#04 MARCH 2019

PUBLISHED BY Secura

SecurAware

INSIGHT

Red Teaming in ICS/SCADA Environments

EVENT

Black Hat Sessions 2019: Protecting Your Critical Systems

REFERENCE CASE

Rob de Lange, CISO at Water Board WDO Delta

NEWS

Launch of Secura IoT Security Lab

RECENT HACKS

Data Leaks and Ethics

INTERVIEW

Ali Abbasi, Post-Doctoral Researcher at the Chair for System Security of Ruhr-University

DIRK JAN VAN DEN HEUVEL, MANAGING DIRECTOR

Cyber-physical security: a challenging domain

In the 80s we had PCs without internet. Since the middle of the 90s these got connected to the internet. At the start of this century, we progressed to cloud applications. Nowadays we speak a lot of the 'Internet of Things' (IoT). Sensors, cameras, robots: everything is connected to the internet. For instance in smart homes, smart cars, manufacturing processes (Industry 4.0) and medical devices.

Security followed a similar path. First we spoke a lot about Network Security (protect the outside and keep the intruder out!) and End-Point Protection. Application Security and Software Security followed it (because we cannot keep intruders out).
The next wave is cyber-physical security. We see it popping up everywhere: in the world of IoT devices, embedded software and Industrial Control Systems (ICS). In this domain the cyber world controls the physical world and vice versa.

The attack surface of cyber physical systems usually differs from traditional IT systems:

- The entry into a smart car could be through the mobile app (linked to the car); or it could be through the infotainment system of a car (with a proprietary OS); or it could be through the CANbus (which connects most controllers in the car). The risk is obvious. Cars are becoming more autonomous and need protection against cyber criminals.

- The entry into a smart building could be through the Smart TV; or the alarm system; or the thermostat; or the wireless router.

- Medical devices may contain all kinds of special hardware and embedded software. Up until now security didn't receive sufficient priority in these systems. Do we allow hackers to win this battle? Of course not! This risk needs to be reduced. We need to study and test the hardware, embedded software and related software (like cloud apps and mobile apps).

- Utility companies (energy sector) and chemical plants use Operational Technology (OT) consisting of Industrial Control Systems (ICS) using Programmable Logic Controllers (PLCs) and SCADA technology. Most of this OT was not designed for remote connectivity. The attack surface of OT systems usually differs quite a lot from IT systems. That's why we offer services like Threat Modeling to these kind of clients.

- Similar holds for tunnels, bridges and airport control systems in the government domain.

To summarize: We see the cyber world connecting more and more to the physical world. Also to (very) critical systems and processes. That's why Secura now (also) focusses on the world of IoT, embedded and cyber-physical security. We help you to take control of your digital security.

In this issue you can read about the launch of our Secura IoT Security Lab. You can read about the Black Hat Sessions about Protecting your Critical Systems (June 13 in Nieuwegein). Some of the presentations will focus on the cyber-physical world. You are most welcome to come and hear about these latest trends.

I hope you enjoy reading this SecurAware. We value your opinion and feedback on this magazine, our cyber-physical focus and on us as a company.

Enjoy reading!

Dirk Jan van den Heuvel
Managing Director

NEWS

Expanding Amsterdam Office

In November 2017 we opened our Amsterdam office. Since then we have grown rapidly. Secura welcomed many new employees and we required more meeting space for customer visits. **As of March 15, 2019 we are doubling our office space and have the full 1st floor in The Yard (Karspeldreef 8 in Amsterdam).** Thank you for your trust in Secura. This allows us to grow and be an even stronger partner for all your security needs.

AGENDA

TestingStage
29-30 March 2019 | Kiev, UA

https://testingstage.com/en

TestingStage is an Ukrainian industry conference for professionals in the areas of test automation & management, performance, security and embedded systems. In his talk, Jos Wetzels, Principal Consultant and Security Researcher at Secura aims to present a big picture introduction to the security issues facing connected embedded systems.

Risk Event 2019 – ISACA NL Chapter
11 April 2019 | Amsterdam, NL

https://www.aanmelder.nl/risk-event-2019

On Thursday 11 April 2019, the second IT Risk Event of ISACA, NOREA, PvIB, IIA, KNVI, ISC2 and SSA will take place, with a wide variety of speakers and various main streams. We are happy to meet you there.

Secura Joins IoT Security Foundation

To enhance its commitment towards the improvement of IoT security, **Secura joined the IoT Security Foundation**, one of the leading international security organizations. The IoT Security Foundation Framework and associated certification program fit perfectly in the range of services of our Secura IoT Security Lab. Under this dedicated lab, the security of products from multiple industry domains (consumer, medical, industrial systems, automotive, payments, telecom) can assessed.

We are happy and proud to support you towards a more secure, connected world! More insights on the IoT Security Framework and our IoT Security Lab, can be found in this SecurAware.

IoT Security Foundation

WE'RE CONNECTED

BHS

Black Hat Sessions 2019

13 June 2019 | Nieuwegein, NL

https://www.blackhatsessions.com

REGISTER NOW

Black Hat Sessions (BHS) is Secura's annual security conference where you will be informed about the latest trends, threats and solutions in the world of digital security.

The theme for this year's BHS is: Protecting your Critical Systems. Cyber hacks are in the news every day. We all know about the relevance of digital security. But how to protect ourselves? Get inspired by our speakers on how they deal with their challenges. There will be several tracks in the conference, and this year, we have more technical speakers than last editions. The day-long programme consists of technical sessions, managerial topics, keynotes, case studies, workshops and a student Capture the Flag (CTF). Please see the attached flyer for more information.

Save the date, register to reserve your seat and keep an eye out for more news about the speaker line-up.

Relations of Secura will only pay 240 euro instead of 320 euro excl. VAT until April 20, 2019. To do this, use the code **VisitBHS19#** in your online registration.

COLOFON

Contributors
Ali Abbasi
Floris Duvekot
Mentor Emurlai
Dirk Jan van den Heuvel
Erwin Jansen
Rob de Lange
Ralph Moonen
Maayke van Remmen
Razvan Venter
Jos Wetzels

Art director
Jacqueline Bayot/
Studio Novi

Contact
editorial@secura.com

Secura B.V.
Vestdijk 59
5611 CA Eindhoven
Netherlands

Karspeldreef 8
1101 CJ Amsterdam
Netherlands

T +31 (0)40 23 77 990
E info@secura.com
W www.secura.com

Follow us on

Maayke van Remmen & Floris Duvekot

The Biggest Challenge is the Human Factor

© Water Board WDO Delta

Interview with Rob de Lange, CISO at Water Board WDO Delta & Tactical Manager CERT-WM at ‘Het Waterschapshuis’.

The Water Board WDO Delta (WDO Delta) established in Zwolle was formed on the 1st of January 2016 when two regional water boards, ‘Reest & Wieden’ and ‘Groot Salland’, in the Provinces Overijssel and Drenthe merged.

What is the prime task of WDO Delta?

WDO Delta is responsible for protecting a northern part of the Netherlands against high floods, providing a proper functional regional water system and for water purification of sewage.

Your job title is CISO at WDO Delta. What does this job require?

I am an information security advisor with the function of CISO (Corporate Information Security Officer). It is my task to ensure that the water board implements information security norms and standards to ensure that our information is protected and we comply with: for example, the Dutch Baseline Information Security Standard for governmental organizations.

How does WDO Delta cooperate with other water boards?

All water boards work actively together, they organize regular meetings to discuss current and possible challenges and solutions we face. Next to our regular meetings we contribute to the Information Sharing and Analysis Centre (ISAC) ‘Keren and Beheren’ (K&B) where cyber security and information sharing is discussed at a strategical/ tactical level.

What role does Het Waterschaphuis play in the cooperation between other water boards?

Het Waterschapshuis provides direction and implementation advice for the 21 Dutch water boards on the subject of information and communication technology. They stimulate cooperation between water boards and other government organizations who are active in the water sector.

Formally, I work for Het Waterschapshuis to manage a CERT (CERT-WM); the so-called ‘Computer Emergency Response Team Watermanagement’ that was established in 2017. The water boards provide employees to the CERT-WM, which is part of the Security Operation Center (SOC) of Rijkswaterstaat. By establishing the CERT-WM we have, one could say, created a digital fire brigade which ensures that we are better prepared for the future.

Which standard frameworks are relevant for water boards?

All water boards must of course comply with the new privacy regulation, such as the general data protection regulation (GDPR). On top of that, we maintain our own information security standards that are customized for water boards. Previously, this was the Baseline

Information Security Water Board (BIWA). With the introduction of the BIO (the Dutch public authorities) in 2019 that standard was replaced. 2019 will be the transition year. From the 1st of January 2020 the BIO will apply to all water boards in the Netherlands.

Because ICS/SCADA systems are insufficient as mentioned in this baseline, the water boards have adapted the IEC62443 as additional norm.

What will change with the introduction of the BIO?

The BIO was developed in cooperation between the national government, municipalities and water boards. A standard framework for information security is important to ensure that the vital governmental infrastructure will have a solid level of information security. The responsibility to achieve a solid level of information security within the governmental sector is a multi-partner shared responsibility. A standard frame that is widely supported helps to achieve a solid level of information security. In the meantime, we have taken all necessary measures at WDO Delta.

The BIWA and BIO are both additions on the ISA27000X standard. However, an important difference is that the BIO defines security levels. The water boards have agreed to comply with level 2 (out of in total 3 levels) as basic security level. By performing risk assessments on internal projects, we are able to scale up the security level if necessary.

What are the biggest challenges for WDO Delta concerning digital security?

The biggest challenge is the human factor. Every water board knows how to build dikes and how to secure the ICS/SCADA environment. However, if a social engineer physically figures out how to break into our systems, we have a problem. Until now, the market has spent a lot of attention updating the technical part of security. However, the human part of information security needs a lot of attention as well. Luckily, we see a turnaround in the market. We are becoming a more information-guided organization, which makes the sense of urgency more relevant.

The dependency on information is part of the digital transformation. This requires a change in management, but also a change in the basic skills of our employees. The knowledge and skills have to be guaranteed by the employees of the water board and everyone must be aware of their individual responsibility. In the ideal situation employees will understand how to adequately handle security incidents. To achieve that goal, awareness is the first step as handling according to the standards and is currently the biggest challenge for our employees.

Drents Overijsselse Delta
uw waterschap

What do you do to keep the risks under control?

Influencing attitude and behavior involves an understanding of psychology; this is in most cases not a part of the discipline of a CISO. On top of that we employ a large group of people; 625 FTE with different backgrounds and interests.

To incorporate this 'culture change' we need external expertise. That is why we started with the SAFE program of Secura on the 14th of February. The goal of this program is to stimulate learning and provide our employees with basic knowledge about information security. During the program, Secura gauges the level of awareness and checks if the results improve. We do not only focus on awareness, as the most important factor is changing the actual behavior. However, when employees are informed about the implications of security incidents it will be easier to implement technical measurements in the future.

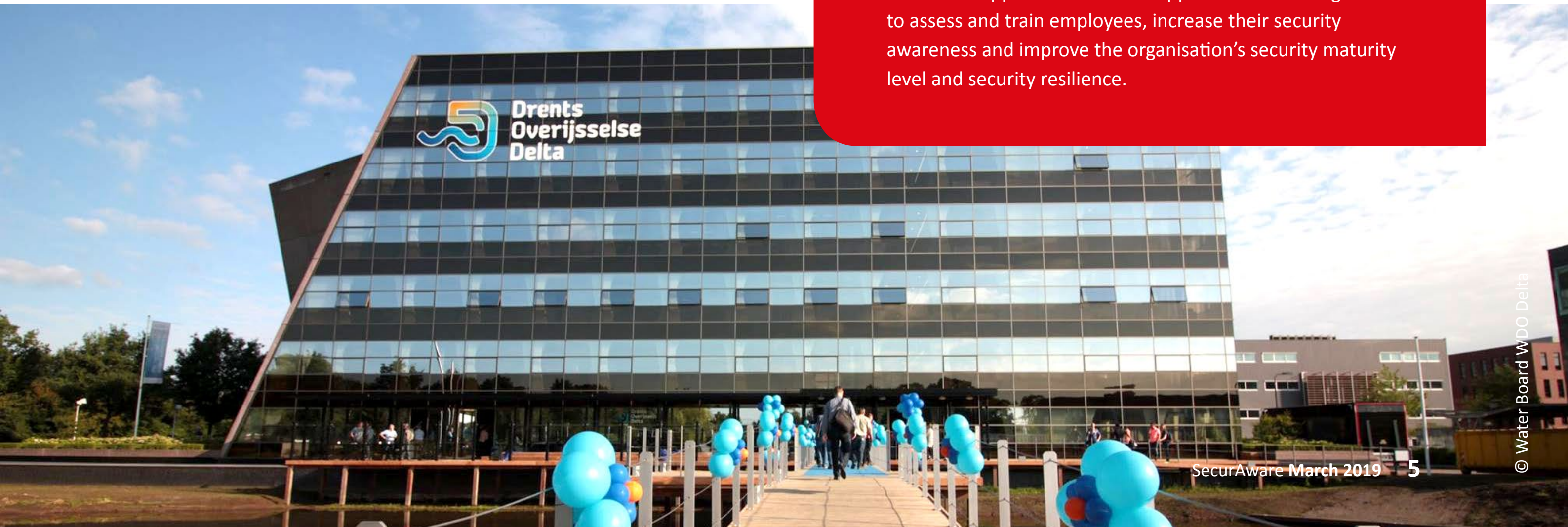
What are your experiences with Secura?

Our cooperation with Secura goes back to the time of 'Madison Gurkha'. With the transition of Madison Gurkha to Secura and the addition of certain expertise to the current package of digital security, our cooperation has become more intense. Secura understands what we want and has developed a product that fits our needs. By supplying awareness and education programs like SAFE we can finely influence attitude and behavior of our employees.

SAFE WDO DELTA & SECURA

Water Board Reest and Wieden and Secura joined forces in 2012. Collaboration continued after the merger in 2016 into WDO Delta. In 2018 the SAFE program was initiated. SAFE is an acronym for: Security Awareness For Everyone and aims at strengthening the information security culture of WDO Delta.

SAFE is a 2-year long program targeting people, processes and technology. It uses an holistic view and helps the organisation by providing continuous focus on information security. SAFE consists of assessment and education. The program employs social engineering, phishing, employee surveys, road shows, demo's, classroom training, eLearning and other elements in structured approach. This SAFE approach enables organisations to assess and train employees, increase their security awareness and improve the organisation's security maturity level and security resilience.



© Water Board WDO Delta

Razvan Venter & Mentor Emurlai

Standardizing IoT Security: The Secura IoT Security Framework

The Internet of Things (IoT) is one of the most encompassing terms in the current day. IoT comprises a wide variety of domains such as critical infrastructures, healthcare, transport, retail, smart buildings and consumer products. By the year 2008, there were already more IoT devices connected to the Internet than humans. It is estimated that there will be over 20 billion IoT devices in 2020 and over 50 billion IoT devices in 2050. The consumers accounted for a majority (62%) of the total IoT devices in 2017. IoT makes life a lot easier by introducing devices such as smart- thermostats, lights, door locks, alarm systems and doorbells inside the home environment. IoT opens doors to many opportunities, but also to many security challenges, as these devices are now connected to the Internet and to each other.

It is safe to say that IoT is growing faster than the ability to defend it. The lagging development of IoT security can partially be ascribed due to the lack of existing regulations and commonly recognized standards. This has led to manufacturers being responsible for equipping their 'off-the-shelfproducts' with the appropriate levels of security. Manufacturers, on the other hand, have a hard time defining what security features to integrate into their product, ensuring sufficient security implementation. The enforcement of regulations and certifications for IoT would ensure that manufacturers of IoT are obliged to incorporate sufficient security measures in their products. In the absence of such regulations or certification programs, manufacturers can and should make use of internationally recognized standards for guiding their design processes.

Two important benefits of internationally recognized standards are:

- They provide for a confirmed and state of the art view on IoT Security
- They are recognized and acknowledged on both national and international level, thus providing for a common language for debate, comparison and align

> "IoT is growing faster than the ability to defend it.

Current situation and key challenges

Currently there are many standards, frameworks, guidelines and best practices publications addressing the security of IoT products and services. Although there is some degree of convergence towards baseline IoT security specifications across various relevant publications, there are also considerable differences between them. These differences can be seen especially from a requirements maturity perspective, as well as from a practical applicability point of view. The OWASP IoT Testing Guide for example, provides clear testing scenarios compared to other publications, which are more general, offering more flexibility such as the IoT Security Compliance Framework.

For this reason, we believe key challenges in the standardization of IoT security can be organized around two topics:

- The difficulty of setting a Security Baseline for IoT security across the entire IoT consumer domain, due to publications fragmentation
- The difficulty of adopting existing IoT security publications, as support for the design processes

Secura identified the IoT security publications fragmentation issue while keeping a close eye on the recent developments regarding IoT security regulations, standards and certification schemes. Considering that there are multiple publications available, it makes it hard to choose a "winner", as this might leave out important aspects provided by others. Each publication has its own strengths that can be leveraged. For this reason, Secura focused on developing a "Unified IoT Security Assessment Framework", by relying on several existing publications and bridging the gaps between them.

Towards a Unified IoT Security Assessment Framework

In the process of developing the proprietary Framework, a systematic approach was undertaken to ensure the quality and usefulness of the Framework in performing IoT security assessments. The whole process of developing the Framework was documented to enable traceability for each of the requirements and in order to allow future expansion. The research that was performed started by identifying a subset of internationally recognized IoT security publications:

- IoT Security Compliance Framework by IoT SF
- GSMA IoT Guidelines
- OWASP IoT Testing Guidelines
- ISA/IEC 62444
- ENISA Baseline Requirements
- DHS IoT Principles
- BITAG IoT Security and Privacy Recommendations
- OTA IoT Trust Framework

The above publications were analyzed based on aspects such as practical applicability, international recognition and state of the art. Not only did we perform analysis based on industry factors, but also from an academic point of view establishing their completeness. The analysis resulted in the selection of four publications, for the first version of the Unified Framework:

- The IoT Security Compliance Framework by the IoT Security Foundation
- GSMA IoT Guidelines
- ISA/IEC 62443
- OWASP IoT Testing Guide

The security requirements from the selected publications were further extracted and overlapped with the aim of creating a concrete, single set of requirements, thus getting closer to the desired baseline. The resulted requirements were provided with additional guidance and explanations as well as priority classes, based on the specific risks that they are addressing. The Unified Framework provides for a clear testing methodology, based on which Secura currently executes IoT Security Assessments. The Framework consists of 14 categories, split into product-related categories and process-related categories. Examples of product-related categories include physical security, wired and wireless interfaces, authentication or authorization. Examples of process-related requirements are business security processes, privacy or device ownership transfer.

Using the Unified IoT Security Assessment Framework

The configurability of the framework allows for the selection of a defined set of requirements by applying filters. By this means, the Framework can be tailored based on the necessities of the client. Additionally, we defined several “assessment packages” which address topics such as physical security, communications, software/applications and secure OS. In light of newly publicized national initiatives concerning IoT security, we have been able to map the requirements of the Unified Framework to publications such as the UK Code of Practice for Consumer IoT Security and NIST-IR 8228.

The IoT Security Assessment Framework represents a tool which will enable Secura to deliver efficient, complete and customer-tailored IoT security assessments, under the umbrella of the newly released Secura IoT Security Lab.

Maayke van Remmen

Interview with Ali Abbasi

Ali Abbasi is a Post-Doctoral researcher at the Chair for System Security of Ruhr-University Bochum, Germany. During the Black Hat Sessions on June 13th he will give a technical presentation on the binary security of embedded control systems: An Industrial Control System Protection Approach. In this (technical) interview, Ali shines light on the questions we asked him in the run-up to the conference.

What project/research are you currently working on?

I am currently involved in three different research projects. In the first research, we are trying to bring coverage-guided fuzzing to embedded control devices. I am also involved in a project related to finding hidden engineering (or backdoors) in Programmable Logic Controllers (PLCs). Finally, I am involved in a project for data-flow integrity for real-time embedded systems.

What real (world) challenges are you trying to address with your research?

I think we can agree that the security ecosystems in both industrial control system domain and especially in embedded control devices are falling behind when compared to general-purpose computers. To be more specific, in general-purpose computer domain we have various security mitigations, more advanced vulnerability discovery techniques and tools. In contrast, we do not have these kinds of mitigations or techniques in embedded control devices domain. These issues alone might not seem problematic, but when we consider this situation in the context of increased exposure of these devices to the internet (e.g., IIoT), then we suddenly have a different case: a bunch of devices which control the critical infrastructures of nations, connected to the internet which has low hanging fruit vulnerabilities. This is a real-world issue.

To address these multi-dimensional issues during my Ph.D. studies, I was involved in designing more advanced security mechanisms for these devices while considering the environment which they are operating. Additionally, to improve the security of embedded devices in ICS, we need to have better ways to detect and discover vulnerabilities in them. So I am working to address this challenge by creating a framework for fuzzing embedded ICS devices.

What can you tell us about the challenges of hardening COTS embedded systems against the exploitation of memory corruption vulnerabilities, especially systems with real-time requirements as they are found in various safety-critical domains such as automotive or industrial automation?

Generally, designing security mitigation for embedded systems with limited resources is hard, but it is much more challenging when you also consider timelines. The first challenge is an architectural problem: the real-time requirement automatically preempts security in its nature. Therefore, you have the situation where you have a delay on threat detection, and you must accept system compromise over timeliness. It means that in a real-time environment you must consider system compromise as an acceptable outcome (despite detecting the attack). Finally, you can not kill real-time PLC software during the attack and put the operator in a situation where she/he loses control of the cyber-physical process.

The second challenge is how to cope with diversity in the embedded domain. After all, embedded domain with respect to hardware and resources is heterogeneous and thus you can not apply the same security policy in devices with different hardware features. This means that you must design different security policies per different embedded hardware families.

How or why is systems engineering for securing embedded systems different from securing basic IT systems?

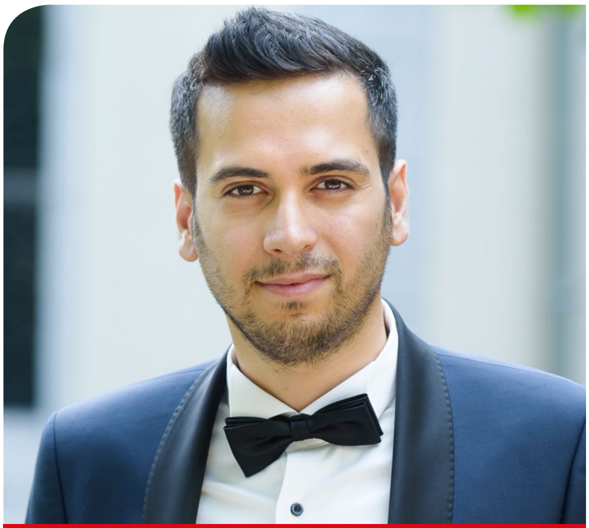
There are so many differences, take for example certification issues. You can not just design a security solution without considering how your design affects already obtained certificates. So for example, if you have an avionic system which has a DO-178B certificate, any major modification to the software means that vendor must reapply for certification, so when designing a new security mechanism you should consider this issue. Other examples which I mentioned earlier are real-time requirement or diversity in hardware. Therefore any solution to secure embedded devices should consider these issues.

What do you think about the future of embedded systems?

In the context of cyber security, I think embedded systems, for a short period, will follow general-purpose computers. This means that security solutions first get introduced in the general-purpose domain and then get adopted to the embedded world. However, this condition will change as more and more hardware-based security features get adopted into high-end embedded systems. Take for example ARM v8.5A memory tagging or ARM v8.3 pointer authentication or ARM CoreSight (equivalant to Intel PT). So we can see that some high-end embedded SoCs reduce the gap or even take over on hardware support for security features.

ICS embedded security is also a keystone of Black Hat Sessions 2019. You will provide a technical presentation at the event. Can you give a glimpse of what you are going to present on the 13th of June?

I am going to talk about how to improve the security of embedded control devices. I'll start by looking at how an attacker can target a plant (regardless of what kind of embedded device being used), I will then discuss existing security solutions for embedded devices and how an attacker can exploit an embedded device without being detected by existing security mitigations. Afterwards, I'll discuss better security solutions for embedded control systems and especially talk about detecting code reuse attacks in such devices. Eventually, I am going to give a glimpse on the challenges of fuzzing embedded control devices and what we can do to address them.



ABOUT ALI ABBASI

Ali is a Post-Doctoral researcher at the Chair for System Security of Ruhr-University Bochum, Germany. His research interests are Embedded Control Systems Binary Security, Real-Time Operating Systems Security and Automotive Security. Ali received a PhD degree from Eindhoven University of Technology, the Netherlands. In Eindhoven he was working at the Security Group on code-reuse defenses for Programable Logic Controllers (PLC). Abbasi also received a MSc in Computer Science from Tsinghua University, Beijing, China in 2013 and a BSc in Industrial Engineering from Mazandaran University of Science and Technology, Iran.

Twitter: @bl4ckic3
Website: http://homepages.rub.de/ali.abbasi-i4q/

> A bunch of devices which control the critical infrastructures of nations, connected to the internet which has low hanging fruit vulnerabilities. This is a real-world issue.

Ralph Moonen

Data Leaks and Ethics

Although data 'leaks' and 'breaches'*[1] have been very common over the past few years, the scale and frequency of very large breaches has increased over the last year or so.

Connected with that, the disclosure of large leaks to the public has also increased, not in the least thanks to the work of the GDI Foundation. This foundation, started by security researcher Victor Gevers, locates vulnerable systems in order to warn the owners. Without active hacking, the foundation searches the internet for vulnerable systems. It then performs OSINT (Open Source Intelligence) research to find out who the vulnerable systems belong to, and works with them to fix the issues.

Finding vulnerable systems on the internet is extremely easy these days due to services such as Shodan.io, censys.io and zoomeye.org. These services scan the internet continuously, performing port scans and gathering information about those systems, whether they are webcams, databases or Industrial Control Systems (ICS). It would be very impractical to research all those systems to warn the owners, so the GDI Foundation is focusing on the 'high impact' targets: databases with huge amounts of data or very sensitive data.

Modern applications often use databases that do not use Structured Query Language (SQL) but rather are a collection of individual records in simple 'name:value' pairs or JSON structures. Such 'NoSQL' databases are often used to store large amounts of data, many times very sensitive data. One type of database in particular is of interest, because it often does not have any authentication configured when installed with the default settings: MongoDB. It also happens to be a very popular database: a search on Shodan reveals 66.009 MongoDB instances reachable on the internet at

[1] We consider a 'leak' to be an unintentional disclosure of confidential data, whereas a 'breach' is the consequence of an act of malice (i.e: hack).

the time of writing. Approximately 35.000 of these are open to the public. You can see for yourself at https://www.shodan.io/report/nlrw9g59. Since it is very easy to find such databases, one should consider all of these compromised: they are hacked, copied and ransomed very soon after appearing on the internet.

Fortunately, most of these open databases are not used at all or only contain fake test data. But once every while a database pops up that grabs the attention. The most recent example is a case that brings up a lot of questions, regarding security, big data, politics, ethics and human rights. In February 2019, an open MongoDB instance was found in China, in the Xinjiang region. This region is controversial to the Chinese because the native Uygur population is mostly Muslim and the Chinese government is known for human rights violations of the Uygur. Upon some further inspection, the database (owned by a company called SenseNets) appeared to contain data of over 2.5 million people, from various ethnic groups. SenseNets make artificial intelligence-based security software systems for face recognition, crowd analysis, and personal verification.

The data in the database concerned personal information like ID card number, issue and expiration date, sex, nation, address, birthday, photo and employer. But it also contained location information: when was this person last seen walking past a 'tracker'. It turns out that a large number of cameras including those at police stations, are enrolled in a facial recognition system, that allows SenseNets to track users whereabouts using these cameras. Given that these include cameras apparently in police stations, the Chinese government would have to be at least cooperating on this project. The trackers are all concentrated in the Xinjiang region, and appear to be focused on tracking Muslim Uygur's movements without their knowledge and consent.

This of course raises some eyebrows, to say the least. Why are these people being tracked? Why did SenseNets put this data on the internet in an unprotected public database? Why does the Chinese government appear to be cooperating with this project? Several obvious but unsavory answers present themselves. But how about the role of the infosec community? What should we do when we find such a thing that shouldn't be on the internet, if it should even exist at all? The GDI Foundation warned SenseNets before the full scope of the database was clear, and SenseNets place a firewall in front of the database. But not before a sample of records was secured to be able to identify the use and location of the 'trackers' (the cameras with facial recognition). Would it have been better, to simply delete the database? Should it have been copied in totality before being firewalled (according to log files, it was already copied by several parties before this leak was disclosed)?

More general: what should be disclosed about systems that run contrary to our democratic values? It could be argued that rogue activism will not help in the long run, but on the other hand the human rights of minorities are difficult to weigh against technicalities such as open databases.

Please join Victor Gevers of the GDI Foundation at our Black Hat Sessions XVII in June, where he will provide more insight into the techniques they use to identify and alert on such huge data leaks and what the possibilities are to incorporate these into a global framework for responsible disclosure.

Jos Wetzels

Red Teaming in ICS/SCADA Environments

Ever since the Stuxnet malware destroyed hundreds of Iranian nuclear enrichment centrifuges in 2009, persistent, targeted attacks on industrial & infrastructure organizations have been on the rise with cyber-induced blackouts hitting the Ukraine power-grid twice and the recent TRITON attack on a Saudi petrochemical facility that could have caused major physical damage. In this article we'll take a look at the nuances of red teaming ICS/SCADA environments in order to test how vulnerable your organisation truly is to such attacks.

The electric grid, water distribution & control, public transportation, oil & gas, nuclear facilities, when talking about the cyber security of such critical systems to people unfamiliar with the subject matter their first response is often "surely these systems are some of the most secure ones out there? Or at the very least air-gapped, right?".

But anyone familiar with the world of ICS cyber security knows the horror stories: increasing connectivity driven by very real operational gains has dissolved the air gap. The systems are insecure by design, patching is rare or doesn't happen at all as per policy, there's little to no network segmentation, improperly configured RDP connections allow for direct access to the ICS networks, Human Machine Interfaces (HMIs) are openly exposed to the internet and easily found with a simple Shodan search and default credentials are everywhere.

Meanwhile, the threats are very real and range from state-sponsored sabotage operations and industrial espionage to extortion, with Alan Paller of SANS calling the ongoing multi-million dollar extortion of utility companies using ICS/SCADA systems "the biggest untold story of the cybercrime industry".

The Need for Red Teaming

However, while ICS security posture is unfortunately all too often still severely lacking, the “Stuxnet days” are increasingly in the rearview mirror and ICS security is being taken more seriously by manufacturers, asset owners and system integrators.

Compliance requirements are a driving force in ICS security and while they are having a positive impact, compliance and real-world robustness are not the same. Compliance doesn’t allow you to evaluate your overall organisational security posture in the event of a real attack by a highly motivated and well-resourced attacker.

While the impact of compliance violations can be serious, as a recent $10 million NERC CIP fine demonstrated, it pales in comparison to the impact of the loss of key trade secrets or an actual process-affecting cyber-attack causing disruptions which might cost millions of dollars per day in lost revenue and materials, idle labor, restart, cleanup and disposal cost and reputational damage. Not to mention the potential impact of attacks actually achieving physical damage to equipment, disruption of critical infrastructure or causing loss of life.

Red teaming begins where compliance ends. It involves the simulation of a skilled, persistent threat actor(s) utilizing realistic adversarial Tactics, Techniques & Procedures (TTPs). These TTPs can be drawn from relevant threat intelligence, as emphasized by the TIBER framework, but can also incorporate tailored in-house methods. Red teaming aids defenders in planning for worst-case scenarios by practicing their detection, mitigation and incident response skills and measuring the actual security effectiveness and organisational responses in the event of a real-world incident.

Unlike a more conventional and narrowly scoped penetration test, a red teaming engagement will involve full spectrum operations against not only technological systems but against the organisation as a whole, including people and processes. It involves everything from physical breaches and compromising wireless networks to social engineering and hacking camera systems, all with the full security stack in place.

ICS/SCADA Red Teaming is Different

For many industrial & infrastructural organisations traditional IT security concerns such as confidentiality, integrity and availability (CIA) take a back seat to process-oriented concerns such as controllability, operability and observability (CO2) and this affects red teaming operations. Understanding and emulating the unique threats faced by ICS/SCADA environments requires a red team to comprehend not only the Operational Technology (OT) landscape involved by also very process-specific risks.

These nuances show up, for example, when determining an organisation’s “crown jewels”. In ICS/SCADA environments these can be as diverse as a Safety Instrumented System (SIS) protecting a particular hazardous part of a process or a Distributed Control System (DCS) database holding proprietary recipes & formulas.

Another example would be the complexities of determining impact, merely showing compromise of a workstation or Programmable Logic Controller (PLC) is often insufficient here. An ICS-oriented red team will have to be able to answer questions such as “what automation protocol does that Intelligent Electronic Device (IED) use? What are the security measures and could I use it to open this or that circuit breaker in order to de-energize a given power line?” or “If I cause a denial-of-service against that PLC, will that prevent the control logic inside from opening a valve in time so that I can cause a tank to overflow?”.

Finally, the sheer size and complexity of ICS/SCADA environments require a red team to possess a highly diverse skillset while allowing for many different avenues of approach. A red team could decide to infiltrate enterprise IT systems through spear phishing and subsequently escalate access to OT networks by pivoting through a compromised historian or breaching a vulnerable firewall. But they could also decide to hack upstream by obtaining physical access to an (often unmanned) remote electrical substation or gas compressor station and hacking into SCADA systems through the Remote Terminal Unit (RTU)’s network access.

Ethics, Safety & Realism

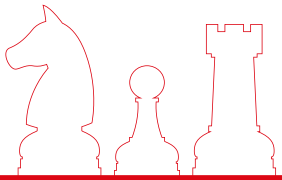
A major concern in ICS/SCADA red teaming is keeping the engagement both safe and realistic. Careless red teaming practices in live ICS/SCADA environments might pose unacceptable operational and safety risks to the process, facility personnel and the red team itself.

A classic example is a simple network scan causing devices to crash due to unstable, untested protocol stacks with undesirable or even dangerous process upsets as a result. Another example would be a red team on a physical access engagement cluelessly wandering into dangerous areas with hazardous fumes, vapors and particles.

Or what to think of a red team breaching a 3rd party contractor or system integrator in order to obtain sensitive Piping & Instrumentation Diagrams (P&IDs), or bribing an insider for remote access to an engineering workstation? But both legal issues and a good ethical code of conduct would prevent the red team from hacking into a non-consenting 3rd party or ensnaring an unknowing employee in illegal activity.

Yet the goal of a red teaming engagement is to simulate a realistic adversary with high risk appetite and little regard for all these matters.

In order to balance these concerns, it is important that the red team plans offensive operations in close cooperation with a white team involving qualified safety personnel. In addition, compensating operations can be planned for those activities where safety & ethical concerns would be overriding. For example, by performing them during maintenance windows or against lab setups and by modeling 3rd party breaches and malicious insiders by having the white team deliver the equivalent information and access to the red team.



INTERESTED IN RED TEAMING?

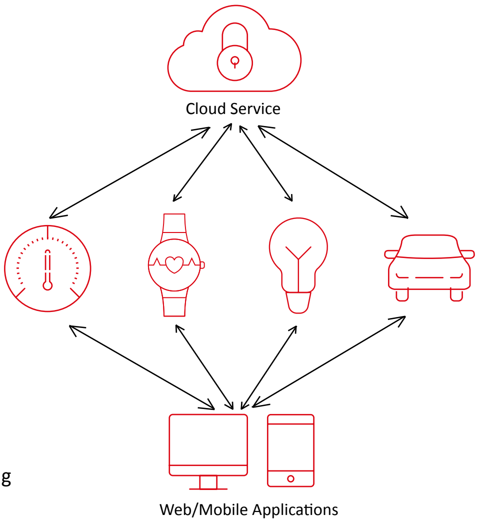
Join our free ICS/SCADA Red Teaming webinar on April 11, 2019.
Register here: secura.com/webinar-ics-scada-red-teaming

Razvan Venter

Launching the Secura IoT Security Lab

View on the IoT Environment

The Internet of Things (IoT) IoT is truly a holistic concept, resulted by the fact that the world becomes more and more connected. The combination of “smart” devices, mobile or web applications used to interact with them and cloud services allowing them connect with each other lead to the development of overlapped IoT ecosystems. Therefore, even if differences in products and solutions can occur across various verticals, by making use of these building blocks, the security of IoT solutions can be addressed in an efficient way.



The Secura IoT Security Lab

Secura has launched the IoT Security Lab, focused on providing an efficient approach on IoT security across various domains. The services provided by the lab are focusing on the IoT building blocks: devices, web/mobile applications and cloud connectivity. For each of these building blocks, Secura is providing a complete and flexible service offering, including:

- Design Reviews and/or Threat Modelling Sessions: Tailored reviews of the specific solution, with highlighting of specific risks and design vulnerabilities
- (Standardized) testing: Assessing the presence and sufficiency of implemented security features, in line with relevant international publications. The testing is performed in a tailored way, by selecting relevant requirements from considered publications.
- Compliance and certification: Ensuring the security by testing in line with the applicable requirements of relevant international publications (ex. IEC 62443, IoT Security Foundation Framework, OWASP Testing Guide, etc.), while also offering support for security certifications or regulations.

SECURA IoT SECURITY LAB SERVICES	VERTICALS (INDUSTRIES)					
Devices & Systems	Consumer IoT	Medical Devices	Industrial Control Systems	Smart Vehicles	Financial and Payments	Telecom
Web/Mobile Apps						
Cloud						

🔴 Testing, Compliance and/or Certification (Industry specific)

⚫ Testing, Compliance and/or Certification (Industry agnostic)

> Even if differences can occur across various verticals, by making use of building blocks, the security of IoT solutions can be addressed in an efficient way.

Industry Specific IoT Security

CONSUMER IoT

Secura can support with security assessments covering many dimensions of the consumer IoT ecosystem. For the individual end-products, design reviews from the early stages of development can be performed on both hardware and software aspects. The security of these products can be assessed in line with internationally recognized publications, ensuring an assessment which takes into account all the various security relevant aspects (ex. Hardware, operating system, applications, interfaces, authentication/authorization, etc.). For such assessments, Secura makes use of an IoT security assessment framework, resulted after overlapping the security requirements of state-of-the-art publications such as the IoT Security Foundation Framework, IEC 62443, OWASP IoT Testing Guide and the GSMA IoT checklist.

MEDICAL DEVICES

Secura can support you with the assessment of medical devices, starting from a design review, and continuing with a standardized security testing, in line with internationally recognized publications (e.g. IEC 62443, UL2900). This ensures that the testing activities carried on the medical device or system are covering the security of the device in a state-of-the-art way. As the same time, Secura can support you with preparing for the FDA or EU medical device approval, by executing security testing in line with the requirements of these regulations, and helping with the development of the required documentation.

SMART VEHICLES

Secura has designed services addressed at the whole smart vehicles ecosystem. The security of the cars or their high risk systems can be assessed by a design review or by making use of relevant international publications, such as IEC 62443, US Department of Transportation framework or the ENISA Smart Cars practices. By following such standardized assessments, Secura can ensure manufacturers that their vehicles or subsystems are compliant with the relevant state of the art security measures, reducing the risk of a security incident. At the same time, Secura is at the forefront of international cyber security regulations related to the automotive domain. Secura can support you in preparing for the upcoming regulations (such as the UN/ECE regulation on Cyber security or Software Updates), including the preparation of required documentation and the execution of required testing and documentation review. This will allow manufacturers to stay in control of their security processes, and ensure that they can satisfy the requirements of the regulations, the moment when they will be enforced.

INDUSTRIAL CONTROL SYSTEMS

For assessing ICS components and systems, an initial design review from the early stages of development can help ensuring a security by design approach. The security features can be tested in line with internationally recognized standards such as IEC 62443. IEC 62443 can be used to assess the security of either individual components, as well as systems made out of components (e.g. a system composed of a DCS and a HMI). Testing according to this standard can represent a valuable way to ensure that the products are protected against state of the art practical attacks. On top of standardized testing, Secura can support you in the process of following internationally recognized certification schemes such as IECEE.

FINANCIAL AND PAYMENTS

In this complex ecosystem, Secura designed services aimed at supporting most of the involved actors. For payment devices manufacturers, design reviews (for both hardware and software security) can ensure that the products are including sufficient security elements. Penetration testing activities can ensure that the devices include sufficient security features. At the same time, support in building certification specific documentation (ex. PCI PTS) can be offered.

TELECOM

Secura provides assessment services designed to highlight possible issues with these types of products and infrastructures. Secura can provide dedicated design reviews focused on the security of various network products. Such design reviews can provide valuable feedback to product manufacturers, as well as for network integrators. Besides this, penetration testing activities can be performed on products and networks, addressing security features such as encryption mechanisms, secure storage, physical security, authentication, authorization, etc. Finally, in the case of network products, the highest level of assurance can be obtained by means of certification. Secura can support you in the process of obtaining the BSPA label, enabling you to highlight the security of your products

Horizontal IoT Security

SECURE WEB AND MOBILE APPLICATIONS

Secura makes use of the OWASP Application/Mobile Testing Guide and Mobile/Application Security Verification Standard in order to assess the security of these applications. As a result, tailored services can be provided, in the form of design reviews and black/grey/crystal box investigations, approaching the security of the app from a real life hacker's point of view. The diversity of these offered solutions allows customers to have the flexibility of choosing the best approach for assessing their software, in line with their needs and testing appetite.

SECURE CLOUD

Secura can support both IoT developers and cloud service providers by performing tailored design review and penetration testing on specific cloud platforms (ex. testing the security of the provided APIs). Moreover, Secura can support with the preparation for cloud certification schemes (such as the CSA STAR certification) by performing cloud security compliance audits in line with the requirements of the CSA Cloud Control Matrix.

SecurAcademy

EXPAND YOUR KNOWLEDGE ON DIGITAL SECURITY

Secura's experts are pleased to share their knowledge with you.
Sign up for interactive training courses, workshops and free live webinars.

SIGN UP NOW:

- **Secure Programming Training** | 18 April 2019, Eindhoven/Amsterdam
- **The Hacker Mindset Workshop** | 13 June 2019, Nieuwegein (part of BHS programme)
- **ICS SCADA Workshop** | 13 June 2019, Nieuwegein (part of BHS programme)

TRAINING COURSES & WORKSHOPS

- **GDPR/DPIA Training** (1 day)
- **Threat modeling Training** (1 day)
- **Pen Test Training** (2 days)
- **Hands-on Hacking workshop** (1 day)
- **Mobile application Hacking Training** (2 days)
- **ICS Security Training** (2 days)
- **Automotive Security Training** (2 days)

For more information and registration:
SECURA.COM/SECURACADEMY

FREE WEBINARS

Sign up for live webinars with industry-leading experts.
More in this webinar series will follow.

- **Mobile Application Security** | 26 March 2019 – 11.00 PM – 11.45 PM CET LIVE
- **ICS SCADA Red Teaming** | 11 April 2019 – 3.00 PM – 4.00 PM CET LIVE
- **IoT Security** | 23 May 2019 – 3.00 PM – 4.00 PM CET LIVE
- **Impact wijzigingen DigiD** | 26 September 2019 – 3.00 PM – 4.00 PM CET LIVE

For registration and recordings: **SECURA.COM/WEBINARS**

Secura