Chapter 45

An Invariant-Based Approach for Detecting Attacks Against Data in Web Applications

Romaric Ludinard
Supélec, France

Éric Totel
Supélec, France

Frédéric Tronel
Supélec, France

Vincent Nicomette
CNRS, LAAS, France & INSA, LAAS, Université de Toulouse, France

Mohamed Kaâniche
CNRS, LAAS, France & Université de Toulouse, France

Éric Alata
CNRS, LAAS, France & INSA, LAAS, Université de Toulouse, France

Rim Akrout
CNRS, LAAS, France & LAAS, Université de Toulouse, France

Yann Bachy
CNRS, LAAS, France & LAAS, Université de Toulouse, France

ABSTRACT

RRABIDS (Ruby on Rails Anomaly Based Intrusion Detection System) is an application level intrusion detection system (IDS) for applications implemented with the Ruby on Rails framework. The goal of this intrusion detection system is to detect attacks against data in the context of web applications. This anomaly based IDS focuses on the modelling of the normal application profile using invariants. These invariants are discovered during a learning phase. Then, they are used to instrument the web application at source code level, so that a deviation from the normal profile can be detected at run-time. This paper illustrates on simple examples how the approach detects well-known categories of web attacks that involve a state violation of the application, such as SQL injections. Finally, an assessment phase is performed to evaluate the accuracy of the detection provided by the proposed approach.

DOI: 10.4018/978-1-5225-3422-8.ch045

Nowadays there is an important trend to transform traditional applications into their equivalent online counterpart, making possible for end users to remotely interact with their information systems through their Web browser. Such web-based applications offer all functionalities required by the end-user (e.g., webmail, online calendars, e-business, e-banking…). This paradigm shift did not lead to a significant change of the methodology and processes employed during the application development. Hence, the design faults that are commonly encountered with traditional applications are still present in these new web-based applications. As illustrated by recent statistics (see e.g., (IBM, 2012), these applications still exhibit a high number of vulnerabilities. They have become one of the preferred targets for the attackers. The consequences of these attacks are at least as critical as they were with traditional applications. Worse, the corresponding vulnerabilities can now be remotely exploited.

Several mechanisms have been developed to protect web applications against potential attacks. These mechanisms can be used at the network level (such as applicative firewalls), and at application level (such as input sanitization techniques). However such prevention mechanisms remain largely insufficient, as they do not take into account the semantic of the applications they are supposed to protect, thus providing a rather low protection. Hence, it is important to propose mechanisms that could more efficiently detect attacks affecting the integrity of the application state.

In this paper, we propose an approach to anomaly based intrusion detection at the application level that focuses on violations of the application state. This approach is based on the automatic generation of invariants that are discovered during a learning phase and verified during the execution of the application. The paper extends the results presented in Ludinard et al. (2012) by providing more details about the implementation of the approach and the generation of the invariants. First Section State of the Art presents previous work about intrusion detection that can be applied in the context of web applications. Section Context and Case Study presents the context and a case study of our work. In Section Invariant Constraints in an Application, a typical example illustrates the ideas we are relying on. Then, a general overview our approach is outlined in Section Invariant based Detection Model), together with a discussion of how it can be applied to web applications (Section Ruby On Rails Implementation). The last part of the paper (Section IDS Assessment) shows how the intrusion detection mechanisms have been assessed, in order to demonstrate that they accurately detect the types of attacks we focus on.

STATE OF THE ART

Most work in the context of web attack detection focuses on abnormal network packets (Robertson, Vigna, Kruegel, & Kemmerer, 2006) or requests (Vigna, Robertson, Kher, & Kemmerer, 2003) and do not take into account the state of the web application itself. We believe that application level mechanisms can help improving the intrusion detection performance as they are able to take advantage of the internal state of the monitored program. Indeed, they have access to all the internal data structures and algorithms used by the program.

Three types of approaches can be distinguished for detecting intrusions at application level: the first approach focuses on the correctness of the Control Flow Graph of the program such as Abadi, Budiu, Erlingsson, and Ligatti (2005) and Kiriansky, Bruening, and Amarasinghe (2002) and consists in verifying that the actions in the program are executed in a correct order. This work does not permit to detect attacks on data. The second approach focuses on the correctness of the data manipulations during program execution such as in Akritidis, Cadar, Raiciu, Costa, and Castro (2008) or in Castro, Costa,

Related Content

Collaborative Modeling: Roles, Activities and Team Organization

Peter Rittgen (2010). *International Journal of Information System Modeling and Design (pp. 1-19).*

www.irma-international.org/article/collaborative-modeling-roles-activities-team/45923

A Method and Case Study for Using Malware Analysis to Improve Security Requirements

Nancy R. Mead, Jose Andre Moralesand Gregory Paul Alice (2015). *International Journal of Secure Software Engineering (pp. 1-23).*

www.irma-international.org/article/a-method-and-case-study-for-using-malware-analysis-to-improve-security-requirements/123452

Reusing Transaction Models for Dependable Cloud Computing

Barbara Gallinaand Nicolas Guelfi (2012). *Software Reuse in the Emerging Cloud Computing Era (pp. 248-277).*

www.irma-international.org/chapter/reusing-transaction-models-dependable-cloud/65175

Graph Classification Using Back Propagation Learning Algorithms

Abhijit Bera, Mrinal Kanti Ghoseand Dibyendu Kumar Pal (2020). *International Journal of Systems and Software Security and Protection (pp. 1-12).*

www.irma-international.org/article/graph-classification-using-back-propagation-learning-algorithms/259417

Clustering-Based Approach for Clustering Journals in Computer Science

J. K. D. B. G. Jayaneththiand Banage T. G. S. Kumara (2019). *International Journal of Systems and Service-Oriented Engineering (pp. 35-51).*

www.irma-international.org/article/clustering-based-approach-for-clustering-journals-in-computer-science/256135