workshop III. Franconia, USA, 1990: 139-148
- [9] Kemmerer R A. Shared resource matrix methodology: A practical approach to identifying covert channels. ACM Transactions on Computer Systems, 1983, 1(3): 256-277
- [10] Kemmerer R A. Covert flow trees: A visual approach to analyzing covert storage channels. IEEE Transactions on Software Engineering, 1991, 17(11): 1166-1185
- [11] Goguen J A, Meseguer J. Security policies and security models//Proceedings of the IEEE Symposium on Security and Privacy. Oakland, USA, 1982: 11-20
- [12] Tsai C R, Gligor V D, Chandrasekaran C S. A formal method for the identification of covert storage channels in source code//Proceedings of the IEEE Symposium on Security and Privacy. Oakland, USA, 1987: 74-87
- [13] Qing Si-Han, Zhu Ji-Feng. Covert channel analysis on AN-SHENG secure operating system. Journal of Software, 2004, 15(9): 1385-1392(in Chinese)
(卿斯汉, 朱继锋. 安胜安全操作系统的隐蔽通道分析. 软件学报, 2004, 15(9): 1385-1392)
- [14] Liu Wen-Qing, Han Nai-Ping, Chen Zhe. Identifying and dealing with covert channel of the secure OS-Slinux. Acta Electronica Sinica, 2007, 35(1): 153-156(in Chinese)
(刘文清, 韩乃平, 陈喆. 一个安全操作系统 SLinux 隐蔽通道标识与处理. 电子学报, 2007, 35(1): 153-156)
- [15] Hu Wei-Ming. Reducing timing channels with fuzzy time//Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy. Oakland, USA, 1991: 8-20
- [16] Ogurtsov N, Orman H, Schroepel R, O'Malley S, Spatscheck O. Experimental results of covert channel limitation in one-way communication systems//Proceedings of the Network and Distributed System Security. San Diego, USA, 1997: 2-15
- [17] Kang M H, Moskowitz I S. A pump for rapid, reliable, secure communication//Proceedings of the 1st ACM Conference on Computer and Communications Security. Fairfax, USA, 1993: 119-129
- [18] Wang Chang-Da. Research on the computational aspect of covert channels[Ph. D. dissertation]. Jiangsu University, Zhenjiang, 2006(in Chinese)
(王昌达. 隐通道可计算性的研究[博士学位论文]. 江苏大学, 镇江, 2006)
- [19] Shieh S P. Estimating and measuring covert channel bandwidth in multilevel secure operating systems. Journal of Information Science and Engineering, 1999, 15: 91-106
- [20] Venkatraman B R, Newman-Wolfe R E. Capacity estimation and auditability of network covert channels//Proceedings of the IEEE Symposium on Security and Privacy. Washington, DC, USA, 1995: 186-198
- [21] Tsai C R, Gligor V D. A bandwidth computation model for covert storage channels and its applications//Proceedings of the IEEE Symposium on Security and Privacy. Oakland, USA, 1988: 108-121
- [22] Subasic P, Hirota K. Similarity rules and gradual rules for analogical and interpolative reasoning with imprecise data. Fuzzy Sets and Systems, 1998, 96(1): 53-75

[23] Ross K A, Wright C R. Discrete Mathematics. 5th Edition. Prentice-Hall, 2002

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

[25] Huskamp J C. Covert communication channels in timesharing systems. Technical Report UCB-CS-78-02, 1978

[26] Shieh S P, Gligor V. Auditing the used of covert storage channels in secure system//Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy. Oakland, USA, 1990: 285-295

[27] Tsai C R. Covert channel analysis in secure computer system [Ph. D dissertation]. University of Maryland College Park, 1987

[28] Qing Si-Han, Shen Chang-Xiang. Design of high level secure operating system. Science in China, Series E, 2007, 37(2): 238-253(in Chinese)
(卿斯汉, 沈昌祥. 高等级安全操作系统的设计. 中国科学, E 辑, 2007, 37(2): 238-253)

[29] Wang Chang-Da, Ju Shi-Guang. Simulation analysis of covert channels. Journal of System Simulation, 2006, 18(6): 1488-1492(in Chinese)
(王昌达, 鞠时光. 隐通道的仿真分析. 系统仿真学报, 2006, 18(6): 1488-1492)



WANG Chang-Da, born in 1971, Ph. D. , associate professor. He mainly is engaged in the research and development of network and information security.

JU Shi-Guang, born in 1955, Ph. D. , professor, Ph. D. supervisor. His research interests include information security and spatial database.

ZHOU Cong-Hua, born in 1978, Ph. D. , lecturer. His research interest is information security.

SONG Xiang-Mei, born in 1979, Ph. D. candidate, lecturer. Her research interest is information security.

Background

The work belongs to the project “Research on Covert Channels Detection Based on Information Flow Analysis”, which is supported by the National Natural Science Foundation of China under grant No. 60773049, the Nature Science Foundation of Jiangsu Province under grant No. BK2007086, the Fundamental Research Project of Nature Science in Colleges of Jiangsu Province under grant No. 07KJB520016, and Person with Ability Project of Jiangsu University under grant No. 07JDG053.

Covert channels present a serious risk to data security in computer systems and networks. Almost all of trust evaluation criteria, e. g. TCSEC, CC and GB17859-1999, list covert channel as an important item for higher levels trust evaluation. In the past three decades, most researchers have paid

more attention to detection and mitigation methods for covert channels. A few known works about auditing were limited in scope to how one calculates the bandwidth/capacity of covert channels. The criterias motioned above use bandwidth as the only parameter to measure the threat of covert channels, which neglect many factors, such as the security level difference, sensitive parameter, the duration and instantaneous time of covert channels, etc. So they cannot give a comprehensive evaluation of the threat of covert channels. The method presented in this paper integrates all of the factors mentioned above to measure the threat of covert channels. The topology change of covert channels is also considered under the support of an algebra system. Moreover, it is compatible with the traditional bandwidth measurement method.