UPDATE ON THE CERN COMPUTING AND NETWORK INFRASTRUCTURE FOR CONTROLS (CNIC)

S. Lüders on behalf of the CNIC WG

CERN IT/CO, Geneva, Switzerland

ABSTRACT Over the last five years modern accelerator and experiment control systems have increasingly been based on commercial-off-the-shelf products (VME crates, PLCs, SCADA systems, etc.), on Windows or Linux PCs and on communication infrastructure using Ethernet and TCP/IP. Despite the benefits coming with this evolution, new vulnerabilities are inherited too. Worms that spread via both TCP/IP and Ethernet, and attackers are becoming interested in control systems. Unfortunately, control PCs cannot be patched as fast as office PCs. Even worse, vulnerability scans at CERN using standard IT tools have shown that commercial automation systems lack fundamental security precautions: Some systems crashed during the scan, others could easily be stopped or their process data be altered [1]. During the two years following the presentation of the CERN Security Policy at ICALEPCS[2003][2] a “Defense-in-Depth” approach has been applied to protect CERN’s control systems. This presentation will give a review of its thorough implementation and its deployment. Particularly, measures to secure the controls network and tools for user-driven management of Windows and Linux control PCs will be discussed.

CERN’s Mitigation: “Defense-in-Depth”

“Defense-in-Depth” means security on every layer:
- ...of the security of the device itself, ...of the firmware and operating system, ...of the network connections & protocols, ...of the software applications (for PLC programming, SCADA, etc.), ...of third party software, and ...together with users, developers & operators.

CERN’s solution is based on the “Good Practice Guidelines Part 1-7” of the U.K. Centre for the Protection of the National Infrastructure (CPNI) [3].

From experience at CERN, only centrally managed and patched PCs have shown to be secure in the long run.
- Use centrally managed systems whenever possible
- Ensure prompt security updates: OS, applications, anti-virus, etc.

Development of a User-driven PC management system:
- Security responsibility and security measures to the User
- HE decides IMWEN to install WHAT on WHICH control PCs (revised list of the IT people)
- IT will send out email notifications of new patches to be installed
- HE has to ensure security
- PCs might be blocked if threat for others

With Windows Terminal Servers & SSH gateways
- Remote interactive access
- From “outside”, i.e. office, wireless, home
- Windows Terminal Servers & SSH gateways
- Methods to access control applications & control PCs (i.e. SSH, RDP, native PVS)