Multi-model run-time security analysis - July 2017

Submitted by Jamie Presken on Mon, 06/12/2017 - 9:20am

Public Audience

Purpose: To highlight progress. Information is generally at a higher level which is accessible to the interested public.

PI(s): David Garlan, Bradley Schmerl

1) HARD PROBLEM(S) ADDRESSED (with short descriptions)

- **Composability** through multiple semantic models (here, architectural, organizational, and behavioral), which provide separation of concerns, while supporting synergistic benefits through integrated analyses.
- **Scalability** to large complex distributed systems using architectural models.
- **Resilient architectures** through the use of adaptive models that can be used at run-time to predict, detect and repair security attacks.
- **Predictive** security metrics by adapting social network-based metrics to the problem of architecture-level anomaly detection.

2) PUBLICATIONS

Ryan Wagner, David Garlan, and Matt Frederiksen. An Advanced Persistent Threat Exemplar. Institute for Software Engineering Technical Report CMU-ISR-TR-17-100, 2017.

3) KEY HIGHLIGHTS

An alpha (internal) release of the advanced persistent threat exemplar has been released. The full release is anticipated by the end of summer.

4) COMMUNITY ENGAGEMENTS

5) **EDUCATIONAL ADVANCES**

We have engaged a team from the Master of Information Technology Strategy program for development of the the exemplar testbed as part of their practicum project, a Masters of Softwre Engineering student in an independent study for formal modeling of advanced persistent threats, and an undergraduate from Duke University to implement an instance of a simulated advanced persistent threat scenario on the exemplar testbed.

Approved by NSA Scalability and Composability Metrics Resilient Architectures Multi-Model Run-Time Security Analysis