CYBERSECURITY IN ALICE DCS

Peter Chochula[1], André Augustinus[1], Lennart Jirdén[1], Peter Rosinský[1,2]

[1]CERN, Geneva, Switzerland; [2]Comenius University, Bratislava, Slovakia

Abstract

In the design of the control system for the ALICE experiment much emphasis has been put on cyber security. The control system operates on a dedicated network isolated from the campus network and remote access is only granted via a set of Windows Server 2003 machines configured as application gateways. The operator consoles are also separated from the control system by means of a cluster of terminal servers. Computer virtualization techniques are deployed to grant time-restricted access for sensitive tasks such as control system modifications. This paper will describe the global access control architecture, the policy and the operational rules defined. The role-based authorization schema will also be described as well as the tools implemented to achieve this task. The authentication based on smartcard certificates will also be discussed.

THE ALICE DCS NETWORK AND COMPUTING INFRASTRUCUTRE

Safe and stable operation of the ALICE Detector Control System (DCS) largely depends on its computing and networking infrastructure. 1200 devices performing the DCS tasks are currently connected to the ALICE DCS network. This covers the underground experimental hall, counting and control rooms and service building on the surface.

The DCS computing infrastructure is composed of 150 servers. The core of the control system is based on the commercial SCADA system PVSSII running on 90 Windows XP computers. Additional servers provide backend services, interface to front-end electronics and host the user interface.

Direct communication to front-end electronics is established via 800 single board computers running Linux. The majority of them are DCS boards mounted directly on the detector chambers.

The computers involved in running the control system are called Worker Nodes (WN) and are grouped detector wise. Interaction between the user and DCS is handled by Operator Nodes (ON). A minimum functional DCS cell consists of one Operator Node and one Worker Node.

NETWORK-LEVEL SECURITY

The DCS network is designed to be able to operate in complete isolation of external networks, including the CERN General Purpose Network (GPN). The separation mechanism is implemented in the network infrastructure and is based on CNIC tools and recommendations [1].

External hosts are visible from the DCS network if they belong to a set of trusted devices. This list of such trusted devices is maintained by ALICE network managers and covers services required for network operation such as Name Servers, Time Servers, Central Authentication Service, etc. Caching of these services inside the DCS network allows for smooth operation in case of connectivity problems. Packet filtering mechanism is based on MAC address and is implemented directly in the DCS routers.

The list of trusted services also covers computers and PLCs installed on other CNIC-compatible networks, such as the CERN Technical Network. Information provided by these resources is required for the experiment operation, but is not essential for the detector safety. All mission critical services are installed on the DCS network.

Selected DCS computers are exposed to external networks and are thus accessible from remote locations. The set of exposed machines covers remote access gateways, file exchange servers and servers publishing ALICE information to the LHC control system.

Connection of new devices to the network is strictly controlled. The registration process is formalized and requires authorization by the DCS network managers. The owner of the connected device must provide all information concerning its role in the DCS; device type, location and operation details. After approval, device MAC address is assigned to a dedicated network outlet and registered in the SHCP service.

REMOTE ACCESS TO DCS COMPUTERS

Remote access to the DCS network is based on Applications Gateways (AGW). A cluster of dedicated servers is configured to run Windows Terminal Service. These servers are exposed to the CERN GPN and accept connections from CERN campus network.

Users requiring access to DCS resources must first establish connection to the application gateway using RDP. All internal DCS resources are then reachable from the gateway.

If access from locations remote to CERN is desired, a similar procedure applies. User first need to logon to CERN application gateway and from there they can access the DCS gateway. The described mechanism is shown in Figure 1.

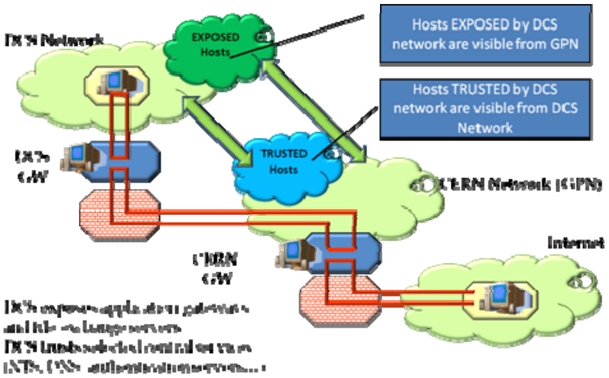
DCS Network
EXPOSED Hosts
Hosts EXPOSED by DCS network are visible from GPN
Hosts TRUSTED by DCS network are visible from DCS Network
DCS GW
TRUSTED Hosts
CERN Network (GPN)
Internet
CERN GW
DCS exposes application gateways and file exchange servers
DCS trusts selected central servers (NTP, DNS, authentication servers...)

Figure 1: Principle of the remote access mechanism to the ALICE DCS network.

OPERATING SYSTEM-LEVEL SECURITY

During operation of the experiment, the normal user logon is restricted to Operator Nodes. Experts however can also gain access to the Worker Nodes.

Authentication is based on the CERN credential system and is validated by central servers. Caching of credentials on DCS computers allows for smooth operation also during temporary connectivity problems between the DCS network and IT services.

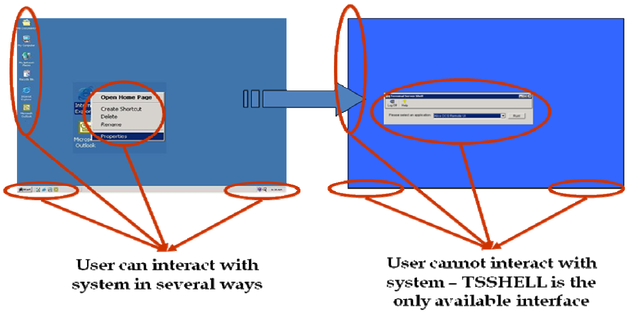
Open Home Page
Create Shortcut
Delete
Rename
Properties
User can interact with system in several ways
User cannot interact with system – TSSHELL is the only available interface

Figure 2: The DCS custom shell.

Authorization is based on AD security groups. Access policies are configured per detector and are common for all its computers.

Users are divided into two groups called “Users” and “Experts”. Members of the “Users” group can logon to the DCS application gateways and to the Operator Node of their detector. “Experts” can in addition get logon privileges to their Worker Nodes.

Interaction between the user and the operating system is restricted to a limited set of actions. “Users” are authorized to start the DCS UI, while “Experts” can in addition launch debugging tools or logon to the worker nodes. To enforce the policies, the standard Windows shell has been replaced by a custom application called TSSHELL [2] as shown in Figure 2. The “user” can only start applications offered in the pull down menu. The list of applications is dynamically modified according to the “user” group affiliation.

APPLICATION- LEVEL SECURITY

The security measures applied at the network and operating system levels protect DCS against unauthorized access and malicious attacks. The task of the application-level security is to protect the system against inadvertent errors.

PVSSII is built as a collection of highly specialized program modules called managers. These communicate via TCP/IP protocol and can be scattered across several computers. In addition, a distribution mechanism allows for creation of large distributed system. In this configuration several individual systems communicate, share data and access remote functions. The global ALICE system is built as a big distributed system of distributed detector systems. It consists of 90 detector systems and runs about 900 managers.

Interactions between the user and the control system are restricted to actions accessible through the DCS UI [3]. This has been standardized for all ALICE detectors and systems and it run on detector Operator Nodes. In this configuration, several users can logon to a ON simultaneously and run their private instance of the UI as shown in Figure 3.

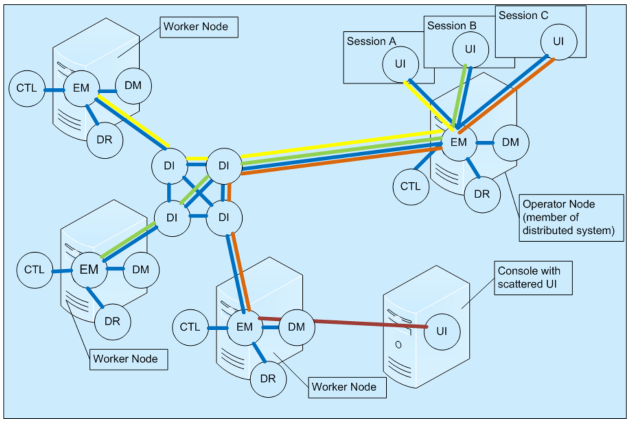

Figure 3: DCS UI configuration.

ALICE DCS access control is applied at the UI level. After starting the interface, all panel elements are available in read-only mode and the user is requested to enter his credentials. These are passed by UI to central access control server as shown in Figure 4. As a first step the user credentials are verified by the CERN authentication servers. If they pass, a list of granted privileges is made available to the UI. An action requiring a certain level of authorization is executed only if the corresponding privileges are granted to the current user.

The access control servers and tools were developed by JCOP and are available as Access Control component in the JCOP framework [4].

ALICE DCS is divided into access control domains. One domain is defined for each detector, and separate domains are created for services and central DCS. Additional sub-domains for LV subsystem, HV subsystem, cooling, front-end, etc., can be defined for each detector.

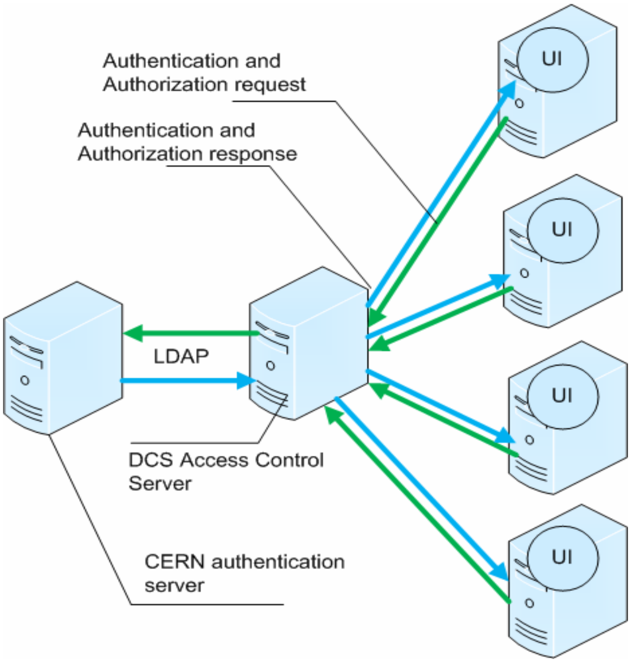

Figure 4: DCS Access Control Server.

According to their role (observer, operator, expert, developer or administrator), the users acquire one or more privileges for a domain or sub-domain:

- **Monitor** allows read only access to DCS parameters;
- **Control** allows changing some parameters and sending commands to the detector via the FSM tools;
- **debug** allows change of parameters, such as alert or trip limits;
- **modify** allows to modify structure of objects (for example to add new device channels or to change the structure of datapoints);
- **administer** allows for the administration of domains.

ACCESSING THE UI

The UI is executed on Operator Nodes as described above. However, physical access to these computers is reserved to administrators. Users can logon to operator Nodes using the RDP protocol and remote desktop client.

From the ALICE control room on experimental site, each user can connect to any ON from the console computers. These are configured as detector-independent and provide only terminal server client software.

Access to the DCS UI from CERN campus network is granted via the DCS application gateways. During the experiment operation, the access control component drops the rights of the remote users logged to the application gateways and only monitoring privileges are assigned to them.

To acquire full privileges, user must logon to a dedicated server, called Remote Expert Gateway (REG). Authentication to this server requires presence of SmartCard containing user's certificate. ALICE policies require explicit permission by the shift crew before establishing connection to REG

As shown in Figure 5, user's logged into application gateways can only access the PVSSII UI, while REG users have additional possibility to establish connection to operator and worker nodes.

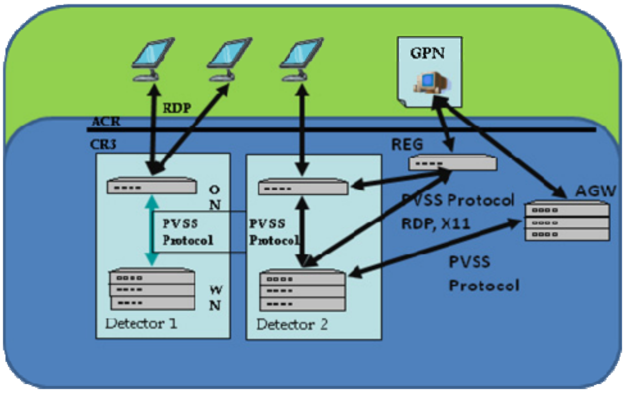

Figure 5: Remote access to DCS UI.

CONCLUSIONS

The ALICE access control mechanism provides protection at the level of the network, the operating system and thea pplication. The system is protected against malicious attacks and inadvertent errors.

The implemented policy satisfies the CERN security rules, the collaboration requirements and the existing infrastructure.

REFERENCES

[1] S. Lüders, Computing and Networking Infrastructure for Controls (CNIC), these proceedings

[2] Ruben Gaspar Aparicio, Private communication

[3] L. Jirden, ALICE Control System — Ready for Operation, these proceedings and http://alicedcs.web.cern.ch/alicedcs/Software

[4] O. Holme *et al.*, The JCOP Framework, ICALEPCS 2005, Geneva, Switzerland