LUARM:
An Audit Engine for Insider Misuse Detection

G. Magklaras, University of Plymouth, UK
S. Furnell, University of Plymouth, UK
M. Papadaki, University of Plymouth, UK

ABSTRACT

Logging User Actions in Relational Mode (LUARM) is an open source audit engine for Linux. It provides a near real-time snapshot of a number of user action data such as file access, program execution and network endpoint user activities, all organized in easily searchable relational tables. LUARM attempts to solve two fundamental problems of the insider IT misuse domain. The first concerns the lack of insider misuse case data repositories that could be used by post-case forensic examiners to aid an incident investigation. The second problem relates to how information security researchers can enhance their ability to specify accurately insider threats at system level. This paper presents LUARM’s design perspectives and a ‘post mortem’ case study of an insider IT misuse incident. The results show that the prototype audit engine has good potential to provide a valuable insight into the way insider IT misuse incidents manifest on IT systems and can be a valuable complement to forensic investigators of IT misuse incidents.

Keywords: Auditing, Forensics, Insiders, IT Misuse, Logging, Misuse Detection

INTRODUCTION

The problem of insider IT misuse is a very real threat for the health of IT infrastructures encompassing both intentional activities (e.g., targeted information theft and accidental misuse (e.g., unintentional information leak). Numerous studies have tried to define an “insider” in the context of Information Security. A generic definition from Probst et al. (2009) is “a person that has been legitimately empowered with the right to access, represent, or decide about one or more assets of the organization’s structure”.

The most widely known insider misuse cases are usually about intellectual property theft. The arrest of Lan Lee and Yuefei Ge by FBI agents (Cha, 2008) is a classic case. The arrested men were engineers of NetLogic Microsystems (NLM) until July 2003. During the time of their employment, they were downloading trade sensitive documents from the NLM headquarters into their home computers. These documents contained detailed descriptions of the NLM microprocessor product line. Eventually, their ties to the Chinese government and military

DOI: 10.4018/jdcf.2011070103
were discovered by investigators. However, both mass media case descriptions and relevant security surveys do not provide the tools or the methodology to systemically study and mitigate the problem. Insider IT misuse is a multi-faceted problem and one of the things insider misuse researchers really need is a repository of more detailed case descriptions with a focus on the impact insider misuse actions have at computer system level (NSTISSAM). This is the area of Insider Threat Specification, the core concept behind the proposed logging engine which is examined in the next section.

**INSIDER THREAT SPECIFICATION**

Threat specifications follow the principles of intrusion specification, a concept which is not new in the information security world. Techniques to describe threats exist for an entire range of information security products, from anti-virus software to several intrusion detection/prevention systems (IDS/IPS) (Bace, 2000) where threats are specified by anomaly detection, pattern matching (also known as misuse detection) mechanisms or a heuristic-based combination of the two. Insider Threat Specification is the process of using a standardized vocabulary to describe in an abstract way how the aspects and behaviour of an insider relate to a security policy defined misuse scenario. Figure 1 shows the information flow of a typical IT misuse detection system. The security specialist translates the Security (and resulting monitoring policy) into a set of misuse scenario signatures, standard descriptions of IT misuse acts that describe the behaviour of a user at process execution, filesystem and network endpoint level (Magklaras et al., 2006). The misuse scenario signatures and collected audit data (Bace, 2000) from the IT infrastructure are fed into a misuse detection engine.

Vital to insider threat specification is the structure and content of the audit record, at the center of Figure 1. If the audit record is incomplete, in terms of the type of information we need to log or unavailable, because the data are vanished due to bad system design or intentional data corruption, the specification of insider threats is useless. This is one of the primary objectives that LUARM tries to address by providing an evidence rich and reliable audit record format.

**INSIDER MISUSE DETECTION AUDITING REQUIREMENTS**

Bace (2000) discusses intrusion detection (and hence misuse detection) as an audit reduction