Lessons Learned from NATO's Cyber Defence exercise Locked Shields 2015

The increased focus on Supervisory Control and Data Acquisition/ Industrial Control Systems (SCADA/ICS) in the military domain will lead to measures for improving cyber-physical security and the development of operational capabilities. For the member states of NATO exercises in the cyber-physical field contribute to this process and to the exchange of experiences and skills. A team consisting of members of the German Bundeswehr and the Dutch Defence Computer Emergency Response Team (DefCERT), gained 10th place overall in Locked Shields 2015. In the forensic challenge, a separate part in the exercise, a 3rd place was obtained. SCADA/ICS was an element of the complete exercise, unlike forensics which was a separate challenge. This team was rewarded for not only protecting their own SCADA/ICS element, but all the other teams as well. However the protection for the other teams was reverted to provide the opportunity for the other teams to do a meaningful exercise on SCADA/ICS. The world's largest cyber exercise was informative and generated many lessons learned.

*A.D. Dijk MSc**
J.M.G. Meulendijks BSc, second lieutenant of the Royal Netherlands Air Force
Prof. dr. ir. F.G.J. Absil

This article briefly describes the set-up of the Locked Shields 2015 exercise where a fictive country needs to be protected against cyber-attacks. The focus of this article is on a simulated SCADA/ICS scenario, in which a drone command centre is dependent on a power generator. After investigating the risks and vulnerabilities of the networked power generator, the contribution and countermeasures of the SCADA/ICS sub team from our Blue Team will be presented. Finally, we describe our future research goals, aimed at increased SCADA/ICS security by investigating the potential of semantics of the physical process.

Introduction: Cyber as a Warfare Domain

The potential of networking military systems was recognised in the Network Centric Warfare (NCW) approach. Basically, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace.[1] This stimulated the development of Network-Enabled Capabilities (NEC), which promises better decision-making and better effects. For example, within the Purple

* Allard Dijk is Senior Innovation Developer (JIVC/KIXS) and PhD candidate Embedded Security (TU/e); Bas Meulendijks is Analyst SCADA-ICS/SEWACO (DMO/DefCERT); Frans Absil is Professor Combat Systems at the Netherlands Defence Academy.

1 D.S. Alberts, J.J. Gartska, F.P. Stein, Assistant Secretary of Defense (C3I/Command Control Research Program), *Network Centric Warfare: Developing and Leveraging Information Superiority* (Washington, D.C., EMC2, 2000) 292.

PHOTO NATO CCDCOE

The NATO Cooperative Cyber Defence Centre of Excellence organises the international exercise Locked Shields to train cyber specialists in dealing with attacks or malfunctions

NECtar exercise the Dutch Ministry of Defence yearly experiments with innovations developed by joint defence, industry and knowledge institutes. The goal of the exercise is to improve a shared situational awareness of all staff and units, to achieve better effects of the joint (military and civil) operations.
The primary focus around the year 2000 was on the Information Grid,[2] increasing the NEC maturity level of Command, Control and Communication Systems. In the first decade of the new millennium, as the importance of the Internet increased, the awareness of cyber threats grew. As more hardware components and Industrial Control Systems (ICS) became part of the network a new perceived threat emerged in the so-called cyber-physical domain.[3] ICS are interesting for attackers, because they can provide access and control to a physical process by means of cyber. If attackers are in control, circumvent all security and safety protections and also discover methods to inflict physical damage, they could trigger a catastrophic disaster in the physical world.

The cyber-physical field demands better security,[4] ranging from embedded security in hardware design[5] to the search for Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS) security standards.[6] SCADA is a commonly used term, which depicts a sub-category within ICS. For example, these kind of systems can be found in power plants, chemical plants and other factories. Data from sensors registering values

2 An Interconnected set of information capabilities for collecting, processing, storing, disseminating and managing information on demand.
3 H. Sandberg, A. Saurabh and K.H. Johansson, 'Cyberphysical Security in Networked Control Systems; An Introduction to the Issue', in: *IEEE Control Systems Magazine* (2015) (35) 20-23.
4 M. Cheminod, L. Durante and A. Valenziano, 'Review of Security Issues in Industrial Networks', in: *IEEE Transactions on Industrial Informatics* (2013) (9) 277-293.
5 D. Karaklajić, J.-M. Schmidt and I. Verbauwhede, 'Hardware Designer's Guide to Fault Attacks', in: *IEEE Transactions on Very Large Scale Integration Systems* (2013) (21) 2295-2306.
6 R.S.H. Piggin, 'Development of Industrial Cyber Security Standards: IEC 6243 For SCADA and Industrial Control System Security', in: *IET Conference on Control and Automation* (2013) 1-6.

like temperature, pressure and flow-rate are collected by small dedicated industrial computers (PLCs)[7] and transported to remote systems for the purpose of logging, monitoring and controlling by operators.

The cyber-physical domain meets the military environment both at platform level (ships, vehicles, aircraft) and in current combat systems, like in the Sensor and Shooter Grid of the NCW approach. Platform automation and the linking with a Combat Management System (CMS) will require serious investigation of defence weaknesses and attack potential. Integrating procured weapon systems through hardware and software interfacing is a serious security issue. Around the globe, governments and military departments have developed cyber policies and are implementing system security measures and researching cyber (physical) operational capabilities.

According to the Cyber Policy and Strategy document *Defensie Cyber Strategie* (DCS) of the Dutch Ministry of Defence, cyberspace, the fifth warfare domain after land, air, sea and space, will be more and more integrated into military actions.[8] The DCS assures improved and increased security levels. The use of cyber capabilities as a weapon or as an intelligence tool is in full development throughout the world. However, the more we rely on cyber capabilities, the greater the impact of a limited availability will be, for example, due to attacks by adversaries or malfunctions. In February 2015, the Dutch Minister of Defence updated the DCS, resulting in the *seven points of attention*:[9]

1. Getting cyber professionals interested, getting them on board and further developing their skills;
2. Effective innovation and acquisition;
3. Joining forces and working together;
4. Knowledge and cyber awareness: broadening and widening;
5. Strengthening digital resilience;
6. Strengthening digital intelligence;
7. Strengthening cyber assets during missions.

However, to implement the DCS, technical equipment and cyber specialists are required. These cyber specialists will be trained, for example, in dealing with attacks or malfunctions for which Locked Shields,[10] an international cyber exercise organised by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), provides an opportunity. This exercise provides insight into how complex a modern cyber defence crisis can be and what is required from nations in order to be able to cope with such threats. In the exercise each team has ist own responsibilities and colour-based codenames that are commonly used in the IT sector. The White Team is responsible for refereeing an engagement between a Red Team of mock attackers and a Blue Team of defenders of information systems.[11]

Locked Shields cyber exercise

Locked Shields is a large-scale real-time network defence exercise, organised annually since 2010 by the NATO Cooperative Cyber Defence Centre of Excellence.[12] The CCDCOE is an international Military Organisation with a mission to enhance the capability, cooperation and information sharing among NATO, its member nations and partners in cyber defence by virtue of education, research and development, lessons learned and consultation.[13] Locked Shields is hosted from Tallinn, Estonia, while participating countries join the exercise from their own location. In the 2015 edition, held in April, 16 countries and the NATO Computer Incident Response Capability participated in Locked Shields as 15 different

7 Programmable Logic Controller, device with a microcontroller, which controls electronic outputs based on information on its inputs.
8 *Kamerstukken II 2011-12*, 33 321, nr. 1, 'Defensie Cyber Strategie', 4.
9 *Kamerstukken II 2014-15*, 33 321, nr. 5, 'Actualisering Defensie Cyber Strategie', retrieved from: http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2015/02/23/kamerbrief-over-actualisering-defensie-cyber-strategie/kamerbrief-over-actualisering-defensie-cyber-strategie.pdf.
10 http://www.nato.int/cps/en/natohq/news_119085.htm.
11 Cyber Defence Exercise Locked Shields 2012 – After Action Report, retrieved from: https://ccdcoe.org/publications/LockedShields12_AAR.pdf.
12 NATO CCDCOE, 'Locked Shields 2015', (2015), retrieved from: https://ccdcoe.org/locked-shields-2015.html.
13 Retrieved from: www.ccdcoe.org.

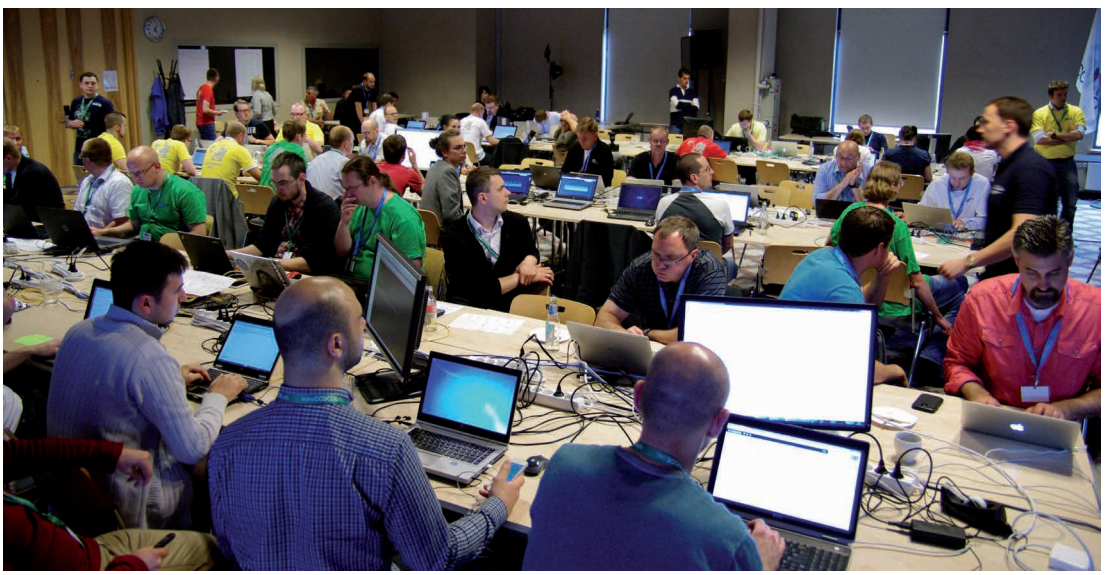

PHOTO NATO CCDCOE

Despite of all countermeasures, the attackers in Locked Shields penetrated deep in the network

Blue Teams. Their task: to defend a simulated network of a fictional country from a wide range of attacks (carried out by the Red Team). The network consisted of several voice and web services, office networks with Linux and Windows machines, Internet Service Providers and a drone command centre dependent on a power generator.

The exercise is competitive and teams are ranked on a scoreboard. The scoring system of Locked Shields works by testing the availability of all systems frequently; for each time tick a service like a website was available Blue Teams earned points. The scoreboard gave Blue Teams a live feedback of all services they had to defend and was used to set tactical priorities which systems to fix and defend first, based on the earnable points. Next to the technical aspect, points could also be earned by completing specials tasks. Besides the technical aspect, a forensic challenge,[14] media and legal injects contributed to a comprehensive cyber exercise.

The forensic specialists had to react under time and resource constrained conditions by modeling a realistic threat source and contingencies and were given the opportunity to learn new tools and methods. The forensics challenge encompassed offline and live responses, an acquisition and analysis part and host and network investigations. Their task was to provide two reports of a specific case and collaborate with the legal team.

The public relations advisors where tasked with following the local news and respond to media inquiries to exercise crisis communication. The White Team evaluated the speed, accuracy, logic and reaction of Blue Teams' spokespeople when responding to media requests. The aim of the media simulation was to illustrate the exercise with 'news from the real world' and add pressure to the Blue Teams with injects other than Red Team activities.

Legal advisors where tasked with briefing other members of the Blue Team about their legal status, applicable law, rights and obligations, as well as answering different questions on legal aspects raised by Head Quarters. They also were supposed to answer out-of-the-game technical quizzes.

Like 2014, members of the German Bundeswehr and the Dutch Defence Computer Emergency Response Team (DefCERT) –

14 http://mastersicurezza.di.uniroma1.it/mastersicurezza/images/materiali/ls_sapienza.pdf.

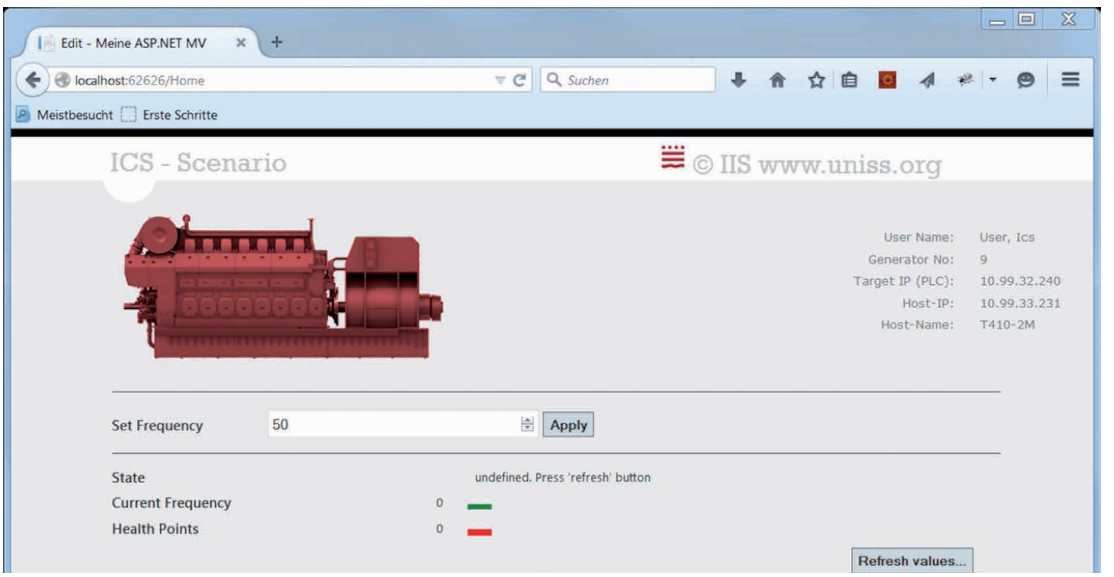

Figure 1 The Human Machine Interface, realised as a web application and hosted on a Windows 2008R2 server

approximately 16 people in total – teamed up as one of the Blue Teams: Blue Team 03 (BT03). The innovations of Locked Shields 2015 included active defence and a SCADA/ICS element implemented as power generator to support the drone command centre. A subteam of Blue Team 03 was responsible for this new SCADA/ICS element and had to implement technical countermeasures to mitigate attacks from Red Team on a power generator. The approach and results are described in the next paragraphs.

SCADA/ICS in the Exercise Scenario

SCADA/ICS systems are used to control and monitor hardware components commonly found in an industrial environment, for example, in a power plant.[15] In Locked Shields 2015 every Blue Team was responsible for the cyber defence of a simulated power generator. A real – not simulated – Programmable Logic Controller (PLC) controlled this. Managing the power generator by means of the PLC was achieved by using a Human Machine Interface (HMI). On the HMI it was possible to set the frequency of the power generator and see the health in the form of Health Points, which was used for scoring in the exercise. The HMI was realised as a web application (figure 1) and hosted on a Windows 2008R2 server.

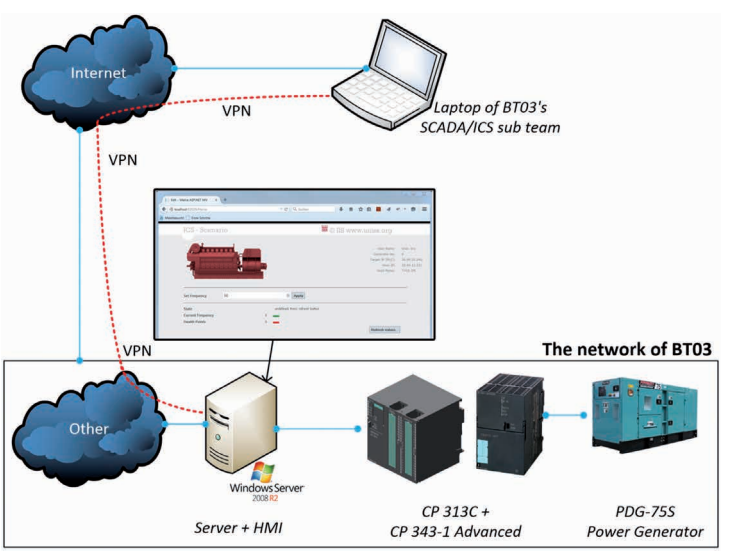

Figure 2 A simplified representation of Blue Team 03's network during Locked Shields 2015

Figure 2 shows a simplified representation of Blue Team 03's network during the exercise, with the SCADA/ICS part elaborated.

15 B. Galloway and G.P. Hankce, 'Introduction to Industrial Control Networks', in: *IEEE Communications Surveys & Tutorials* (2012) (15) 1.

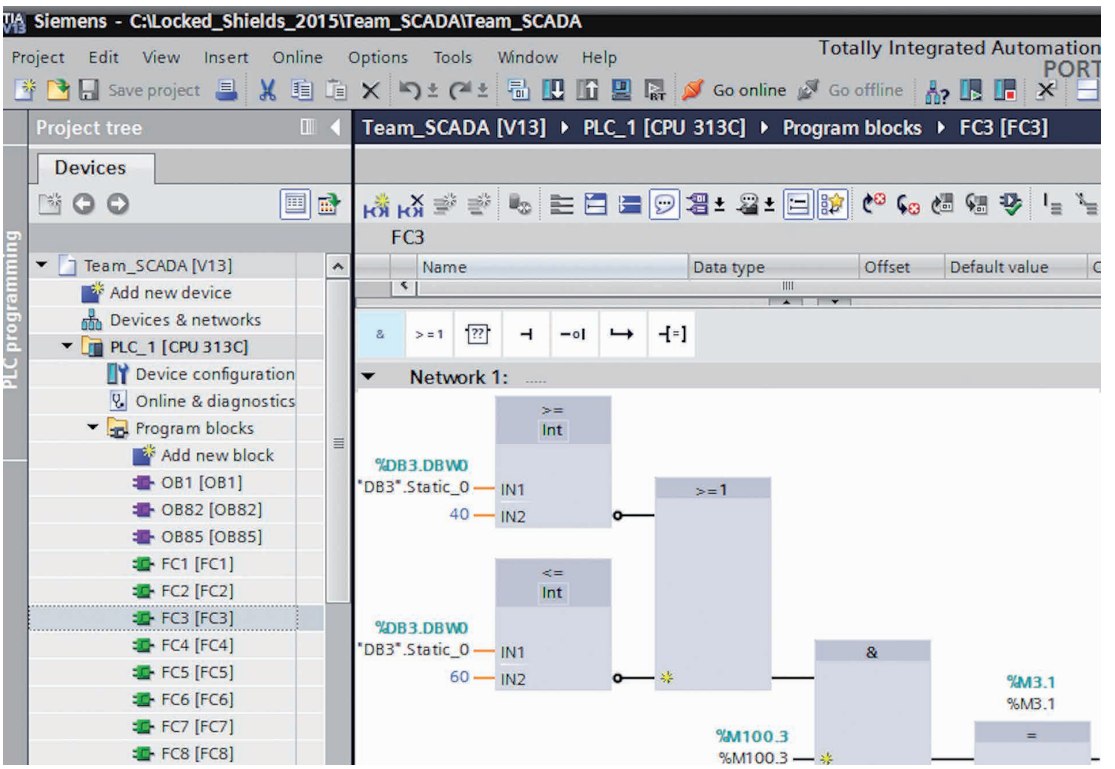

Figure 3 The amount of Health Points of the power generator was one of the areas where the subteam could score points for Blue Team 03

The Windows 2008R2 server hosted the web application and was connected to the rest of the network ('other'). First, input values in the Human Machine Interface were sent to the PLC, which consisted of a SIEMENS CP 313C and a SIEMENS CP 343-1 Advanced module. Then, the PLC processed the inputs from the Human Machine Interface and controlled the simulated power generator. The power generator shown in figure 3 is a PDG-75S Power Generator and is used here for illustration purposes. The part with the remote laptop and the Virtual Private Network (VPN)[16] connection will be explained later.

The subteam could score points for Blue Team 03 in two areas: the amount of Health Points of the power generator and the availability of the Windows 2008R2 server. The more Health Points the power generator would have at the end of the exercise, the more points Blue Team 03 would score. The power generator started with an initial value of 100 Health Points. The generator's safe operating frequency range was 40 Hz to 60 Hz. With the Human Machine Interface it was possible to change the operating frequency within those limits. Obviously, Red Team would focus on changing this frequency to a value outside the safe range. If they succeeded in manipulating the generator by having it operating at a wrong frequency, for example 100 Hz, the power generator would malfunction and HP's would be lost. At the Windows 2008R2 server, scoring relied on preserving availability for several functionalities, like access to Human Machine Interface and Remote Desktop. Every time an availability check was performed, points would be scored if the functionalities were up and running.

Risks and vulnerabilities

To protect the Windows 2008R2 server, the PLC and thus the power generator, it was necessary

16 A method to build a private and potentially trusted network over a Wide Area Network (Internet).

to map the risks[17] and the vulnerabilities[18] of the soft- and hardware. A first security scan revealed that the Windows 2008R2 server contained several vulnerabilities (4 critical, 51 high, 35 medium and 3 low), because important patches had not been installed. Also, malware and backdoors[19] were present on the system. Secondly, the PLC was not password protected, yielding to manipulation of the firmware. Finally, the web application did not have any vulnerability at first sight and blocked values outside the range of 40 to 60 Hz by validating the user input. Being aware of most of the risks and vulnerabilities, the next step was to develop and implement defensive countermeasures.

Countermeasures

In the SCADA/ICS scenario it was possible to implement multiple layers of security by securing the PLC itself and the Windows 2008R2 server. Since we discovered the PLC was not password protected, we gained full control over it. The possibility presented itself to retrieve the power generator firmware from the PLC and modify it, so values outside the range of 40 to 60 Hz were not accepted by the PLC. This could be the solution, because even if Red Team compromised the Windows 2008R2 server and dangerous frequencies were sent to the power generator, the PLC would not accept these and the power generator should keep functioning.

To implement this countermeasure, a new VPN connection was made between a remote laptop and the server (see figure 2). A commercially available PLC toolkit installed on the laptop could reach the PLC and read its firmware. It displayed the firmware in human readable and understandable form by representing it visually with blocks as shown in figure 3. It turned out that instead of 15 PLC's – one for each Blue Team – just one PLC was present. This single PLC simulated all the power generators for each Blue Team, which can be seen on the left in figure 3 (FC1, FC2, et cetera). Furthermore figure 3 shows one of the networks ('Network 1:') found in the PLC with the toolkit, which is responsible for the HP's of the power generator of Blue Team 03. Adding specific blocks to this network assures that any value outside the frequency limits is converted to either 40 Hz or 60 Hz. With this solution, no HP's could be lost and the power generator was protected.

Another step taken was to harden the Windows 2008R2 server against cyber attacks. Several patches were installed, dealing with the most critical vulnerabilities in the operating system. Identified malware and backdoors were removed and an anti-virus client was installed. Also, a basic concept of a SCADA/ICS Intrusion Detection System (IDS), built in Python,[20] was developed and implemented. With this Intrusion Detection System it was possible to monitor network traffic to the PLC and automate the detection of hacking attempts on the network. If values were sent to the PLC on the system where the Human Machine Interface is located, the Intrusion Detection System would detect and display these, even when the original installed Human Machine Interface software was bypassed. Therefore, the Intrusion Detection System contributed to a better Situational Awareness (SA) by monitoring traffic. As stated bij Etalle et alteri, there is a great need of monitoring SCADA/ICS systems, 'because a malfunction in any of these systems might cause the entire industrial process to fail.'[21] In the scenario of Locked Shields 2015, a power generator failure implies the breakdown of a critical functionality, disrupting the ability to do missions with available drones.

Aftermath

With the modification to the PLC firmware, the SCADA/ICS scenario in Locked Shields 2015 was protected for Blue Team 03 (see the internal news item in figure 4).

17 In this article risks are defined as the possible ways of losing control over a system.
18 In this article vulnerabilities are defined as flaws in software, which lead to an exploitable system.
19 Malicious code on a compromised system, which allows adversaries to gain unauthorised and covert access.
20 Python is a widely used open-source programming language.
21 S. Etalle, C. Gregory, D. Bolzoni, E. Zambon and D. Trivellato, 'Monitoring Industrial Control Systems to improve operations and security', (2013) 2, retrieved from: http://secmatters.com/sites/www.secmatters.com/files/documents/whitepaper_monitoring_EU.pdf.

News *Just another WordPress site*

Blue team 3 corrects a risk of manipulation on all teams' ICS/SCADA systems – "They taught us a lesson"

BY EDITOR · APRIL 23, 2015

This is a view of the green team's IP camera monitoring the PLC in Karlsruhe, Germany.

One of the blue teams participating the Locked Shields 2015 cyber defense exercise was about to nullify a number of attacks on all teams' simulated ICS/SCADA systems, presumably with good intentions to help all teams protect themselves better.

The simulated power generators of all 16 blue teams on the Locked Shields 2015 exercise are ran via a single PLC (Programmable Logic Controller), which is located in Karlsruhe, Germany. There are also two extra generators, which are for the red team's testing purposes. The green team in Tallinn, Estonia is following the situation on the PLC via an screen of an IP camera in front of the PLC.

Figure 4 With the modification to the PLC firmware, the SCADA/ICS scenario in Locked Shields 2015 was protected for Blue Team 03

For Red Team, it was impossible to take out the power generator, since they were not allowed to modify the firmware of the PLC. However, Blue Teams were not allowed to modify the PLC either, but this was not communicated. Therefore, the modifications made in the PLC firmware were maintained only for Blue Team 03 by CCDCOE, the organisers of the exercise. On the other hand, Red Team did succeed in taking over the Windows 2008R2 server, allowing them to change the administrator password. Without this new password our access to the server was denied. We suspect they performed a Man-in-the-Middle Attack (MitM). Without going into too much detail, the adversary was able to wiretap and modify the communication between the server and our client laptop, which we used for remote connection. Because of a known vulnerability in the version of the Remote Desktop Protocol we used, it was possible for an attacker to take over our Remote Desktop session and give commands to the server with our Administrator credentials. However, while we did not have any control on the server anymore, we still had full control over the PLC, because Red Team did not disable the VPN connection from the remote laptop to the server (see figure 3). Luckily, the required functionalities for scoring points were also not turned off by the Red Team. In conclusion, the power generator was completely protected with the change in the PLC firmware and kept its 100 Health Points. The Windows 2008R2 server was eventually taken over, but points were still scored for the availability, since Red Team did not attack those services.

Blue Team 03, consisting of members of the German Bundeswehr and the Dutch DefCERT, gained 10th place overall in Locked Shields 2015. With the forensic challenge, a separate part in the exercise, 3rd place was obtained. The world's largest cyber exercise was informative and generated many lessons learned.

Future Research

In Locked Shields 2015 it was relatively easy to protect the simulated power generator. However, protecting real SCADA/ICS systems is much more complicated and failure will have much bigger consequences. First, if a PLC of a power plant controlling a real power generator is overtaken, serious damage could be done. Not only the power generator itself could be destroyed, but critical infrastructure depending on this power generator would also not be functioning for a while due to a lack of supplied energy.

A power blackout in March 2015 in the Netherlands for example caused big problems and serious financial damages to a wide spectrum of services that are deeply integrated in modern life, like mobile providers and the public broadcast system. The temperature of a data centre rose too high, forcing all servers to be

PHOTO NATO CCDCOE

Locked Shields is an innovative and competetive exercise, where teams are ranked on a scoreboard that produces live feedback

shut down. This was caused by drained backup power sources, which were responsible for the backup cooling. Chemical plants switched to a special safety-mode and had to flare excessive gas. People were stuck in elevators and public transport and flights were cancelled.

Secondly, in the scenario of Locked Shields 2015, only one variable – the operating frequency – was taken into account. However, a real power plant has a lot more important variables and their behaviour in complex dynamic systems can be unclear. Therefore, it is much harder to defend real SCADA/ICS. One approach to protect those systems is to further develop the Intrusion Detection System, which is quite a challenge since most SCADA/ICS systems use complex proprietary protocols,[22] which need to be understood first.

Thirdly, another challenge is dealing with the semantics of the physical process. For example, a variable sent to a PLC can be in a safe range. But what if operating with that specific variable over an extended time period can be harmful to a system? How can that be detected? As an example, we will describe a real identified problem of a sluice with lock gates. When the gates are opened water is levelled and ships can sail in and out. However, the sluice walls show signs of erosion or overpressure caused by a very strong current. Keeping the time the gates are opened to a minimum mitigates this problem. The sluice controls the process of opening and closing the lock gates with a PLC. When an attacker is in control of the PLC and discovers the details of the physical process of opening and closing the gates, he will be able to manipulate this process.
One way to sabotage the system would be to keep the doors open much longer than necessary, allowing the strong flow to damage the walls, eventually leading to an unusable sluice. So, even if a value is in the safe range of a PLC, maintaining it too long can have serious consequences. One kind of technique used in Intrusion Detection Systems is anomaly-based

22 A proprietary protocol is owned by a company and is not open-source.

detection. An Intrusion Detection System could be trained to understand the normal behaviour of the process and would know how long the lock gates normally would be open. When an attacker keeps its modifications in the safe range of the PLC, the IDS will not be triggered. But when it detects strange behaviour because the locked gates are opened longer than it has initially learned, it will warn for possible hack or sabotage attempts and more damage could be prevented.

While most research is done on synthetic data[23] sets we conduct our research using inputs from at least 3 real SCADA/ICS facilities with different functionalities. Nowadays, most research uses static models for time agnostic validation. These models are unaware of time; they only look at the current state and not at its duration. For the aforementioned timing-based attacks, like the sluice, more research is needed on the semantics of the physical process. By using real input from a facility new methods and techniques can be validated to detect, defend and respond to attacks on SCADA/ICS systems.

Conclusion

Operators have the ability to use – from their perspective – normal functionalities to control a cyber-physical system. However, the same functionalities that are integrated in cyber-physical systems can be exploited to perform potentially damaging activities. In Locked Shields the goal of the Red Team was to set the operating frequency outside its safe range, resulting in a damaged power generator and loss of electricity needed for drone-based operations. We suggest preventing, whenever possible, the ability for an attacker to set any unsafe value like a too high frequency.
We only had to take care of the frequency variable in the Locked Shields scenario. In real systems hundreds or thousands of variables can be found and this makes protecting them more complex and it demands good coordination with the process experts of the specific Cyber-Physical System. To protect a specific variable by limiting its range can only be done when all consequences are known, which is difficult in complex Cyber-Physical Systems.
We suggest focusing on detection of an attack or attempt of sabotage before doing automatic protection or intrusion prevention. The Intrusion Detection System first needs to be trained with the normal behavior of the Cyber-Physical System. After the training period, the IDS will signal an alarm when some activity behaves different. It is possible this behaviour is normal for the operators and they acknowledge the alarm as a false positive. The output of all these acknowledges can be used to train the Intrusion Detection System so less false positive alarms are generated. In the case of a true positive alarm, it would be interesting to put effort into automatically protecting against the attack, for example, by setting hard limits in the design that are impossible to override.
The exercise gave us an opportunity to test and improve our skills. We experienced the importance of an Intrusion Detection System based on anomaly detection. The attackers in Locked Shields penetrated deep in the network despite of all countermeasures. Even when a Cyber-Physical System has no permanent connection with the office network or the internet, a so called air-gap, it can be attacked, like the Uranium Enrichment Facility in Iran.[24] The air-gap helps, but is by no means the solution for perfect security. We suggest to assume an attacker is already inside your networks despite all countermeasures like anti-virus, security patch efforts, firewalls and air-gaps. With a trained Intrusion Detection System based on behaviour, an attacker can be detected even when he uses previously unknown attacks, so-called zero days. Such a system gives the defender the important ability to kill the attack chain[25] in an early attack phase.[26] ■

23 Data that doesn't originate from real world objects, but is artificially created for research.

24 R. Langner, 'Stuxnet: Dissecting a cyberwarfare weapon', in: *IEEE Security Privacy*, vol. 9, no. 3, (2011) 49–51.

25 E.M. Hutchins, M.J. Cloppert and R.M. Amin, 'Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains', in: *6th International Conference on Information Warfare and Security* (2011).

26 M. Krotofil, A. Cardenas, J. Larsen and D. Gollmann, 'Vulnerabilities of cyber-physical systems to stale data - Determining the optimal time to launch attacks', in: *International Journal of Critical Infrastructure Protection* (2014) (7) 213-232.