Information Security Assessment of CERN Access and Safety Systems

Access and safety systems are traditionally considered critical in organizations and they are therefore usually well isolated from the rest of the network. However, recent years have seen a number of cases, where such systems have been compromised even when in principle well protected. The tendency has also been to increase information exchange between these systems and the rest of the world to facilitate operation and maintenance, which further serves to make these systems more vulnerable. In order to gain insight on the overall level of information security of CERN access and safety systems, a security assessment was carried out. This process consisted not only of a logical evaluation of the architecture and implementation, but also of active probing for various types of vulnerabilities on test bench installations.

CERN personnel safety and access systems

LACS (LHC Access Control System) – who enters LHC and when
LASS (LHC Access Safety System) – it is safe for beam or access at LHC
PASS (PS Access Control System) – who enters the PS Complex and when
PASS (PS Access Safety System) – it is safe for beam or access at PS
SP5/P5 – integrated personnel safety system for SPS
SPS Primary Ion Interface – personnel safety during SPS mixed ion/proton runs
SSA (Surveillance des Sites) – who enters CERN sites and areas other than the accelerators.
CSAM (CERN Security Alarm Monitoring) – alarms for the fire brigade
SIP/SAM (Site Information Panels / Simple Access Messages) – display relevant info at access points
SSA (Safety System Atlas) – personnel access and safety system for the Atlas detector

Motivation: why a security assessment?

Control systems traditionally not very secure
- Used for isolated systems: process control, safety systems.
- Critical systems may need to be kept in isolation anyway.
- Security is complicated: it is easier to avoid the hassle if possible.
- Vendors have recommended or required private isolated networks.
- Need input from control systems for other systems (ERP, alarm systems, web...)
- Need remote access to control systems (supervision, operation, maintenance).
- Technology is there, ergo, it will happen.
- Need to know what we’re talking about.
- What is our level of security? How can it be better? At what cost?
- Should (2) and co. open a lot of eyes – soon to be.

Findings

- Several devices needing patches.
- Found a number of configuration issues.
- What is the criticality of the device? If it fails, will people get hurt? Will beam be lost?
- Categorize all the different network-connected devices of the target systems.
- Carry out the assessment on their respective test bench installations.
- Assess the level of information security of CERN access and safety systems.

Level of access is key:
- Keep external access well controlled.
- Segment internal access according to need.
- Above all, restrict physical access to sensitive facilities.

Other observations and findings

Tunneling out of a private network
- Private networks may not be as private as believed!
- The DNS protocol allows DNS queries and responses to carry arbitrary extra data [1].
  1. A special DNS client is installed on a machine in the private network.
  2. A special DNS server is set up in the Internet with its own top domain.
  3. Client makes a DNS query to a subdomain of the top domain with a data payload.
  5. Client makes another DNS query to a different subdomain.

Importance of physical access
- If an expert has access to restricted areas, he/she can do a lot…
- …and there are tools to help in that: enter a USB keyboard injection device

References