Factors for Differentiating Human from Automated Attacks

Kelly Greeling, Alex Withers, Masooda Bashir

University of Illinois at Urbana-Champaign, School of Information Sciences
University of Illinois at Urbana-Champaign, National Center for Supercomputing Applications
University of Illinois at Urbana-Champaign, School of Information Sciences

Abstract

Many Intrusion Detection Systems and Intrusion Protection Systems utilize behavior-based methodology, which seeks to identify a baseline of normal user that they then use to compare against *real-time* and *non-real-time* events in an effort to locate malicious activity. However, the rise of automated attacks has created a great deal of noise for security personnel to wade through to identify malicious behavior. The growth of automated attacks that has led even CERT/CC (2004) to abandon their use of the count of network attacks, to assess the scope and effects of system attacks. If a human based attack is significantly different than an automated attack it would be extremely useful for security personnel to have a way to separate the behavior of an automated cyberattack tool from that of a human actor, as this would allow them to create separate tools to deal with each. This paper is an exploratory study into whether it is viable to use event time-difference and event pattern-occurrence as factors in behavior-based Intrusion Detection Systems for identifying the difference between human and automated program behavior.