文章编号:1671-8860(2008)10-1092-03
文献标志码:A

基于无干扰原理的终端安全模型研究

王 飞[1,2] 刘 毅[1] 李 勇[1]

(1 信息工程大学电子技术学院,郑州市商城东路12号,450004)
(2 解放军装备指挥技术学院,北京市怀柔区3380信箱93号,101416)

摘 要:终端是信息系统中所有安全风险的根源,借鉴无干扰信息流的思想,从终端的访问行为安全的角度提出一种无干扰的终端安全模型。模型以终端的访问行为为基本元素,详细讨论了访问行为安全应满足的条件,指出安全策略与隔离性是保障终端安全的根本,并在此基础上扩展到整个终端安全。

关键词:可信计算;终端安全;信息流;无干扰
中图法分类号:TP316

终端的所有行为都可以归结为主体、客体、操作三个要素的行为实施[1,2]。通过模型对主体、客体及操作进行量化,即可对终端的操作进行控制。然而,主体、客体以及所有操作都会成为终端当前的运行环境的一部分,会对终端安全产生相应的影响。如果同时能够对运行环境的安全性进行量化,会大大提高终端操作安全性和可靠性。本文将终端操作行为的三要素扩充为四要素,分别为主体、客体、操作和访问环境,如图1所示。

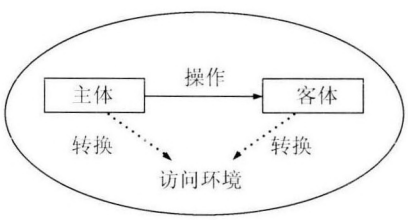

图1 终端操作四要素关系图

Fig. 1 Four Factors of Terminal Operation

信息流无干扰的思想最早由Goguen和Meseguer提出,提供了一种用于规范和分析安全策略以及实施机制的形式化方法[3-5]。

由信息流的无干扰原理可以得到关于终端访问行为安全的无干扰原理。对于一个特定的访问行为,如果系统执行给定访问行为序列后的状态和清除了该访问行为序列中所有对该访问行为不产生干扰的访问行为后,所得到的状态是观察等价的,则可以认为该次访问行为是安全的。否则,一定存在某个潜在的访问行为干扰了该访问行为的执行,并导致其不安全。

1 访问行为安全

1.1 基本定义

定义1 一个终端系统M由如下元素构成:S为系统主体集合,$s\in S$,$S_0=\phi$为终端初始状态主体集合;O为系统客体集合,$o\in O$,$O_0=\phi$为终端初始状态客体集合;OP为系统操作集合,r_1,r_2,r_3,$\cdots\in OP$,R_1,R_2,$\cdots\subset OP$;AE为系统访问环境,P_0,P_1,P_2,$\cdots\subset AE$,$P_0=\phi$为终端初始访问环境。

因此,一个终端系统可记为$M(S,O,OP,AE)$,$(s\times o\times r\times p)$称为终端系统的一次访问行为。

定义2 一个终端系统M的安全状态记为集合Z,状态$z\in Z$。

定义3 安全性判定函数

$$\text{judge}:S|O|OP|K|S\times O\times OP|S\times O\times OP\times AE\rightarrow\{\text{TRUE},\text{FALSE}\}$$

定义4 单步转换函数:

$$\text{step}:Z\times(S\times O\times OP\times AE)\rightarrow Z$$

访问环境转换函数:

$$\text{result}:S\times O\times OP\times AE\rightarrow AE$$

收稿日期:2008-08-28。
项目来源:国家863计划资助项目(2006AA01Z440);国家973计划资助项目(2007CB311100,2007CB31307107)。

系统运行函数:

$$go: Z \times (S \times O \times OP \times AE)^* \rightarrow Z$$

1.2 安全要素之间的关系

1) 一个终端上的实体,可以作为主体或客体存在,也可以作为主体和客体同时存在。

2) 主体对客体操作的安全性受到当前访问环境安全性的制约,同时操作也会对访问环境的安全性造成影响。

3) 四个要素的安全性都关系到整个终端的安全性,即访问行为的安全性关系到整个终端的安全性。

1.3 基于无干扰的访问行为安全

定义 5　对于任一终端访问行为$(s \times o \times r \times p) \in M$,函数 $\mathrm{pure}((s \times o \times r), p)$表示从当前环境 p 中删除所有执行 $s \xrightarrow{r} o$ 时,不对其安全产生影响的元素后的集合,表示如下:

$$\mathrm{pure}((s \times o \times r), p) = \begin{cases} p', p' \subset p \wedge p' \neq \phi, \text{其他} \\ \phi, \exists s' \in p', \mathrm{judge}(s' \times r' \times o) = \mathrm{False} \vee \exists o' \in p', \mathrm{judge}(s \times r'' \times o') = \mathrm{False} \end{cases}$$

定理 1(访问行为无干扰定理)　若终端某一个访问行为 $(s \times o \times r \times p)$ 满足 $\mathrm{judge}(p) = \mathrm{TRUE}$,且满足 $\mathrm{pure}((s \times o \times r), p) = \phi$,则认为访问行为$(s \times o \times r \times p)$是当前安全的。

证明:由定义可知:

$$p = p_0 \cup S_t \cup O_t \cup R_t$$

其中,S_t、O_t、R_t 分别表示执行该访问行为时的主体集、客体集和操作集。

由于 $\mathrm{judge}(p) = \mathrm{TRUE}$,且

$$\mathrm{pure}((s \times o \times r), p) = \phi \tag{1}$$

可知当前的访问环境是安全的,并且不存在能够干扰$(s \times o \times r)$操作的不安全因素。

又因为 $p_0 \subset p$,且 $\mathrm{judge}(p) = \mathrm{TRUE}$,所以 $\mathrm{judge}(p_0) = \mathrm{TRUE}$,且和式(1),得:

$$\mathrm{judge}(s \times o \times r) = \mathrm{TRUE} \tag{2}$$

由定义 4 知:

$$\mathrm{result}(s \times o \times r \times p) \rightarrow p' \tag{3}$$

由 $\mathrm{pure}((s \times o \times r), p) = \phi$ 可知:

$$\mathrm{judge}(s \times o \times r) \prec \mathrm{judge}(M) \tag{4}$$

其中符号$\prec$表示影响关系。

由式(1)~式(4)可知:

$$\mathrm{judge}(p') = \mathrm{TRUE}$$

又因为 $S_{t+1} = S_t \cup \{s\}$,$O_{t+1} = O_t \cup \{o\}$,$R_{t+1} = R_t \cup \{r\}$,故 $\mathrm{judge}(S_{t+1}) = \mathrm{TRUE} \wedge \mathrm{judge}(O_{t+1}) = \mathrm{TRUE} \wedge \mathrm{judge}(R_{t+1}) = \mathrm{TRUE}$;故在时刻 t,$(s \times o \times r \times p)$是安全的。

定理 2　如果终端系统的安全策略是完备的,并且当前访问环境中不存在不安全因素干扰主体对客体的操作,那么这个访问行为当前是安全的。

定理 3(访问行为传递安全定理)　若终端能够满足以下条件,对终端 M 任意的访问行为$(s \times o \times r \times p) \in M$ 都是安全的:

1) $\mathrm{judge}(p_0) = \mathrm{TRUE}$;

2) $\mathrm{pure}((s \times o \times r), p) = \phi$。

可以利用数学归纳法对访问行为序列长度进行归纳。限于篇幅,不予证明。

2 终端安全条件

2.1 终端状态的构成

终端系统的运行过程可以看成是一系列终端状态的转移,而终端状态的变迁又是建立在终端系统访问行为实施的基础上,因此,终端系统的访问行为和终端的安全状态是相关联的。

定义 6　一个终端系统状态 $z \in Z$,是一个二元组$(z_{\mathrm{pro}}, (s \times o \times r \times p)^*)$,其中 $z_{\mathrm{pro}} \in Z$ 是状态 z 之前的一个状态,访问行为序列$(s \times o \times r \times p)^*$包括系统从状态 z_{pro} 开始到达状态 z 时所有的访问行为。

定义 7　设 z_0 是终端系统的初始状态,则一个终端系统状态 $z \in Z$ 称为终端系统可达的状态,当存在一个访问行为序列$(s \times o \times r \times p)^*$,使得 $z = \mathrm{go}(z_0, (s \times o \times r \times p)^*)$。

定理 4　设 z_0 是终端系统的初始状态,任一终端系统的可达状态 z 的安全性可认为是由初始状态 z_0 及某一个访问行为序列$(s \times o \times r \times p)^*$的安全性决定。

证明　Θz 是终端系统的一个可达状态,由定义 6 可知:

$$z = (z_{pro}, (s \times o \times r \times p)^{*1}) \tag{5}$$

由定义 7 可知,必存在一个访问行为序列$(s \times o \times r \times p)^{*2}$,使得:

$$\mathrm{go}(z_0, (s \times o \times r \times p)^{*2}) = z_{\mathrm{pro}} \tag{6}$$

则由式(1)、式(2)可知:

$$\mathrm{go}(z_{pro}, (s \times o \times r \times p)^{*1}) =$$
$$\mathrm{go}(\mathrm{go}(z_0, (s \times o \times r \times p)^{*2}), (s \times o \times r \times p)^{*1}) =$$
$$\mathrm{go}(z_0, (s \times o \times r \times p)^{*2+*1}) =$$
$$\mathrm{go}(z_0, (s \times o \times r \times p)^*) = z$$

由上式可知,状态 z 的安全性同终端系统初始状态 z_0 和终端访问行为序列$(s \times o \times r \times p)^*$相

关。

2.2 终端系统传递安全定理

公理1 当一个终端系统 M 满足 $\forall z \in Z$，其中 z 是终端系统可达状态，且 z 是安全状态，则称终端系统 M 是安全系统。

定义8 如果一个系统的初始访问行为 $(s \times o \times r \times p)$ 是安全的，且其可以执行终端安全策略的监视进程，则称 $(s \times o \times r \times p)$ 为该系统的安全根。

定理5(终端系统传递安全定理) 一个终端系统 M，当满足如下两个条件时是安全的：

1) M 从安全根开始运行；

2) M 中的任意一个访问行为 $(s \times o \times r \times p) \in M$ 满足访问行为传递安全定理。

该定理可由定理4容易推得。

定理5说明，一个终端系统中如果所有的访问行为都能满足传递安全性质，那么系统本身的运行就是安全的。

参 考 文 献

[1] 沈昌祥. 信息安全保障建设中的等级保护[J]. 信息技术与标准化，2007，11：5-6

[2] 沈昌祥，张焕国，冯登国，等. 信息安全综述[J]. 中国科学(E辑)，2007，37(2)：129-150

[3] Goguen J A, Meseguer J. Security Policies and Security Models[C]. The 1982 IEEE Symposium on Security and Privacy, Qakland, California, 1982

[4] Goguen J A, Meseguer J. Unwinding and Inference Control[C]. The 1984 IEEE Symposium on Security and Privacy, USA, 1984

[5] Rushby J. Noninterference, Transitivity, and Channel-control Security Policies [R]. Technical Report, CSL-92-02, Menlo Park: Stanford Research Institute, 1992

第一作者简介：王飞，博士生，主要研究方向为信息安全、安全操作系统。

E-mail：wangfei791009@163.com

Research of Terminal Security Model Based on Noninterference

WANG Fei[1,2] *LIU Yi*[1] *LI Yong*[1]

(1 Institute of Electronic Technology, Information Engineering University, 12 East Shangchen Road, Zhengzhou 450004, China)

(2 The PLA Institute of Equipment and Command Technology, Huairou, Beijing 101416, China)

Abstract: According to the theory of noninterference information flow, a kind of noninterference security model is put forward based on access security of terminal. The terminal access is the basic element of the model; and some security conditions of access are discussed in detail based on it; it is shown that the security policy and isolation are the root of terminal security. And it expands access security into all terminal security.

Key words: trusted computing; terminal security; information flow; noninterference

About the first author: WANG Fei, Ph.D candidate, his research fields include Information Security and Security Operation System.

E-mail: wangfei791009@163.com