NIMI, Tissue and Baseline Enforcement

Troy Dawson
dawson@fnal.gov
HEPIX Spring 2009

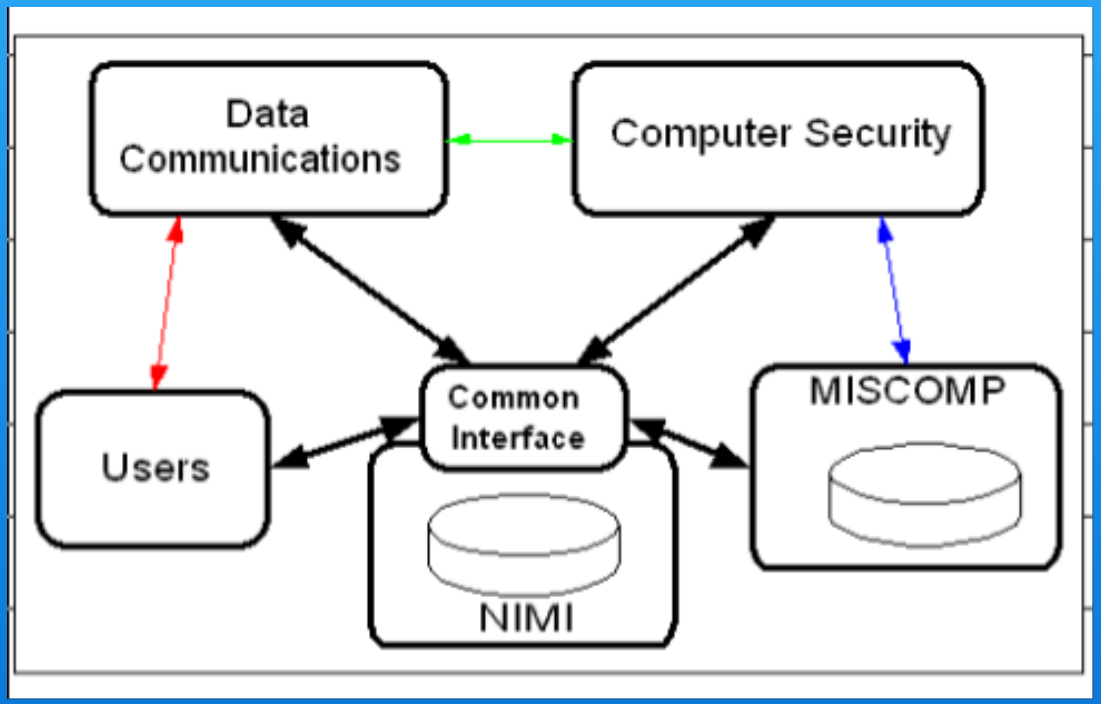
Overview

This presentation is just an overview, it does not go into detail of various tools, but is to show how various tools written at Fermilab have been combined to make the world a safer place for computers.

Agenda

- NIMI
- Tissue
- SMS / OCS Inventory
- Baseline Enforceing

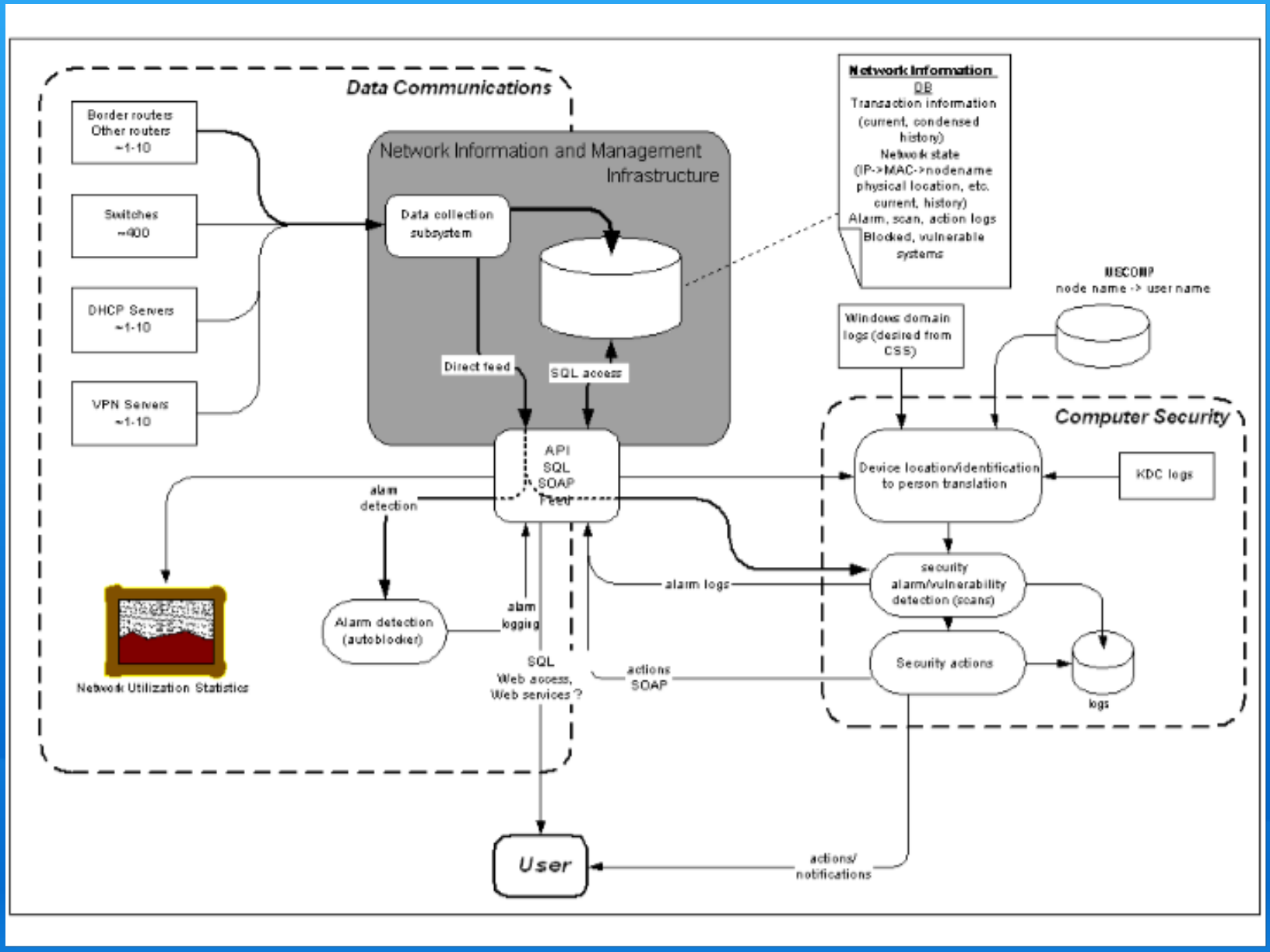
Communication Through NIMI



- Place NIMI in the middle of the picture
- Use it as:
  - Operational workflow information storage
  - Common data storage
  - Inter-group communication media

- Do not preclude existing tools, means of communication, encourage using new ones

NIMI Design


Data Communications
Border routers
Other routers
~1-10
Switches
~400
DHCP Servers
~1-10
VPN Servers
~1-10
Network Information and Management Infrastructure
Data collection subsystem
Direct feed
SQL access
Network Information DB
Transaction information (current, condensed history)
Network state (IP->MAC->nodename physical location, etc. current, history)
Alarm, scan, action logs
Blocked, vulnerable systems
NESCOMP
node name -> user name
Windows domain logs (desired from CSS)
Computer Security
API
SQL
SOAP
Feed
alarm detection
Device location/identification to person translation
KDC logs
alarm logs
security alarm/vulnerability detection (scans)
Alarm detection (autoblocker)
alarm logging
Network Utilization Statistics
SQL
Web access, Web services ?
actions
SOAP
Security actions
logs
User
actions/ notifications

Advantages of using NIMI

- Common well-known documented interfaces
  - WWW, SOAP, SQL, HTML
  - Grid? OGSI?
- Common authentication/authorization solutions
  - Kerberos, PKI/GSI
- Common centralized data storage
  - Easy data access for all parties
  - Single point of contact for all parties
  - Workflow management
  - Easier to maintain and support
- Flexibility
  - Hiding internals behind interfaces
  - Add new data as needed, not new interfaces
  - Build new SQL-based tools as needed
  - Archive/compile/purge old data

TISSUE

- TIssue is a database and workflow system for managing network blocks of systems.
- It is able to give warnings or completely block a system from the network.
- Network blocks handled via TIssue require manual intervention to resolve the problem that necessitated the block (such as patching the critical vulnerability)

TISSUE

- When a TIssue event is generated for a node, the registered system adminstrators (both the Primary and all Authorized Administrators in the SysAdmin database) are sent an E-mail message identifying the node and the crititical vulnerabity that will cause the node the node to be blocked.
- This message contains a link to the TIssue event so the responsible person can remediate the event after fixing the problem.

SMS / OCS Inventory

- All computers are supposed to be reporting to a central inventory system
- These central inventory systems must keep track of what software, and version of software is on a machine
- Windows - SMS
- Mac OS - SMS (using Centrify)
- Linux - OCS Inventory

Baseline Enforcement

- Baselines are documents describing the minimum setup a machine should be at to be able to be on Fermilab's network.
- A baseline has been written for all of the supported operating systems at the lab.
- In the past we had a very hard time enforcing or even letting users know if their machine was not following the baseling

Baseline Enforcement

- With SMS and OCS Inventory we are able to tell if a machine is not following the security baseline.
- With Tissue, we are not able to warn the admins, and then block the machines that are not following the baselines.

Baseline Enforcement

- Problems we are thinking about
  - Machines that are not connecting to SMS or OCS Inventory
  - Linux machines running non-standard versions of Linux
  - Appliances (printers etc..)