Available online at www.sciencedirect.com
ScienceDirect
ELSEVIER
June 2012, 19(Suppl. 1): 108–111
www.sciencedirect.com/science/journal/10058885
The Journal of China Universities of Posts and Telecommunications
http://jcupt.xsw.bupt.cn

Dynamic analysis for covert channel based on grey relational analysis algorithm

PAN Qin-xue (✉), CAI Mian

School of Computer Science, Beijing University of Technology, Beijing 100124, China

Abstract

Search and recognition is the most important part of the covert channel analysis. At present, most of the covert channel search methods are static analysis on system. It has many shortcomings, such as heavy workload, omission, inaccurate, and so on. It is necessary to find the dynamic search method for covert channel during a system is running. This paper presented a covert channel dynamic search method based on grey relational analysis algorithm (GRAA) in gray theory. The method is efficient and can be used in conjunction with existing covert channel search methods. Finally, a closed-loop feedback will be formed so that the system's safety mechanism can be self-improvement gradually.

Keywords covert channel, dynamic analysis, grey theory, grey relational analysis algorithm

1 Introduction

Covert channel is a mechanism that allows a high security level user with mandatory security policy to transfer information to a lower security level user in a manner that violates the system's security policy [1]. In systems with mandatory security policy, covert channel usually exists widely and may pose dangerous threats. Because of this, covert channel in high level security information systems is strongly required to be analyzed and processed according to many information system security standards, both domestic and foreign [2–4]. Covert channel analysis includes channel identification, measurement and disposal, the first and the foundation is searching for all potential covert channels in system. By now, most of search methods of covert channel are static analysis which usually based on top-level description or system source code. In order to find out whether there are covert channels, every possible information flow of systems will be recognized and validated [5–7]. Because information flow exists everywhere in system, prone to omissions is common during analysis process, on the other hand, a lot of information flow which exits theoretically but are non-existent practically will be found, the elimination of these channels will consume too much system resources and may cause unnecessary the system efficiency decline [8]. In order to solve these problems of static search methods, it is necessary to find dynamic search methods for covert channel in running system which don't need top-level description or system source code, also don't need any judgment of the legality of every possible information flow in a system. This method only analyzes the actual existing information flow. This kind of approach is able to reduce analysis complexity, and comprehensive cost is lower than static analysis. Based on GRAA, this paper provides a dynamic analysis method and a comprehensive disposal plan for covert channel.

2 The principle and necessary conditions of covert channel

2.1 The principle of covert channel

Since the discovery of covert channel, it has been given a variety of different descriptive definitions by researchers. The comprehensive definition given by Tsai et al is the most comprehensive and widely accepted [9].

Received date: 20-03-2012
Corresponding author: PAN Qin-xue, E-mail: qiuxuewen@gmail.com
DOI: 10.1016/S1005-8885(11)60460-3

The definition of covert channel (Tsai et al): given a mandatory security policy model M and its interpretation in an operating system $I(M)$, the communication between the two subjects $I(S_h)$ and $I(S_l)$ in the $I(M)$ is covert, if and only if (IFF) any communication between the S_h and S_l is illegal, and communication channel between the S_h and S_l is covert channel [2]. Based on this definition, covert channel is only related with the mandatory access policy model of a system, and both of the two subjects involved in the covert channel communication have different security levels [1].

According to the definition of covert channel and the results of present research, if the two subjects use covert channel to communicate, they must share an object that is used to transmit information. So, the principle of the covert channel can be expressed that Fig. 1, in security system, high-level S_h changes shared-object O_i or its attributes O_i->A_j by M (trusted computing base (TCB) primitive), and low-level S_i can sense the changes of the object by G (TCB primitive), and in this way the information will flow from high level to low level, as the dotted line shown in Fig. 1, which results in leaks of confidential information of the system

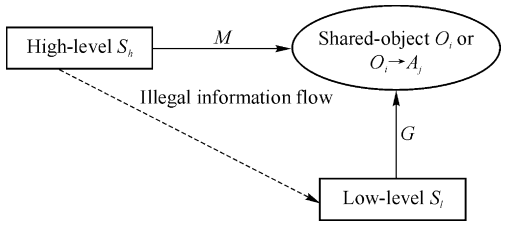

Fig. 1 The working principle of the covert channel

2.2 The necessary conditions of covert channel

Identification is the basis of the covert channel analysis. There are lots of information channels which have many forms between subjects, this leads to difficult searching for the covert channel. Refs. [2,10] gives the necessary conditions for covert channel. It provides a theoretical basis for the search and elimination of covert channels, as follows:

1) Sender and receiver must be able to access the same attributes of the shared resources.

2) Sender's security level must higher than receiver' security level.

3) There must be a way to change the attributes for the sender.

4) There must be a way to know the changes of the attributes for receiver.

5) Sender and receiver can be initialized by some kind of mechanism, suited synchronization mechanism should also be established to ensure the correctness, accuracy, and sent/receive order of transmitted information.

Depending on the type of shared objects, covert channels can be divided into storage covert channel and time covert channels, both of the two channels' nature have no differences. Storage covert channels use storage resources and time covert channels use time resources in system. Therefore, all necessary conditions of them can be expressed into the five points above.

As covert channels use system resources that are not originally used to transmit data, system's inherent security mechanisms are not able to detect and control any of the communication ways generally. The necessary conditions of covert channel are its minimum ones are not indispensable [8]. Therefore, based on the necessary conditions of the covert channel, we can set appropriate security mechanism to detect covert channels in system.

3 Covert channel analysis based on the correlation degree

At present, most of covert channel search methods are based on the necessary conditions. The first four ones of them are static description of system operation, which is the basis of static analysis. The last one is a key factor in formation of covert channel and can't be detected by the static analysis. Therefore, the synchronization behavior of different security subjects could be detected to search for covert channels in the running system accurately.

According to the principle of the covert channel, the sender changes an object and the receiver can discover the changes of objects, and the process is known as a transmission cycle. In one cycle, one bit can be transferred and the operations of the sender and the receiver must have a strict collaboration. In general, it requires more than one transmission cycle to transfer data, and the operations of transmission will show a certain periodicity. So the data sequences of their execution frequency also are closely associated. GRAA is the algorithm that can be used to analyze the association between two or more data sequences in the grey theory. So GRAA can be used to detect the synchronous behaviors, which can identify covert channels in running system.

Download English Version:

https://daneshyari.com/en/article/721994

Download Persian Version:

https://daneshyari.com/article/721994

Daneshyari.com