Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P565-cd

Practical Barriers in Implementing Intrusion Detection Systems in Control Systems in Electric Utilites

Jon-Martin Storm
Institute of Informatics, University Of Oslo, Norway. E-mail: jonmartp@uio.no

Janne Hagen
Institute of Informatics, University Of Oslo, Norway. E-mail: jannehag@uio.no

The last ten years have seen an increased Cyber-risk against Industrial Control Systems (ICS). ICS is paramount for everything in our lives, from industrial manufacturing to controlling critical infrastructure. While many cybersecurity controls are adjusted to work in these systems, some essential measures have yet to see broad implementation. One is Intrusion Detection Systems (IDS), which detect cyberattacks and incidents that preventive controls have not stopped. We have conducted a case study based on audit reports and interviews with five security experts in Norwegian electric utilities to explore barriers to implementing IDS. We have found that detection control is more commonly applied at an ICS's perimeter than through an IDS. The study implies that security experts in the utilities consider human resources the main barrier to implementing IDS. There are also differences between experts working at utilities and those working for CERTs on how they value the benefits of IDS.

Keywords: Intrusion Detection System, Cybersecurity, Organizational Challenges, OT, Critical Infrastructure, Energy Utilities, Industrial Control System

1. Introduction

Industrial control systems (ICS) are digital systems that control physical processes in some sense. ICSs are used in everything from supporting and controlling industrial processes related to manufacturing cars to controlling and operating critical infrastructures like, for instance, electric power supply. Failure in ICS can impact physical processes and thus cause actual physical damage and even impact health and life. At the same time, ICS is a digital system vulnerable to cyber-attacks. The last decade has shown that various attackers are motivated and willing to attack these systems. Well-known cyberattacks in the press include the cyberattack on the nuclear facility in Natanz, Iran in 2011 (Falliere, Murchu, and Chien 2011), attacks on the power grid in Ukraine in 2015 and 2016 (Lee, Assante, and Conway 2016), attack on Norsk Hydro's aluminum extruders in 2019 (Kaspersky 2019), and colonial pipeline in 2021 (Bing et al. 2021) to mention a few. Cyberattacks have also shed light on supply chain vulnerabilities and the wide-reaching consequences such attacks might have for users of services provided by those suppliers. Well-known attacks cover Solarwind (Alkhadra et al. 2021) and Volue (Kovacs 2021). ENISA threat report 2022 (ENISA 2022) gives a brief overview of cyberattacks in 2022 and lists eight types of cyberattacks: Ransomware, malware, social engineering, denial of service, internet-threats, disinformation, and supply-chain attacks.

Like other digital systems, ICSs need security controls to detect, protect, react, and improve barriers against cyberattacks, insider threats, and human failures. A previous review of scientific studies has shown only a small volume of implementation-ready Intrusion Detection Systems (IDS) for ICS (Storm, Hagen, and Toftegaard 2021). Another study on Norwegian utilities showed that compliance with regulations demanding the use of ICS IDS is high (Storm, Hagen, and Selnes 2022). These contradictory findings trigger three questions:

(i) What do security practitioners in electric utilities consider being a detection control?
(ii) Is the lack of tested IDS for ICS in research not a barrier to implementing ICS IDS in

electric utilities?

(iii) What are the barriers when implementing detection controls in ICS in electric utilities?

The rest of the paper is structured like this: Chapter 2 presents ICS and ICS IDS concepts and related research. Chapter 3 presents our methodology and data sources. Chapter 4 gives a brief overview of the main findings. Chapter 5 includes some remarks regarding further work rather than a conclusion.

2. Industrial Control Systems and Intrusion Detection Systems

2.1. *Industrial Control Systems*

Industrial processes and manufacturing often use digital systems to automate production. These systems are generally called Industrial Control Systems (ICS) and, more recently, Operational Technology (OT). NIST's Guide to Industrial Control Systems (ICS) Security (800-82 rev2) presents a commonly used definition:

> Definition 1: "An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy)." (Stouffer et al. 2015, p. 2-1)

This definition fits well with the ICS used in electric utilities, where the ICS is used to control flow in the grid or generation of electric energy. We also find variants called Supervisory Control and Data Acquisition (SCADA) systems and Distributed Control Systems (DCS) in electric utilities. However, the concept is the same, a digital system that helps automate the physical process.

2.2. *Intrusion Detection Systems*

Intrusion detection systems (IDS) are digital systems designed to collect and analyze data from a digital system to detect and alert on possible intrusions or attacks. The traditional data sources are network or host data (Scarfone and Mell 2007). The term IDS has been used on different systems, from Security Information and Event Management (SIEM) systems to more basic systems doing Syslog aggregation (Knapp and Langill 2014). There is still an essential difference between a SIEM and a pure IDS, as a SIEM can be set up to correlate logs and events to detect more advanced incidents (Knapp and Langill 2014; Harris and Maymi 2018; Scarfone and Mell 2007; McLauglin 2014).

IDSs need to be adjusted to work well in ICSs. Vital differences between ICSs and more typical IT systems affect the implementation and use of IDSs (Knapp and Langill 2014). Key differences are the need for real-time communication, a larger ratio of embedded systems, and direct control of physical processes (Storm, Hagen, and Toftegaard 2021).

3. Related research

(Werlinger et al. 2008) examined the challenges of deploying and maintaining an IDS by analyzing nine interviews with IT security practitioners. They found that practitioners found it difficult to decide where to place the IDS and how best to configure it for use in a distributed environment.

Based on these results, (Werlinger, Hawkey, and Beznosov 2009) created a framework of human, organizational, and technological challenges and their interplay that security experts face in their organizations. The framework provides a way to classify challenges that security practitioners face, which is relevant to use in our case study.

(Thompson, Rantanen, and Yurcik 2006) looked into using textual and visual tools to help network security engineers detect intrusions in computer networks. However, they focused on the challenges of using an IDS, not implementing it.

We have yet to identify case studies looking into challenges in implementing IDS in ICS, and our research is novel.

4. Methodology

4.1. *Exploratory research strategy*

We selected an exploratory research strategy with a case study (Flyvbjerg 2011) as the research methodology. Using case study methodology, we can collect data from secondary sources, like

documents, and add more qualitative information from personal interviews with subject matter experts in the Norwegian power sector. We then used a qualitative description approach to answer the research questions, relying on the empirical data from interviews with security experts in Norwegian power companies and findings in information security audits. (Sandelowski 2000, 2010; Lambert and Lambert 2012)

We developed an interview guide with three main questions that guided the semi-structured discussions with the subject matter experts:

- What do security practitioners consider when they describe IDS, detection system, or monitoring system?
- Do companies develop their detection systems or buy commercial-of-the-shelf systems?
- What are the challenges and opportunities they see in using some detection systems for ICS?

In addition to data collected through interviews, we base the case study on statistics from audit reports.

4.2. *Data Collection*

4.2.1. *Semi-structured interviews*

We conducted five semi-structured interviews with six security experts working in five Norwegian companies within the electric power sector. The selected experts have experience with the use of IDS in ICS for almost ten years. We conducted the interviews in late 2022 and early 2023.

We conducted two interviews with security practitioners from power production companies, two interviews with security practitioners from grid companies, and one interview with a security expert from the national energy CERT.

Initially, we contacted ten companies and explicitly stated that we would not use the information for audit purposes. Due to various reasons, five companies refused to participate. The stated reasons were that they lacked time, were uncomfortable sharing sensitive information, or feared that our institute would use the information in an audit later.

4.2.2. *Security audits*

The Norwegian Water Resources and Energy Directorate (NVE) conducted 25 on-site audits on ICS from 2013 until 2022 with energy utilities, both grid companies and energy generators. The on-site audits aimed to evaluate compliance with the Power Contingency Regulation (Olje- og energidepartementet 2018). The regulation covers specific cybersecurity requirements for prevention, detection, response, and recovery controls for ICS. The last expansion of the regulation also expanded the cybersecurity requirements to apply to all digital information systems owned and operated by energy utilities. The audits were documented in confidential audit reports, which we first anonymized and then could use in our study.

4.3. *Data analysis*

We used thematic analysis (Clarke, Braun, and Hayfield 2015) with the concepts found in the data. We used an interactive set of categories and themes and coded for concepts. We also used the frequency of categories where possible.

4.4. *Method weakness*

A case study is a flexible method especially useful in pilot research. However, there are a few limitations as well. It is difficult to generalize the findings as the sample size is often small, and there is a risk of bias where our, as researchers, opinions influence the research. We did only five interviews, so we only got a small sample of the total number of companies (150). We have aimed to mitigate this by using another source of data, the audits. However, we must be aware that our findings only represent the body of data we have examined.

Another area for improvement in our study is that we only used one interviewer in the interviews, which again introduces a possibility for bias. We have addressed this bias by reviewing the central answers in the interview notes together with the interviewee at the end of the interview. A better option would be to transcribe the interview; however, the study's time frame limited our options.

Still, with the interviews done, we can explore the topic under study and showcase some differences in experiences between subject matter experts.

5. Findings

5.1. *Audit reports*

We studied 25 audit reports from 2013 to 2022, of which ten did not cover compliance with using ICS IDS. We studied the description of the non-compliance from two requirements. One of the ICS security requirements is establishing automatic monitoring, logging, assessment, and alerts. The other ICS requirement is to detect and handle errors and faults. We grouped the answers by category and noted the frequency in table 1.

Table 1. Frequency of different categories of description of non-compliance for detection control in IDS for Norwegian electric utilities.

Category	freq
Ongoing implementation	3
No procedure to respond to security events	3
Total lack, no plans	2
IDS only in some parts of the system	2
Lack of personnel to handle events	2
No procedure to handle errors in software	2
Lack of procedure to alert CERT	1

5.2. *Interviews*

We did a thematic analysis of the interviews and classified the topics into eight themes:

(i) Definitions
(ii) Systems used for detection
(iii) Suppliers and procurement
(iv) Feelings
(v) Opportunities
(vi) Challenges
(vii) IT/OT
(viii) Competence

The next sections present each of them.

5.2.1. *Definitions*

This category includes the interviewees' different topics regarding their understanding of a detection system. Their understanding included "a system to detect something,"; "log analysis", "log collection", "detecting abnormal behavior", "intrusion detection system", "detection of exploitation in applications or systems", "detection and preventing attacks", "some alerts and some analysis" and "automated detection".

5.2.2. *Systems used for detection*

This category sums up the systems used for detection in the IT/OT infrastructure for the different companies. The systems were; "firewall with IDS", "firewall with logs", "endpoint detection and response (EDR)", "antivirus", "MS365 audit logging and monitoring", "AD-audit logs", "Security Information and Event Management (SIEM)", "endpoint logging".

5.2.3. *Suppliers and procurement*

The interviewees also talked about suppliers of security operations center (SOC) services and procurement of IDS and SIEMs. In this category, there were a few themes present; "great value from buying services", "no value from buying services", "24/7 detection and response only present when using suppliers", "need for internal resources and competence when using supplier", "developed own SIEM", "bought SIEM", "bought IDS", "most buy detection from a supplier/service provider".

5.2.4. *Feelings*

We coded some parts of the interviews into a category of feelings. "happy with detection capabilities", "CISO sleeps better", "no guilty conscience", "not happy, no time to do it properly", "not satisfied, need better detection".

5.2.5. *Challenges*

We categorized challenges into comments connected to implementation, operations, or response. For implementation, "Long setup time, tuning", "[IDS] needs to be tailored to our system", "differences in perception between IT and OT per-

sonnel", "underestimation of resources needed to acquire [IDS]", "lack of resources to do proper setup/tuning", "need more competence to tune", "difficulties centralizing logs", "difficult to setup proper Dashboards". For operations, "manual audit of logs", "time-consuming to add alerts manually", "hard to keep IDS setup correctly in changing systems", "not sure to handle alerts", "not 24/7 operations". For response; "needs an internal team that can handle incidents", "lack of shift schedule, alert handling based on voluntary service", "evenings/nights have always been ok since everything has been handled", "too many different systems, lack of coordination".

5.2.6. *Opportunities*

Opportunities were covered both achieved and potential opportunities; "Better overview and control", "view of actual network traffic", "cleaned up a lot of network traffic and devices", "Used a lot in troubleshooting", "better visibility", "24/7 surveillance and alerts", "more time for the stuff we spend much time on", "error fixing covers the cost alone".

5.2.7. *IT/OT differences*

Some answers contained themes related to IT/OT peculiarities or differences; "IT-infrastructure not affected by IDS implementation", "need to do changes in OT for implementing IDS", "need to give more access in OT", "challenges in ring-networks in OT", "the same IDS in OT and IT", "tuning is simple in OT", "different IDS in OT and IT", "events are handled as IT-management", "implemented IDS in IT, not yet OT", "how to show alerts to operators in OT?", "detection needs network segmentation, but this was already done."

5.2.8. *Competence*

The last category covers competence, both technical competence and security competence for the organization. For the technical competence; "Little additional expertise was required, only extra resources", "needs the competence to understand your infrastructure", "needed to learn the new systems", "if you know firewalls, it is mostly the same [about IDS integrated into firewalls]", "Needs security competence in procurements", "needs competence IT-security, network, maintenance, and OT-operations", "had the necessary skills". For the organization, "Not hard to get the budget, security-aware leadership", "needed multi-organizational approval for a cross-organizational acquisition", "not challenging to get approval", "maturity assessment in the leadership-team made the approval easy", "needed to do a maturity assessment before the leadership were aware of the security issues".

6. Discussion

6.1. *What do security practitioners in electric utilities consider being a detection control?*

The results show that conceptually there is a range of different understandings of a detection system. The category includes answers related to collecting information and analyzing logs to look for abnormal behavior or exploitation, and finally, alerting.

The actual systems used for detection mirrored the conceptual understanding of what a detection system could be, which is broader than a pure IDS. For example, firewall logs and antivirus are considered detection systems by the interviewees. Other interpretations are; pure audit logging and monitoring and the more expected SIEM system. This finding indicates that our assumption about IDS as the primary detection control is erroneous and that we should broaden our perception of detection control in further studies.

6.2. *Is the lack of tested IDS for ICS in research, not a barrier to implementing ICS IDS in electric utilities?*

The answers show that the experts choose different options for implementing IDS in IT and OT. Some buy and manage products in-house, some buy SOC solutions, and others build their detection based on a SIEM solution. The expert from the CERT said that they experienced that most organizations buy a detection service from a service provider, but we did not see that mirrored in our sample. Nothing in the interviews

indicates that the lack of tested IDS for ICS in research affects the implementation of actual IDS in ICS. One of the interviewees mentioned a specific IDS for ICS vendor, which they already use, which indicates that one of the assumptions in our previous research that commercial options are not present in research might be correct (Storm, Hagen, and Toftegaard 2021). The audit reports could have given some insights into this but lacked information about the reason for not implementing detection in ICS.

6.3. *What are the barriers when implementing detection controls in ICS in electric utilities?*

Based on the details in the audit reports' text, it was impossible to find the reason for the lack of implementation or compliance and map it to the challenges presented by (Werlinger, Hawkey, and Beznosov 2009). The audit reports detail the requirements with which the company lacked compliance, what the lack was, and how to fix it, but not any details about the reason behind the non-compliance. However, the interviews gave us some insights into the barriers and challenges that the security practitioners phased.

Of the challenges related to human issues (Werlinger, Hawkey, and Beznosov 2009), the interviews' analysis shows no gap concerning lack of training or experience. However, there might be some issues regarding culture and how to communicate security issues. In the competence category, we identified one answer regarding the need for maturity assessment before the leadership understood the need for detection controls. There seems also to be differences in perception between IT and OT personnel in at least one of the coded answers in the challenges category.

We also have findings regarding challenges in risk estimation and tight schedules for organization issues (Werlinger, Hawkey, and Beznosov 2009). For risk estimation, we regard the same point as the need for a maturity assessment before perceiving the risk correctly. Furthermore, multiple contents indicate a tight schedule or lack of time to be a challenge in the challenges category.

Most interviewees had no issues with getting top management support. For the other organizational challenges mentioned in (Werlinger, Hawkey, and Beznosov 2009), we found nothing indicating an issue in our case. For completion's sake, these are; "open environments and academic freedom", "lack of budget", "security is a low priority", "business relationships with other organizations", "distribution of IT responsibilities", "access control to sensitive data" and "the size of the organization".

Regarding technical issues, we only found one case. The finding was that mobility and distributed access were challenging, especially concerning difficulties centralizing logs. There were no issues regarding the complexity of systems, vulnerabilities, or lack of effective security tools. As mentioned earlier, this last point is surprising, as our earlier work (Storm, Hagen, and Toftegaard 2021) found a lack of IDS for OT in the current pool of research. However, there are two other possible answers to this, first; in the interviews, we saw that they consider multiple other detection tools as well. Secondly, Many commercial IDS tools for OT exist that we did not find mentioned in the research surveyed in 2021, such as Darktrace DETECT, Nozomi Networks, S-NOK, Cisco CyberVision, and Omicron StationGuard.

7. Further work

This case study has indicated that companies in the Norwegian energy sector do not necessarily find most of the classical challenges in IT security management when implementing detection controls in IT and OT. Even though earlier research has found that there are not many possible IDS suppliers for OT, this is not the only tool for detection. The companies in the case study use a variety of loggings and systems for detection based on them, some use SIEMs without IDSs, and some use firewalls with IDS possibilities. (Dragos 2023) presents a view that only 86% of their engagements in the electric sector had network visibility issues, which is per our findings. But there is still a need to investigate the detection possibilities and see if the proposed solutions in the interviews give sufficient network visibility or only perimeter visibility. Another venue for research is to look

into the different suppliers of IDS in ICS, which are used in electric utilities, and if they detect ICS-specific attacks or is just an IT-based IDS placed in ICS for compliance.

Acknowledgement

The Norwegian Water Resources and Energy Directorate funded the study in the R&D project FoU-80166. We would like to thank the directorate for access to confidential data and for answering our questions related to the audits.

References

Alkhadra, Rahaf, Joud Abuzaid, Mariam AlShammari, and Nazeeruddin Mohammad. 2021. "Solar winds hack: In-depth analysis and countermeasures." In *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT),* 1–7. IEEE. https://doi.org/10.1109/icccnt51525.2021.9579611.

Bing, Christopher, Stephanie Kelly, Christopher Bing, and Stephanie Kelly. 2021. "Cyber attack shuts down U.S. fuel pipeline 'jugular,' Biden briefed," May 8, 2021. Accessed March 30, 2023. https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/.

Clarke, Victoria, Virginia Braun, and Nikki Hayfield. 2015. "Thematic analysis." In *Qualitative psychology: A practical guide to research methods,* 3rd ed., edited by Jonathan A. Smith, 222–248. Sage.

Dragos. 2023. *2022 Dragos ICS/OT Cybersecurity Year in Review* [in en]. Technical report 2022. Dragos. Accessed March 30, 2023. https://www.dragos.com/blog/industry-news/2022-dragos-year-in-review-now-available/.

ENISA. 2022. *ENISA Threat Landscape 2022* [in en]. Technical report 2022. European Union Agency for Cybersecurity (ENISA). Accessed March 30, 2023. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.

Falliere, Nicolas, Liam O Murchu, and Eric Chien. 2011. "W32. stuxnet dossier." *White paper, symantec corp., security response* 5 (6): 29.

Flyvbjerg, Bent. 2011. "Case study." In *The SAGE handbook of qualitative research,* 4th ed., edited by Norman K. Denzin and Yvonna S. Lincoln, 301–316. SAGE Publications.

Harris, Shon, and Fernando Maymi. 2018. *CISSP All-in-One Exam Guide, Eighth Edition* [in English]. 8 edition. New York: McGraw-Hill Education, October. ISBN: 978-1-260-14265-5.

Kaspersky. 2019. "Metallurgical giant Norsk Hydro attacked by encrypting malware." Kaspersky ICS CERT, March 22, 2019. Accessed May 18, 2020. https://ics-cert.kaspersky.com/news/2019/03/22/metallurgical-giant-norsk-hydro-attacked-by-encrypting-malware/.

Knapp, Eric D., and Joel Thomas Langill. 2014. *Industrial Network Security, Second Edition: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems* [in English]. 2nd ed. Syngress, December. ISBN: 0-12-420114-8.

Kovacs, Eduard. 2021. "Green Energy Company Volue Hit by Ransomware." SECURITYWEEK, May 13, 2021. Accessed March 30, 2023. https://www.securityweek.com/green-energy-company-volue-hit-ransomware/.

Lambert, Vickie A., and Clinton E. Lambert. 2012. "Qualitative descriptive research: An acceptable design." *Pacific Rim international journal of nursing research* 16 (4): 255–256.

Lee, Robtert M., Michael J. Assante, and Tim Conway. 2016. "Analysis of the cyber attack on the Ukrainian power grid." *Electricity Information Sharing and Analysis Center (E-ISAC)* 388:1–29.

McLauglin, Kieran. 2014. *Intrusion Detection for SCADA Systems,* April.

Olje- og energidepartementet. 2018. *Forskrift om sikkerhet og beredskap i kraftforsyningen (kraftberedskapsforskriften).* Norway. https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157.

Sandelowski, Margarete. 2000. "Whatever happened to qualitative description?" *Research in nursing & health* 23 (4): 334–340. https://doi.org/https://doi.org/10.1002/1098-240X(200008)23:4⟨334::AID-NUR9⟩3.0.CO;2-G.

———. 2010. "What's in a name? Qualitative description revisited." *Research in nursing & health* 33 (1): 77–84. https://doi.org/https://doi.org/10.1002/nur.20362.

Scarfone, Karen, and Peter Mell. 2007. *Guide to Intrusion Detection and Prevention Systems (IDPS)* [in en]. Technical report NIST Special Publication (SP) 800-94. National Institute of Standards and Technology, February. Accessed March 20, 2020. https://doi.org/https://doi.org/10.6028/NIST.SP.800-94. https://csrc.nist.gov/publications/detail/sp/800-94/final.

Storm, Jon-Martin, Janne Hagen, and Selnes Haug Selnes. 2022. "The Effect of Regulation and Audits on Implementation of Cybersecurity Controls in Norwegian Grid Companies." In *Proceedings of the 32nd European Safety and Reliability Conference (ESREL 2022).* Dublin, Ireland: RESEARCH PUBLISHING, SINGAPORE. ISBN: 978-981-18518-3-4. https://doi.org/10.3850/978-981-18-5183-4_R09-03-295-cd.

Storm, Jon-Martin, Janne Hagen, and Øyvind Anders Arntzen Toftegaard. 2021. "A Survey of Using Process Data and Features of Industrial Control Systems in Intrusion Detection." In *2021 IEEE International Conference on Big Data (Big Data),* 2170–2177. IEEE. https://doi.org/https://doi.org/10.1109/BigData52589.2021.9671325.

Stouffer, Keith, Suzanne Lightman, Victoria Pillitteri, Marshall Abrams, and Adam Hahn. 2015. *Guide to Industrial Control Systems (ICS) Security* [in en]. Technical report NIST Special Publication (SP) 800-82 Rev. 2. National Institute of Standards and Technology, June. Accessed March 20, 2020. https://doi.org/https://doi.org/10.6028/NIST.SP.800-82r2. https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final.

Thompson, Ramona Su, Esa M Rantanen, and William Yurcik. 2006. "Network intrusion detection cognitive task analysis: Textual and visual tool usage and recommendations." In *Proceedings of the human factors and ergonomics society annual meeting,* 50:669–673. 5. SAGE Publications Sage CA: Los Angeles, CA. https://doi.org/https://doi.org/10.1177/154193120605000511.

Werlinger, Rodrigo, Kirstie Hawkey, and Konstantin Beznosov. 2009. "An integrated view of human, organizational, and technological challenges of IT security management." *Information Management & Computer Security* 17 (1): 4–19. https://doi.org/https://doi.org/10.1108/09685220910944722.

Werlinger, Rodrigo, Kirstie Hawkey, Kasia Muldner, Pooya Jaferian, and Konstantin Beznosov. 2008. "The challenges of using an intrusion detection system: is it worth the effort?" In *Proceedings of the 4th symposium on Usable privacy and security,* 107–118. https://doi.org/https://doi.org/10.1145/1408664.1408679.