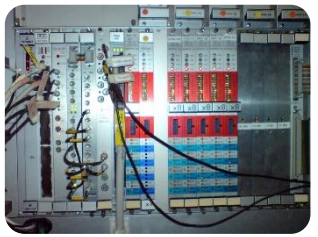
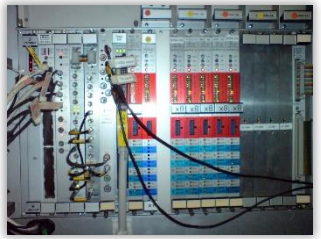

CERN

Control system network security issues and recommendations

Stephen Page



The role of a control system network



- Contain controls equipment.
- Provide separation from non-critical devices, such as office computing.
- Prime purpose is to operate the accelerator complex and its technical infrastructure.
- Should be largely independent of other networks.
- Should be physically available in control rooms, equipment halls and in the accelerators themselves.
- Should allow decoupled operation of accelerators or at least critical infrastructure services in the event of a computer security incident.

Rules for connection

- Devices should be well-described.
- They should conform to a naming convention.
- They must not bridge to other networks.
- WiFi interfaces are forbidden.
- There should be a declared person or team responsible for them.
- There should be a strategy for keeping them patched and up-to-date.

Challenges typical to the control system

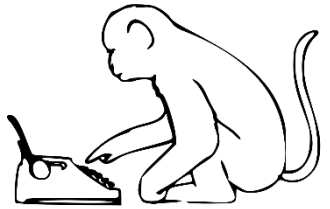
- Many devices connected to the accelerator network are old, obsolete, out-of-support or otherwise difficult to secure and therefore are vulnerable. It is not practical to replace all of them. They therefore must be contained within the network.
- Even the patching of modern systems is constrained by the accelerator schedule.
- We therefore depend strongly upon securing the perimeter of the controls network.
- Features and functionality of the control system tend to be of far greater perceived priority than its security.

Control system network users

- The controls network must accommodate multiple types of users, with different needs and access rights:
  - Accelerator operators
  - Equipment experts
  - Software developers
- Some of those people may be working outside of the accelerator networks: in offices, or even at home, if they are on-call.
- The rights of those different classes of user within the control system must be managed.
- So-called ‘service accounts’, whose credentials may be known by multiple people, should be avoided where possible and otherwise have their scope carefully controlled.

Types of control system network access

- **Services**:
  - Control system servers providing access to operational data or services.
  - Office network servers which either provide services needed from the control system or because they need access to it.
- **Interactive**:
  - Servers & virtual machines for expert access and software development.
  - Windows terminal servers running expert applications.



Both of the above types of access are required:

- Office network central services are needed on the control system network.
- Software development requires access to the control system network as separating it can mean significant duplication of systems and accelerator equipment and final validation against the accelerator complex is often needed.
- Experts need to be able to intervene from outside the control room to keep the complex running.

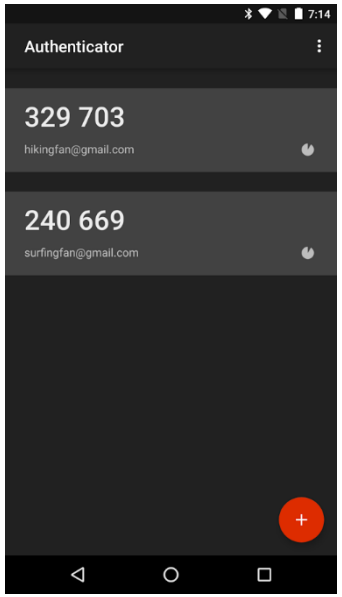
Define network rules for inter-network services

- Historically, the approach for computers on one network needing to access services on another has been to grant them full access to that network.
- The causes a proliferation of varied points of entry into the controls network.
- We now define rules permitting access to only the required services, with connections allowed only in the needed direction.
- Applying rules to existing services is very time-consuming.
- The ability to define such rules on a large network can be limited by the type of hardware used, so it is important to take these security considerations into account when designing the network infrastructure.

Bastion hosts as network entry points

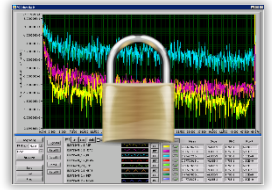
- A bastion host is a secured server providing minimal services to access a resource.
- In our case, bastions will be used as secure gateways for interactive access between the office network and the accelerator network.
- SSH, web and Windows remote desktop services will be supported.
- No applications or development will be able to run on the bastions themselves.
- Only accounts belonging to individual people will be allowed to connect.
- All accesses will be rigorously logged.
- Two-factor authentication and other security policies can be implemented on the bastions as technology evolves.

Two-factor authentication



- Both the user's password and a physical second factor would be needed for access.
- The second factor can be a USB key, smartphone application (e.g. Google Authenticator) or SMS with a one-time password.
- Prevents access if a password is compromised.
- To be integrated into central account management and applied to SSH, web (Single Sign-On) and Windows remote desktop.
- Should be applied on the bastion hosts and required when passing over the perimeter of the accelerator network.

Security within the control system



- Systems such as RBAC provide access control **within** the control system, not computer or network security.
- This is independent of computer and network security and instead controls access to accelerator equipment and devices from applications.
- RBAC allows us to define **who** can access which devices, **when** and from **where**.
- RBAC is mostly intended to protect against well-intentioned users, but nonetheless should follow computer security principles.
- Such access control systems are relatively recent and should be retrofitted to older parts of the accelerator complex.

Summary

- The problem of controls network security is multifaceted, involving: computers, networks, users and controls equipment.
- Our strategy is to:
  - Define fine-grained rules permitting only needed services between networks.
  - Limit and control points of entry.
  - Ensure that users identify themselves personally.
  - Log all accesses in and out.
  - Adopt modern security technologies at the points of entry.
  - Manage rights within the control system via roles.
- Nurturing a culture of security remains an ongoing challenge.


CERN