



Augmenting Threat Analysis Capabilities Using Intelligent Threat Agents

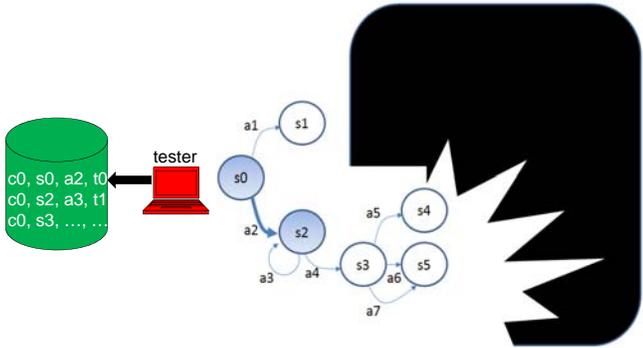


S&T Campaign: Assessment & Analysis Assessing Mission Capability of Systems

Jaime C. Acosta, Ph.D., (575) 678-8115
jaime.c.acosta.civ@mail.mil

Research Objective

- Develop algorithms, models, and tools that will lead to the development of automated agents that benefit network security evaluators during assessments (focusing on maximizing coverage) and after assessments (focusing on providing optimal remediation solutions)
- Leveraging public and in-house knowledge-bases, agents will identify best-course-of-action given the observed environmental states



Scenario, c = network and node configurations
State, s = network state from testers perspective (e.g., ip: 10.0.2.11, TCP, port 21 ip: 10.0.2.20, ...)
Action, a = keystrokes and mouse clicks (e.g., nmap 10.0.2.0/24)
Time, t = timestamp

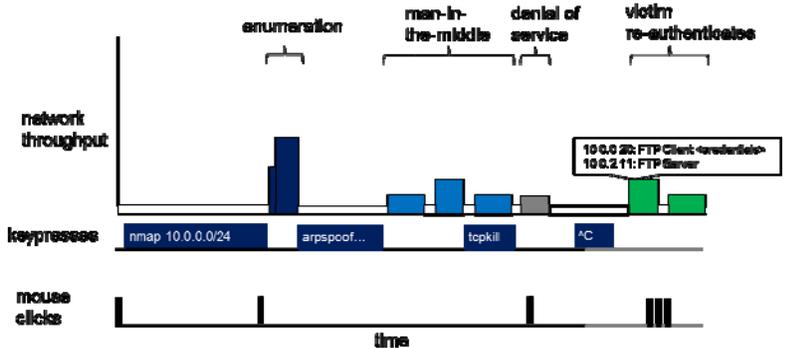
During an assessment scenario, evaluators traverse the network by executing actions based on the current observed state of the network and past experience – this data is collected in a knowledge-base.

Challenges

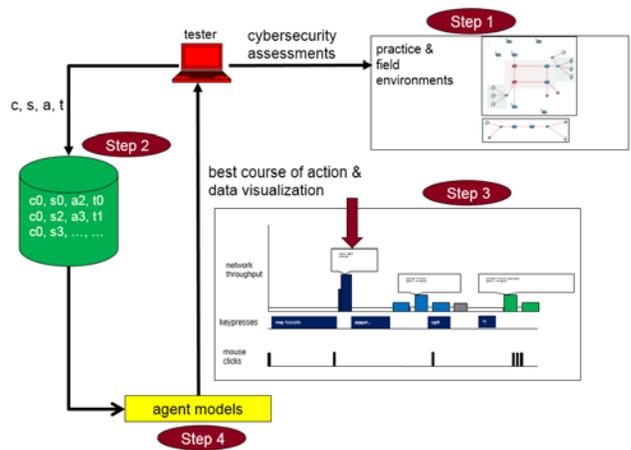
- Assessment methodologies lack fidelity; the quality of an assessment largely depends on particular tester experience
- Other works in automated network security analysis ignore critical factors such as exploit execution times, state-space explosion, and working with partial system knowledge

ARL Facilities and Capabilities Available to Support Collaborative Research

- A scalable cybersecurity assessment testbed that allows analysts to create and manage scenarios (both tactical and strategic) that are realistic and repeatable
- A unique knowledge-base that consists of assessment data (collected using capture the flag scenarios) that contains observed network states and evaluator actions
- Abundant threat assessment expert personnel



Knowledge-base data can be visualized and salient features may be used to build intelligent agents.



The envisioned workflow consists of agent models that will aid evaluators by leveraging past data.

Complementary Expertise/ Facilities/ Capabilities Sought in Collaboration

- Expertise in the fields of network security, machine learning, big data, expert systems, or intelligent agents
- Facilities that may be used to host “capture the flag” events for data collection
- Suggestions for improving the network security assessment process