ICALEPCS 2015
International Conference on Accelerator & Large Experimental Physics Control Systems

Information Security Assessment of CERN Access and Safety Systems

Melbourne, Australia
17-23 October 2015

T. Hakulinen, X.B. Costa Lopez, P. Ninin, P. Oser –
CERN, Geneva, Switzerland

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 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) – is it safe for beam or access at LHC
PACS (PS Access Control System) – who enters the PS Complex and when
PASS (PS Access Safety System) – is it safe for beam or access at PS
SPS PSS – integrated personnel safety system for SPS
SPS Primary Ion Interlock – personnel safety during SPS mixed ion/proton runs
SUSI (Surveillance des Sites) – who enters CERN sites and areas other than the accelerators
CSAM (CERN Safety Alarm Monitoring) – alarms for the fire brigade
Sniffer – gas detection in CERN tunnels and caverns
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.

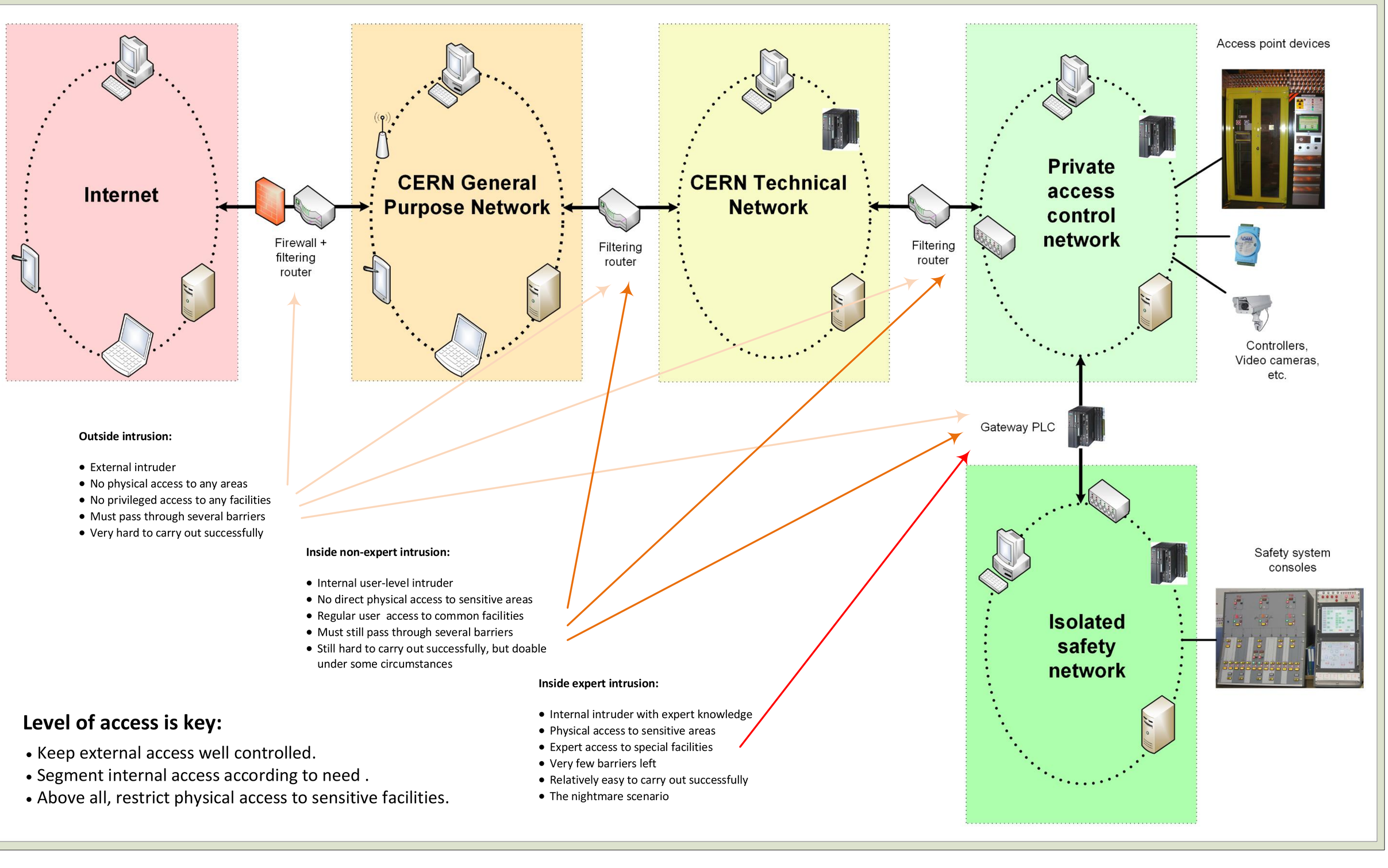
Situation changing: isolation may not be an option for much longer
- Need input from control systems for other systems (ERP, alarm systems, web…).
- Need remote access to control systems (supervision, operation, maintenance).
- Technology is there, ergo, it will happen.

Need to know what we're talking about
- What is our level of security? How can it be better? At what cost?
- Stuxnet [1] and co. opened a lot of eyes – ours too!

Characteristics of CERN personnel safety and access systems

Safety systems
- Mission critical – ensure safety of personnel, don't unnecessarily disturb operation.
- Built following the principles of safety engineering: redundant, diverse, failsafe.
- Technologies: PLC automation, wired logic.
- For the most part isolated from other networks.

Access control systems
- Authenticate identity, verify authorization, allow/deny passage, record.
- Very heterogeneous control systems: many integrated elements and technologies.
- Badge readers, biometry scanners, interphones, video, key distributors, info screens.
- Share network with other services, or if in private segment, have connectivity to selected CERN services.



Level of access is key:

- Keep external access well controlled.
- Segment internal access according to need .
- Above all, restrict physical access to sensitive facilities.

Information security assessment

Mission
- Assess the level of information security of CERN access and safety systems.
- Concentrate on two most visible systems, LHC and PS access systems.
- Carry out the assessment on their respective test bench installations.

Inventory
- Categorize all the different network-connected devices of the target systems.
- What is the role of the device? Which vendor? What software does it run?
- What is the criticality of the device? If it fails, will people get hurt? Will beam be lost?

Methodology
- Deterministic intrusion techniques (local and remote).
- "Fuzzing" - try to find deficiencies in the software by fuzzy testing techniques.

Large number of tools available
- Kali Linux [2,3], Metasploit, nMAP, Wireshark, Backfuzz, W3af, Nikto, BeEF, THC suite…

Findings
- Classified using OWASP criteria [4].
- Found a number of configuration issues.
- Several devices needing patches.
- Non-secured PLCs vulnerable [5].

Best practices
- Tools exist for enforcing best practices in information security.
- Lynis for auditing Unix and Linux systems [6].
- OpenVAS framework [7].

	Probability Rating		Criticality Rating
1	Skill level of hackers	1	How much data is affected that could be disclosed
	(1) No technical skills (3) Some technical skills (4) Advanced computer user (6) Network & programming skills (9) Security penetration skills		(2) Minimal non-sensitive data disclosed (6) Minimal critical data disclosed (6) Extensive non-sensitive data disclosed (9)Extensive critical data disclosed or all data disclosed
2	How motivated they are	2	How sensitive is the data that could be disclosed
	(1) Low or no reward (4) Possible reward (9) High reward		(2) Minimal non-sensitive data disclosed (6) Minimal critical data disclosed (6) Extensive non-sensitive data disclosed (9)Extensive critical data disclosed or all data disclosed

Example of OWASP classification.

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 [8]:
  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.
  4. Server answers with its own data-stuffed packet.
  5. Client makes another DNS query to a different subdomain avoid DNS caching, etc.
- Mitigation: restrict DNS queries to internal domain.

Issues with IPv6
- IPv6 [9] is still being implemented and, therefore, not a well known protocol.
- New features and functionalities to facilitate network management.
- New vulnerabilities are constantly being discovered.
- Mitigation: turn off IPv6 if not needed.

New IPv6 vulnerabilities per year.

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:*

A USB keyboard injection device "Rubber Ducky" [10]. When connected to a USB port, it registers itself as a keyboard device and runs a prewritten script very rapidly.

Conclusions

Information security landscape for control systems is changing
- Not immune to intrusion and even actively targeted.
- Control systems notoriously hard to secure.
- Traditionally not taken seriously by vendors.
- Consequences of security breaches can be grave, particularly in case of personnel safety systems.

Important mitigation measures
- Strict access controls to sensitive areas to know who enters and when.
- Devices in locked racks away from manipulation.
- Disabling of any unnecessary network protocols.
- Updated firewalls and monitoring of suspect traffic.
- Defense-in-depth: keep even isolated devices updated and patched as much as possible.

References

[1] https://en.wikipedia.org/wiki/Stuxnet
[2] B.J. & B. Andrew, Hacking with Kali, Elsevier, 2013.
[3] http://www.kali.org
[4] https://www.owasp.org
[5] http://libnodave.sourceforge.net
[6] http://sourceforge.net/projects/lynis
[7] http://www.openvas.org
[8] http://code.kryo.se/iodine/
[9] https://en.wikipedia.org/wiki/IPv6
[10] http://usbrubberducky.com

CERN