Security Event Standardization

“SES”, Moving security messages throughout the ether.

Workshop on GENI and Security
UC-Davis, January 2009
Doug Pearson / Wes Young

Addressing

- Addressing the Workshop question:
  - How can GENI itself be adequately secured and protected from attack?
- Operationally protecting GENI, experiments, and connected infrastructures

Idea

- Share, in real-time, security event information within a trusted federation, and among federations; and
- Apply the shared information to local protection and response.

Partial Solution

- The Idea is just one small part of a necessary total security solution
- Is designed to augment and enhance other components of a total solution; and
- Is designed to integrate with other operational processes

At its roots, not a new Idea

- Lots of security event information is being shared right now
  - Private communities
  - Semi-private communities
  - Public sources

Issues

- Current methods cumbersome
  - Many rely on e-mail
  - Not easily automated
  - Requires the “human interrupt” signal
  - Not structured for correlation
- Multiple data representations
  - Non-standard
  - Not easily parsed
  - Not easily acted on
  - Hard to measure confidence

Issues

- Long-term Intelligence
  - Hostage to our inboxes
  - Difficulty of correlation
  - Difficulty of coordinated or cooperative analysis
- Multiple Federations
  - Trust relationships
  - Political and organizational boundaries

Building a Solution

- Based on work started at Argonne National Laboratory – “Federated Model”
- Development in progress
  - REN-ISAC
  - In cooperation with Internet2/CSI2
  - Funded by DoJ grant to Internet2 for a number of security projects and activities
  - Cooperating with parallel work at Argonne, funded by DoE.

Building a Solution

- Standardization
  - IDMEF - Security standard for representing mid-level security messages in XML
  - Developed in early 2000's
- Extensions
  - Understanding "Sites" (via ASN, CIDR)
  - Understanding "Federations"

Building a Solution

- Interoperation with EDDY (End-to-end Diagnostic Discovery)
  - Transport option
  - Local option for advanced event management
- Request Tracker (RT) – Solves the “UI”, “ACL” and “Workflow” problem. Allows us to build on existing, rich, open-source technology.

Phase I Solution

- Local log (IDS, firewall, sshd, DNS, darknet sensor, etc.) parsing to yield “mid-level events”.
- Normalized data description in IDMEF
- Transport, storage, and retrieval
- Trusted federation
- Real-time security event information sharing → protection and response.

Phase I Solution

- Pilot Deployment
  - Sharing of data within REN-ISAC and Department of Energy federations
  - Sharing between REN-ISAC and DOE federations
  - Sharing real-time event and analysis (e.g. top-offending) data
- Production deployments in REN-ISAC and DOE

Building a Framework

- Framework for the incorporation of additional correlation and analysis tools
- Interface with systems that notify abuse contacts regarding infected systems, e.g. the REN-ISAC notification system
- Interface with systems that treat higher-level incident information in a federated context

Extending the Framework

- Long term intelligence storage
- Feed of security intelligence to other federations and mitigation communities
- Threat analysis platform
- The Future
  - Rapid application development
  - “Super Crunching” of data

The Result

- A better understanding of:
  - Who our attackers are
  - What they're doing
  - How they're doing it
- Rapid and comprehensive protection

Contacts

- Doug Pearson
  - dodpears@ren-isac.net
- Wes Young
  - wes@barely3am.com