NECAP

Feasibility Study/
Discussion

Agenda

- Keep it informal – fact finding and collaboration
- Open discussion on the event space and the apparent need for an event focused set of specifications
- Discussion of potential additional specifications required to provide the full breadth of capability desired
- Gather ideas and feedback from the group
- Look for additional avenues of research that may facilitate in determining the need and feasibility of such a set of specifications

So What?

- There is no current program/protocol at NIST for Network Event Automation
  - There is no “NECAP” program, this is only a research project name
- Studying the feasibility of such a program and implications
- Aligning with Common Event Expression (CEE) analysis from the perspective of timing
- Attempt to determine the value proposition of a full suite of specifications for the processing of events
- While the potential specification is NOT security specific, the first use cases are security related thus the apparent focus on security

Criteria

- The achievability of associated goals
- Value proposition
- Maturity of potential components
- Potential interaction with existing protocols (SCAP)
- Applying SCAP lessons learned about Enumeration, Expression, Metrology and validation

Potential Components

- CEE – Syntax, Taxonomy, Transport, and Recommendations for event logging
- Attack – Common Attack Pattern Enumeration and Classification(CAPEC)?
- Is a language to express CAPEC (or similar) needed, feasible?
- Threat – Would there be value in enumeration, expression, and measurement of threats?

Potential Components (Cont.)

- Reporting – Should there be a standardized way to extract reports from event data?
- Query – Should there be a standardized way to query events and relate them?
- Policy – What if any means of setting and maintaining logging policy should/can be created?

Potential Interactions

- SCAP
  - Would it be beneficial to standardize how attacks and other events are correlated to CVE, CCE, and CPE data in an automated way during reporting, query, and correlation?
  - Interaction appears more feasible for log consumers vs. log producers (speed and overhead concerns). Is this an issue?

Actions

- NIST is performing a feasibility and will release a white paper by the end of fiscal year ‘09
- MITRE, DoD and NIST continue to collaborate and communicate on the specifications, activities, and issues
- Industry experts and stakeholders are involved through various outreach efforts

Summary

- NECAP is not a program, but rather a research project conducted by NIST with assistance from DoD, MITRE, and Industry
- The results of the study will be released to the community by the end of the fiscal year
- This subject is very complex and thus will continue to warrant research, validation of concepts, and collaboration

Contact

George Saylor

george.saylor@g2-inc.com