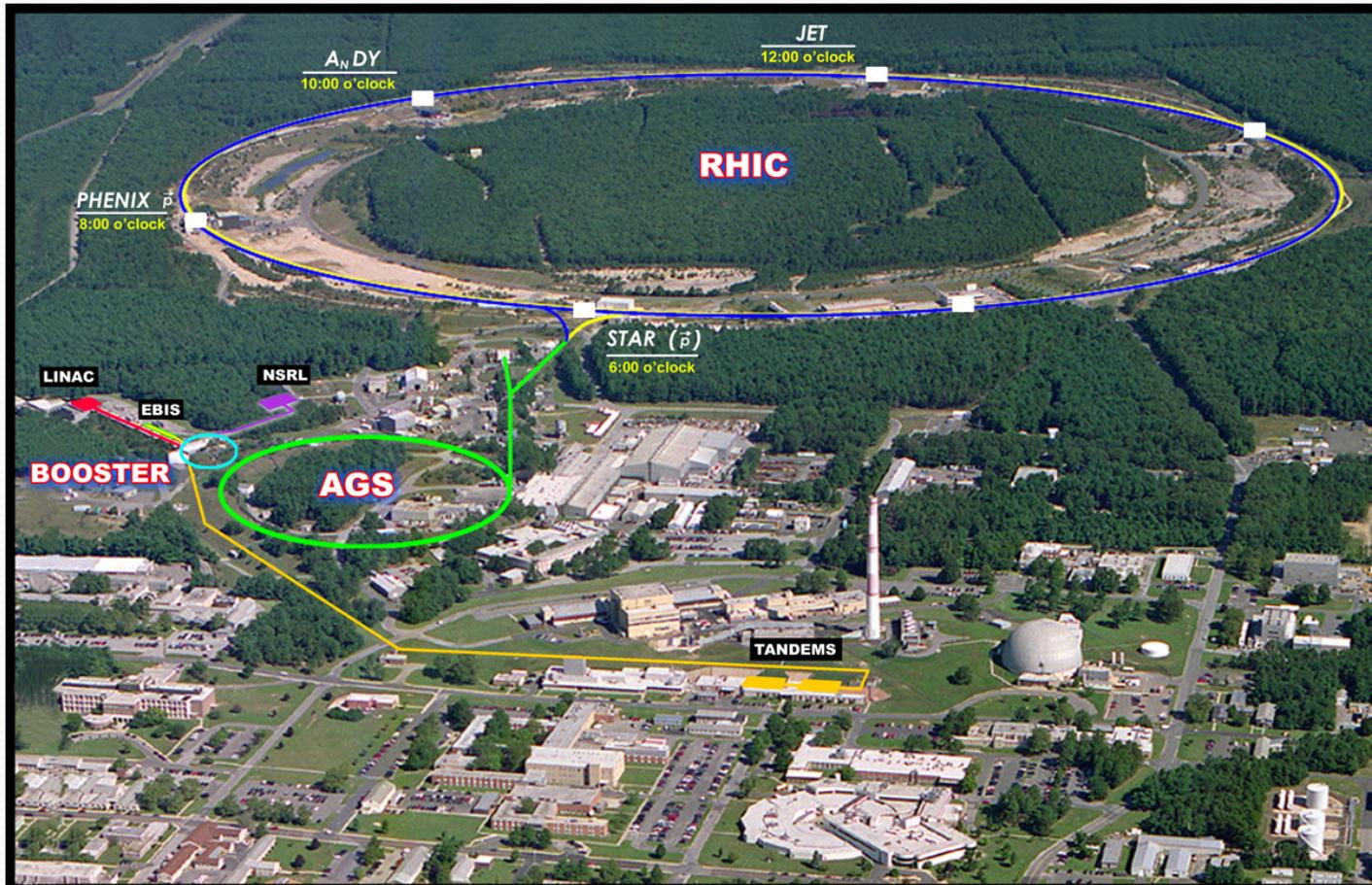


C-AD Cyber Security Event Involving the Access Control System

Ed Lessard and Nick Franco, BNL Collider-Accelerator Department



C-AD Accelerators



Access Controls System Incident

- What was the incident?
- How was it detected?
- What damage did it cause?
- What was done about it?

What was the incident?

C-AD FIREWALL



Subnets to water systems, cryogenic systems, access control systems, Main Control Room...)



ACS communication layer includes servers, HMI PCs, cameras, IRIS Scanners, key trees, etc (infected)

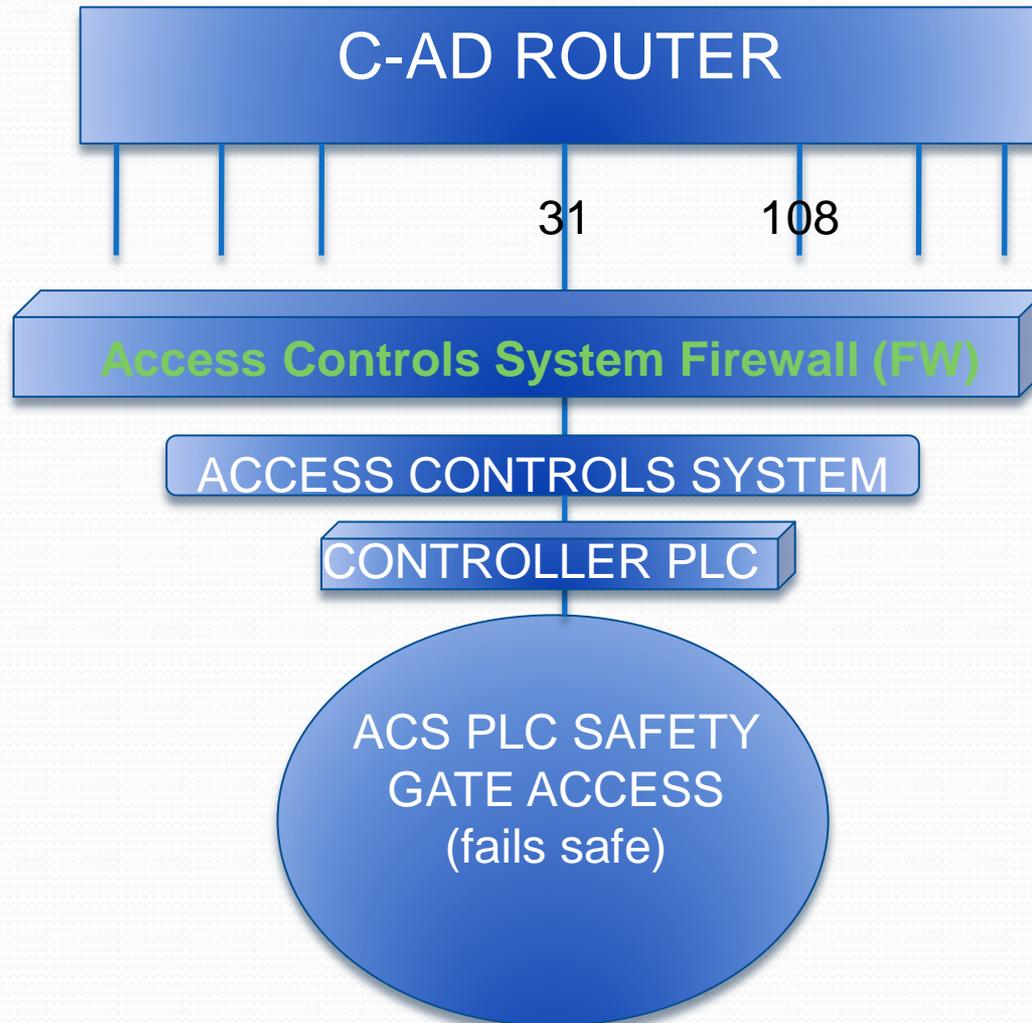


Functional Layer: gate interlocks, critical devices, crash buttons (not infected)

Real time anti virus scans not used since it interferes with operations of ACS

What was the incident?

C-AD FIREWALL



A year prior to event, we added ACS firewall (FW) with a rule set that kept blowing up. Blow up due to communication with key trees, HMI PCs and IRIS scanners that were too numerous to easily track; we took FW rule set out and ran anyway

Months later we added a sniffer to monitor and log communications in order to develop a rule set for the ACS FW

What was the incident?

Server in
Russia



ACS Human
Machine Interface
(HMI PC) without
anti virus software
at C-AD

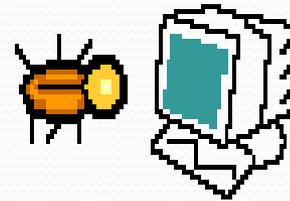
- ACS HMI is touch screen; mouse and keyboard locked away
- Did not use anti virus; no way for operator to stop scan or close pages/pop-up boxes
- As soon as sniffer was in, we saw communication between ACS HMI PC and Russian server
- Two-way chat never completed; information going out only
- Russia never used the link to hop into other parts of BNL
- ACS firewall immediately used to block communications with Russian server

What was the incident?

How did this happen?



- Software installed on HMI PC using a USB memory stick – contaminated



- No anti-virus protection installed on HMI PC – we assumed we were “isolated”
- Malware installed itself

- Malware installed in Oct. 23, 2010
- HMI PC in service on Oct. 29, 2010

How was it detected?

- Firewall installed in passive mode and sniffer collecting communications data on April 26, 2011
- Malware observed phoning home (detected within 1 hour)
- Firewall rule set used to block communications with Russia
- C-AD Management informed by ACS Group
- BNL Cyber Security informed by C-AD
- BNL informed DOE
- Access Controls System subnet (.31) blocked within BNL

What damage did it cause?

- No detrimental effects were realized
- ACS subnet blocked at BNL to the C-AD Firewall
- Three ACS computers found with the malware
- RHIC Run-11 continued as normal
- ACS communications layer was affected, but not safety
- Bad timing – C-AD's Authority to Operate due for renewal and ORNL, PNNL, JLab just had events

What was done about it?

C-AD critique ordered by C-AD Department Chair



MEMBERS: Kevin Brown (C-AD), Ed Lessard (C-AD), Nick Franco (C-AD), Dana Beavis (Physics Department), James Fung (ITD), Pat Sullivan (DOE)

What was done about it?

- Operations procedures written for Cyber Security management within C-AD
- Responsible personnel appointed at Department level
 - Cyber Security Administrator (CSA)
 - Cyber Security Officer (CSO)
- Training

What was done about it?

- Examples of C-AD Operations Procedures:
 - CSA rules to oversee setup of all computer systems in C-AD
 - CSO rules to approve any device connected to the C-AD network
 - Rules for retrievable approval records for variances to the basic cyber-security requirements
 - CSO rules to control the request and renewal of all variances
 - Rules for use of USB drives and removable media
 - Rules to report suspect behavior

What was done about it?

- Training for key personnel (CSA, CSO, system owners, etc.)
- Cyber Security Forum for Department leaders and system owners