Network Information and Management Infrastructure

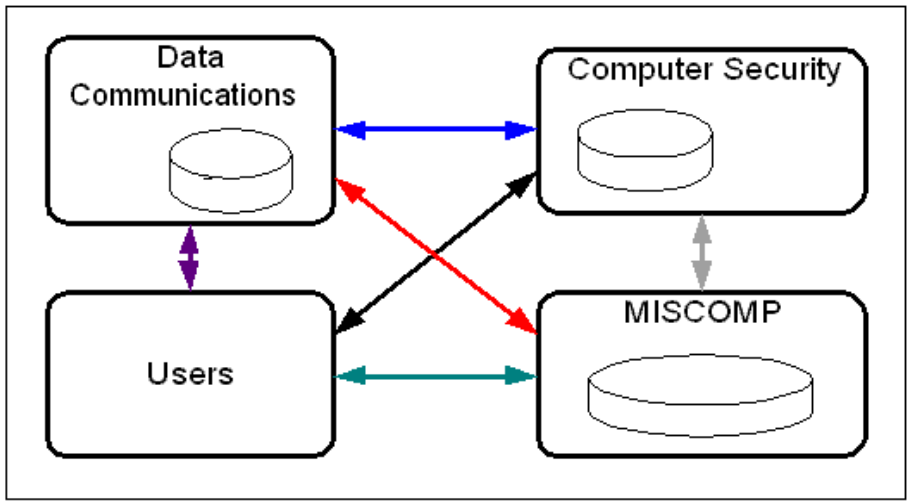
Computing Division briefing presentation

Igor Mandrichenko
CCF

Problem Description

- Specifics of FNAL network
  - Large
  - Open, dynamic
  - Exposed
- Successful network and network security management requires coordinated cooperation of key players:
  - Data Communications
  - Computer Security
  - Users
  - Desktop support
- Cooperation is impossible without communication
- Historically network management communication has been developing in ad-hoc fashion

Absence of Cooperation Infrastructure

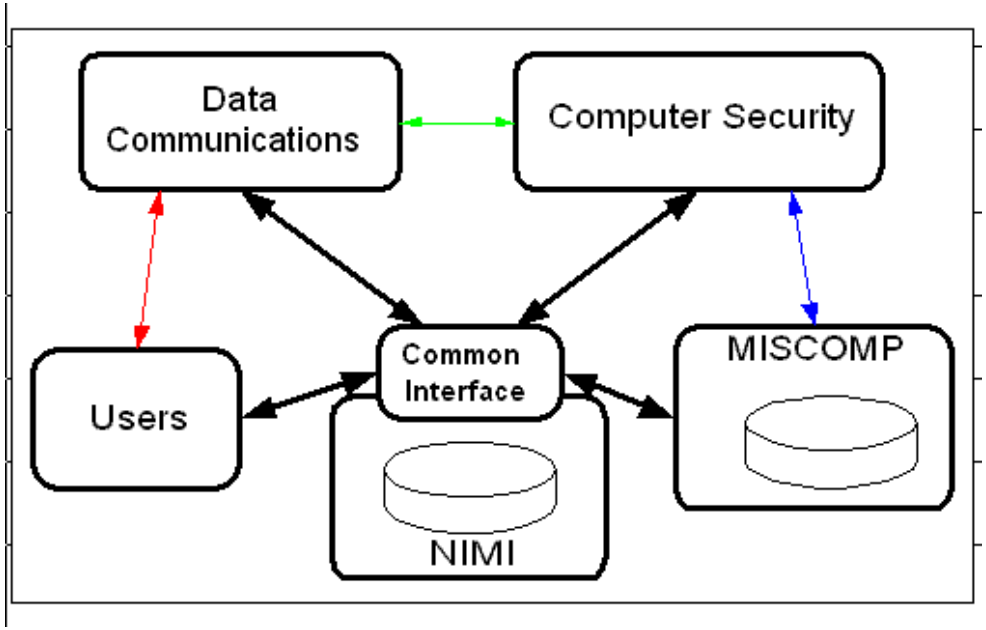


- Many-to-many communication topology
- Variety of interfaces, data storage formats and locations
- E-mail is not only primary media for communication but also is used for workflow management and data storage

ssentially, there is no operational infrastructure in place

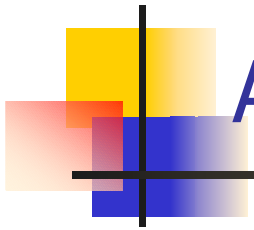
ecent Welchia worm outbreak demonstrated that without such infrastructure in place it is extremely difficult to maintain network security and avoid confusion and errors

Communication Through NIMI



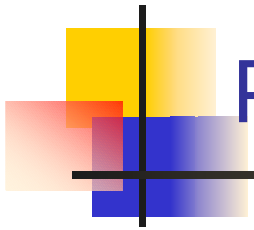
- Place NIMI in the middle of the picture
- Use it as:
  - Operational workflow information storage
  - Common data storage
  - Inter-group communication media

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



Advantages of using NIMI

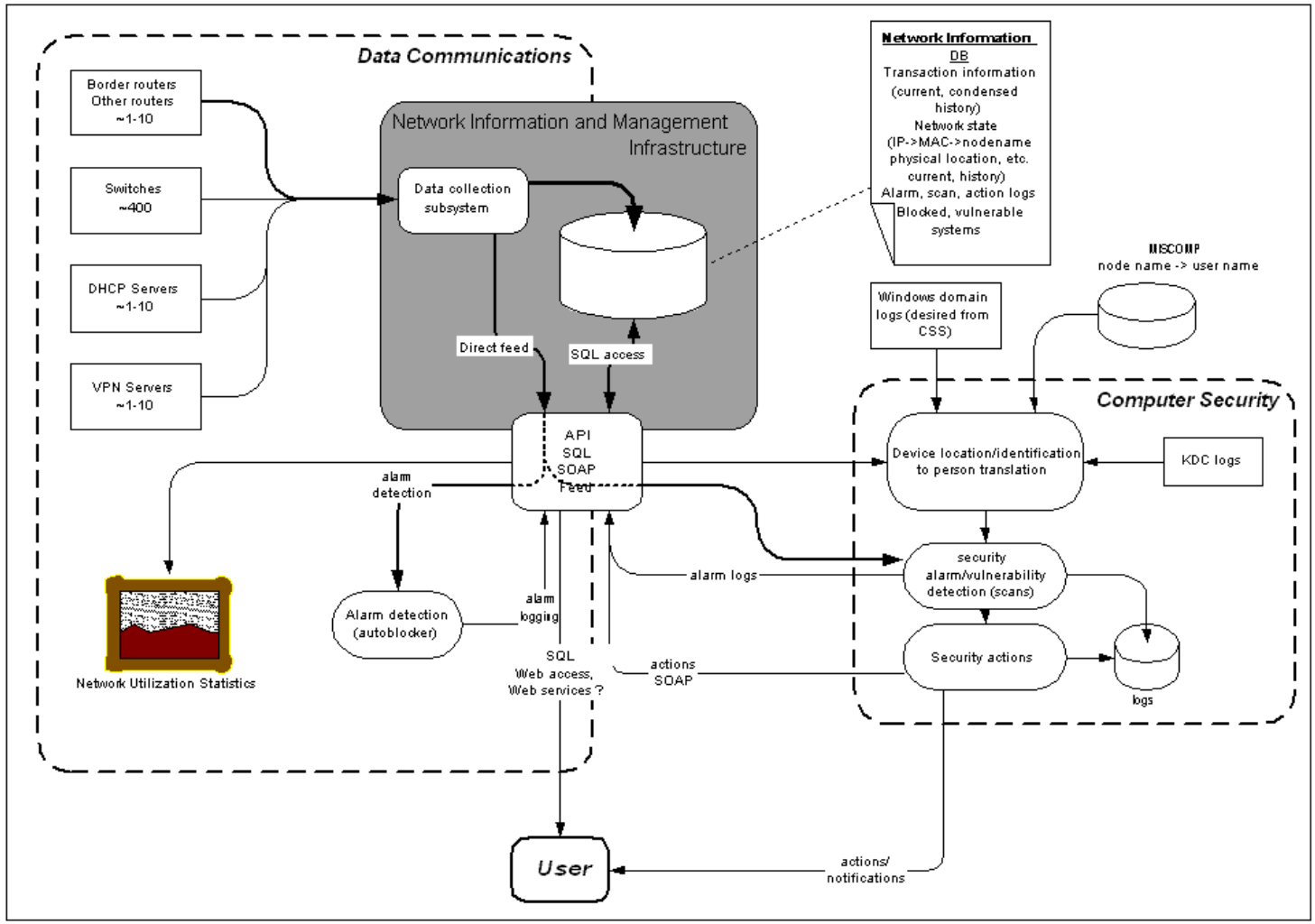
- Common well-known documented interfaces
  - WWW, SOAP, SQL, HTML
  - Grid? OGSI?
- Common authentication/authorization solutions
  - Kerberos, PKI/GSI
- Common centralized data storage
  - Easy data access for all parties
  - Single point of contact for all parties
  - Workflow management
  - Easier 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

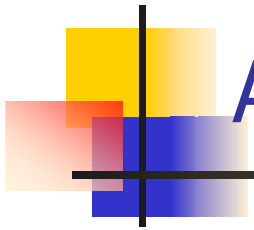


Project Status

- Since October 2003, done:
  - Problem analysis – not completely
  - Requirements gathering
  - Design proposal and discussion
- Currently we are in the middle of tool selection, trial integration and prototyping work
- We have put together test/development server “fcstst2”
- Current choices:
  - Linux
  - PostgresSQL database (alternative: mySQL)
  - Python (alternatives: Perl, Java)
  - Zope, Plone (exploring alternatives)
  - SOAP

Proposed NIMI Design





Areas of Future Work, Research

- Problem analysis
  - Data model
- Database performance
  - Can we store netflow information ?
- Workflow management
- Interfaces
  - DB API, client package
  - Authentication, authorization
  - Web interfaces (HTTP, HTTPS, SOAP, WSDL)
- Data Collection Subsystem
  - Performance
  - Robustness
  - Efficiency

Possible Impact

- Better organization of network monitoring, management
  - More efficient operations
  - Faster, more efficient response to security-related incidents
  - Availability of data
  - More user-friendly procedures
- Possible interface to other network management projects such as Lambda Station