ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THBPA01

CYBER THREATS, THE WORLD IS NO LONGER WHAT WE KNEW…

S. Perez, CEA/DIF, Bruyères le Châtel, 91297, Arpajon, France

Abstract

Security policies are becoming hard to apply as instruments are smarter than ever. Every oscilloscope gets its own stick with a Windows tag, everybody would like to control his huge installation through the air, IOT is on every lip…

Stuxnet, the recent Snowden revelations have shown that cyber threats on SCADAs cannot be only played in James Bond movies.

This paper aims to give simple advises in order to protect and make our installations more and more secure.

How to write security files? What are the main precautions we have to take care of? Where are the vulnerabilities of my installation?

Cyber security is everyone's matter, not only the cyber staff's.

INTRODUCTION

ICALEPCS is the conference where Large Experimental Physics Systems describe their Industrial Control Systems (ICS) architecture.

Most of these systems can be represented using the Purdue model, as shown in Figure 1.

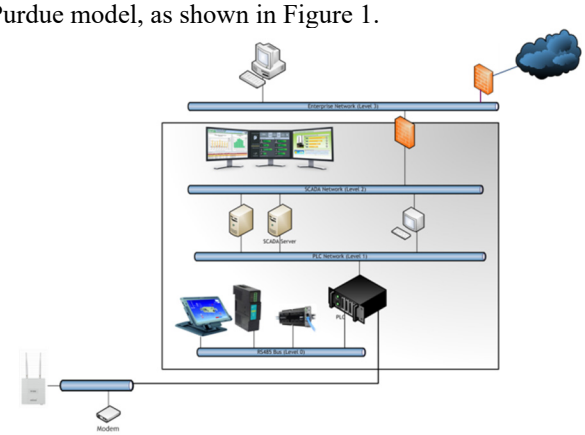

Figure 1: ICS Architecture.

The 4 main levels of this schematic include:

- Level 0: Sensors low level buses,
- Level 1: PLC network,
- Level 2: SCADA,
- Level 3: Office network.

External access can be added:

- Remote through WiFi, Bluetooth, modems…
- Internet.
- Contractors.
- Direct access through USB drives.

Figure 2: ICS Vulnerabilities.

But each benefit of this architecture shows us vulnerabilities (Figure 2):

- Remote access can be attacked using non secure access points,
- Firewalls may be non-sufficient if rules are not correct.
- Internet remote access is a source of multiple attacks (deny of services, open ports access, non-secured protocols…).
- PLCs can be trapped.
- Maintenance systems can be hacked and, by the way, give access to malware installations.
- The use of USB keys can compromise systems using rootkits, infected files, and macros or even destroy systems with devices like USB killers technologies.

In 2016, Security trends and vulnerabilities review shows that SACA and PLCs are on the top level of ICS component [1]. Particularly this study reported that Siemens and Schneider Electric represented 32% and 18% of the vendors concerned by the number of vulnerabilities. Between 2012 and 2015, there have been almost 150 to 200 vulnerabilities discovered each year. Center for Strategic and International Studies pointed out 218 cyber-attacks dated from May 2006 to August 2016 and this list is still growing [2].

SOME EXAMPLES [3]

Attack on the BP Baku-Tbilisi-Ceyhan Turkish Pipeline

In 2008, hackers planned a combined physical and cyber-attack on a pipeline located between Turkey and Azerbaijan that caused an explosion with flames as high as 50 meters… The attack was made through a non-protected wireless network, making disconnections of

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THBPA01

security alarms and survey cameras. More than 1 Million dollars lost and 20 days of disruption due to equipment destruction. Cyber attackers were said to have gained access to the pipeline's control system and were able to suppress alarms, manipulate the process, and blind system operators. The source in the Bloomberg report indicated that the control room operators did not learn about the rupture and explosion until 40 minutes after it had happened [4].

The installation should have used network layers, improve the physical access of the system and secure wireless and camera networks. A new architecture using separated networks between the main SCADA and IP based cameras are a way to improve security of the installation.

Emergency Stop in a Nuclear Plant (Hatch Georgia)

Same year, March 2008, and due to unintended consequence of a contractor update, the Hatch nuclear plant restarted after full data synchronization between the updated system and the contractor's computer. This action made the plant's unit #2 set into automatic shutdown for 2 days [5].

This is not a volunteer hack but this shows us:

- The need of setting up updates protocols,
- The importance of building network separation between critical systems and data servers.

Close to the LMJ[1] facility, CEA uses the PFI, a specific area where every system and application patches, interfaces between sub-systems are tested before using it in the operational instrument: there is a physical separation between the tests area and the operational system [6].

Chemical Settings Change at Water Treatment plant

In 2015, led by money winning, hackers took access of the payment application of the Kemuri Water Company [7].

This system ran, on a single IBM AS/400, the water district's valve and flow control application that was responsible for manipulating hundreds of programmable logic controllers (PLCs), and housed customer and billing information, as well as the company's financials.

The hackers exploited unpatched web vulnerabilities but, as they didn't have a complete knowledge of the installation, they manipulated the PLC's that managed the amount of chemicals used to treat the water and to make it safe to drink.

Again, this shows us:

- The need of network separation between the SCADA and the payment apps,
- A strong authentication for credentials access,
- Regular analysis of Web exposed apps.

Target, 40 Million Credit Cards Stolen

High ranking people were fired, $5 million investment in cybersecurity coalition, still dozen of new cyber security jobs promoted in 2017. These are the consequences of 40 million of credit cards stolen from "Target" in 2013 and sold on the black market [8].

The attack started from a Trojan-Horse delivered in an email, targeting a small heating and air conditioning firm in Pennsylvania. A direct communication between air conditioning PLC's network and point of sale servers made the hacker access to the core system.

No network separation between 2 critical parts (financial and air conditioning systems), lack of knowledge on credentials strength.

Every state or laboratory is, of course, highly concerned by these Cyber Problems: US Department of Homeland Security, main internet page explained "how do I protect myself from Cyber Attacks" and "how do I report Cyber incidents", ANSSI[2], in France, is helping companies to protect against cyber hacking, CERN's Computer Security Team details that even if individual users are fully responsible for securing their computers, the Team is ready to help uses with training, services or recommendations, SLAC Cyber Security Training is required to maintain a SLAC computer account, Brookhaven National Lab asks new guests following Cyber Security training course prior to their arrival…

RECOMMANDATIONS

Regarding the analysis of these past examples, we will point out 5 specific recommendations for ICS:

- The use of Defense in Depth.
- Handling external USB devices.
- Contractors Cyber Management.
- Monitor and survey an ICS.
- Writing security reports.

Defense-in-Depth

Like during the antics or middle ages periods, a robust Defense-in-Depth solution can make systems unattractive targets to would-be attackers [9]. Several layered security measure can be used.

- **Physical protection** must prevent access to the main facility, ICS control and server rooms. The use of cameras and motion detectors can be used

[1] Laser MegaJoules, French Laser Facility (www-lmj.cea.fr)

[2] Agence Nationale de la Sécurité des Systèmes d'Informations

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THBPA01

to monitor the facility, specific credentials and procedures for visitors can be used…

- **Virtual LAN's** divides physical networks into smaller units, making the system a multiple grape of independent networks. This avoid, using specific infrastructures, virus and malwares to propagate in the entire factory.

- Strong **authentication** systems with key cards or PIN technologies can prevent access into the protected systems.

- Real **network segregation** with the "real" world must be taken in count. A particular attention should be taken with internet access, remote control and radio communication tools (Wi-Fi, Bluetooth, ZigBee…).

USB devices Management

USB devices, often used for sharing information, are surely a way for malware and virus ICS contamination **(**Figure 3**).** They can even be used for computer destruction with the USB killer device **(**Figure 4). This "flash drive" that can easily be bought on the regular market for a very cheap price, includes a pump diode electronic system that is able to generate -200V spikes using the 5V USB computer connector. There is, of course, a complete destruction of the computer.

Figure 3 : USB Stick.

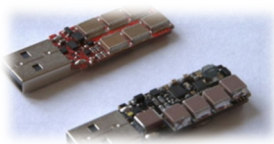
Figure 4 : USB Killer.

In April 2015, Matthew Tischery dropped 297 USB devices in a large US university campus [10]. Some groups of keys had different appearances: unlabeled drive, drive with keys, drive with return label, confidential drive and exam solutions drive. The main result shows that ~50% devices were connected inside the campus network…

Each company should have a decontamination area dedicated to external USB key, and scan for malwares and viruses the specific files that are useful for the ICS operation. As most of the vulnerabilities are Windows targeted, the key should be plugged in a Linux OS specific computer. A $35 raspberry pi could also be used and even act as a fuse in front of a USB killer device.

Contractors Management

US Department of Homeland Security wrote a "Cyber Security Procurement Language for Control Systems" guide dedicated to provides example language to incorporate into procurement specifications [11]. This technical guide is the language and the minimum background necessary for a provider to integrate cyber security in the system they provide and maintain.

Contractors often use portable devices for onsite maintenance operations. An ICS policy must include cyber rules for contractors and sub-contractors.

The procedure that allows an external portable device also used for outside ICS or that was connected to the Internet without the proof of safety control is a risk for the installation. For these reasons, a specific portable device should be used for each industrial system. The best option would be based on residential contractor's computers and the use of protected file transfers for updates described in the flowchart in Figure 5: industrial portable devices for maintenance operation should remain the ICS property and therefore stay inside the installation. Upgrade of the Operating System, specific component software or configuration files must be transferred to the maintenance computer through a transfer box that includes a strong vulnerabilities analysis.

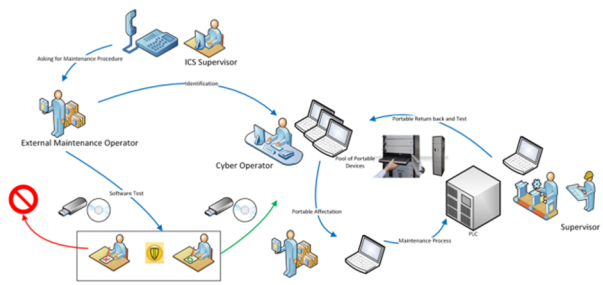

Figure 5: Portable devices stay at home.

This flowchart described in Figure 5 shows the use of devices delivery for a maintenance procedure: portable devices are stored inside a keycard controlled cabinet with specific access controlled delivered to the maintenance operator only. Maintenance PLC's disk images can be downloaded to each computer and specific configurations are fully analyzed before using it. After each maintenance operation, the contractor needs to return the computer back to the cabinet before granted the authorization for living the plant.

SOC

A Security Operation Center (SOC) (Figure 6) is used to monitor ICS networks. Particularly, it provides a way to get information on computer access, unknown computers connected to the system or log file configured for safety control. The SOC is used to provide alerts and information for future reports.

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THBPA01

Figure 6 : Examples of SOC

The use of a software toolbox like the open source IVRE[3] can help gathering data and making flow analysis. Based on Nmap, Masscan and Zmap, IVRE is developed by CEA and is available from GitHub. Figure 7 shows in a simple graph, the use of IVRE with information flow exchanged between components of the ICS. Each point is an IP address, each line is a link between to elements as shown in Figure 7.

IVRE can be used to point out flows between equipment that are not supposed to happen or, for instance, new connected devices.

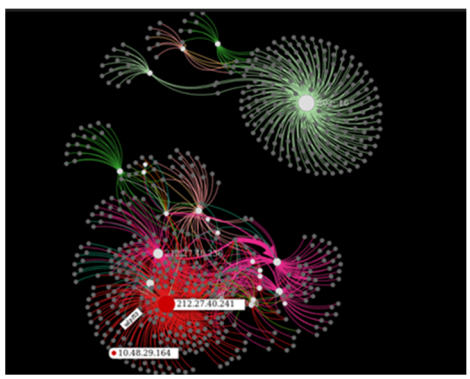

Figure 7 : Flow analysis with IVRE

Miasm is another open source toolbox that can allow protocol learning, can provide the detection of unpredictable data sent by a component of the ICS.

Nevertheless, human resources are still necessary to understand and correctly use these specific tools.

Security Report

SANS institute describes, in a large poster, 20 critical controls that have to be analyzed in order to maintain security of a system [12]. For each ICS, these 20 points must be felt up (even if non applicable) in order to make the security operator asking each question:

1. Inventory of Authorized and Unauthorized Devices.
2. Inventory of Authorized and Unauthorized Software.
3. Secure Configurations for Hard and Soft on Mobil Devices, Laptops, WS, and Servers.
4. Continuous Vulnerability Assessment and Remediation.
5. Malware Defenses.
6. Application Software Security.
7. Wireless Access Control.
8. Data Recovery Capability.
9. Security Skills Assessment and Appropriate Training to Fill Gaps.
10. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches.
11. Limitation and Control of Network Ports, Protocols, and Services.
12. Controlled Use of Administrative Privileges.
13. Boundary Defense.
14. Maintenance, Monitoring, and Analysis of Audit Logs.
15. Controlled Access Based on the Need to Know.
16. Account Monitoring and Control.
17. Data Protection.
18. Incident Response and Management.
19. Secure Network Engineering.
20. Penetration Tests and Red Team Exercises.

These elements that have to be found in a security report are also described in numerous papers and organisms. Particularly, ANSSI, in France, proposed more than 40 points in order to help ICS cyber team writing their security report, WaterISAC Security Information Center provides 10 measures for cybersecurity [13]. This last document has been written in partnership with the U.S. Department of Homeland Security.

The first ICS cyber-protection is a detailed documentation that goes deep in the understanding of the system. Details of the report must include the system architecture, software and credential details.

As our ICS are mostly based on the Purdue model, we have to answer, for each level, the question of credentials that are used for PLCs, SCADA access, the computer, on which the SCADA is operational, access and contractor's computers access. With this complete description of the system, we could understand the elements that need to be improved in order to make the system as "cyber-controlled" as possible….

CONCLUSION

Cyber security of ICS is never a simple task, but plenty of organizations are hardly working for help. This starts from simple documents like the SOPHOS paper "IT Security DOs and DON'Ts" [14] to more complete guide like the CNIC CERN cyber policy one [15].

In this paper, and through some examples of vulnerabilities, we have shown that network segregations

[3] IVRE : Instrument de Veille sur les Réseaux Extérieurs

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THBPA01

are necessary in order to secure technical sensitive parts of the ICS.

A special attention should be taken on external vectors like USB devices or portable computers often used by contractors for maintenance operations.

A Security Operation Center is a way to analyze network flows and monitor the whole installation.

A complete documentation of the system is a precious tool for understanding and point out the vulnerabilities of ICS. Useful guides are provide by states and companies and should be used even in the simple form.

But remember, the question is not to know IF but WHEN you'll be hacked…

REFERENCES

[1] Security Trends & Vulnerabilities Review – Industrial Control Systems, https://www.ptsecurity.com/upload/iblock/6bd/ics_vulnerability_2016_eng.pdf, 2016.

[2] Significant Cyber Incidents Since 2006 – CSIS (Center for Strategic & international Studies) Washington DC.

[3] Fiches Incidents Cyber SI Industriels – CLUSIF – April 2017.

[4] R. M. Lee, M. J. Assante, T. Conway, "Media report of the Baku-Tbilisi-Ceyhan (BTC) pipeline Cyber Attack", (ICS Defense Use Case (DUC) Dec 20, 2014).

[5] Cyber Security at Civil Nuclear Facilities Understanding the Risks, Chatham House Report by Caroline Baylon with Roger Brunt and David Livingstone.

[6] J.P. Arnoul, J. Fleury, A. Mugnier, "The Laser Megajoule ICCS Integration Plateforme", in *ICALEPCS 2013*, San Francisco, CA, USA, October 2013.

[7] Attackers Alter Water Treatment Systems in Utility Hack: Report by Eduard Kovacs on March 22, 2016.

[8] Inside Target Corp., Days After 2013 Breach (web source).

[9] Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, ICS CERT, Homeland Security - September 2016.

[10] Matthew Tischery, *et al*., "Users Really Do Plug in USB Drives They Find".

[11] Cyber Security Procurement Language for Control Systems – DHS – September 2009.

[12] 20 Critical Security Controls for effective cyber defense – SANS institute – Spring 2013.

[13] 10 cybersecurity measures – WaterISAC – June 2015.

[14] IT Security DOs and DON'Ts - SOPHOS.

[15] CNIC (Computing and Network Infrastructure for Controls) Security Policy – V2.4 – 01/07/2011.