ARTICLE IN PRESS

+ MODEL

Available online at www.sciencedirect.com

ScienceDirect

Karbala International Journal of Modern Science xx (2018) 1–13

http://www.journals.elsevier.com/karbala-international-journal-of-modern-science/

Theoretical framework of quantitative analysis based information leakage warning system

Kushal Anjaria*, Arun Mishra

Defence Institute of Advanced Technology, Pune, India

Received 28 September 2017; revised 21 December 2017; accepted 9 January 2018

Abstract

The paper aims to propose a framework of information leakage warning system based on the principle of quantitative information flow. The quantification of information leakage has been widely used to decide the threshold of information leakage in program code but the purpose of the proposed framework is to use quantification based information leakage threshold to design practical information leakage warning system for real-time software. In the proposed framework, the software is considered as a collection of functions and each function is considered as register automata. Using the register automata working principles, the information leakage will be quantified during runtime of the software and when the software is in its pristine form. Based on the quantified amount of information leakage in both the cases, the framework warns the user about information leakage. Algorithmic steps of the proposed approach are also included in the paper. The proposed quantitative analysis based framework leads to flexible information security policy.

Keywords: Information security; Information security modeling; Quantitative analysis of information leakage; Trust

1. Introduction

Nowadays, there is a growing interest in quantitative information flow analysis as it offers an attractive way to design flexible information security framework. Its implications lie in the areas related to confidentiality properties like secure information flow, anonymity protocols and side channel analysis. In general terms, quantitative analysis of information flow provides a technique to measure information leakage in computer programs. Denning [1] pioneered the quantitative information flow analysis. She suggested that for quantitative information flow analysis, software or codebase should be divided into the set of states, and then, uncertainty associated with the secure content can be measured before the execution and after the execution of each state. To measure the uncertainty, information theoretic concepts like Shannon's entropy [2] are used.

One motivating example of the information leaking system is password checking system [3]. The password checking system verifies password provided by the user and based on that password it grants or denies the access. The close observation of the password checking system reveals that it may leak sensitive

* Corresponding author.
E-mail address: kushal.anjaria@gmail.com (K. Anjaria).
Peer review under responsibility of University of Kerbala.

https://doi.org/10.1016/j.kijoms.2018.01.002

information. Suppose, an attacker enters the password randomly into the system and if he gets the access then he will be able to infer that his randomly entered password is correct (depicts complete information leakage). If his entered password is incorrect then he will be able to remove one possibility of the probable password from his/her search space. Information leakage in the case of password checking system is unavoidable because it is important from software usability perspective to provide information to the user about access grant or denial.

The quantitative analysis of information leakage has been widely used as a tool in abstract computational systems [4,5], imperative programs [6,7], imperative multithreaded programs [3,8] and Service Oriented Architecture [9]. From this mentioned literature about the quantitative analysis of information leakage and the example of password checking system, following points can be derived:

1. Information leakage analysis provides very strict measures of information leakage. For practical systems, the system designer will not be interested in strict measures because he himself will deliberately allow the system to leak some information in order to provide usability and availability to the users (Consider aforementioned example of password checking system. In this system, designer has to inform user about the success or failure in login process).
2. Quantitative analysis of leakage has been widely used in literature to detect violation of non-interference property [10]. The non-interference is a static security property which divides computer system into low-security sensitive and high-security sensitive content. After that, it prevents interference between low-security sensitive and high-security sensitive content. The quantitative analysis hasn't been used to detect the cause of information leakage during runtime of the system.
3. The fundamentals of quantitative analysis of information leakage have been applied to large codebases but it hasn't been widely used to detect information leakage in actual software systems. In literature, only Heusser and Malacaria [11] have successfully attempted to quantify information leakage in an actual software system. But their analysis was static software analysis rather than runtime analysis.

In the present work, a framework of a system has been proposed, which uses the quantitative analysis of information leakage at runtime to alert the user if the quantity of leaked information is more than the predefined threshold. That means, as per the quantitative information flow principles, if information processing system or software leaks x bits of secret information, then in the proposed framework x bits have been used in runtime to provide a warning to the users of that software or information processing system. The framework, proposed in the paper uses information confinement concept proposed by Lampson [12] to detect information leakage at runtime. The framework doesn't use very strict measures of the leakage which restrict the developer of the system. The proposed framework will not only detect the violation of non-interference property but also detect the information leakage if the confidential content is written in the permanent file, memory location, temporary file or encoded bill during runtime. It will detect the leakage caused by the variation in the ratio of computing input, output or paging rate. Thus, based on the quantitative information flow analysis principles, the proposed framework intuitively ought to satisfy the dynamic state execution described in Fig. 1.

State, described in Fig. 1 is an execution of variable or statements in the software. As shown in the Fig. 1, after state execution, at runtime, initial uncertainty will be divided into two halves: information leaked and remaining uncertainty. The proposed framework will use these halves and analyze runtime to take decisions. The framework uses register automata theory [13,14] for quantitative analysis of information leakage. Once the framework is ready, the trusted implementation of the proposed framework is also discussed in the paper.

The primary goal of the quantitative analysis of information leakage is to shift focus from “Does the software leak?” to “How much does the software leak?” The proposed work tries to go one more step further and not only focused on “How much does the software leak?” but also on “How much does the software leak at runtime?”

The quantitative analysis based approach, proposed in the present work provides flexibility in maintaining confidentiality property to users and industries. The flexibility is very important property in security fields because the recent security solutions to solve information security challenges provide very strict measures. It is very difficult for the IT industry to decide flexible and allowable information leakage based information security framework. If the software is leaking within the range of allowable leakage at runtime then industries can choose to ignore the leakage. The approach proposed in the present work tries to provide

Please cite this article in press as: K. Anjaria, A. Mishra, Theoretical framework of quantitative analysis based information leakage warning system, Karbala International Journal of Modern Science (2018), https://doi.org/10.1016/j.kijoms.2018.01.002