Markus Braendle, Control System Security Manager, ABB Power Systems, 2009-02-03

How to Upgrade the Security of the Control Systems You Already Own

SANS Process Control & SCADA Security Summit

Content

- Use what is there
- System hardening – the basics
- System hardening – the second step
- Patch management
- Flaw remediation – a lesson learned

Use what is there
Actively managing your system

Account Management

- Make use of the possibility to have **personal** accounts
- Make use of the ability to **change** passwords
- Make use of role based access control to **limit** access privileges

Access can be controlled from the system level down to the object level. Access can be limited, defining for example the right to open a single valve, or start a complete boiler.

ABB System 800xA for Power Generation

Monitor log files **regularly**

DCS/SCADA log, system event logs, security log files, etc.

Alerts → use and **listen** to them

- Make use of reporting capabilities of the DCS/SCADA System
- Third party products are often able to generate alarm and event in the DCS/SCADA environment

System Hardening
The basics

All systems already deployed can be hardened.

Servers and Workstations

- Removal of unused software
- Disabling unused services
- Removal unused accounts
- Change of default passwords

Network and other Devices

- Disabling unused services.
- Removal unused accounts.
- Change of default passwords.

Verify your setup (on a redundant or test system)

- Various tools available for auditing, e.g. Bandolier project by DigitalBond

System Hardening
The second step

Host Based Firewalls

Antivirus software

Intrusion Detection Systems

Security Management Systems

ABB supports integration with third-party Security Management Systems (SMS). Alerts from the SMS can be picked up from Network Manager in the form of SNMPv3 traps, providing a capability to generate events/alarms for the operator on duty in addition to whatever notification mechanisms the SMS may support.

ABB Network Manager

- Have a process for updating, maintaining and monitoring
- Deploy them correctly

Patch Management

For most DCS / SCADA systems vendors have a patch management process is in place → **use it!**

ABB evaluates all Microsoft security updates for relevance and system compatibility as they are released by Microsoft. Our goal is to communicate the validation plan for these updates within 24 hours of the release and publish the results of the validation within 7 days. Microsoft Service packs will be tested against the subsequent ABB System service pack or product release.

ABB System 800xA

Most vendors test patches on baseline systems as part of service contracts

If that is not enough you should first test the update on a redundant or test systems

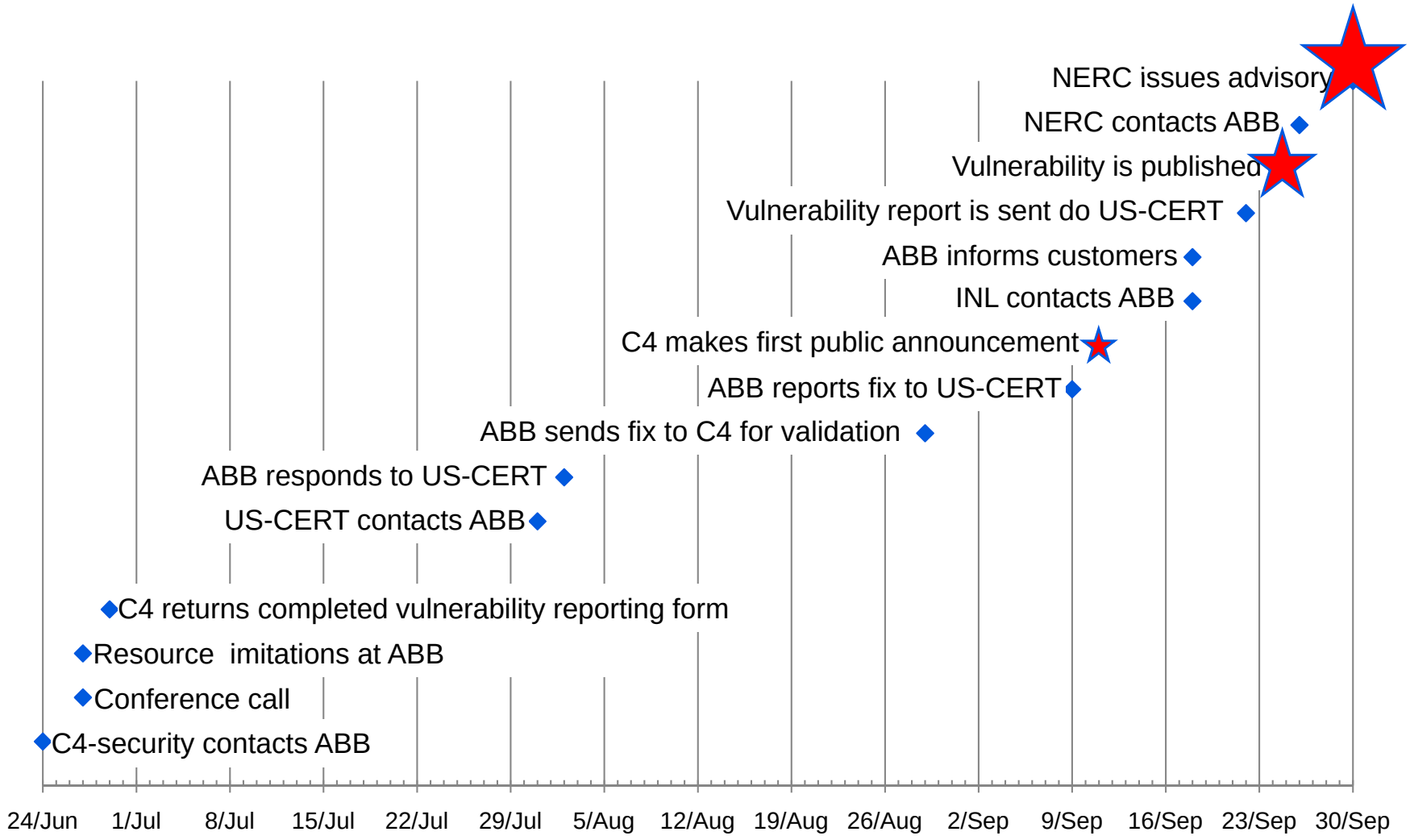
Flaw remediation

- In 2008 this was on of **THE** hot topics
- Security researches got bashed for disclosing vulnerabilities
- Vendors got bashed for not reacting properly and in a timely fashion
- And it was exciting to follow …

… until it hit us!

Flaw remediation
The ABB story

Content
Use what is there
System hardening I
System hardening II
Patch management
Flaw remediation
Summary



Flaw remediation
Lessons learned

1. Cooperation with external company went well
   BUT initial contact made through personal contact
2. Internal process worked well
   BUT it will be revised and formalized even more
3. Communication to affected customers worked well
   BUT overall external communications must be improved
4. Government organization were very cooperative
   BUT NERC advisory used different text then ABB vulnerability disclosure
5. Patch and mitigation was made available
   BUT will you use / install them?

Summary

Tools and techniques are available to add security to existing control systems

Use the Procurement Language to challenge your vendor

But allow the vendor to challenge you

Contact for questions and comments

Dr. Markus Braendle

Control System Security Manager

Power Systems

ABB Switzerland Ltd

Segelhofstr. 1K

CH-5405 Baden 5 Dättwil

Telefon +41 58 586 82 90

Mobile +41 79 378 67 28

E-Mail: markus.braendle@ch.abb.com

Power and productivity
for a better world™