DCAFE: A Distributed Cyber Security Automation Framework For Experiments

George Rush

ABSTRACT
Cyber security has quickly become an overwhelming challenge for governments, businesses, private organizations, and individuals. In an increasingly connected world, the trend is for resources to be accessible from anywhere at any time. Greater access to resources implies more targets and potentially a larger surface area for attacks, which makes securing systems more difficult. Automated and semi-automated solutions are needed to keep up with the deluge of modern threats, but designing such systems requires a distributed architecture to support development and testing. Several such architectures exist, but most only focus on providing a platform for running cyber security experiments as opposed to automating experiment processes. In response to this need, we have built a distributed framework based on software agents which can manage system roles, automate data collection, analyze results, and run new experiments without human intervention. This paper provides a detailed description of our distributed automation framework for cyber security experiments.

*The publication of this abstract is intended for educational purposes only from an internal symposium and its content has not been peer-reviewed.*