Contribution ID: **271** Type: **Poster presentation**

NSTXU RedHawk Linux Realtime Security Measures and Their Effect on Determinism

Tuesday, June 7, 2016 3:00 PM (1h 30m)

The National Spherical Torus Experiment Upgrade (NSTXU) at the Princeton Plasma Physics Laboratory (PPPL) successfully began its first year of operations. NSTXU is a magnetic fusion device whose major mission is to develop the physics basis for an STbased Fusion Nuclear Science Facility (FNSF). The STbased FNSF has the promise of achieving the high neutron fluence needed for reactor component testing with relatively modest tritium consumption. At the same time, the unique operating regimes of NSTXU can contribute to several important issues in the physics of burning plasmas to optimize the performance of ITER.
NSTXU uses multiple realtime RedHawk Linux systems based on RedHat Enterprise Linux 6 (RHEL) for both coil protection and plasma control. NSTXU further uses standard RHEL6 systems for support services such as housing configuration data and nonrealtime user interface applications. All of these systems perform critical roles in the success of the NSTXU project, and it is becoming increasingly apparent that there is a growing risk with respect to protecting these assets from a security standpoint.
Typically, realtime assets stay hidden behind external protective measures such as virtual LANs (VLANs) and internal firewalls. With the evolving requirements that organizations place on all computing assets, these previously sufficient external approaches are no longer enough to meet all of their goals. Unfortunately, local security policies tend to have an adverse effect on the deterministic nature of a realtime Linux system, and most policies involve coarse and inflexible settings.
As part of an ongoing initiative to protect computing assets from both malicious and accidental threats, NSTXU developed multiple approaches to blend tight controls with careful study of realtime effects. Included here will be coverage of how NSTXU managed to balance the primary purpose of the Linux systems with additional security constraints, including using Security Enhanced Linux (SELinux), specific firewall settings, Linux “capabilities” (that is, specific superuser privileges that do not require superuser access), and numerous other security measures. In all cases where a security change negatively affected realtime performance, that change was either mitigated or reverted. What remains is a grouping of safe alternatives that show that both security and realtime determinism are both practical and useful.

Primary author: ERICKSON, Keith (Princeton University)

Presenter: ERICKSON, Keith (Princeton University)

Session Classification: Poster session 1

Track Classification: Real Time Safety and Security