Cooperative Intrusion Detection for Web Applications

Nathalie Dagorn

Laboratory of Algorithmics, Cryptology and Security (LACS)
University of Luxembourg
162a Avenue de la Faïencerie, L-1511 Luxembourg, Luxembourg
nathalie.dagorn@uni.lu
http://lacs.uni.lu/

Abstract. This contribution involves cooperative information systems, and more precisely interorganizational systems (IOS). Indeed, experience of real enterprises shows that most IOS interoperate today over the Web. To "ensure" security of these IOS on the Web (in particular, security of the applications they are made of), various hardware and software protection can be employed. Our work falls into the field of intrusion detection, and covers more precisely intrusion detection for Web applications. Several misuse-based intrusion detection systems (IDSs) were developed recently for Web applications, whereas, to our knowledge, only one anomaly-based Web IDS exists and works effectively to date. This one was unfortunately conceived disregarding any kind of cooperation. In previous work, we improved it to gain in sensitivity and specificity. This paper describes a cooperation feature added to the IDS, so that it is able to perform an *alarm correlation* with other detectors, allowing coo-perative intrusion detection, as well as an *event correlation* to detect distributed attacks. The first experiments in real environment show encouraging results.

1 Introduction

In the field of computer security, application level attacks have particularly been increasing for the last years. About 75% of intrusions come today via the Web [26]. The development of intrusion detection systems (IDSs) for Web-based systems is an important topic, which has not been extensively explored yet. Several Web IDSs based on signatures (*misuse* detection) exist and show good results [1,6,13]. Recently, an *anomaly*-based Web IDS was proposed [22], having the advantage to detect unknown attacks. We improved this system over the last months; our work on the subject was described in two previous papers: [9] presents original work, our improvements and our proposal to date, motivated by theoretical and practical examples, whereas [10] focuses on the system's implementation (functional and technical architecture), evaluation and ongoing efforts.

This paper describes a complementary cooperation feature added to the system to allow cooperative intrusion detection (by alarm correlation) and the detection of distributed attacks (by event correlation).

D. Pointcheval, Y. Mu, and K. Chen (Eds.): CANS 2006, LNCS 4301 , pp. 286 – 302, 2006.

The paper is organized as follows. Section 2 describes the context and motivation of our research: first, it outlines aspects of IOS, with a particular focus on different cooperation situations, proposing five cooperation levels, a typology and a synthesis table; then, some Web security issues are indicated in this context. Section 3 sums up related work on cooperative IDSs, as well as our previous work on the subject (the development of an anomaly-based IDS for Web applications), in order to provide the reader a good background. Section 4 presents the added cooperation feature: alarms raised in one IDS are propagated to other IDSs to improve detection accuracy and to detect distributed attacks; details on the feature's implementation and a motivating example are also provided. Section 5 describes the complete system's evaluation to date, discusses the preliminary results and outlines ongoing efforts. Section 6 contains some concluding remarks.

2 Context and Motivation

Today, information systems overlap the organizational boundaries. For many organizations, the *intra-organizational integration phase* is complete (or is going well). In order to access new markets or to benefit from synergy effects enabling them to reduce the costs, some of those organizations choose to merge with other powerful actors of their sector, to ally with partners or even competitors. More and more activities of the organization also depend on activities realized outside its boundaries. Organizations thus turn now to an *interorganizational cooperation phase*, for which many benefits in terms of effectiveness are expected.

2.1 Identification of Cooperation Levels

The concepts of integration and interoperability are not restricted to cooperation between organizations. They can apply to various levels or objects, at a large or small scale: organizational units, processes, applications, software, hardware… We propose in [11] to identify five cooperation levels (Fig. 1): the highest level concerns cooperation between organizations, involving technical as well as social concepts like confidence [14,15,27]. Both levels below focus on cooperation between information systems and between applications; they are detailed in the next paragraph. The lowest levels concern cooperation between processes and even components; the more one goes down in the figure, the more the cooperation relates to a very technical level.

2.2 Proposal for an IOS Typology

The levels, which are relevant for us in this paper, are those, which relate to cooperation between information systems and between applications. Several typologies exist, classifying IOS according either to theoretical perspectives [17], or to their functional characteristics [25], or to the type of interdependence existing between the different organizations using the IOS [4]. Essentially based on this last perspective, we tried to find examples of IOS relating to each type of cooperation identified[1].

[1] We specify that these groups are only "virtual", so that one IOS could be classified in a group or another according to the circumstances. More details about this topology are available in [11].