Survey on system-level graph-based and anomaly-based intrusion detection

Fanny Dijoud*[1,2,3], Michel Hurfin[1,2,3], Pierre-Francois Gimenez[1,2,4], Frédéric Majorczyk[1,2,5], and Barbara Pilastre[5]

[1]Université de Rennes – Université de Rennes – France
[2]Institut de Recherche en Informatique et Systèmes Aléatoires – Université de Rennes, Institut National des Sciences Appliquées - Rennes, Université de Bretagne Sud, École normale supérieure - Rennes, Institut National de Recherche en Informatique et en Automatique, CentraleSupélec, Centre National de la Recherche Scientifique, IMT Atlantique – France
[3]L'Institut National de Recherche en Informatique et en Automatique – L'Institut National de Recherche en Informatique et e n Automatique (INRIA) – France
[4]CentraleSupelec – CentraleSupélec, Centrale Supélec – France
[5]DGA Maîtrise de línformation – Direction générale de l'Armement (DGA) – France

Résumé

Intrusion Detection Systems (IDS) are tools for monitoring a system, in order to identify potential malicious activities within it. This survey presents an analysis of graph-based anomaly-based IDS at system level. We also present open issues regarding those IDS, and propose a taxonomy of suitable features to compare them.

*Intervenant