Keeping Up with the Joneses

Controls System Cyber Security Application & Concerns at RHIC

James Jamilkowski, Severino Binello, William Eisele, John Morris, Seth Nemesure

BROOKHAVEN NATIONAL LABORATORY

U.S. DEPARTMENT OF ENERGY

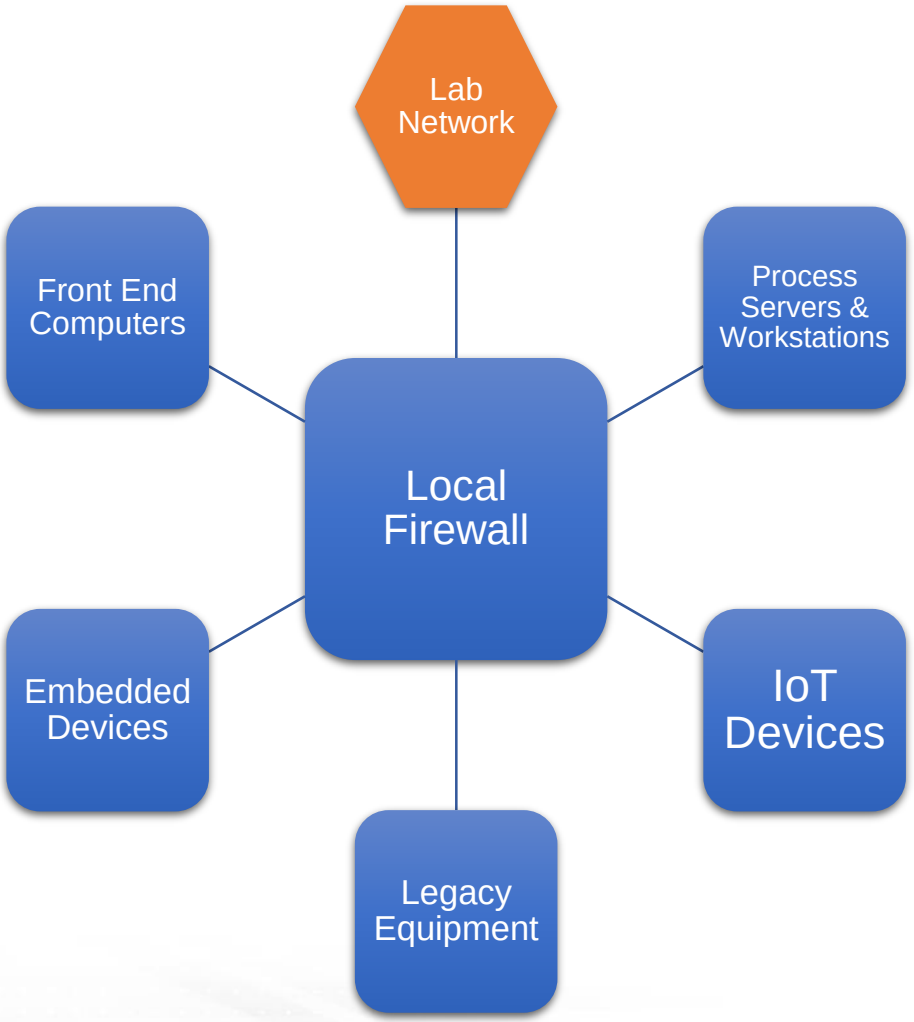
BROOKHAVEN SCIENCE ASSOCIATES

Overview

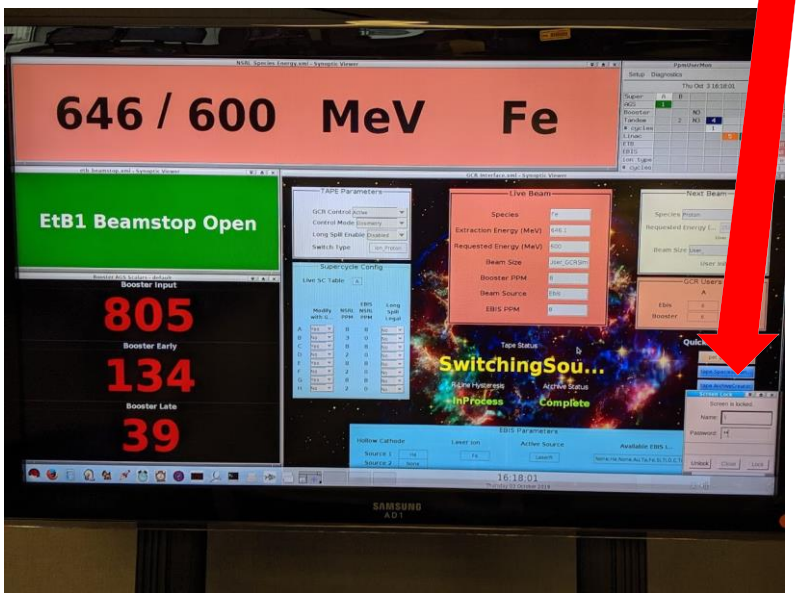
- Network Topology at RHIC
- Workstation Level Authentication
- Remote Logins
- Device Level Access
- Code Repositories & Procedures
- Improving Access to Information
- Sensitive Networks
- Networked Devices: Embedded, IoT, & Legacy
- Cyber Security Concerns
- Ideas for Improvement
- Conclusions

Network Topology

- Default user category resides outside of the local firewall
- Only users with roles requiring frequent interaction with machine operations reside inside the local firewall
- Workstations in control rooms providing full access use Screen Lock utility for authentication (sometimes with RFID-based room access for off-hours)
- Network devices are typically segregated on subnets, grouped by operational impact on one or more accelerators/systems as well as by behavioral concerns



Workstation Level Access

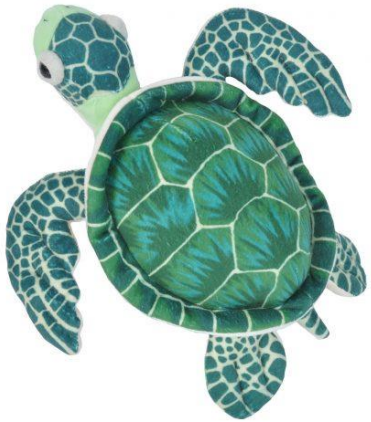


- Personal accounts vs. Shared Accounts
- Screen Lock utility
- Lab-level centralized authentication for both Lab-wide and local web services
  - We're working on replacing legacy services where authentication was done using ad-hoc schemes with independent password management and requirements

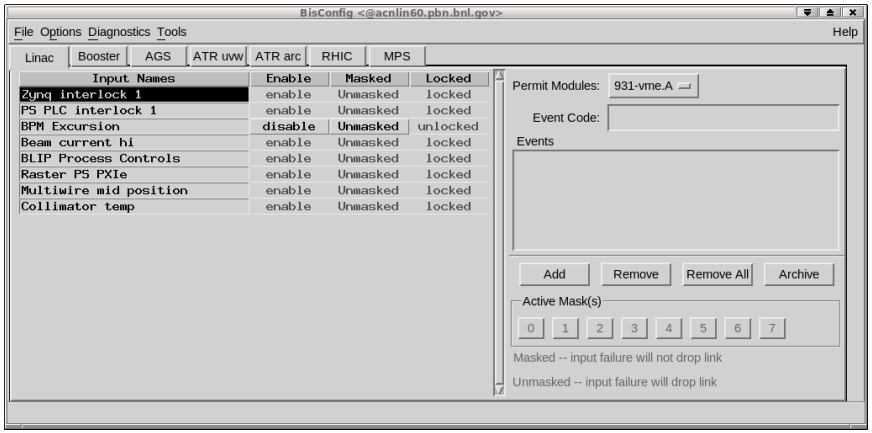
Remote Logins

- We've converted from using RSA tokens to a competing Two-Factor Authentication service
  - No significant issues were encountered during or after the transition process

Device Level Access (1/2)



- General Philosophy
  - Hard shell defense strategy
  - Opt-in for extra protection on a system and parameter level, using existing ad-hoc software solutions…
- Special Cases
  - Restricting access to Machine Protection parameters
    - By Linux group…



Device Level Access (2/2)

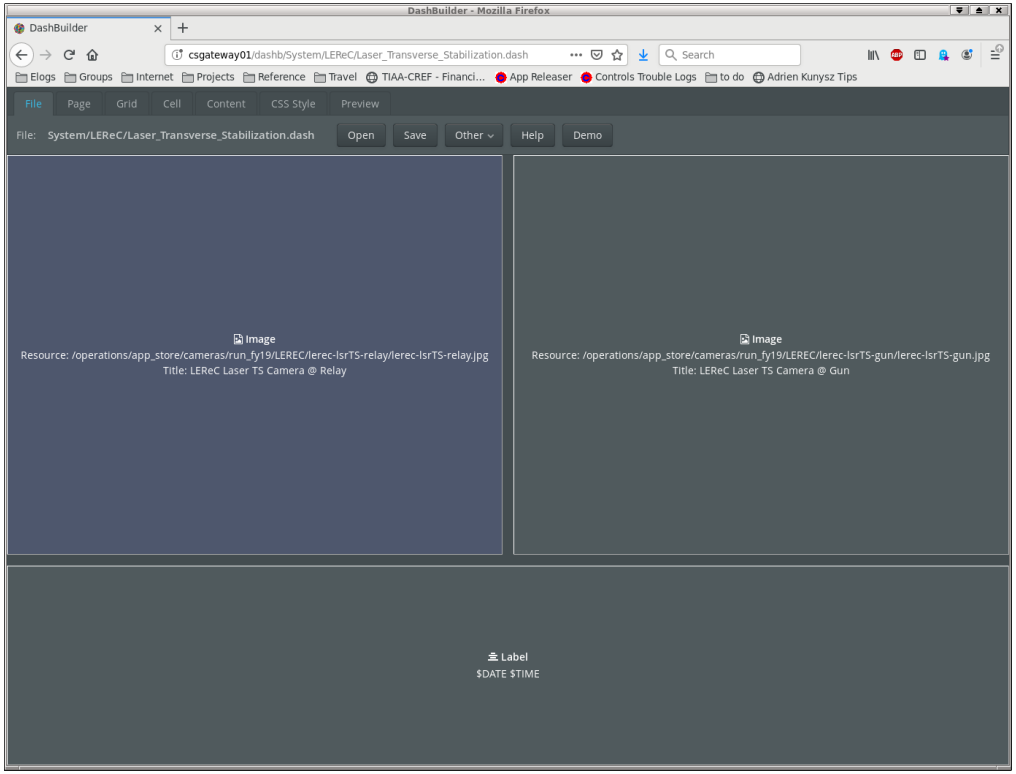
- Andrei Suhkanov described an authentication scheme at the ‘17 Workshop (*Device Access Security at RHIC*) that was built into Python-based control software
  - Implemented successfully alongside a Machine Protection system interface since the presentation
  - The design and codebase limit the short-term potential impact, but this concept has served as a reference for future development

Code Repositories & Procedures

- We primarily use ClearCase and Git
- Our repos are all hosted locally, inside firewalls
- We don’t often make use of public repos for acquiring software, though code in the Open Source domain seems less of a concern
- We maintain published code release procedures and monitor activity
  - All release activity is logged, including in dedicated Elog
  - Follow a common release model: commissioning, developer, & operations

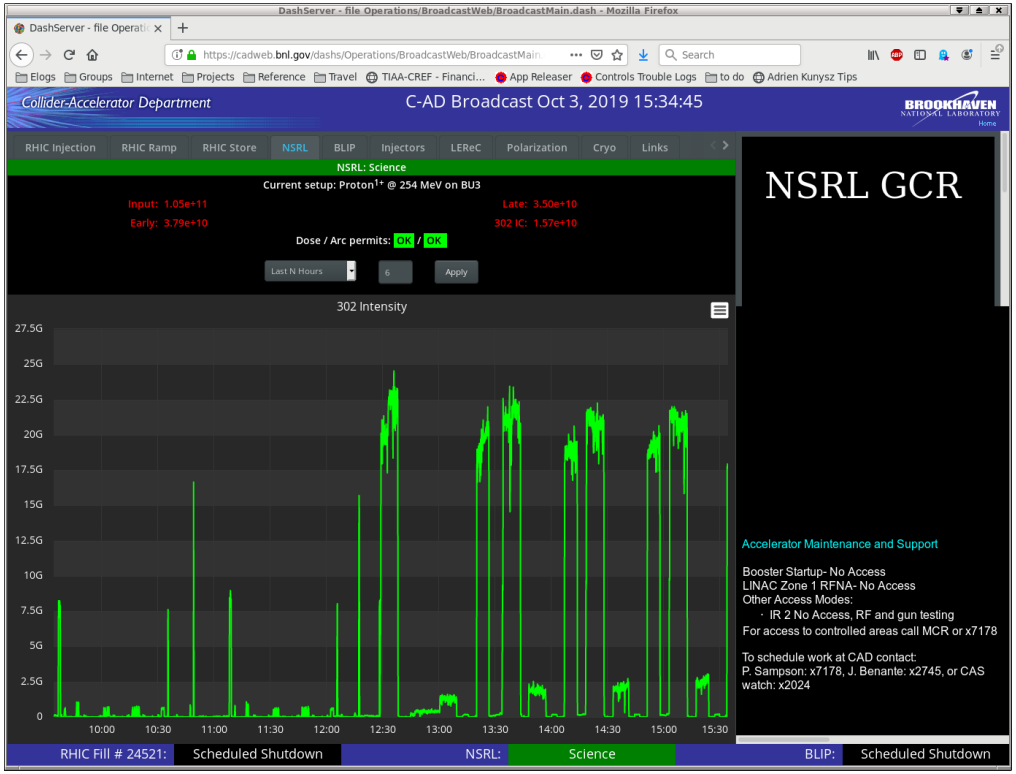
Improving Access to Information (1/2)

- Dash Server
  - General use web content delivery system for any parameter-based information
  - Based on Vaadin Platform, Java-based HTML5 service
  - Used both in an internal configuration without restrictions and a separate public-facing configuration (vetted for injection-type exploits)



Improving Access to Information (2/2)

- Here's an example top-level Dash page maintained by Operations
- Remote access to Electronic Logbooks via IOS & Android apps



Sensitive Networks (1/2)

- Personnel Security systems
  - Reside on an isolated (air-gapped) network
  - Rely on administrative and technical enforcement of physical access restriction policies involving ethernet, USB, etc.
  - How thorough can we be in the area of enforcement?
    - Application of monitoring using whitelisted devices

Sensitive Networks (2/2)

- Sometimes, additional physical security is necessary…
- Not a scalable approach for every switch and USB port

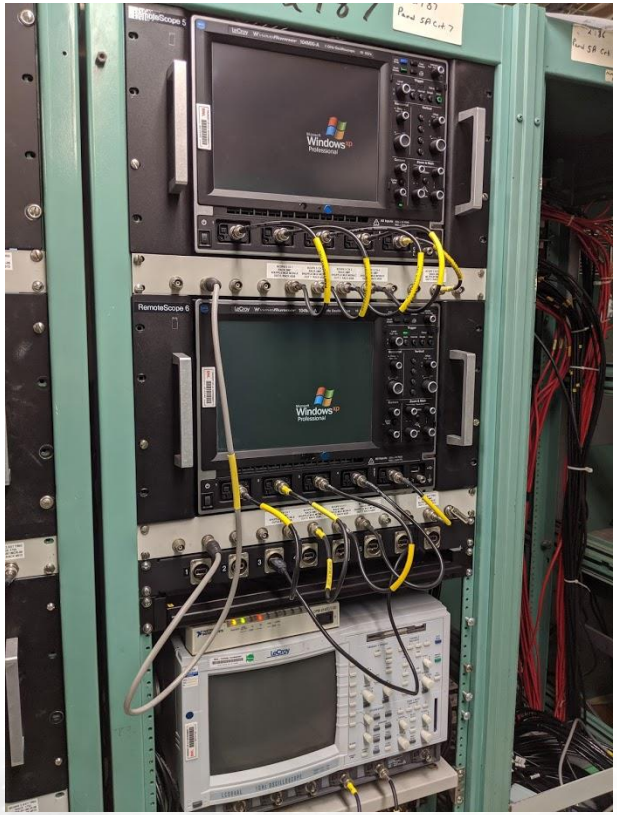
Embedded Devices

- The volume of this type of device is increasing rapidly
- The proportion of devices running Linux is increasing
- Firmware is often ancient, and patches may not be available or practical to apply
- All devices go through a vetting process in a controlled environment to mitigate the risk
  - Sniff for undesirable traffic
  - Scan for unacceptable vulnerabilities
  - Explicit operating procedure reinforces the vetting requirement, backed up by network monitoring
- Beware of “knock-off” COTS devices!
  - We have detected a set of mislabeled IP cameras in a particular batch that were attempting to contact a cloud-hosted systems as well as a network associated with a foreign military

IoT Devices

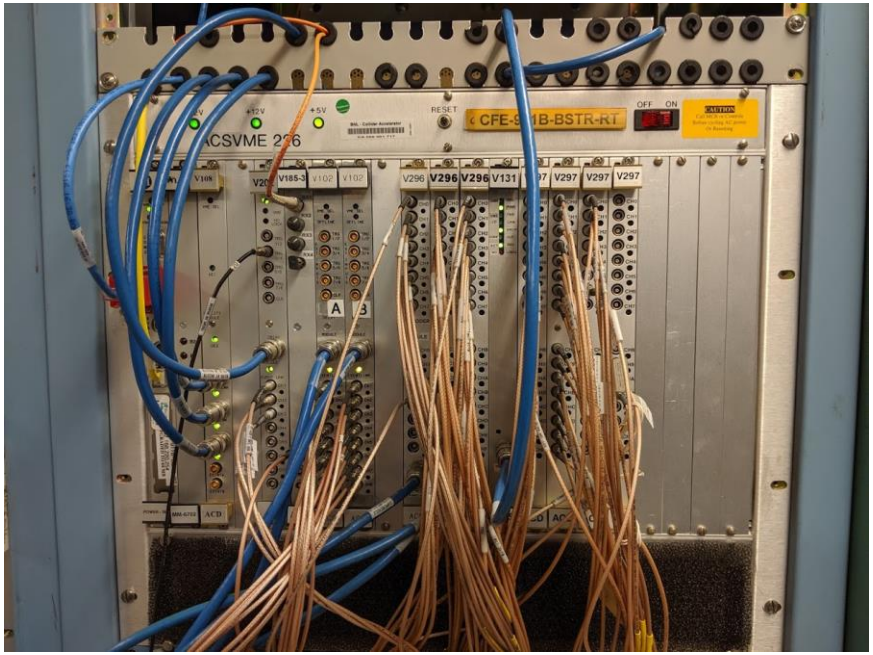
- We host a small, yet increasing number of IoT devices for field monitoring
- In the race to minimize cost, they often have substandard interfaces
  - Beware of cleartext logins!
- Password management of field equipment is a concern that would benefit from attention
  - Does anyone use a centralized management scheme?

Legacy Devices (1/2)



- The balance between supporting equipment with known vulnerabilities that can't be patched and retirement or replacement (hopefully, for the devices!) is often difficult to manage
- Administering this type of equipment can be burdensome, which isn't always properly accounted for in the planning process
- Segregated networks using private subnets to isolate from Internet access are a requirement
- The speed at which devices become "legacy" due to cyber security and other behavioral concerns seems to be increasing

Legacy Devices (2/2)



- We support 300+ Front End Computers running versions of the VxWorks RTOS
- Many crates are critical to operations
- Some platforms have firmware bugs, leaving them vulnerable to even non-malicious traffic
- Key (known) bugs remained unpatched for many years, at least until after ending a support contract
- The long term strategy is replacement with newer systems, but the volume and complexity probably limits this to the 10-20 year timescale

General Concerns

- Under-funded Cyber Security Mandates
  - Is this more common than it should be?
- VPNs for Remote Access
  - They’re easy to use, but then the protected network is exposed to anything on the remote system
- 2FA isn’t a panacea

Ideas for Improvements

- Establish “De-Militarized Zone” networks
  - Utilize Access Control Lists (ACLs) to restrict traffic past the DMZ
  - This strategy makes sense for new machines/projects, but is much more challenging to apply to well established ones
- Update our control software infrastructure to embed access restriction functionality at the lower level libraries, rather than ad-hoc or within only a portion of our codebase
  - RPC layer option
  - We’re still weighing both the different use-cases as well as the level of interest

Conclusions

- There’s a continuous tension between cyber security concerns, supporting networked equipment for extended periods that may fall afoul of security requirements, as well as increasing threats from malicious and poorly designed equipment
- Balancing stakeholder needs versus minimizing the risks to operations and data management is the challenge
  - This tension appears to be manageable for public facing information portals, such as with DashServer and our Elog system
- In some areas, we’re developing an interest in exploring use of better management tools (ex. IoT or legacy devices)