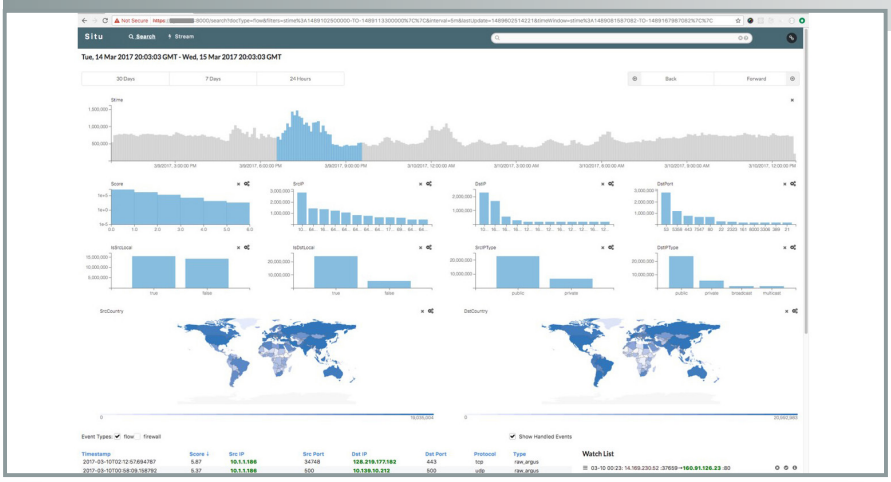
SITU—Real-Time Situational Understanding and Discovery of Cyber Attacks



Technology Summary

In the deluge of data in today's networks, operators need better tools to help identify suspicious behavior that bypasses automated security systems. Further, operators need to understand what makes an event suspicious to determine the importance and impact of the event. Highlighting such suspicious behavior helps operators focus their limited time on the most suspicious events within vast amounts of data.

Researchers at ORNL have developed Situ, a scalable, real-time platform for discovering and explaining suspicious behavior that current technologies cannot detect. The ORNL approach to anomaly detection is based on unsupervised, probabilistic modeling. Key to the approach is modeling events in different contexts or at multiple scales; each event is modeled and scored by multiple anomaly detectors to identify different kinds of anomalous behavior. The anomaly detectors update the behavior models online as new data are streamed into the system. The detectors score each event for each context based on the likelihood of new events occurring given the probability model of prior behavior. Scoring the anomalousness of events for multiple contexts provides analysts with an understanding of why an event is anomalous. By examining these contexts, operators can understand how different event features contribute to the overall anomaly score.

Situ helps network operators discover and understand suspicious events that would otherwise go undetected. It reduces the huge volumes of raw network data to a smaller, manageable number of events that should be examined by human domain experts. By highlighting suspicious activity, Situ enables the discovery of novel attacks, but can also alert operators to insider threats, policy violations, misconfigurations, and new kinds of behavior that may require some investigation. Through the application of multiple contexts, Situ can look for a wide range of activity. Different contexts perform better for different kinds of attacks. Multiple contexts can also help explain why an event is suspicious as the varying scores will point operators to specific kinds of behaviors.

Advantages

- Helps network operators discover and understand suspicious events that would otherwise go undetected
- Reduces huge volumes of raw network data to the smaller, manageable number of events that should be examined by domain experts
- Hardware and operating system agnostic
- Doesn't require labeled training data
- Operates on real-time streaming data
- Online training of models
- Detects insider threats, policy violations, misconfigurations
- Applicable to multiple domains

Potential Applications

- Defense against zero-day threats
- Fraud detection in a variety of domains (e.g., banks, credit cards, mobile devices)
- Intrusion detection in the cyber security domain
- Structural fault detection
- Diagnosis (medical anomaly detection)
- Analysis of streaming data
- Event detection in sensor networks
- Surveillance activities

Patent

Erik M. Ferragut, Jason A. Laska, and Robert A Bridges. *Detection of Anomalous Events,* US Patent 9,361,463, issued June 7, 2016.

Erik M. Ferragut, John R. Goodall, Michael D. Iannacone, Jason A. Laska, and Lane T. Harrison. *Real-Time Detection and Classification of Anomolous Events in Streaming Data,* US Patent 9,319,421 issued April 19, 2016.

Inventor Point of Contact

John R. Goodall
Computational Sciences and Engineering Division
Oak Ridge National Laboratory

Licensing Contact

David L. Sims
Technology Commercialization Manager
Technology Commercialization
UT-Battelle, LLC
Oak Ridge National Laboratory
Office Phone: 865.241.3808
Email: simsdl@ornl.gov

To view this and other ORNL inventions, visit ORNL Partnerships at
http://www.ornl.gov/connect-with-ornl/for-industry/partnerships/technology-licensing/available-technologies