

SALSA - NetAuth

SALSA Security Briefing
Conference Call
September 23rd, 2004

What led to the creation of NetAuth?

- Various methods and techniques currently exist to provide identification, registration, and authorized access to campus networks.
- The problems posed by the scope and scale of recent security incidents such as MSBlast and Polybot have shown the value of these data.
- Security management requires a rich set of data across disparate data sources to provide a cohesive network information base for device location and incident remediation.

[SALSA-NetAuth Charter]

The SALSA-NetAuth Working Group will consider the data requirements, implementation, integration, and automation technologies associated with understanding and extending network security management related to:

1. Authorized Network Access (keyed by person and/or system)
2. Style and behavior of transit traffic (declarative and passive)
3. Forensic support for investigation of abuse

SALSA-NetAuth Working Group:

Initial Activities:

- Investigation of requirements and implementations of network database and registration services in support of network security management;
- Investigation of extensions to these services to proactively detect and prevent unauthorized or malicious network activity.
- Analysis and proposal toward a pilot and eventual implementation to support network access to visiting scientists among federated institutions.
- Analysis of security applications that may result from extending these implementations.


SALSA-NetAuth Working Group:

- Participate in the NetAuth
 - Working group is open to all members of the Educause / Internet2 community.
 - Contribute to future documents
- Homepage
 - <http://security.internet2.edu/netauth/index.html>
 - Draft charter
 - Mailing list
- Additional contacts
 - Steve Olshansky
 - Charles Yun
 - Christopher Misra
- Volunteers Needed

SALSA-NetAuth Working Group:

Initial Deliverables:

- Strategies for Automating Network Policy Enforcement
 - Eric Gauthier, Phil Rodrigues, 16 July 2004
 - <http://security.internet2.edu/netauth/docs/draft-internet2-salsa-netauth-summary-00.html>
- Pre-Requisites to Automating Network Policy Enforcement
 - Kevin Miller – in progress
- System Requirements and Future Goals
 - Ongoing Discussions

A decorative graphic consisting of a thin yellow circle on the left side, partially overlapping a horizontal yellow bar. A large black left square bracket is positioned on the left side of the bar, and a large yellow right square bracket is on the right side. The title text is centered within the yellow bar.

Strategies for Automating Network Policy Enforcement

Eric Gauthier & Phil Rodrigues

<http://security.internet2.edu/netauth/docs/draft-internet2-salsa-netauth-summary-02.html>

Strategies for Automating Network Policy Enforcement: Overview

- The document is a summary of some approaches for automating technical policy enforcement as a condition for network access in colleges and universities including:
 - Host isolation into specialized networks
 - Captive Portal-like Remediation
 - Conditional network access
- The document lays out a common framework for classifying various systems

Strategies for Automating Network Policy Enforcement: Issues

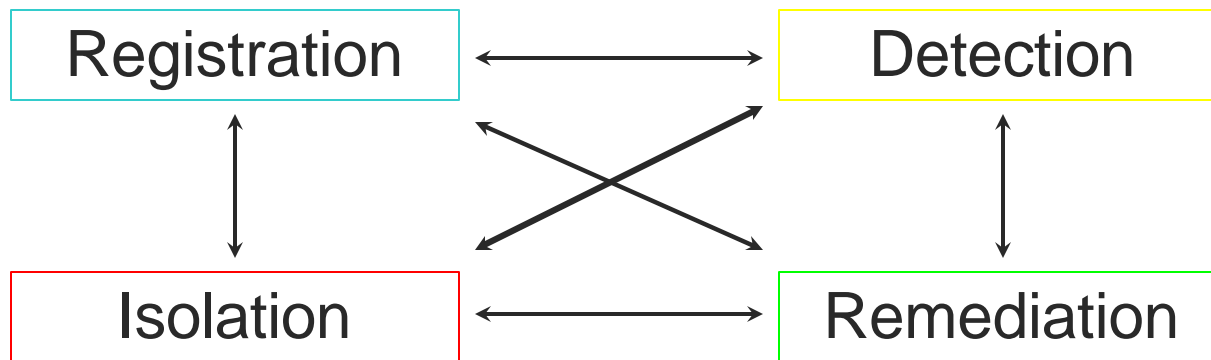
- Threat:
 - Large numbers of unsecured computers prone to mass infection (Malware/Botnets)
 - Unsecured hosts for use in Distributed file distribution, Spam, and Attack networks.
 - Remediation often requires manual investigation but its time intensive
- Challenge:
 - Thousands of privately owned and unmanaged computers
 - Lack of central control over student computers
 - Inability to tie the actions of these computers to particular individuals.
 - Large-scale security incidents requiring massive support intervention.

Strategies for Automating Network Policy Enforcement: Value

- Preventative policy enforcement reduces
 - Total number of technical security vulnerabilities
 - The success of a particular piece of malware or attack technique.
- Isolation networks separate compromised and infected hosts
 - Minimize the spread of infection
 - Block external access from attackers.
- Automated remediation systems have a positive impact on a large number of hosts with a relatively small time investment from computing staff.

Automating Network Policy Enforcement: Common Process

The process common to all implementations involves four steps



Automating Network Policy Enforcement: Registration

■ Registration

- A prerequisite that identifies a responsible party
- May be user-based or system-based
- Highly site specific
- Many available implementations
- Details are outside the scope of this document.

Automating Network Policy Enforcement: Detection

- Attempt to determine compliance with local network policy.
 - Proper patch level
 - Presence of up-to-date antivirus software
 - Presence of administrative passwords.
- Detection can take place before or after registration
- May result in isolation if the host is not in compliance.
- Detection may not be possible
 - Host firewalled
 - Agent not installed cleanly on a host.
- Inability to detection may cause registration to fail open or closed

Automating Network Policy Enforcement: Isolation/Remediation

- Isolation
 - Often happens after a deficiency has been discovered in the detection phase.
 - Placing the host into a different network space
 - Allow access to necessary updates
 - Protect host from external connections
 - Protect other hosts from it.
- Remediation
 - Where corrective action is recommended
 - Notification of appropriate support steps
 - Support contact information
 - May allow self-service including:
 - Patch availability, etc
 - Notify support staff of steps user has taken
 - Self removal from isolation network
 - May require support staff intervention

Automating Network Policy Enforcement: Policy Implications

- More questions than answers
- Three categories:
 - Government Regulations
 - FERPA, COPPA, etc.
 - Policy Implications
 - Privacy, records management and retention
 - Liability
 - Possible damage caused by installed agent
 - Patch licensing



Panel Discussion

Eric Gauthier - Boston University

Kevin Miller – Duke University

Chris Misra - University of Massachusetts

Jonathan Moore – University of Pennsylvania

Phil Rodrigues – New York University