False Positive and False Negatives in Intrusion Detection Systems: Reasons, Challenges and Handling

Dr. Neminath Hubballi

September 30, 2014

Abstract

A network based Intrusion Detection System (IDS) gathers and analyzes network packets and report possible low level security violations to a system administrator. In a large network setup, these low level and partial reports become unmanageable to the administrator resulting in some unattended events. Further it is known that state of the art IDS generate many false alarms. In this tutorial we will discuss reasons for false alarms (both false positives and false negatives) in different types of IDSs (Signature-based, Anomaly-based and Event-based) and also critically review the performance of various methods. We also compare commercial Security Information and Event Management (SIEM) tools and their ability to handle false alarms.

1 Target Audience

Information Security Practitioners
Undergraduate and Postgraduate Students
Research Scholars
Teachers of Engineering Colleges

2 Prerequisites

Basics of Information Security
Knowledge of Computer Networking

3 Expected Enrolment

As the material covered is useful for both students, teachers and information security practitioners.

The topic is of practical significance, several security researchers and system designers would be interested to know the reasons for false alarms in intrusion detection systems and techniques available in the literature. This tutorial covers research and methods from both academia and industry with a discussion of commercial tools available.
4 Topics to be Covered

- Basics of Intrusion Detection Systems (30 Minutes)
- False Positives (FP) in Signature based Intrusion Detection Systems (1 Hour 15 Minutes)
  - Reasons for FP generation
  - Methods available for handling including a taxonomy
  - Commercial SIEM tools performance and comparison
- False Negatives (FN) in Signature based Intrusion Detection Systems (1 Hour 15 Minutes)
  - Reasons for FN generation
  - Improving the performance
  - Active verification Methods
- False Positives and Negatives in Anomaly based Intrusion Detection Systems (1 Hour)
  - Reasons for FP and FN generation
  - Different approaches of FP/FN minimization
  - Improving the performance

5 Reference Material

- Bo Zong et al., “Towards Scalable Critical Alert Mining ”, KDD 2014

6 Biography of Presenter

Dr Neminath Hubballi is an assistant professor in the department of Computer Science and Engineering at Indian Institute of Technology Indore, India. He earned his Ph.D from the department of Computer Science and Engineering at Indian Institute of Technology Guwahati. His areas of interest include Network Security, System Security, Cloud Security and dependable systems. Prior to the current role he was with corporate R&D centers namely Samsung R&D working on mobile security, Infosys Labs working on Cloud Security and Hewlett-Packard working on message oriented middleware. He has several publications in the area of security and is a regular reviewer in many security journals and conferences and also served as TPC member of conferences. He also participated in Ph.D forum at COMSNETS 2011.