SECURING MOBILE CONTROL SYSTEM DEVICES: DEVELOPMENT AND TESTING

Stefani Banerian*, Clinical Neutron Therapy System, University of Washington School of Medicine, Seattle, WA, 98105, USA

Abstract

Recent advances in portable devices allow end users convenient ways to access data over the network. Networked control systems have traditionally been kept on local or internal networks to prevent external threats and isolate traffic. The UMWC Clinical Neutron Therapy System has its control system on such an isolated network. Engineers have been updating the control system with EPICS, and have developed EDM-based interfaces for control and monitoring. This project describes a tablet-based monitoring device being developed to allow the engineers to monitor the system, while, e.g. moving from rack to rack, or room to room. EDM is being made available via the tablet. Methods to maintain security of the control system and tablet, while providing ease of access and meaningful data for management are being created. In parallel with the tablet development, security and penetration tests are also being produced.

INTRODUCTION

The Radiation Oncology Department at the University of Washington Medical Center is unique in that it has a Clinical Neutron Therapy System (CNTS) for treatment of selected types of cancer. The CNTS has been in operation since 1984. The system includes on Isocentric treatment room, with a gantry and leaf collimator for the cancer treatment, and a fixed beam room for experimentation. Additionally there are beam lines for isotope production and specialty operation, testing, and development. Initially, the system had a vendor-made control system, running on a PDP-11 computer. In 1999, the therapy portion of the control was replaced with VxWorks running on a Motorola 68040 board in a VME crate [1].

The engineers and staff of the CNTS are now in the process of converting both the cyclotron and therapy portions of the control system to the EPICS[2] control program. Over the past seven years, much of the cyclotron system has been converted, the main significant remaining piece of the control system being the RF control. The therapy control system is in the process of being converted to a combination of EPICS, special python programs, with use of PostgreSQL for maintaining tratment data.

Concomitant with the change of the control systems, new operator interfaces are also being created. EDM displays now serve as many of the operational displays of the cyclotron control. The therapy system is also being converted, in several stages, to an EDM-based display.

For ease of use by Radiation Treatment Therapists (RTTs), we have opted to try a modern touch-screen LCD for some displays. Initially the layout of the treatment display will mimic the current interface, the exception being that the source is EDM running on a Linux PC, with the touch-screen monitor replacing the need for keyboard and mouse input.

Display and tablet PC advances have allowed the opportunity to consider mobile device support at the CNTS. This paper describes some issues, considerations, and limitations that need to be addressed for such devices.

CONSIDERATIONS

For this development process, designing of the mobile devices proceeds with the same process used in many other scenarios. Indentification of the the users comes first; the userbase is rather narrow, as the CNTS and Department itself is limited. Typically, only engineeers or operators, physicists, and therapists are even allowed to access the controls, and even so, only in well-defined and circumscribed instances. Thus, for example, therapists constitute one user group, and can access only selected devices, with a small set of interface displays at the therapy system. Physicists are another small group, and only access the Isocentric Gantry room and Fixed-beam room controls through a separate set of displays. Engineers have a third set of displays, and operators use a subset of those used by engineers.

System access is then to be constrained by considering authentication and authorizations. Frequently medical devices have been configured with a common (single) systemID. Our authentication tries to employ the one-id-per-person standard, with a strong methodology for mapping a user to some standard secure account ceredentials. We have determining the four types of users, thus four groups for authorization to access a device or display.

For mobile devices, one also would like to find ways to identify, authenticate, and authorize the device itself.

The clinical situation in a hospital offers another set of matters. Safety of the accelerator and its controls, minimization of exposure to staff, correct and verifiable treatment of patients, institutional and management concerns, administrative requirements, oversight by external entities, legal requirements, et al., need to be determined.

*banerian@uw.edu

ISBN 978-3-95450-139-7

The physical environment of the department, designed for radiation treatment of cancer, offers more concerns. Our department employs electrons, X-rays, gamma rays, and protons and neutrons. Thus thick shielding is ubiquitous, and RF wifi transimission may be limited or interfered with.

The UW hospital has its own set of standards for protection of patient data, including both in transit and at rest. Although the network is considered "safe" for unencrypted transport of data locally, we opt for a more rigourous design. Common cryptographic standards, for protection of data across the network, should be maintained for wireless or wired traffic. We need stong crypto, but we likely do not need to defeat the NSA. Thus we do want to take good measures, but we can select what is best for the situation.

CHOICES

Authentication of Personnel

Over time a very well defined Identity and Access Management (IAM) system has been developed by the University of Washington. This IAM provides for controls of all employees of the UW, and they have conveniently chosen to use kerberos[3] for authentication credentials. The CNTS and the Radiaion Oncology Department itself have made use of this UW system to provide an easily managed authentication process for devices which can be so configured. Kerberos provides a cryptographically secure method, and with system logging, we can determine which person has logged in to use a device, at a well-defined time; kerberos requires faily accurate timestamps to provide credentials once a user has been authenticated.

Authorization of Personnel

The system employed uses either of two standard methods to identify groups of users, Unix groups and LDAP. For some stand-alone devices which may not always have adequate network access, Unix groups define what an individual might be allowed to do. For wired workstations, more typically OpenLDAP is used for the group definition. As such, wireless devices are limited to per-device group definitions.

Authentication of Devices

The wireless network access in the department has overlapping "jurisdictions". There is hospital (via UW) access for "Patients and Visitors"; there is separate access for UW staff, employees, and students; there is the Clinical Engineering group, which manages certain types of clinical devices; there are ad-hoc networks, perhaps set up in areas of poor coverage, by individuals, for their own convenience. We have defined a separate engineering network for the CNTS. The wireless access point (AP) is configured to allow access only to devices with specified MAC addresses. Only those devices may connect, and then they have to be capable of using the proper cryptographic protocol, in our case WPA2-AES-DH-PSK (WPA version 2, advanced encryption standard, Diffie-Helmen exchange with preshared key).

Once authenticated to the AP, the device still needs to be assigned a proper IPv4 network address. That is determind be a separate process, and predefined addresses are assigned to specific devices.

Badillo et al.[4] use a Limited Field Communication (LFC) to minimize exposure of their wifi network. In the system described here, output power modification of the antenna was also adjusted. Another method used to limit access to the wireless network via the AP is by use of a directional antenna. The AP selected for use has an optimal 60 degree sector; however, at full power, the signal remains quite good at 120 degrees. It was also found that there was little difficulty obtraining good network speed even inside a concrete-and dirt surrounded treatment vault. The particular device selected by us, Ubiquity NanoStation, used for many large scale commercial projects, sometimes overwhelmed the signals of the other wireless networks. Even with power adjustment, the signal was always excellent.

Patient Data Protection

Due to the need to protect patient data, which would be accessed by therapists, the decision was made to consider greater cryptographic authentication between device and therapy controls. As such, under development is a process to have the device authenticate to a therapy control device with a cryptographic certificate, and then either employ IPSEC or other encrypted tunnelling of traffic. Addtitionally, this can also be used to restrict network access to the mobile devices.

Other authentication protocols considered were one-time passwords (OTP) and secure remote passwords (SRP), the former requiring little or no encryption during the authentication phase, the latter eliminating transmission of a password over the network.

SYSTEM DEVELOPMENT ISSUES

All hardware and firmware are to be kept under consideration. The AP selected employs firmware based on Free Open Source Software (FOSS), Linux operating system, with typical FOSS applications running underneath. Local modification of the firmware is possible; however one is still faced with firmware upgrades from the vendor. Software and configuration changes need to be kept in source control.

The mobile devices selected are also FOSS-based, as much as possible. Thus, the standared test device was a Asus Nexus 7 running Android 4.2 The device was unlocked, rooted, and a number of applications installed to better control the internals of the device, such as USB devices, network drivers, and storage.

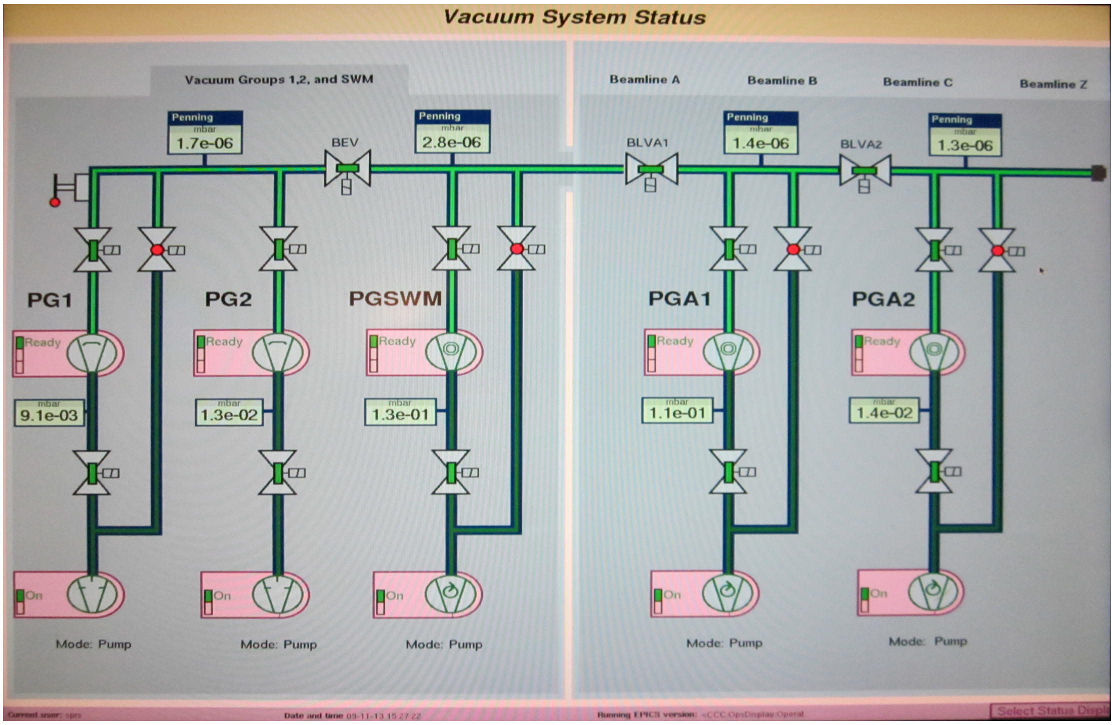

Figure 1: Example of an engineer's status display screen. This particular screen shows the vacuum system status, pressures, meters, valves. Other screens are available via a popup menu indicated at lower right.

Cyanogenmod[5] was also tested on devices. Experiments are ongoing, but this seems a better platform for further modification of operating system and software to be used.

Ultimately, the plan is to install Linux on the touch devices, so that programs may run natively, without engineering workarounds. The first installation attempted was an Ubuntu Touch[6,7] version, from April 2013. The device at that time did not perform in a manner sufficiently stable to be useful except for extreme engineering tests.

Whatever operating system was chosen, the issue of upgrades has to be addressed. During this development phase, Android itself has gone through at least three public updates, Cyanogenmod has moved from 10.1 to 10.4, and the Linux kernel stays in constant development, now in a stable branch well past what is maintained in common Linux distributions.

Ultimately, the device selected for operational use was a Samsung Nexus 10 (10" diagonal surface) tablet. Initially, Ubuntu Touch was installed, but was not found to be stable enough to be usable in any meaningful way. Android was reinstalled, and from there, we proceeded with installation of a Linux chroot environment, X-server app on the Android, and compilation of EPICS 3.14.12.2 with EDM 1.20.80. With proper selection of start-up scripts, EDM displays were found usable on the touch surface of the tablet (Figure 1).

STATUS

Mobile device support is a fairly new program at the CNTS, and dependent has only recently started. The therapy system can only be tested in small intervals when treatment is not happening nor imminent, so there is a significant restriction on access for testing. Most therapy system changes under development have not yet been released for regular use. Significant changes in underlying code, on Android, as well as X-server applications, have temporarily rendered some access less useful.

CONCLUSIONS

Wireless mobile network devices provide convenient access to the control system of the CNTS at the UWMC. Engineers, Physicits, and Therapists all benefit from the easy ("intuitive") touch interface, and the mobility allowed. Strict access controls still need to be implemented, both to protect the safety and privacy of the patient, as well as to maintain proper record keeping for administrative and medical purposes. Vendor-supplied solutions are tyically inadequate to address clinical and documentation needs. When Linux is installed on the tablet, wither natively, or within a chroot, development and use of toolkits, is faster, more consistent, safer, and remains in line with the development of the rest of the CNTS control and therapy systems.

ISBN 978-3-95450-139-7

ACKNOWLEDGEMENTS

Thanks are due to Robert Emery, Eric Dorman, Jon Jacky, Tobin Weber, and Steven Steininger, all from the CNTS at the UW School of Medicine, for assistence and suggestions made during testing and development.

REFERENCES

[1] R. Risler, S. Banerian, J.G. Douglas, R.C. Emery, I. Kalet, G.E. Laramore, and D. Reid, 25 Years of Continuous Operation of the Seattle Clinical Cyclotron Facility. In Yujin Yuan, Lina Sheng, and Lijun Mao, editors, "Proceedings of the Nineteenth International Conference on Cyclotrons and Their Applications", p. 68-70 (2010).

[2] Experimental Physics and Industrial Control Systems: http://www.aps.anl.gov/epics/

[3] RFC 4556, Public Key Cryptography for Initial Authentication in Kerberos (PKInit), http://tools.ietf.org/html/rfc4556

[4] I. Badillo et al., "Android Based Mobile Monitoring System for EPICS Networks: Vacuum System Application, Proceedings of IPAC2011, pp 2337-2339 (2011)

[5] Cyanogenmod http://www.cyanogenmod.org

[6] Ubuntu http://www.ubuntu.com

[7] Ubuntu Touch http://wiki.ubuntu.com/Touch/Install