RADAR: Real-time Advanced Detection and Attack Reconstruction

Stony Brook University

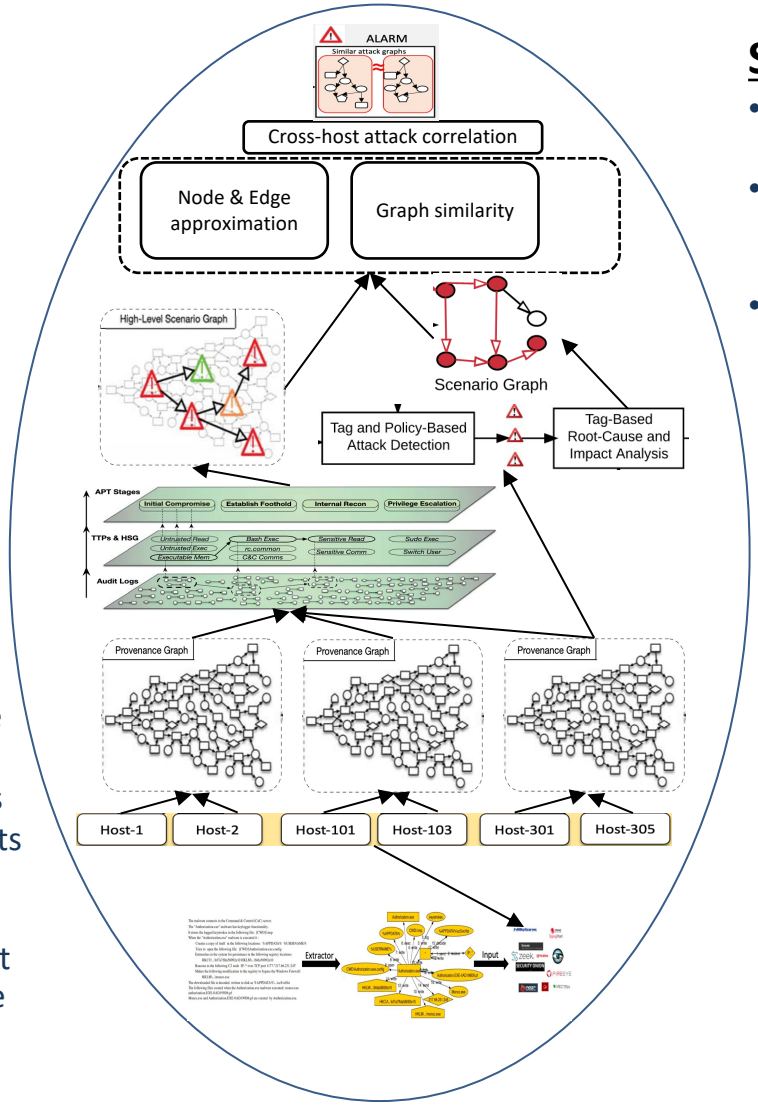
THE UNIVERSITY OF ILLINOIS AT CHICAGO

Challenge:

- Real-time APT detection along with attack scenario reconstruction
- Extraction of actionable graphs of attack behavior from natural language CTI reports
- Correlation of alerts generated by underlying IDSes from different hosts

Solution:

- Main-memory based fast, scalable provenance graph generation from audit logs
- Novel *tag-based* propagation and detection policies on the provenance graph
- Usage of MITRE ATT&CK framework's TTPs to bridge low-level system events and attacker stages and generate attack scenario graphs
- Graph and similarity-based cross-host correlation of alerts using novel node and graph similarity metrics
- Threat hunting by capturing attack behavior graphs from CTI reports identifying connected entities without focusing on single IOCs



Scientific Impact:

- Increased usage of MITRE TTPs in recent literature
- Increased the level of difficulty for the attackers to evade or remain stealthy
- Reduce the work-load of cyber analysts by false positives reduction and cross-host alert correlation

Broader Impact and Broader Participation:

- More resilient host infrastructures
- Our methods can leverage off-the-shelf monitoring systems
- 4 PhD students (UIC & SBU)

Award Number: 1918667
Program Manager: Jeremy Epstein
Principal Investigators: R. Sekar, V.N. Venkatakrishnan
Date: June 1-2, 2022