Securing Communication and Identifying Threats in RTUs: A Vulnerability Analysis

Engla Rencelj Ling
Jose Eduardo Urrea Cabus
Ismail Butun
Robert Lagerström
{englal|jeuc|butun|robertl}@kth.se
Division of Network and Systems Engineering
KTH Royal Institute of Technology
Stockholm, Sweden

Johannes Olegard
johannes.olegard@dsv.su.se
Department of Computer and Systems Sciences
Stockholm University
Kista, Sweden

ABSTRACT

This paper investigates methods to secure Remote Terminal Units (RTUs) which are the building blocks of a smart grid systems - the next generation version to replace the power grid systems that are being used today. RTUs are identified as the heart of automation and control (SCADA) systems by the systems engineers. As such, security and maintaining nominal operability of such devices has prime importance, especially for the industrial automation networks such as the smart grid. A way of measuring the security of systems and networks is executing a series of cybersecurity weakness assessment tests called penetration testing. Another way of such an assessment is called vulnerability analysis by threat modelling which involves careful investigation and modelling of each and every component of a network/system under investigation. This article, aims at marrying these two methodologies for the vulnerability assessment of the RTUs in a methodological and scientific way.

CCS CONCEPTS

• **Security and privacy** → **Domain-specific security and privacy architectures**; • **Networks** → Network reliability.

KEYWORDS

SCADA, smart grid, power grid, RTU, threat modelling, attack graph, penetration testing

ACM Reference Format:
Engla Rencelj Ling, Jose Eduardo Urrea Cabus, Ismail Butun, Robert Lagerström, and Johannes Olegard. 2022. Securing Communication and Identifying Threats in RTUs: A Vulnerability Analysis. In *The 17th International Conference on Availability, Reliability and Security (ARES 2022), August 23–26, 2022, Vienna, Austria.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3538969.3544483

ARES 2022, August 23–26, 2022, Vienna, Austria

ACM ISBN 978-1-4503-9670-7/22/08.
https://doi.org/10.1145/3538969.3544483

1 INTRODUCTION

In a wide range of industries and sectors, automation systems have been used to run and monitor sensitive operations, including power plants and industrial assets. These technologies have been implemented in several countries around the world. Then, since the primary purpose of a smart city is to improve the quality of life of its inhabitants, it may enable our planet to reduce the strain of overpopulation by offering cities that are properly managed together with sustainable resources (energy, water, etc.) [6, 21, 24].

Historically, the individual systems and networks that made up the components of the infrastructure were both physically and conceptually distinct from one another. They did not engage in much communication or maintain connections with one another or the other parts of the system [4, 16]. As a result of developments in technology, the processes within each industry have been automated and are now linked to one another via computers and other forms of communication infrastructure. As a consequence of this, the flow of power, oil, gas, and telecommunications is linked (though occasionally indirectly) throughout the country. However, the links have resulted in a blurring of conventional security borders. This increased reliance on interconnected skills helps to make the economy and nation more efficient and possibly stronger; however, it also makes the country more vulnerable to disruption and terrorism. Because it has evolved into a complex system with a single point of failure in each component, this interconnected and linked infrastructure is increasingly susceptible to disruptions caused by both physical and digital attacks [4, 10, 16, 25].

As the size and complexity of the power grid continues to grow, it is becoming increasingly necessary to have a solid understanding of the emergent behaviors that are capable of occurring inside the system. Having said that, one of the most significant concerns and issues that must be resolved as smart cities continue to rapidly expand is how it will affect people's safety and privacy [4, 6, 21, 24]. The adoption of smart grid technology will result in a rise in the complexity of the current system as well as the inclusion of a great number of additional communication channels. The increased complexity and broadened communication channels may easily result in a heightened susceptibility to cyberattacks. It is difficult to foresee how an attacker may show itself in a fully developed smart grid because of its vastness (millions of nodes), which makes it tough to forecast how an intelligent opponent would behave. Smart Grid technology, which has been shown to be vulnerable to certain types of attacks, has already been used in some parts of the current power system [4–6, 10, 16, 21, 23–25].

Hence, IT systems are getting more and more complex every other day. Defending these systems against cyber attacks is also becoming a burdensome task to handle [20]. As such, the tasks for cyber security specialists are expanding in all dimensions of this complex world. As a remedy, formal methods and formal analysis tools help cybersecurity experts investigate the rightful implementation and usage of cryptographic materials in a cyber-defense solution [5, 10, 20, 23]. The world is highly dependent on IT systems today. Our society relies on these systems in almost every imaginable area, from the banking sector to the electricity domain and transportation [6, 24]. To cater for more and more functions, these systems have over the years grown large and complex, and there is still a way to go. At the same time, unfortunately, the consequences of cyber attacks have grown from barely financial losses to additionally posing a danger to human lives and causing catastrophes [4–6, 20].

Nowadays, businesses have begun to see the benefits of incorporating control systems into their power system applications. It is possible to make improvements to control and data collection systems by using a variety of data gathering devices. Some examples of these devices are Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs) (Supervisory Control and Data Acquisition (SCADA) systems). These devices are able to be connected to a wide variety of other pieces of field equipment, including alarms, protection relays, and digital meters [9, 26, 27].

Since the 1970s, when the first RTUs were put into operation, there has been a consistent rise in the number of situations in which they are used. For instance, they have been applied to essential infrastructures such as treatment facilities, power transmission systems, transportation systems, smart cities, and so on. A system's vulnerability may be defined as the degree to which its efficiency drops after being subjected to an attack. Hence, vulnerability is connected to threats. In addition, the protection of such critical infrastructure in terms of cyberattacks is of the utmost significance since the failure of these systems may endanger both property and, more crucially, human lives. Because of this, intrusion detection is a very important part of the system that manages cyber security and could be thought of as the main support for a cyber defense strategy [4–6, 9, 10, 16, 20, 21, 23–27].

An important part of securing RTUs from cyberattacks is to be pro-active and foresee potential attacks. This allows for securing the RTU appropriately before any damage has been done. Penetration testing is a method used to foresee attacks, by attempting to attack a device or system before an attacker does so. Doing this will provide valuable information regarding any potential security flaws that should be mitigated. Another approach to foresee attacks is with threat modelling. With threat modelling one creates a model of the device or system and attempt to evaluate which potential threats that exits.

In this paper, we aim to combine the two approaches of penetration testing with threat modelling. We do so by collecting data in the penetrating testing phase and providing this data to a threat model. With the threat model we are then able to run simulations and generate attack graphs. These attack graphs will give information regarding the different attack paths of a potential attacker.

2 BACKGROUND

2.1 Remote Terminal Units (RTUs)

To improve the reliability of the power system, more and more technologies are being developed and used. RTU-based systems are designed to construct network connectivity that enables control centers and the vast number of power grid assets to exchange information and operate remotely [9, 26, 27].

RTUs are SCADA system devices that serve as the electrical grid's "eyes, ears and hands". This analogy could be understood because they are in charge of gathering data from multiple equipment, analyzing it, and delivering it to the master unit via data transmission protocols ("eyes and ears"). They do this so that the master unit may have a better understanding of how the power system is working. The parallel between "hands" on the master unit and control instructions received from the RTU, which are subsequently transferred to the equipment, is validated by the RTU, where these control orders are then executed [9, 16, 26, 27].

An RTU should be designed to provide high levels of dependability, effectiveness, long-term stability, and security. The embedded system's communication network must be robust and dependable, regardless of the kind. These smart devices connect control systems to real-world assets, and they are employed in a broad spectrum of vital infrastructure, so protecting them is essential. Reviewing the relevant literature shows that RTUs usually support a number of standard protocols, such as Modbus, DNP3, IEC 60870-5-101/103/104, IEC 60870-6-ICCP, IEC 61850, and IEC 61131-3 programming standards for PLCs, as well as different routing protocols that can work over serial, Ethernet, or wireless links. Thereafter, it is critical to draw attention to and provide specific recommendations on the security features, capabilities, and industry standards that must be included in RTU systems in order to keep them robust, dependable, and efficient while also allowing for future growth [5, 9, 16, 26, 27].

2.2 Attacks on RTUs

Over the course of the past few decades, SCADA, Critical Infrastructure Systems (CIS), Industrial Control System (ICS), and other MODBUS-based systems have consistently been the focus of a wide variety of attacks. As a result of the rapid expansion of the internet, these systems have become significantly more susceptible to being compromised [8, 14]. As a result, because of the critical role it plays in the overall system of cyber security, intrusion detection can be referred to as the central pillar of cyber defence. Several studies have been conducted, and the term "Intrusion Detection Systems" (IDSs) refers to any and all functions and systems that work toward the same goal [5, 6, 8, 14]. IDS employs four of the most prevalent methods for diagnosing a system [5, 6]:

(1) File Integrity Checking: This is one of the most powerful tools that is used in IDSs, and it has the capability of effectively detecting forms of unauthorized activity (tampering with) of vital system files (in Windows systems, mostly.dll and.bat files) in addition to data files.
(2) Network Scanning: These are the applications that investigate potentially dangerous configuration problems and vulnerabilities in essential network systems and services. It

is similar to a weapon in that it is helpful to people when held by trustworthy individuals, but it may do harm when in the hands of invaders.

(3) Network Sniffing: These technologies will monitor the network packets because it might be evaluated and any suspicious behaviour may be located.

(4) Log Analysis:The process of gathering and evaluating diagnostic status information from the various software and hardware components of a network is known as network monitoring. The notion of logging is the most significant for intrusion detection systems and the recovery process that they use.

Assume a hypothetical situation in which an adversary is able to effectively introduce a transmitter and receiver gadget among two nodes. This adversary then has the ability to track, disrupt, and reconfigure the information exchange or even completely compromise it [13]. The inability of a monitoring system's data transmission elements to function properly can result in a loss of awareness of the service's environments and, as a consequence, in ill-informed decisions that could have a negative impact on the service's overall performance. A state-of-the-art study is required because assessment methods to robustly assessing the security vulnerabilities of interlinked facilities, such as structural vulnerability and functional vulnerability, require such an analysis to gain a deeper understanding of such vulnerabilities, as well as to develop and test defence systems, it is necessary to examine the primary components of the connectivity, which include messages, alarms, links, sensor systems, assessment centres, routers, management systems, and RTUs [7, 8, 13].

For instance, some catastrophic cyberattack events are presented as follows [13]: A portion of the Trans-Siberian gas project was destroyed in 1982 as a result of a Trojan virus that infiltrated its SCADA system. APT1, a hacker group, took complete control of a US hydroelectric power plant decoy system in 2003. In the same year, seven American states were forced to operate without power due to malware that destroyed several CIS. The Stuxnet malware systematically destroyed a fifth of Iran's nuclear centrifuges in 2010 by causing them to run out of control. McAfee reported in 2011 that several of its clients (electricity companies) had been targeted by a series of Chinese-originating attacks. In 2013, two ICS experts used radio frequency pathways to compromise various industrial facilities. They gained control of thermocouples and were able to disprove real-world data.

The bottlenecks of the technological components that comprise the system are a significant issue that needs to be taken into consideration when assessing the vulnerabilities of a power grid and SCADA systems. There have been a number of articles and research projects carried out to study the vulnerabilities of SCADA systems that are based on MODBUS TCP or that are connected to the internet. As a consequence of this, it is of the utmost importance to determine the weaknesses that are brought about by the interconnection of the transmission and distribution power grid and communication devices. MODBUS, which comprises MODBUS/TCP for Ethernet networks and MODBUS RTU or MODBUS ASCII for serial port networks, is a standard application layer protocol for MTU-to-RTU communication. So, because wrecked MODBUS protocols are the backbones of SCADA and CIS systems, which are in charge of essential duties, ruined systems might cause not only massive harm but also loss of life. Denial of service, response injection, command injection, and reconnaissance attacks are four prevalent forms of cyberattacks targeting industrial system control network applications [7, 8, 14, 18].

According to [14], the most obvious problem in the MODBUS serial protocol is the lack of built-in security protection. There is currently no built-in command for detecting or validating the validity of connected devices. Furthermore, the communications are sent in an unencrypted, plain-text readable format that does not require decoding.

As part of their research, stakeholders are investigating analytical techniques for operating state estimation security assessment in the event of a SCADA system cyber-attack that involves injecting false data into previously stored or transmitted records. This can occur against the network infrastructure, data storage facilities located within the control centre, or even SCADA-RTUs. For example, researchers at [13] focused on RTU-level threats and on false data injection attacks in particular. The RTU's data is altered maliciously to values chosen by an attacker, so instead of the actual measured data being sent to a control centre, a maliciously altered value is delivered in its place. Successfully concealing an FDI threat requires knowledge of the grid's characteristics and architecture. RTU measurements can be altered to create a credible, if inaccurate, view of the system state. In addition, the attacker has to know how to estimate the current condition of the network. [11] outlines a system for classifying cyberattacks. Threats against RTU-sensed data, which might occur either straightforwardly at the RTU layer or on the communication networks to the control station, are one of five classes discussed. Authors in [17] showed that many techniques exist for detecting faulty data, and the majority of them rely on the residual, which would be the discrepancy between a measurement's received value and its predicted state value. Therefore, it is possible to draw the conclusion from the previous citations that the nonlinearity of the power flow equations offers advantages to the system operator in relation to this kind of attack. However, this can only be the case if the attacker does not have knowledge of the system data that would enable him to use an attack analysis. If the enemy has these details, he might be able to attack without the state estimation noticing.

In addition, an attack action that is carried out by a trustworthy individual rather than by hackers with malicious intentions can be classified as a penetration test. Penetration tests are an integral component of the risk assessment strategy that an organisation employs. The threat model, which serves as the foundation for security needs, takes into account all of the potentially harmful actions that could be carried out by an adversary. To put it another way, it is essential to model potential threats that decrease the value of an organization's assets from the perspective of an adversary in order to solve security concerns during the design process [3, 22].

2.3 Vulnerability Analysis and Attack Graphs

The cybersecurity analysis of any system can also start from the attacker's point of view, which might be referred to as "counter-intuitive" analysis. As such, Vulnerability Analysis helps researchers and especially security experts in regard to understanding limits of their cyber-defenses as well as open gaps (called vulnerabilities) that their defenses fail to cover [2].

The resultant Vulnerability Analysis Report of a system includes attack (defense) graphs, which provide an intuitive approach to cyber-security. The attack graphs are very useful for cybersecurity specialist to understand the systems under investigation from the attacker's point of view.

For instance, in the automotive domain, cyber-attacks against autonomous and/or electric cars are on the rise as in the example of Tesla hacking showcases, [19]. We are confident that any car vendor would like to end up on the cyber-secure side of the spectrum of vendors while devising their next-generation "smart" vehicles. So, to further ensure that the vehicles are cyber-secure, systems and subsystem components (along with their interactions with the surrounding peripherals, users, and the infrastructure) need to be analyzed with an agile Cyber-Security approaches such as Vulnerability Analysis and Attack (Defense) Graphs. Attack (Defense) Graphs help us to understand the limits and capabilities of our defenses from the cyber attackers point of view.

Vulnerability Analysis of the systems and subsystems of an entity is utmost important for the cybersecurity experts while building/revisiting their cyber-security measures against adversaries. On the other hand, modern IT systems are extremely complex and analysis of such complex systems is non-trivial even for the expert cybersecurity analysts. Automated analysis of cyber threats is therefore a promising solution to tackle this complex problem.

2.4 Meta Attack Language

To address this research point, Meta Attack Language (MAL) is proposed and allows us to execute an automated "Cyber-Security Vulnerability Analysis" of any IT system from various perspectives such as identifying vulnerabilities of the sub-systems, components, data entry and output ports, actors, and their associated roles, etc., [15]. MAL generates the probabilistic attack graph of the system under investigation and helps cyber security analysts with the task of manually generating another graph for the each time a new system is being considered.

MAL is a domain specific language which allows a security analyst to envision system components from a cyber attacker point of view. Which then helps analysing the vulnerabilities associated with the each end point and system components. By identifying the weakest links and huge security gaps, a security analyst can take measures to prevent cyber attacks before happening, which might be referred to as "pro-active approach" to cyber defense (for instance pin pointing the possible Single-Point-of-Failure's in a network).

MAL has been shown to be successful tool in terms of integrating with other cyber security tools as well. Within the same conference last year, we have shown the feasibility of this via a use-case application scenario. For more details, feel free to refer [12], which describes and evaluates a successful integration of MAL with a Security (Social) Behavior Analysis tool called SBA.

3 IDENTIFYING THREATS IN RTUS

As mentioned earlier in this text, there are two methodologies that can be followed in identifying the threats against the RTUs: penetration testing and vulnerability analysis with threat modelling.

3.1 Penetration Testing of an RTU

The penetration test was performed on the RTU by a professional Swedish security company. For the penetration test, the RTU was set up in our lab and the lab setup is illustrated in Figure 1. The RTU was configured to communicate in different five protocols over five connections (or networks) with five other devices:

- IEC 60870-5-101 over a RS232 serial connection,
- IEC 60870-5-104 over TCP/IP (LAN B),
- IEC 61850 over TCP/IP (LAN A),
- IEC 60870-5-103 over a RS485 bus, and
- Modbus over a RS485 bus.

Rudimentary inputs/outputs streams were set up to simulate sensor data being sent via each protocol. The RTU has two "CPU modules" and each module is responsible for communicating with some of the devices. The first CPU communicates "upwards" in the SCADA hierarchy (towards the local and central Human-Machine-Interfaces) and the second CPU communicated "downwards" in the SCADA hierarchy (towards sensors and actuators). Each CPU also provides web-based (HTTPS) Human-Machine-Interface (HMI) for administration. The software "IED Scout"[1] version 5.10.549.0 was used to emulate the 61850-based device. The software "Vinci"[2] version 2.0.0.3 was use to emulate the remaining four devices. The emulators were run on Windows 10 Laptops with appropriate USB-adapters to facilitate each connection. Note that the illustration shows each emulator running on a separate Windows 10 laptop, while in reality the emulators were distributed between two laptops. Furthermore, both of the Ethernet networks were implemented using two separate Virtual Local Area Networks (VLANs) on the same network switch.

The penetration testers were given access to the emulator laptops (via a TightVNC server running on each laptops) as well as to the two Ethernet networks (and this is shown in the illustration using Guy Fawkes masks). Due to Covid-19 the penetration testing was performed remotely, with the testers having access in the lab via an OpenVPN server (which is not shown in the illustration). The penetration testers were given access to a TUN (layer 3) VPN-network with NAT-ed routes to the two Ethernet networks. The penetration testers also had access to four identical Kali Linux version 5.10.0-kali9-amd64 (2021-08-09) Virtual Machines. These Virtual Machines had direct access to all three networks.

The penetration testers were allowed to freely prioritize and structure their tests and time, but were asked to write down approximately what actions were performed and when. The penetration test lasted 10 working days (2021-11-22 thru 2021-12-03).

3.2 Vulnerability Analysis of an RTU

The penetration testing resulted in several discovered attack scenarios, where one was considered the most crucial. It is that the default

[1] see https://www.omicronenergy.com/en/products/iedscout/

[2] see https://the-vinci.com/vinci-software

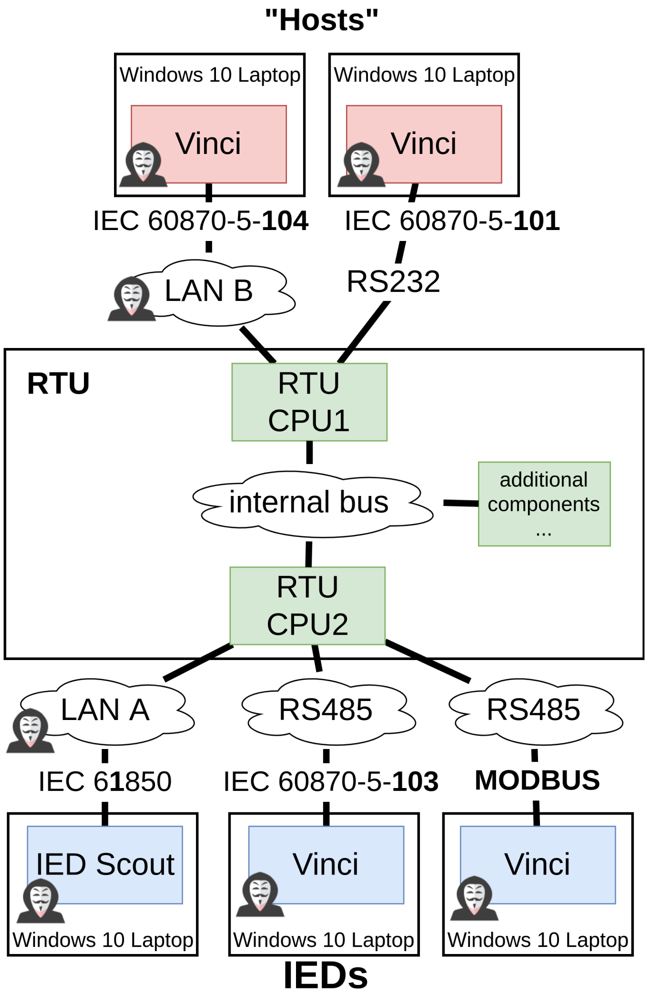

Figure 1: An overview of the lab. setup for the Penetration testing.

passwords were used on the RTU web application, which caused authentication bypass. Also, the web application was exposed on the network for LAN B and was therefore accessible by the penetration tester who had access via the VPN. After the attacker was logged into the RTU web application, they could find confidential information and make changes. We model this scenario to show an alternative way of identifying threats in RTUs. The model is a small example, but the intention is to model the entire system and run attack simulations to find any potential attack paths. In this case, we model that an attacker is using default credentials by using a threat modelling language called icsLang. icsLang has been built by using the frame work MAL. Specifially, the model is based on latest icsLang version built on coreLang 0.4.0[3]. The threat model and attack simulation is created with the software SecuriCAD Professional[4].

The model in Figure 2 illustrates the scenario and the different components and networks. The model shows that the attacker has both access to the credentials and access to the network via VPN to the lab switch. The yellow star in the figure shows the asset that the attacker is trying to attack. In our case it is gaining full access on the RTU web application.

The following assets are included in the threat model:

- Controller extends IcsApplication and is an asset for modelling all controller assets in ICS (RTU/PLC/IED).
- IcsApplication extends Application and is used for modelling all ICS software that may run on ICS hardware.
- ConnectionRule is used for modelling firewall/connection rules between applications and/or networks.
- System is hardware that may run applications.
- Application is used to model any IT software running on System.
- Network is any typical IT/OT network. There are two LANs setup, with the “IEDS” on LAN A and “hosts” on LAN B. The penetration testers gets VPN access to LAN B.
- RoutingFirewall is used to model the entry points of the penetration tester, the lab switch.
- Credentials is a username/password.
- Identity is used for the identity that the credentials are associated with.

4 RESULTS

In the following section we summarize the findings of the penetration testing and the resulting attack graph from the threat modelling.

4.1 Penetration Testing Results

The penetration testing resulted in several vulnerabilities being found, rated between medium to critical according to the OWASP Risk Assessment Framework [?]. Some of the vulnerabilities were caused by the use of weak default passwords in the RTU. Because of this security issue, the penetration testers were able to access the web application of the RTU. While making changes, such as, adding users, the device became entered a failed state. This was however not the intention of the penetration tester, but was caused by instability of device. Essentially the instability made it possible for the penetration testers to generate a Denial-of-Service (DoS) attack since the device was no longer functional.

Via the web application, the penetration testers were also able to use the API for uploading and downloading files to the RTU. Another successful attack was a fuzzing attack, which caused a kernel crash. Regarding the Java applications running on the Human-Machine-Interface (HMI), the penetration testers found hardcoded encryption keys. Regarding the IEC 60870-5 protocol running on the RTU, the attackers found that a network package sent caused a kernel crash, but it is not clear why this happened. They were also able to find robustness problems with the protocol while performing fuzzing attacks.

Besides the vulnerabilities found, the penetration testers were also able to gather information regarding the hardware and software used in the device. They could also retrieve log data via the web application. Moreover the reconnaissance showed that the

[3] icsLang, https://github.com/mal-lang/icsLang [Accessed: 20 May 2022]
[4] securiCAD, https://get.securicad.com/ [Accessed: 20 May 2022]

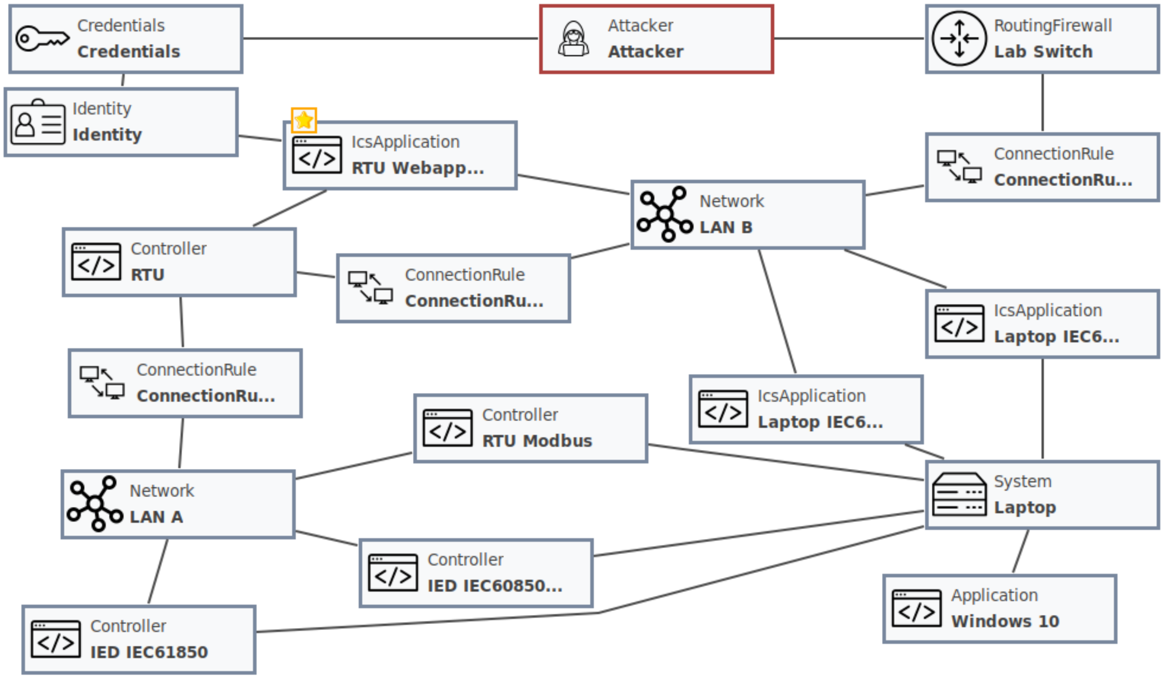

Figure 2: A threat model of one scenario found by the penetration testers.

default security policies had not been changed and that there was no security audit logs being recorded. This could cause a security issue in the future.

4.2 Resultant Attack Graph

After simulating the threat model shown in Figure 2, we are able to see the potential attack paths that an attacker would take in the system. If we look specifically at the attack path that the attack takes to gain full access to the RTU web application, we see that as expected the attacker uses the default credentials by guessing, assumes the identity of the user and authenticate to the web application. The resulting attack graph is shown in Figure 3.

5 DISCUSSIONS AND CONCLUSION

The penetration testing was performed by a few number of people and during a short period of time. There was also no attempt to hide the penetration testing by being stealthy. We acknowledge that their findings may be both individual to the specific experts that find them, that there may be more vulnerabilities that were not found and that in a normal operation the penetration testing would have been found and stopped. The attempted penetration testing that did not result in finding a vulnerability have not been discussed in this paper, but several such tests were performed. There were also results from the penetration testing that were deemed low risk and these have not been discussed in this paper.

For the vulnerability analysis, it is a small proof-of-concept included in this paper. The intention is to model an entire system and run simulations to find any potential attacks. This would make it possible to pro-actively fix those security issues before a potential attack. In this paper we have modeled one example scenario found by the penetration testers to showcase how threat modelling could be used for finding potential attacks in RTUs.

Some of the vulnerabilities found in the RTU were caused by not changing from the default passwords. There we also vulnerabilities caused by lack of robustness of the devices. For future work, the security could be setup differently and devices checked for robustness. This would more closely mimic a real-life system and would result in a different result of the penetration testing.

The penetration testing showed several vulnerabilities and was therefore able to identify threats of the RTU. The small vulnerability analysis example with threat modelling also indicates that a model of the system could be created to run attack simulations. These attack simulations would also indicate were there could be potential threats to the RTU. Potential future work includes modelling the entire system to make a full analysis och compare it to the penetration results. Other future work is to have penetration testers trying to penetrate an entire system and not only focus on one device, which was the RTU in this paper.

ACKNOWLEDGMENTS

This project has received funding from the European Union’s H2020 research and innovation programme under the Grant Agreement No. 832907 as well as the Swedish national research Centre on Resilient Information and Control Systems (RICS).

REFERENCES

[1]]owasp [n. d.]. OWASP Risk Assessment Framework. https://owasp.org/www-project-risk-assessment-framework/. Accessed: 2022-05-20.

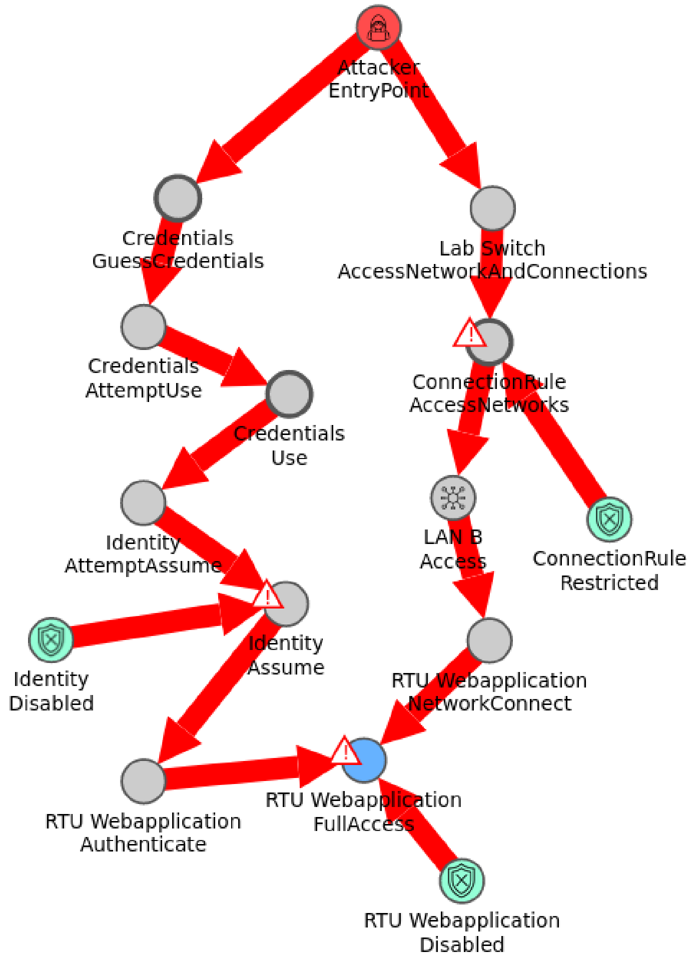

Figure 3: The resulting attack graph after simulating the threat model of a penetration testing attack scenario.

[2] Rachid Ait Maalem Lahcen, Ram Mohapatra, and Manish Kumar. 2018. Cybersecurity: A survey of vulnerability analysis and attack graphs. In *International conference on mathematics and computing*. Springer, 97–111.

[3] Norah Ahmed Almubairik and Gary Wills. 2016. Automated penetration testing based on a threat model. In *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*. IEEE, 413–414.

[4] Göran Andersson, Peyman Mohajerin Esfahani, Maria Vrakopoulou, Kostas Margellos, John Lygeros, André Teixeira, György Dán, Henrik Sandberg, and Karl H Johansson. 2012. Cyber-security of SCADA systems. In *2012 IEEE PES Innovative Smart Grid Technologies (ISGT)*. IEEE, 1–2.

[5] Ismail Butun, Alexios Lekidis, and Daniel Ricardo dos Santos. 2020. Security and Privacy in Smart Grids: Challenges, Current Solutions and Future Opportunities. *ICISSP* 10 (2020), 0009187307330741.

[6] Ismail Butun and Patrik Österberg. 2019. Detecting intrusions in cyber-physical systems of smart cities: Challenges and directions. In *Secure Cyber-Physical Systems for Smart Cities*. IGI Global, 74–102.

[7] Raphael Caire, Jose Sanchez, and Nouredine Hadjsaid. 2013. Vulnerability Analysis of Coupled Heterogeneous Critical Infrastructures: a Co-simulation approach with a testbed validation. In *IEEE PES ISGT Europe 2013*. IEEE, 1–5.

[8] Pravin Chopade and Marwan Bikdash. 2013. Structural and functional vulnerability analysis for survivability of Smart Grid and SCADA network under severe emergencies and WMD attacks. In *2013 IEEE International Conference on Technologies for Homeland Security (HST)*. IEEE, 99–105.

[9] Gordon R Clarke, D Reynders, and W Edwin. 2004. SCADA protocols: DNP3, 60870.5 and related systems.

[10] György Dán, Henrik Sandberg, Mathias Ekstedt, and Gunnar Björkman. 2012. Challenges in power system information security. *IEEE Security & Privacy Magazine* 10, 4 (2012), 62–70.

[11] Annarita Giani, Shankar Sastry, Karl H Johansson, and Henrik Sandberg. 2009. The VIKING project: An initiative on resilient control of power networks. In *2009 2nd International Symposium on Resilient Control Systems*. IEEE, 31–35.

[12] Simon Hacks, Ismail Butun, Robert Lagerström, Andrei Buhaiu, Anna Georgiadou, and Ariadni Michalitsi Psarrou. 2021. Integrating Security Behavior into Attack Simulations. In *The 16th International Conference on Availability, Reliability and Security*. 1–13.

[13] Gabriela Hug and Joseph Andrew Giampapa. 2012. Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks. *IEEE Transactions on smart grid* 3, 3 (2012), 1362–1370.

[14] Gabor Jakaboczki and Eva Adamko. 2015. Vulnerabilities Of Modbus Rtu Protocol–A Case Study. *Nnals Of The Oradea University, Fascicle Of Management And Technological Engineering* 1 (2015).

[15] Pontus Johnson, Robert Lagerström, and Mathias Ekstedt. 2018. A Meta Language for Threat Modeling and Attack Simulations. In *Proceedings of the 13th International Conference on Availability, Reliability and Security* (Hamburg, Germany) *(ARES 2018)*. New York, NY, USA, Article 38, 8 pages. https://doi.org/10.1145/3230833.3232799

[16] Tyson Macaulay and Bryan L Singer. 2011. *Cybersecurity for industrial control systems: SCADA, DCS, PLC, HMI, and SIS*. CRC Press.

[17] Alcir Monticelli. 2000. Electric power system state estimation. *Proc. IEEE* 88, 2 (2000), 262–282.

[18] Thomas Morris, Rayford Vaughn, and Yoginder Dandass. 2012. A retrofit network intrusion detection system for MODBUS RTU and ASCII industrial control systems. In *2012 45th Hawaii International Conference on System Sciences*. IEEE, 2338–2345.

[19] Sen Nie, Ling Liu, and Yuefeng Du. 2017. Free-fall: Hacking tesla from wireless to can bus. *Briefing, Black Hat USA* 25 (2017), 1–16.

[20] Calvin Nobles. 2018. Botching human factors in cybersecurity in business organizations. *HOLISTICA–Journal of Business and Public Administration* 9, 3 (2018), 71–88.

[21] Humera Rafique. 2018. 5.15 Energy Management in Network Systems. (2018).

[22] Giovanni Salzillo, Massimiliano Rak, and Felice Moretta. 2020. Threat modeling based penetration testing: the open energy monitor case study. In *13th International Conference on Security of Information and Networks*. 1–8.

[23] Alparslan Sari, Alexios Lekidis, and Ismail Butun. 2020. Industrial networks and IIoT: Now and future trends. In *Industrial IoT*. Springer, 3–55.

[24] Khairy Sayed and Hossam A Gabbar. 2017. SCADA and smart energy grid control automation. In *Smart energy grid engineering*. Elsevier, 481–514.

[25] Chih-Che Sun, Chen-Ching Liu, and Jing Xie. 2016. Cyber-physical system security of a power grid: State-of-the-art. *Electronics* 5, 3 (2016), 40.

[26] Mini S Thomas and John Douglas McDonald. 2017. *Power system SCADA and smart grids*. CRC press.

[27] Jose Eduardo Urrea Cabus, Ismail Butun, and Robert Lagerström. 2022. Security Considerations for Remote Terminal Units. In *2022 IEEE International Conference on Zooming Innovation in Consumer Electronics International Conference 2022 (ZINC 2022)*. IEEE, –.