2017 9th International Conference on Cyber Conflict
Defending the Core
H. Rõigas, R. Jakschis, L. Lindström, T. Minárik (Eds.)
2017 © NATO CCD COE Publications, Tallinn

Defending the Grid: Back-fitting Non-Expandable Control Systems

Robert Koch
Faculty of Computer Science
Universität der Bundeswehr München
Neubiberg, Germany
robert.koch@UniBw.de

Teo Kühn
Faculty of Computer Science
Universität der Bundeswehr München
Neubiberg, Germany

Abstract: Network security has been a lively research area for more than 35 years and numerous products are available nowadays. In contrast to business networks, which were interconnected from the beginning by design, Industrial Control Systems (ICSs) have always been self-contained networks. Because their key features are real-time capability and their operational constraint to function as specified under maximum load (Carlson 1998), security has played only a subordinate role. Nowadays these systems are increasingly connected to the Internet; for example, wind power is more frequently used and generators are installed in remote and scattered regions that are difficult to access, so remote administration based on mobile communications is required, often using the Internet.

While numerous papers on securing ICSs have been published, interest rose after the incidents in Iran's enrichment plant in Natanz where the SCADA system controlling the centrifuges was attacked by the Stuxnet worm. Even with these intensified efforts, the current security situation is insufficient as numerous security systems perform inadequately in real-world environments. Elderly ICSs are also still in use which cannot be retrofitted easily or at all, and modern systems are often still not developed with 'security by design' in mind. In contrast to general purpose systems, a relatively limited number of processes are executed within ICSs. This enables the use of detection mechanisms based on voltage levels and current drain to build lightweight detection systems without huge databases by measuring the current drain during normal system operation.

Our concept combines the advantages of different detection principles and enhances them to build an Intrusion Detection System usable within ICSs. It is implemented based on low-priced components and can be integrated even in older, originally non-expandable systems.

Keywords: *power-based intrusion detection, ICS and SCADA security, tamper-resistant intrusion detection, anomaly-based IDS, retrofitting IDS, lightweight IDS*

1. INTRODUCTION

Intrusion Detection Systems (IDSs) have been under intense research for more than 35 years. Monitoring system behaviour to learn patterns and detect abnormal behaviour was the first detection technique in 1980. Within this group, anomaly-based detection is the predominant detection principle: benign behaviour is observed over a period of time, and afterwards a model is built based on the observations. During operation, the state of the system is measured and compared to the expectations of the model. If there is a significant deviation above a defined threshold, an alarm is raised. While this approach is able to detect new and unknown threats, it suffers from a high number of false alarms.

More recently, knowledge-based detection techniques have been developed. Here, mainly acquirement of malicious activities is used to realise misuse detection based on attack descriptions (signatures). This technique is able to lower false positive rates, but only known attacks can be detected. In the 1990s, this was a beneficial approach because a limited number of new malicious codes were published repeatedly. Anyway, the rapidly increasing professionalisation of the cybercrime market and the exploding numbers of malicious programs are forcing huge signature databases and time-consuming scans, therefore renewing the need for behaviour-based techniques.

But even with these extensive efforts, successful cyber attacks happen every day with an increasing amount of damage and physical effect. An extensive study of the annual costs to the global economy by McAfee (2014) gives an estimate of more than $400 billion in losses, and an estimate made by Juniper (2015) projects the loss at over $2 trillion by 2019.

ICSs and Supervisory Control and Data Acquisition (SCADA) systems are also under continuous attack. Often designed years or decades ago and originally conceived as isolated networks and systems, nowadays more ICSs are connected to the Internet. For example, wind power is increasingly used in the energy sector and generators are installed in remote regions difficult to access. This requires remote administration which is realised using mobile communications. The interconnection of plants can also be required to open up new business models. Therefore, factories and power plants are no longer conceivable without the use of ICSs.

Even though the security of those systems is obviously very important, this is currently not reflected in the real world. Analysis by Andreeva and colleagues (2016) for Kaspersky Lab concluded that:

> [a]lthough they are designed for critical infrastructures, industrial-sector devices are not secure by default; they contain the same type of vulnerabilities as any other system: including buffer overflows, hardcoded credentials, authentication bypass, cross-site scripting, and many others.

The situation is even more alarming, as the SANS 2016 State of ICS Security Survey (Harp and Gregory-Brown 2016) discloses that 67% of all participants ‘perceived severe or high levels

of threat to control systems, up from 43% in 2015', but 'security for ICSes has not improved in many areas and that many problems identified as high-priority concerns in our past surveys remain as prevalent as ever'. The recent report of the US Department of Energy (2017, p. 18) states:

> In the current environment, the U.S. grid faces imminent danger from cyber attacks. Widespread disruption of electric service because of a transmission failure initiated by a cyber attack at various points of entry could undermine U.S. lifeline networks, critical defense infrastructure, and much of the economy; it could also endanger the health and safety of millions of citizens.

As the required processing power in ICSs is often precisely defined, these systems routinely lack adequate intrusion detection components and cannot be upgraded. This essay will explore how real-world-usable intrusion detection with high detection and low false alarm rates can be realised for ICSs. Section 2 will discuss the particularities of ICSs and also identify available research and its shortcomings. Unlike general purpose systems, a relatively limited number of processes are executed within ICSs. These processes also remain unchanged for a long time. This enables the use of power-based detection mechanisms to build lightweight detection systems without huge databases, by the creation of an extensive comparative dataset and measuring the current drain during normal system operation, which will be presented in Section 3 A. Based on this, different possibilities of distributed intrusion detection for ICS and SCADA are presented in Section 3 B. Finally, Section 4 summarises core aspects and presents next steps.

2. SCADA & ICS CHALLENGES

A. Particularities of ICSs

ICSs control our entire modern everyday life. Not only do factories and power plants rely on them, critical infrastructure like water supply and transportation are completely IT-based. Some challenges for ICSs directly emerge from their regular use:

> Some SCADA systems are placed in remote locations […] and are designed to run nonstop for months or years. Through Internet connections to SCADA systems, managers can have precise and remote control of their infrastructure machinery. This arrangement also reduces the required number of workers in the field. Industrial control systems were originally designed to operate in isolation, without connection to other networks. As a result, cyber security controls were not built in (Wilson 2012, p. 4).

Therefore, due to the originally unplanned interconnection with non-trustworthy networks such as the Internet, there are often no protective measures available: the challenge of the *unavailability* of security components. Neither is air-gapping an adequate protection mechanism nowadays (Andreeva et al. 2016), as not only was bridging the airgap demonstrated impressively by Stuxnet, but numerous new concepts have also been demonstrated (Guri et al. 2016).

Secondly, ICSs are specifically designed for their respective applications: '[a]n important operational constraint of a SCADA network is that it functions as specified under maximum load. Security cannot hinder such operation' (Carlson 1998, p. 6). This highlights a burning issue for securing ICSs which are already in use, as they generally can neither be updated with additional software nor easily retrofitted with additional hardware; this is the challenge of *non-expandability*. Certification can also be a further hurdle in some areas like medical equipment, preventing a change of hardware or software.

Today's development cycles of commercial off-the-shelf (COTS) products are often of less than one year, and products typically have a limited support technology lifetime of only a few years. In contrast, control systems are used for a long time – often several decades. This presents challenges, like the supply of spare parts or fixing bugs in outdated and no longer supported proprietary software.

Even if software support is still available, patching can be challenging, even for general purpose systems. While there is work in progress on improving and automating program repair (Le 2016), patching is still complicated and the complexity of applying patches should not be underestimated (Cavusoglu, Cavusoglu and Zhang 2008). For example, issues can arise based on bad patch quality, being unable to fix the focused software flaws, interrupting software functionality or introducing new vulnerabilities (Mimoso 2015). Childs (2015) highlighted that:

> [i]n the last half of 2014 alone, users incurred major disruptions after installing patches from Microsoft, Apple, Adobe, and Oracle. There are also times when a security patch itself introduces a security problem. In other cases, the patches do not work as advertised.

While this is challenging for all IT systems, applying patches to ICSs is even more difficult because of 24/7 operation, the lack of testing possibilities before applying a patch, or technical limitations of the target systems. This is the challenge of being *unmaintainable*.

Meanwhile, the increasing quality of attacks is endangering the livelihood of today's societies. For example, the service outages of the Ukrainian power distribution company Kyivoblenergo on 23 December 2015 affected seven 110 kV and 23 35 kV substations, resulting in several outages that caused approximately 225,000 customers to lose power across various areas (Lee et al. 2016). The subsequent investigation of the incident showed that the attackers were able to perform long-term reconnaissance and to use and exploit different attack vectors including spear phishing emails, harvesting system and network credentials, operating SCADA systems, writing and distributing malicious firmware and rendering devices inoperable and unrecoverable (Ibid.). This is the challenge of *attack sophistication*.

Currently, Cyber Commands are being built up in nearly every nation worldwide. The significance of the cyber space for military operations is undisputed:

> In July 2016, Allies reaffirmed NATO's defensive mandate and recognised cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea (NATO 2016).

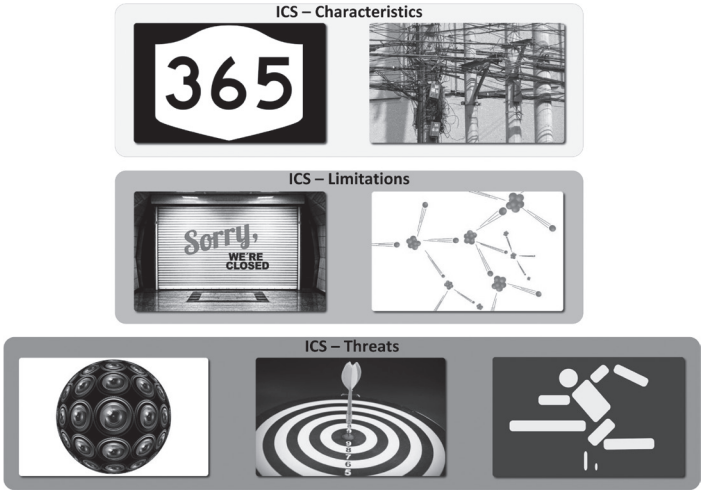
A massive cyberattack could even trigger a collective response by NATO (Reuters 2016). From a military point of view, targeting critical infrastructure can be advantageous, such as disabling the adversary's power grid accurately and promptly without endangering own ground troops, and even being able to make further use of it in contrast to physical destruction (Saglam 2014). Therefore, critical infrastructures are increasingly *eyeballed* as attractive targets.

As the Western critical infrastructures have been scanned systematically for years (Paganini 2014), attack preparation is greatly facilitated. New search engines such as Shodan, scanning all devices connected to the Internet and reading out banner massages, exacerbate the situation even further:

> originally intended to improve security and discover information about machines linked to the Internet, [Shodan] revealed that many SCADA computers that automate water plants and power grids were wide open to exploitation by hackers. The Shodan search engine has reportedly revealed water-treatment facilities, power plants, particle accelerators and other industrial control systems that may have security vulnerabilities (Wilson 2012, p. 4).

While a significant increase in the number of attacks based on Shodan's search results was *not* identified by some research (Bodenheim 2014), at least the reconnaissance is greatly simplified. The situation is getting worse as low-priced Zero Day vulnerabilities for SCADA systems can now be bought easily. For example, the Russian company GLEG Ltd. sells the exploit packages SCADA+ and MedPack, providing hundreds of modules and regularly adding new Zero Day vulnerabilities. For example, SCADA+ 1.5 contained a Zero Day for a vulnerability in 'Carel Plant Visor Pro', which is 'used on nuclear plants e.g. in Canada, [and states that the] exploit allows credentials steal' (GLEG Ltd. 2015). While the cheap prices allow companies to buy products for identifying vulnerabilities in their products and fix them, ICSs are often barely patchable. This opens up the challenge of a *falling attack threshold (easiness of attack)*.

FIGURE 1. PECULIARITIES AND ENDANGERMENTS OF ICSS



Having a look at defence mechanisms,

> some traditional cybersecurity practices and procedures that are standard for office IT systems may not work as well for SCADA systems. For example, because industrial SCADA equipment must send monitoring signals to other industrial controller equipment within milliseconds, traditional antivirus software or network intrusion detection devices will not fit very well (Wilson 2012, p. 7).

One must also not forget that security systems are just program code, introducing an additional number of programming errors (Panko 2008; Baishakhi et al. 2014). Tavis Ormandy (2016) demonstrates that such vulnerabilities are not rare in security programs, such as the remote code execution flaws in CVE-2016-2208. Also, the recommended best practice of building up a defence in depth can be more complicated than expected, as negative effects can occur if the measures are not coordinated in detail (Wolff 2016). This is the challenge of *interference* of traditional security systems.

Taking into consideration an evaluation of control systems cybersecurity made by Idaho National Laboratory (2008), Table 1 summarises and opposes the identified security challenges for general purpose and ICSs.

TABLE 1. COMPARISON OF SECURITY CHALLENGES

Security Challenge	General Purpose	Control Systems
Non-expandable hard-/software	Expandable, interchangeable	Non-expandable
Maintenance	Regular scheduled	Limited, system restrictions
System interference	Generally accepted	Unacceptable
Security systems	Common, widely used	Unavailable, system restrictions
Attack demand	Cybercrime, espionage	Cyber Commands, Terrorism
Attack sophistication	Rising	Rapidly rising
Attack simplification	Countermeasures	Low attack hurdle

B. Related Work

A comprehensive overview of SCADA-specific intrusion detection systems was given by Zhu and Sastry (2010). They analysed and compared different behaviour- and knowledge-based as well as hybrid systems for SCADA (PVAEB, IBM NADS, SRI Modbus, WFBNI, SHARP, IDEM, AAKR-SPRT, EMISDS and MAAC-UFE) and concluded that 'barely any of these systems has a performance evaluation on the false alarms that it generates' (Ibid., p. 13). This will also be a challenge when comparing our evaluation results with other works (see Section 3A.) Mitchell and Chen (2014) surveyed intrusion detection techniques for cyber-physical systems by analysing 28 IDSs. Open research leads in areas such as network-based approaches and the use of behavior-based detection techniques were identified.

Yang et al. (2006) analysed the application of anomaly-based intrusion detection for SCADA systems. They used an auto associative kernel regression model and statistical probability ratio test, applied to a simulated SCADA system. Their results showed that anomaly-based methods can be generally used to detect a variety of common attacks also within SCADA systems. Yang et al. (2014) proposed a multi-attribute SCADA-specific IDS for power networks. Their system consists of three attributes: access control whitelists, protocol-based whitelists and behaviour-based rules, where normal and correct behaviour are found by deep packet inspection. The focus of their evaluation is on the maximum execution time, showing that the standard communication delivery time performance requirements for electric power substation automation (IEEE Standard 1646-2004) are fulfilled. A performance evaluation of the intrusion detection is not given. Also, the system has to be integrated into the target system, cannot cope with encrypted connections, and is limited to power networks.

An integrated OCSVM mechanism for intrusion detection in SCADA systems was proposed by Maglaras et al. (2014). They use a distributed class support vector machine to generate information about the origin and time of an intrusion by reading network traffic and evaluating clusters based on the source of the network packets. Sayegh et al. (2014) proposed a SCADA-specific IDS for detecting attacks based on network traffic behaviour by evaluating frequent patterns of SCADA protocols.

All these publications have in common that the respective systems are implemented in an immersive way as they have to be integrated into the target environment. This violates the identified requirements of *non-expandability* of ICSs and enables unacceptable system *interference*. Recent patents only use trivial approaches, such as creating a whitelist of all connected devices and afterwards creating alerts based on configuration changes like unseen new IP addresses (Mcquillan and Lloyd 2016). Again, the proposed IDS must be integrated into the SCADA system, which prevents the retrofitting of existing systems.

As our proposed concept is based on the evaluation of current drain to respect these requirements with a more tamper-proof system and using better ground truth, respective publications within the area of power-related intrusion detection will be discussed as follows. The need for identifying and evaluating abnormal electric power consumption arose back in the late 90s, when Stajano (1999) was one of the first researchers describing the problem of battery exhaustion attacks.

Nash et al. (2005) proposed an IDS specialised on the detection of battery exhaustion attacks. Their system evaluates parameters like CPU load and disk access of mobile computing devices. The power consumption is estimated using a linear regression model on a per process basis. Based on these evaluations, potential battery exhaustion attacks are identified. In contrast to our approach, the system cannot provide general intrusion and attack detection.

Jacoby and Davis (2007) proposed a battery-based intrusion detection system (B-BID) for mobile handheld devices. Their system consists of three parts: a host intrusion detection engine provides rule-based detection of battery behaviour anomalies based on static threshold levels; a 'source port intrusion engine' is for capturing network packets during suspected attacks and a 'host analysis signature trace engine' which is used to correlate signature patterns in the frequency domain. Its shortcomings are the restriction to mobile systems and the requirements of specific preconditions like the evaluation of busy, idle and suspend states. Our concept is not restricted to battery-powered systems nor does it require knowledge about process states.

Srinivasan et al. (2006) proposed a self-organised agent-based architecture for power-aware intrusion detection (SAPID). It uses a power level and a hybrid metric to determine traffic, and a self-organising map to recognise anomalies in the network. In contrast to our approach, SAPID is not generally applicable, focusing on ad-hoc wireless networks.

Buennemeyer et al. (2006) proposed a battery-sensing intrusion detection system (B-SIPS). B-SIPS senses anomalous patterns in the battery current to identify possible exhaustion attacks and malicious activities. A server-based correlation intrusion detection engine is used to correlate possible attacks with a network-based IDS. While this system improves capabilities of battery-based intrusion detection and lowers false alarm rates, it focuses on attacks on Bluetooth and WiFi. Also, the system depends on smart battery monitoring capabilities, prohibiting its general application. In contrast, our concept is not restricted to specific network interfaces and does not require smart battery capabilities.

Stepanova et al. (2010) made a homogeneity analysis of power consumption for information security purposes. Their system has to be trained with multiple battery-lifetime periods, limiting its applicability to battery-powered devices. Also, it is focused on the detection of malicious SMS Trojans and MMS-transmitting net worms. Our concept is not limited to battery-powered systems nor restricted to specific malicious software.

While different battery-based systems have been proposed and traditional IDS had been extended for the evaluation of power-based features, their capabilities and applicability are still limited. A recent approach called power fingerprinting (PFP) is more promising. It extracts 'references from the execution of trusted software and use[s] them to compare captured traces to determine whether the same code is executing' (Reed and Gonzalez 2012). While this can be used to identify malign behaviour using a difficult-to-manipulate measuring base, the requirements for PFP cannot always be satisfied. Particularly in general-purpose systems, getting references from trusted software for all possible programs which may be executed is typically not possible, quickly resulting in high false alarm rates. The situation will also become more challenging for ICS when an increasing amount of individualised mass production is introduced in the context of 'Industry 4.0'. Learning phases can also be used to identify the normal behaviour of the network, but they often cannot see all benign behaviour, and the target environment already can be compromised, resulting in learning malicious behaviour as benign (Koch 2009).

In contrast to the current approaches with limited detection capabilities, we propose a new concept of a current-sensing based, lightweight IDS using cheap single-board computers which can be deployed within an existing network structure of, for example, a SCADA system. It extends PFP mechanisms by introducing specific power patterns, lowering the risk of learning malicious behaviour when no reference from trusted software is available, as well as reducing false alarm rates.

3. LIGHTWEIGHT INTRUSION DETECTION FOR ICSs

Next, the current-based intrusion detection realised by *Dr.WATTson* is presented and distributed approaches to realise real-world-usable IDSs for ICSs are discussed. We used a design-oriented approach for the development of the concept and the architecture.

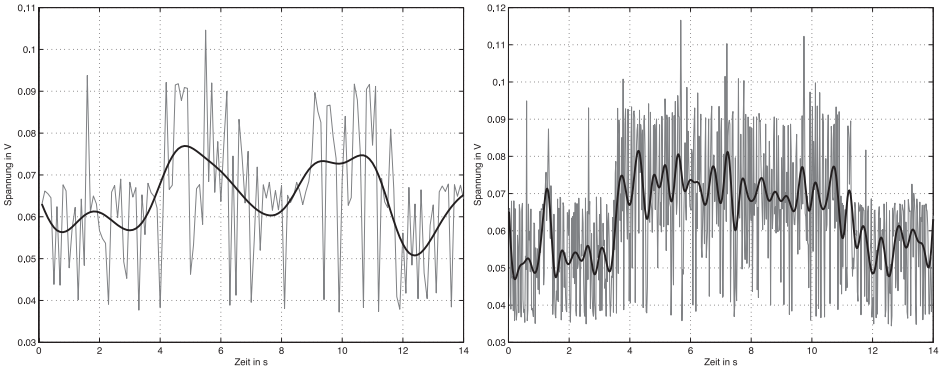
A. Current-Based Intrusion Detection by Dr.WATTson

For the design and development of a lightweight current-based IDS, a low-priced but accurate system with respective IO ports is required for measuring and processing. Therefore, available hardware components and their capabilities were analysed to determine their suitability. First, measurements to identify a tamper-resistant detection scheme which can be generally applied by using low-cost equipment were executed. An ODROID-U3 mini-computer was combined with the ODROID Smart Power which collects voltage and current based on a sampling rate of 10 Hz. The ODROID-U3 is now discontinued, but the available ODROID-C2 is even better and will be used for our upcoming setup (see Section 4). By executing different current and voltage measurements and analysing the accuracy of the Smart Power in comparison with the results of a highly accurate oscilloscope, the accuracy of the low-cost setup was verified: all

measured values were within the announced deviation of 2%. Next, the required sampling rate was analysed.

A comparative voltage metering was done by using a Keithley Series 2700 (440 Hz) and a NI PCI-2651 high-speed card (up to 2.8 MHz). For the latter, corresponding log files had been generated by an additional PC, as the ODROID does not provide a PCIe interface. The firmware of the Smart Power was adapted to provide headless operation, as the graphical output was not needed but raw measurement values for the calculations was. A resulting effect was a more accurate measurement of the Smart Power, as the GUI is implementing some smoothing and filtering out single peaks, while this data remains available by the recorded logs.

FIGURE 2. VOLTAGE CHARACTERISTICS DURING A PORTSCAN SEEN BY 10 HZ AND 50 HZ SAMPLING RATE. THE RED CURVE IS AFTER FILTERING.



To investigate the sampling frequency for the pattern recognition, multiple test runs were evaluated. Figure 2 shows the voltage characteristics during a port scan seen by sampling rates of 10 and 50Hz. Using a frequency of 10Hz, a clear voltage profile can be recognised. The voltage differed between 60 and 75mV and the end of the scan can be seen around second 11. Having a look at the 50Hz sampling rate, more details can be found with peaks going up to 82mV. A further increase in the sampling frequency sharpens the voltage edges but does not provide new valuable information; starting with a sampling rate of 500kHz, all processes of the switching power supply are recorded together with additional noise: this also hampers the evaluation of patterns. As a result, the 10Hz sampling frequency is enough to recognise attack patterns in the power consumption.

Next, the architecture for current-based intrusion detection was developed as depicted in Figure 3. The *ODROID-U3* is the low-cost hardware platform. The processing of the collected measurement values is done by the *Worker*. There, the cross correlations are calculated, the database containing current flow patterns is administrated, and different modules are controlled. The collection of current measurement values is done by *ODROID Power*; multiple Smart Powers can be connected by USB, or IO SHIELD can be used for the data-collection using 36 additional GPIO ports. This also enables the connection of multiple sensors to one mini-computer. *Snort* is integrated as a traditional NIDS, enabling optional alert correlation (e.g.,

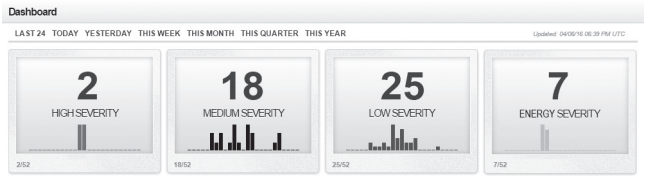
when the monitored system already has a rule-based IDS and specialised rulesets, e.g., from Digital Bond), while *barnyard2* is used for converting Snorts' output. *Snorby* is implemented as a graphical frontend and *ODROID-SHOW* is used for displaying essential operating parameters and current-based alerts directly at the mini-computer.

FIGURE 3. ARCHITECTURE OF DR.WATTSON

The described architecture can also be operated as HIDS to perform current-based intrusion detection for itself: the main operational mode is the application as NIDS, providing current-based intrusion detection for one or multiple systems by using current-sensing information, but HIDS and NIDS can be operated simultaneously for a current-sensing IDS with permanent self-monitoring.

The proposed architecture was implemented by the PoC Dr.WATTson, using Ubuntu 14.04.02 LTS for ARM architecture with kernel 3.8.13.30 configured to use *Performance* as CPU governor and Ruby on Rails for the provision of required libraries and the implementation of the Worker. Snort was implemented to verify the compatibility with this widely used IDS, and to provide an additional source for correlation. For storing and visualising of alerts, the *Unified2Binary* data generated by Snort is taken by the open source interpreter barnyard2 and written to disk for further parsing. For visualisation, Snorby was integrated and extended with the new field *Energy Severity*. This additional display represents only alerts which are generated based on current-based detection. Figure 3 shows a screenshot, presenting the newly integrated display.

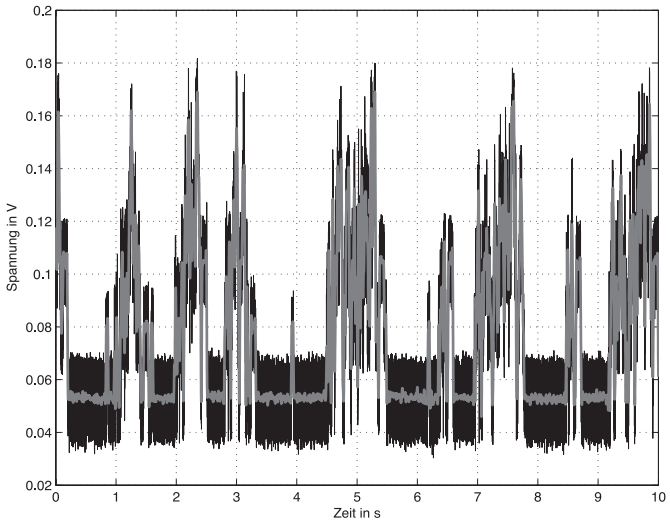
FIGURE 4. EXTENDED SNORBY INTERFACE WITH NEW ALERT CLASS FOR POWER-BASED ALERTS



To exploit that power consumption can be a quite tamper-resistant information source and baseline, first the regular power consumption of the device was evaluated. Reference values were measured using a variety of scenarios to generate comparative values based on this baseline. For systems like ICSs with clearly defined processes, trustworthy comparative data can be generated quite easily by executing multiple measurement cycles. During later operation, measurements have to be compared with the earlier generated current drain values. For the calculation of the similarity, cross correlation functions can be used: a sum function of the cross correlation was implemented to enable a calculation for a discrete base, the recorded measurement values in the logs. Based on these similarity calculations, current-based alerts which are called *Energy Severity Events* are generated.

After the baseline had been established, attack scenarios like DoS, portscans and bruteforce were executed. From the variety of attacks, an SSH bruteforce attack detected by Dr.WATTson is shown in Figure 5. The time frame of ten seconds presents a triangular voltage pattern with steep flanks, which is a typical and explicit power pattern identified for SSH attacks. The measured value series was correlated by the Worker with comparative data from the database to identify possible attacks. With this, a reliable detection of attacks was possible.

FIGURE 5. MEASUREMENT OF DR.WATTSON DURING SSH BRUTEFORCE ATTACK



For the evaluation of Dr.WATTson, the ground truth was generated as previously discussed based on a run of 72 hours. After that, different attack scenarios were executed, each lasting 14 hours and containing 11 discrete attacks per hour. The attack runs were repeated five times to calculate the detection results. The system was able to detect 100% of the executed attacks while delivering a false alarm rate of 0.13%, surpassing the results of other systems. The classification of the resp. attack type, which is a new feature other systems are not able to provide, was correct in 45.5% of cases. The final detection results are summarised in Table 2. Usual research in

the area of power-based intrusion detection typically focuses on specific wireless networks, hampering a comparison of detection results (see, for example, Jacoby and Davis 2007), and does not provide detection and false alarm rates because of the focus on battery exhaustion. Even SAPID is limited to wireless ad-hoc networks, in contrast to the generally applicable Dr.WATTson, while OCSVM and Sayegh cannot be used for retrofitting ICSs.

Also note that the 100% detection rate is not based on an overfitting of the system, but on the clear distinction between normal and malign current patterns. Such detection rates are only reachable in such ICS scenarios, having a limited number of well-defined processes, but not in general purpose systems like a desktop PC browsing in the Internet. Real-world applications are more challenging and may generate more noise and therefore higher false alarm rates. The results achieved were even better than hoped for, providing a promising base for the distributed application of Dr.WATTson in a real SCADA system.

Having a look at the security of the architecture itself, it does not introduce new attack vectors as it is only using voltage levels and current drains collected by sensory which is not intervening into the monitored system. The self-monitoring capability of Dr.WATTson also hampers physical manipulation of the system itself.

TABLE 2. EVALUATION RESULTS OF DR.WATTSON AND COMPARISON WITH OTHER SYSTEMS

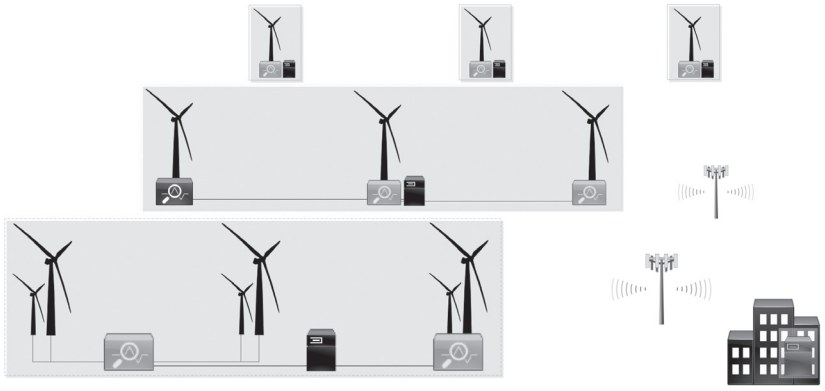
System	Detection Rate	False Alarm Rate	Attack Classification
Dr.WATTson	100	0.13	45.5
SAPID (Srinivasan et al.)	98.0	3.0	-
OCSVM (Maglaras et al, 2014)	96.3	2.5	-
Anomaly-based Intrusion Detection System (Sayegh et al. 2014)	89.9	1.3	-

B. Distributed Intrusion Detection by Dr.WATTson

Based on the detection capabilities of Dr.WATTson, multiple distributed setups for ICSs can be designed. Figure 6 presents a respective SCADA scenario of a wind energy park, consisting of multiple, dislodged generators. The possible visualised measurement setups are:

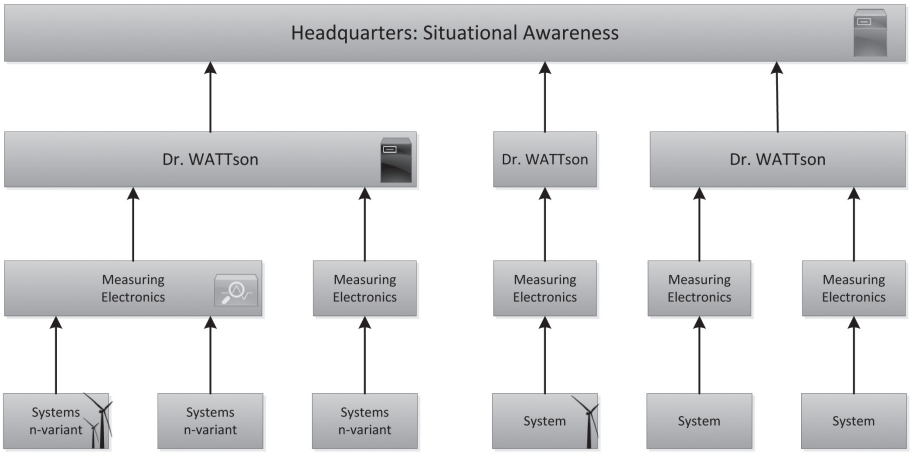
- N-variant systems, centrally measured (first generator line in Figure 6);
- Single systems, decentralised measured (second and third generator line); and, for both cases the possibilities:
- Centrally evaluated (first and second generator line); or
- Decentralised evaluated (third generator line).

FIGURE 6. SCENARIO OF A WIND PARK WITH THREE LINES OF GENERATORS



Note that for a wind park, as each wind generator is a high-value asset, the setup 'single systems, decentralised measured, decentralised evaluated' with providing a consolidate picture for generating the situational awareness at the headquarters would be preferable, while the ICS of a factory with a multitude of components can be likely monitored by a centrally measured, n-variant setup. While centralised measurements of multiple systems saves hardware, the disadvantage is that the 1:1 correlation gets lost: an alert can only be assigned to the measuring instance, not the precise end system. By realising decentralised measurements, the quantity of required hardware is the most, but malign behaviour can be detected and assigned rapidly. The selection of centralised or decentralised evaluation depends on the size of the system to be monitored and the company structure. In all configurations, it is possible to generate a situational awareness picture based on the individual Dr.WATTson instances (see Figure 7).

FIGURE 7. SETUPS FOR DISTRIBUTED INTRUSION DETECTION BY DR.WATTSON



4. OUTLOOK

Intrusion Detection in ICSs and complex SCADA systems is challenging, as several particularities apply. While SCADA systems are increasingly endangered, their security remains inadequate and reports are alarming. Major challenges arise as state-of-the-art IDSs are not able to cope with the special requirements of ICSs and control systems often cannot be retrofitted.

To overcome these shortcomings, we present a new intrusion detection architecture based on low-cost mini-computers which evaluate current drain measurements to achieve intrusion detection. In contrast to other approaches, our system can be used for retrofitting even non-expandable control systems.

Based on the promising results of the prototype Dr.WATTson, we designed a distributed IDS for SCADA systems. Next, a comprehensive test and an evaluation within a productive environment will be done, where we deploy the distributed Dr.WATTson, using an ODROID-C2 hardware base and a new GPU-based pattern evaluation. As the C2 supports GPIOs without additional IO-Shield, system performance is increased but low-priced components are still used. At the moment, we are talking with an energy provider about realising this evaluation of Dr.WATTson within a live SCADA system.

ACKNOWLEDGMENT

This work was partly funded by FLAMINGO, a Network of Excellence project (ICT-318488) supported by the European Commission under its Seventh Framework Programme.

REFERENCES

Andreeva, O., Gordeychik, S., Gritsai, G., Kochetova, O., Potseluevskaya, E., Sidorov, S. I. & Timorin, A. A. (2016). *Industrial Control Systems Vulnerabilities Statistics*. Kaspersky Lab.

Baishakhi, R., Posnett, D., Filkov, V. & Devanbu, P. (2014). A large-scale study of programming languages and code quality in github. *Proceedings of the 22nd ACM SIGSOFT International Symposium on Foundations of Software Engineering*. ACM New York.

Bodenheim, R. C. (2014). *Impact of the Shodan Computer Search Engine on Internet-facing Industrial Control System Devices*. Thesis, AFIT-ENG-14-M-14. Department of the Air Force Air University. Air Force Institute of Technology.

Buennemeyer, T., Jacoby, G., Chiang, W., Marchany, R. & Tront, J. (2006). Battery-sensing intrusion protection system. *Information Assurance Workshop*, pp. 176-183. IEEE.

Carlson, R. (1998). *Towards a Standard for Highly Secure SCADA Systems. Report SAND98-2220C, Sandia National Laboratories, Albuquerque, NM, and Livermore, CA*. Sandia Corporation.

Cavusoglu, H., Cavusoglu, H. & Zhang, J. (2008). 'Security patch management: share the burden or share the damage?' Management Science, 4, pp. 657-670.

Childs, D. (2015) *HP Security Briefing, Episode 22: The hidden dangers of inadequate patching strategies*. April 06. Retrieved January 5, 2017 from https://community.hpe.com/t5/Security-Research/HP-Security-Briefing-Episode-22-The-hidden-dangers-of-inadequate/ba-p/6752022#.WG-1be17a3B.

GLEG Ltd. (2015). *GLEG - information security company. Agora exploit pack developer*. Retrieved January 5, 2017 from http://gleg.net/agora_scada_upd.shtml/.

Guri, M., Solewicz, Y. A., Daidakulov, A. & Elovici, Y. (2016). *DiskFiltration: Data Exfiltration from Speakerless Air-Gapped Computers via Covert Hard Drive Noise.* Ben-Gurion University of the Negev.

Harp, D., & Gregory-Brown, B. (2016). *SANS 2016 State of ICS Security Survey*. SANS Institute.

Idaho National Laboratory. (2008). *Control Systems Cyber Security: Defense in Depth Strategies*. Department of Homeland Security.

Jacoby, G. & Davis, N. (2007). Mobile host-based intrusion detection and attack identification. *IEEE Wireless Communications*, vol. 14, no. 4, pp. 53-60.

Juniper Research. (2015, May 12). 'Cybercrime will Cost Business Over $2 Trillion by 2019'. Retrieved July 6, 2016, from http://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion.

Koch, R. (2009). 'Changing Network Behavior'. *Third International Conference on Network and System Security*. IEEE.

Le, X.-B. D. (2016). *Towards Efficient and Effective Automatic Program Repair*. Singapore Management University, School of Information Systems.

Lee, R. M., Assante, M. J. & Conway, T. (2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid*. Electricity Information Sharing and Analysis Center. Washington DC: SANS Institute.

Maglaras, L. A., Jiang, J. & Cruz, T. (2014). Integrated OCSVM mechanism for intrusion detection in SCADA systems. *Electronics Letters* vol. 50 no. 25, pp. 1935-1936.

McAfee. (2014). *Net Losses: Estimating the Global Cost of Cybercrime*. Santa Clara: Intel Security.

Mcquillan, J. L. & Lloyd, C. A. (2016). SCADA Intrusion Detection Systems, *Publication Number US20160094578 A1, PAT. Application Number US 14/501,672*. Schneider Electric USA, Inc.

Mimoso, M. (2015). 'Creaking Patch Tuesday's Viability Rests with Quality, Speed'. Retrieved January 5, 2017 from threatpost.com: https://threatpost.com/creaking-patch-tuesdays-viability-rests-with-quality-speed/110941/.

Mitchell, R. & Chen, I. (2014). 'A survey of intrusion detection techniques for cyber-physical systems'. *ACM Computing Surveys (CSUR)*, vol. 46, no. 4.

Nash, D., Martin, T., Ha, D. & Hsiao, M. (2005).' Towards an intrusion detection system for battery exhaustion attacks on mobile computing devices'. *Third IEEE International Conference on Pervasive Computing and Communications Workshops*, pp. 141-145.

NATO. (2016). 'NATO: Cyber defence'. Retrieved January 8, 2017 from http://www.nato.int/cps/en/natohq/topics_78170.htm.

Ormandy, T. (28. June 2016). 'How to Compromise the Enterprise Endpoint'. Retrieved July 14, 2016 from http://googleprojectzero.blogspot.de/2016/06/how-to-compromise-enterprise-endpoint.html.

Paganini, P. (2014). 'InfoSec Resources - Foreign Hackers Constantly Target US Critical Infrastructure'. 24 November. Retrieved January 7, 2017 from http://resources.infosecinstitute.com/foreign-hackers-constantly-target-us-critical-infrastructure/#gref.

Panko, R. (2008). 'Error Rates in Programming'. Retrieved July 14, 2016 from http://panko.shidler.hawaii.edu/HumanErr/Index.htm.

Reed, J. H. & Gonzalez, C. R. (2012). 'Enhancing Smart Grid Cyber Security using Power Fingerprinting'. *Future of Instrumentation International Workshop (FIIW)*. IEEE.

REUTERS. (2016). 'Massive cyber attack could trigger NATO response: Stoltenberg'. June 16. Retrieved 7 January 2017, from http://www.reuters.com/article/us-cyber-nato-idUSKCN0Z12NE.

Saglam, M. (2014). *A Military Planning Methodology for Conducting Cyber Attacks on Power Grid*. Master Thesis, Virginia Polytechnic Institute and State University, Falls Church, Virginia.

Sayegh, N., Elhajj, I. H., Kayssi, A. & Chehab, A. (2014). 'SCADA Intrusion Detection System based on temporal behavior of frequent patterns'. *2014 17th IEEE Mediterranean Electrotechnical Conference (MELECON 2014)*, pp. 432-438.

Srinivasan, T., Vijaykumar, V. & Chandrasekar, R. (2006). 'A self-organized agent-based architecture for power-aware intrusion detection in wireless'. *International Conference on Computing & Informatics*, pp. 1-6.

Stajano, F. (1999). 'The resurrecting duckling'. *Security Protocols*, pp. 183-194.

Stepanova, T., Kalinin, M., Baranov, P. & Zegzhda, D. (2010). 'Homogeneity analysis of power consumption for information security purposes'. *Proceedings of the 3rd International Conference on Security of Information and Networks, ser. SIN '10*, pp. 113-117.

Wilson, C. (2012). *Industrial and SCADA Systems May Be Increasingly Targeted for Cyberattack*. University of Maryland University College.

Wolff, J. (2016). 'Perverse Effects in Defense of Computer Systems: When More is Less'. *2016 49th Hawaii International Conference on System Sciences (HICSS)*, pp. 4823-4831.

Yang, D., Usynin, A. & Hines, J. W. (2006). 'Anomaly-based intrusion detection for SCADA systems'. *5th intl. Topical Meeting on Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies*, pp. 12-16.

Yang, Y., McLaughlin, K., Sezer, S., Littler, T., Im, E., Pranggono, B. & Wang, H. F. (2014). 'Multiattribute SCADA-Specific Intrusion Detection System for Power Networks'. *IEEE Transactions on Power Delivery*, vol. 29, no. 3, pp. 1092-1102.

Zhu, B. & Sastry, S. (2010). 'SCADA-specific intrusion detection/prevention systems: a survey and taxonomy'. *Proceedings of the 1st Workshop on Secure Control Systems (SCS)*.