5th Workshop on ICT Uses in Warfare and the Safeguarding of Peace (IWSP'13), 25-27 November 2013

Automated Classification of Computer Network Attacks

Renier van Heerden
Cyber Defence
CSIR
Pretoria, Gauteng
and
Rhodes University
Grahamstown, Eastern Cape
Email: rvheerden@csir.co.za

Louise Leenen
Cyber Defence
CSIR
Pretoria, Gauteng

Barry Irwin
Computer Science
Rhodes University
Grahamstown, Eastern Cape

Abstract

In this paper we demonstrate how an automated reasoner, HermiT, is used to classify instances of computer network based attacks in conjunction with a network attack ontology. The ontology describes different types of network attacks through classes and inter-class relationships and has previously been implemented in the Prot´eg´e ontology editor. Two significant recent instances of network based attacks are presented as individuals in the ontology and correctly classified by the automated reasoner according to the relevant types of attack scenarios depicted in the ontology. The two network attack instances are the Distributed Denial of Service attack on SpamHaus in 2013 and the theft of 42 million Rand ($6.7 million) from South African Postbank in 2012.