A parser-based data collector for intrusion detection

Grégor Quetel*†[1], Eric Alata*‡[2], Pierre-Francois Gimenez§[3], Thomas Robert¶[1], and Laurent Pautet[1]

[1]Télécom Paris – LTCI, Télécom Paris, Institut Polytechnique de Paris – France
[2]LAAS CNRS – LAAS CNRS TOULOUSE – France
[3]CentraleSupélec, Univ. Rennes, IRISA – CentraleSupélec, Univ. Rennes, IRISA – France

Résumé

Intrusion detection systems often struggle to identify attacks directed at applications. A contributing factor is the various syntactical forms these attacks can take. This paper introduces a methodology to design and adapt applicative data collectors (DCs) to software projects by integrating them into the application's parsers. This data collector aims to enhance applications' security by providing semantic information to intrusion detection mechanisms.

*Intervenant
†Auteur correspondant: gregor.quetel@telecom-paris.fr
‡Auteur correspondant: ealata@laas.fr
§Auteur correspondant: pierre-francois.gimenez@centralesupelec.fr
¶Auteur correspondant: thomas.robert@telecom-paris.fr