High Performance Computing Security

Jesse Pollard,
Senior UNIX Analyst
NAVOCEANO MSRC
pollard@navo.hpc.mil
A THANKS TO MY SPONSORS

Naval Oceanographic Office

and

LOGICON
A NORTHROP GRUMMAN COMPANY
High Performance Computing Security

• Needs low overhead
• Protect facility and data
• Easy to use
• Usable audit trails
• Everywhere ...
Security Context

- Host/port addressing
- User identity
- Classification of the user and data
- Privileges of the user
“Network Security” Limitations

- Firewalls can only make decisions based on host/port/protocol
- Have no user or data security context
- Reduces throughput significantly
- Routers have limited audit capability
Host support for IPSec

- User identification/authentication
- User and data security classifications
- Defines port access rules
- Encryption
Host Support for MLS

- User identification and Authentication
- User and data classifications
- Protect internal system configuration
- Provide capability controls
Internal Host Needs

- Capabilities to control network access
  - approved applications
  - approved users

- MLS security classifications
  - protect system data structures
  - protect system applications
  - facility control of users and user data
Host Network (IPSec)

- Pass user identity and authentication
- User and data classification
- Authenticate host to host communications
- Apply packet level encryption based on
  - user and data classifications
  - remote host identity
- Translate remote user and classifications to the local user and classifications
Benefits to the User

• Simplified Applications
  – can use socket level programming safely
  – user, data, and security classifications handled by IPSec and host

• Reduced overhead where possible
  – optional packet level encryption
Benefits to the Facility

• Enforceable security controls
  – defined by the list of trusted hosts and users
  – defined by the location of the hosts
  – cannot be bypassed

• Reliable audit trails
  – controlled by the system
  – cannot be bypassed
Questions?