B3 – Security – FNAL – Kaletka

- FNAL has an incident response team with well practiced response process.
- There are restricted services that only authorized personnel may possess and/or operate.
- Backup is a major player since the most damaging incidents are those that destroy or make data unavailable.
- There is very little concern about data privacy.
- Good acceptance of cryptocards for offsite access (as well as onsite).
- SSHD modified to accept challenge/response.
- Strong Authentication. Single signon Kerberos realm at Fermilab by the end of 2001. Addresses ~1/2 of the analyzed root causes of incidents.
- **Discussion**
  - Kerberos – details of tickets acquisition & forwarding from cron jobs, applications etc. FNAL and Wisc have changed ssh code to add needed features.
  - Java SSH client interest – no production use to date?

A3- Security – U of Minnesota – Karo

- For ~100 machines, most support non-dedicated/multi-user functions.
- Disable as many unnecessary services as possible for security. E.g. Only one machine that accepts telnet/ftp.
- University mandates that they do not use firewalls (publicly funded university, desire to keep broad public access.)
- Looking at SunRays as a method of privacy, simplicity of administration, and the fact that the UDP traffic for these machines don't handle the congestion well.
- Smartcard credit card as physical authorization.
- Do you have to/want to select/customize window managers ?
  - GUI/custom interfaces to e.g batch services ?
  - Mention of GCG - a wrapper around LSF.
  - Expert users looking for the common GUI to aid the training of new users (JLab). (UMinn).
  - Benefit seen in isolation from underlying commands and hooks for local commands. Wisc: for access from palm.

Security – General Discussion/Questions:

- Kerberos
  - About 30% of the attendees are using Kerberos.
  - Overhead of creation of a centralized registry of accounts. NERSC has the problem of being a global resource provider in principal. No one stepped up to the task.
  - Wisconsin: "Kerberos a significant step in complexity" & "Kerberos turns out to be not useful on the cluster and impossible between the clusters."
- About 30% people regularly run crack on their clusters
- Is anyone worrying about application authentication ?
  - Seemed like no.
  - Containing sensitive data to private networks was a theme.
- Global / Site Authentication
  - Wisconsin working on automated exchange between Kerberos tickets and PKI certificates.
  - Globus will require a mapping interface at each site to present a list of
    personnel.
  - Proposal is to keep this a local function.

Questions – and answers..

- Distinction between security policy and usage policy? Not clear
- Most farms/large clusters are behind a firewall.
- Centralized methods of dealing with patch selection and installation? *At least to the level of someone charged with watching the lists and spreading the word.*
- Support Personnel? *NERSC: 3-4FTEs? Sanger has 1 Security. SLAC has 3. JLab has 1 ?, FNAL has 2,*
- Training?
  - *SLAC requires mandatory training for all users.*
  - *ICL has a floor warden for scans and audits.*
  - *Sanger has a public training series*
  - *Wisc largely accepts centralized admin.*
- *User admin of desktops? General theme implied it is a slippery slope to chaos. 100% of the people here admin'd their own machines.*
- Are there scaling problems anticipated with the 1000node scale clusters:
  - *Uniformity of a cluster & limited direct login really helps*
  - *Big issue getting scheduled /down time for maintenance/reconfiguration for (urgent) security patches*
  - *Scalability of the admin tools will help*