IoT Security: Exploring Strategies and Approaches

Claudia Greco[1]

[1]University of Calabria, Italy

Abstract

That of IoT security is an extensive and tough field, which presents significant challenges that can be tackled from various perspectives, ranging from defensive to offensive approaches. The purpose of my research is to explore new attack vectors and protective techniques to address the myriad vulnerabilities plaguing IoT devices, specifically focusing on software security. This goal is pursued by exploring multiple aspects of IoT security, including Binary Analysis of firmware, IoT Penetration Testing and Vulnerability Assessment, and Attack Detection and Prediction, and Code Obfuscation.

Keywords

IoT Security, Vulnerability Discovery, Firmware Re-hosting, Attack Detection and Prediction, Penetration Testing, Code Obfuscation

1. Introduction

Nowadays, we are witnessing a major breakthrough in the computational landscape, since an ever-growing number of everyday objects is incorporating computational power and is continuously connected to the Internet. We are constantly surrounded by a plethora of computing devices and we are living the Internet of Things (IoT) revolution, where objects are becoming smarter and smarter and it looks like there is no application scenario where the extensive connectivity and availability of these devices can be avoided. On the one hand we have a new, glowing set of useful (or often just funny) functionalities for our appliances and even great opportunities for many different ecosystems, such as daily living, healthcare and Industrial Control Systems, to cite a few. The other side of the coin, however, is not as shiny as we may expect. Disastrous security breaches, lack of appropriate security and safety measures, jeopardized privacy, get headlines everyday and IoT devices are dangerously appealing to attackers and they are often considered low hanging fruits for their easy-to-exploit vulnerabilities. It is straightforward to notice how a careful, security oriented assessment of such devices is mandatory. However, traditional analysis techniques are often not applicable at all in the IoT scenario.

That of IoT Security, along with cybersecurity in general, is a vast topic that encompasses various different point of views, each with its own challenges. In my early doctoral studies I analyzed IoT system devices from the “outside”, by considering them as black boxes and assessing their security from an external viewpoint. My initial focus, described in section 1.1, was on scrutinizing the communications between devices, primarily examining jamming attacks

SEBD 2023: 31st Symposium on Advanced Database Systems, July 02–05, 2023, Galzignano Terme, Padua, Italy

claudia.greco@dimes.unical.it (C. Greco)
0000-0003-4929-2289 (C. Greco)

CEUR Workshop Proceedings (CEUR-WS.org)

in drone networks and studying the connections and security issues correlated with such interactions.

In the meantime, I began to study Penetration Testing and Vulnerability Assessment processes and how they apply to IoT environments. My intensive study in this field led me to write a comprehensive literature review paper related to the various applications, limitations, and future work of penetration testing in IoT-related scenarios. Through my research, I have gained a deep understanding of the challenges and opportunities associated with IoT security, and the importance of effective penetration testing in identifying and mitigating potential vulnerabilities. The literature review paper, detailed in section 1.2, presents a critical analysis of existing research in the field, highlighting the key issues and trends that are shaping the future of IoT penetration testing.

Another technique for analyzing IoT system security by treating devices as black boxes was to examine log data related to activities. The outcome of this approach was the development of a method for identifying and predicting malicious activities in Industrial Control Systems by integrating machine learning techniques with the mathematical model of TPP. This research line is described in more detail in section 1.3.

Subsequently, I shifted my attention towards the inner workings of IoT devices and how to assess their security by not simply relying on an external viewpoint. This led me to investigate firmware and I discovered that the existing dynamic analysis techniques are not suitable for IoT environments. This observation resulted in the design of a new methodology to enable the application of traditional dynamic analysis techniques to firmware, as discussed in section 2.

As I delved further, my focus shifted towards understanding the internal structure of firmware and how binaries can be targeted by attackers, piquing my interest in the concept of obfuscation and software protection in general.

1.1. Jamming Detection in FANETs

As wireless networks play an increasingly key role in everyday life, it is necessary to secure them from radio frequency attacks, such as jamming, which are hard to detect, especially because they may be easily mistaken for other network conditions. Jamming attacks are the equivalent of Internet Denial-of-Service (DoS) attacks for radio signals. In particular, jamming is the act of disturbing radio (wireless) communications by causing their Signal-to-Interference-plus-Noise-Ratio (SINR) to decrease, typically transmitting on the same frequency and with the same modulation as the signal to be disturbed.

Many of the existent solutions are not suitable for the context of specific wireless networks, such as drone networks, whose nodes are highly mobile and usually have limited computational capabilities and energy resources. For these reasons I designed a framework for jamming detection in drone networks, relying on a distributed approach based on supervised machine learning techniques, namely, Multi-layer Perceptrons and Decision Trees [1].

Given a reference data packet traceset, the proposed framework computes some predefined metrics, such as throughput, PDR and RSSI, which vary during a jamming attack, and that can therefore be used as features to detect it. The framework was evaluated using datasets coming from both real and simulated communication scenarios. In particular, I used datasets from publicly available standardized jamming attack scenarios with IEEE 802.11p radio data, and datasets generated via NS3-based simulation from networks of drones using WiFi. The performance of the classifiers is shown to improve as the sampling time of the packets decreases. Although both the designed classifiers obtain good performance in terms of jamming detection accuracy, the Multi-layer Perceptron resulted being more effective than the Decision Tree when applied to a novel communication scenario for which had not been trained.

The proposed framework reaches a satisfactory accuracy level of 96%, while requiring low computational and hardware capabilities, thus proving to be suitable for resource-constrained drone networks. To prove the actual usability of the proposed framework, it was tested on a constrained device such as the Raspberry Pi 3, showing that its measured execution times and storage consumption enable its use on limited devices.

1.2. IoT Penetration Testing

I performed a comprehensive review of the literature on penetration testing and vulnerability assessment of IoT devices and systems, with the aims of obtaining an in-depth understanding of the existing state-of-the-art advances. [2]. The literature was explored by systematically consulting popular research motors and using combinations of selected keywords. Specifically, a total of 99 articles published between 2015 and 2021 was reviewed to identify existing and potential IoT penetration testing applications and proposed approaches.The purpose of the review was to find an answer and possibly open a discussion around the following questions:

- RQ1: What are the IoT security issues that penetration testing can help identify?
- RQ2: What penetration testing frameworks have been proposed for IoT systems?
- RQ3: How AI has been used to provide autonomous penetration testing?

This study gave me the opportunity to better understand how the processes of penetration testing and vulnerability assessment can become even more challenging when applied to IoT environments. Due to the complex nature of IoT, involving a wide variety of technologies, traditional pentesting results being insufficient. With traditional pentesting, testers usually have to deal with Windows or Linux operating systems, TCP/IP protocols and common applications. On the contrary, IoT presents a wide number of new architectures such as ARM, MIPS, PowerPC, along with new operating systems such as FreeRTOS and VxWorks, and new communication protocols and technologies such as ZigBee, BLE (Bluetooth Low Energy), SDR (Software Defined Radio), and NFC (Near Field Communication). In the traditional internet, many attacks involve an end user to open an email or click a malicious link, while the mindset behind IoT attacks is very different. In addition, the interconnectivity and interdependency between devices and systems in the ecosystems can also introduce vulnerabilities due to new updates or new exploits being made available.

The discussion carried out in the paper led to the identification of a number of open research challenges related to the application of traditional vulnerability assessment techniques to IoT systems.

1.3. Identification and Prediction of Security Threats in Industrial Scenarios using Neural Network based Temporal Point Process

In recent years we have witnessed a rising paradigm shift in the Industrial Control Systems (*ICS*) landscape, since an ever-increasing number of technologies and devices are migrating from a traditional mechanical or electrotechnical often closed system, landing to integrated modern control systems. The new generation of ICS is based on a tight connection among components, made possible by the spread of both commercial off-the-shelf (*COTS*) products and open protocols, as well as by the price reduction of the hardware components needed for the development of these architectures. However, if on the one hand, the interconnection and the remote availability of ICS led to a reduction of the costs for industrial operators and to an increased efficiency, on the other hand, the growing complexity is coupled with an increasing attack surface [3] and on a change in the profile of the attacker, who is no more necessarily an insider, but can be an external actor exploiting the remote functionalities of the system. The high number of software components generate an endless stream of data of a different nature, ranging from network captures to application logs, from hardware monitoring logs to user interaction, and so on. The analysis of the generated data represents a task of primary importance because it often allows to thwart attacks even before they happen [4]. However, for this to occur, we cannot rely only on the ability of system administrators and domain experts of noticing relevant actions in huge software logs, but we need automated techniques able to analyze in a fast and reliable way all the information available [5, 6, 7, 8].

Critical infrastructures represent nowadays an extremely attractive target for criminals, as demonstrated by recent attacks (e.g. Stuxnet and Flame) and talks or academic papers [9, 10]. The attacks target various kinds of ICS or SCADA (Supervisory Control And Data Acquisition) systems, including industrial sectors such as automotive [11, 12], aerospace [13, 14], electricity [15, 16], oil and gas [17, 18], to cite a few. Due to the peculiar nature of the systems, it is straightforward to note that traditional approaches based on blacklisting (or whitelisting) activities are likely to fail, because, even if we are able to enumerate all malicious activities, we may incur in attacks that are the combination of several different actions that, when analyzed individually, are not considered menaces at all. There is a lot of information that can be inferred by the correct analysis of a log, and this knowledge can help to provide a roadmap to the origin of a specific threat, to identify the agents involved and even to predict future unauthorized behaviors, both from inside attackers and external ones [19, 20, 21].

In my research, I have been focusing on the analysis of logs related to industrial systems from a security viewpoint. My goal is to provide a novel approach to label malicious activity in logs and even predict potential future attacks. My approach is based on *Marked Temporal Point Processes* (MTPPs), a probabilistic stochastic framework which showed its effectiveness in different domains [22], such as earthquake prediction, aftershocks, healthcare, financial trends, activity daily living prediction [23, 24] and so on, but that has found less attention than it deserves in security oriented scenarios.

MTPP provides a useful representation of event streams and knowledge of attack information, making it a suitable technique for future research. The paper [25] and its extension [26] provide theoretical background on MTPP and problem formulation and modeling approach. I use Long Short Term Memory (LSTM) instead of a standard Recurrent Neural Network (RNN) for prediction model, and Recurrent marked TPP to model mark of an event and its occurring time. We implemented two different approaches, namely RMTPP and ERPP, to learn the conditional intensity function without any prior assumptions. Our experimental evaluation concludes that the proposed approach can identify malicious activities and predict future attacks in ICS.

2. Firmware Vulnerability Discovery

During my research I also explored the field of Binary Analysis and the applicability of traditional analysis techniques to embedded devices firmware. When it comes to dynamic analysis, indeed, traditional techniques are often not applicable at all in the IoT scenario. The dynamic analysis of the firmware of embedded devices is usually based on *firmware re-hosting*, which implies that its code is run in a virtual environment, with an appropriate level of accuracy such that the firmware itself is convinced to be executed on real hardware. The goal of transparently emulating a firmware is unsurprisingly hard to achieve, because usually the firmware interacts with on-chip and off-chip peripherals, such as sensors, actuators, communication interfaces, GPIO ports, just to cite a few. Moreover, the enormous heterogeneity in embedded hardware and architectures, as well as the vendor specific highly-integrated chip designs poses additional challenges in the emulation of a firmware.Several techniques have been proposed in literature following different approaches, such as *hardware-in-the-loop* [27, 28, 29, 30, 31], OS or hardware abstractions [32, 33, 34], and learning [35, 36], but they all present individual limitations, along with the fact that they all involve binary instrumentation to intercept calls to functions that perform I/O interactions. The limit behind this is that binary instrumentation is slow and makes the use of dynamic analysis techniques that require an high number of fast executions impractical. I cooperated with the proposal of a new approach for enabling faster security assessment of re-hosted firmware, based on firmware rewriting [37]. The idea behind our proposal is to rely on firmware code rewriting to integrate models of interactions between the firmware and hardware directly into the firmware binaries themselves, in order to avoid the binary instrumentation layer.

2.1. Conclusion and Future Work

The field of cybersecurity encompasses a vast range of challenges that can be approached from various perspectives. The domain of IoT is particularly intriguing due to the resource constraints in terms of computation and memory, which present numerous challenges for the implementation of efficient mitigations. Furthermore, the widespread adoption of IoT devices introduces security challenges due to the multitude of vulnerabilities they exhibit and the accompanying potential for exploitation. Throughout this doctoral program, multiple aspects of IoT security are being analyzed, employing diverse techniques to address various challenges from different angles, all converging towards a common overarching objective. The goal is to enhance the security of IoT systems by identifying and mitigating potential threats arising from malicious code and vulnerabilities that can undermine the integrity and confidentiality of software components. As part of forthcoming research, I am currently engaged in the development of sophisticated methodologies designed to proficiently identify malicious code and vulnerabilities in software, even when confronted with obfuscation techniques. These methodologies aim to overcome the challenges posed by code obfuscation and provide robust detection capabilities that can effectively discern and address potential threats in software systems. By enhancing the resilience of detection mechanisms, this research aims to advance the field of cybersecurity and contribute to the development of comprehensive and reliable solutions for identifying and mitigating malicious code and vulnerabilities in software architectures.

References

[1] C. Greco, P. Pace, S. Basagni, G. Fortino, Jamming detection at the edge of drone networks using multi-layer perceptrons and decision trees, Applied Soft Computing 111 (2021) 107806.

[2] C. Greco, G. Fortino, B. Crispo, K.-K. R. Choo, Ai-enabled iot penetration testing: state-of-the-art and research challenges, Enterprise Information Systems 0 (2022) 2130014. URL: https://doi.org/10.1080/17517575.2022.2130014. doi:10.1080/17517575.2022.2130014. arXiv:https://doi.org/10.1080/17517575.2022.2130014.

[3] P. K. Manadhata, J. M. Wing, An attack surface metric, IEEE Transactions on Software Engineering 37 (2010) 371–386.

[4] J. Babbin, Security log management: identifying patterns in the chaos, Elsevier, 2006.

[5] J. Jang-Jaccard, S. Nepal, A survey of emerging threats in cybersecurity, Journal of Computer and System Sciences 80 (2014) 973–993.

[6] M. Ianni, E. Masciari, Some experiments on high performance anomaly detection, in: 2022 30th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP), 2022, pp. 226–229. doi:10.1109/PDP55904.2022.00042.

[7] P. Zikopoulos, C. Eaton, et al., Understanding big data: Analytics for enterprise class hadoop and streaming data, McGraw-Hill Osborne Media, 2011.

[8] M. Ianni, E. M. DIETI, A compact encoding of security logs for high performance activity detection, in: 2021 29th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP), IEEE, 2021, pp. 240–244.

[9] L. Apa, C. M. Penagos, Compromising industrial facilities from 40 miles away, IOActive Technical White Paper (2013).

[10] B. Meixell, E. Forner, Out of control: Demonstrating scada exploitation, Black Hat (2013) 2013.

[11] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, et al., Experimental security analysis of a modern automobile, in: 2010 IEEE symposium on security and privacy, IEEE, 2010, pp. 447–462.

[12] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno, et al., Comprehensive experimental analyses of automotive attack surfaces., in: USENIX Security Symposium, volume 4, San Francisco, 2011, p. 2021.

[13] P. Bieber, J.-P. Blanquart, G. Descargues, M. Dulucq, Y. Fourastier, E. Hazane, M. Julien, L. Léonardon, G. Sarouille, Security and safety assurance for aerospace embedded systems, in: Embedded Real Time Software and Systems (ERTS2012), 2012.

[14] T. Cockram, S. Lautieri, Combining security and safety principles in practice, in: 2007 2nd

Institution of Engineering and Technology International Conference on System Safety, IET, 2007, pp. 159–164.

[15] A. Lee, T. Brewer, Smart grid cyber security strategy and requirements, Draft Interagency Report NISTIR 7628 (2009).

[16] A. Gumaei, M. M. Hassan, M. S. Huda, M. R. Hassan, D. Camacho, J. D. Ser, G. Fortino, A robust cyberattack detection approach using optimal features of SCADA power systems in smart grids, Appl. Soft Comput. 96 (2020) 106658.

[17] T. O. Grøtan, M. G. Jaatun, K. Øien, T. Onshus, The sesa method for assessing secure remote access to safety instrumented systems, SINTEF Report A 1626 (2007).

[18] S. O. Johnsen, Resilience at interfaces: Improvement of safety and security in distributed control systems by web of influence, Information Management & Computer Security (2012).

[19] E. E. Schultz, A framework for understanding and predicting insider attacks, Computers & Security 21 (2002) 526–531.

[20] K. Kent, M. Souppaya, Guide to computer security log management, NIST special publication 92 (2006) 1–72.

[21] A. Guzzo, M. Ianni, A. Pugliese, D. Saccà, Modeling and efficiently detecting security-critical sequences of actions, Future Generation Computer Systems 113 (2020) 196–206.

[22] J. Yan, H. Xu, L. Li, Modeling and applications for temporal point processes, in: Proceedings of the 25th ACM SIGKDD, 2019, p. 3227–3228.

[23] G. Fortino, A. Guzzo, M. Ianni, F. Leotta, M. Mecella, Exploiting marked temporal point processes for predicting activities of daily living, in: 2020 IEEE International Conference on Human-Machine Systems (ICHMS), IEEE, 2020, pp. 1–6.

[24] G. Fortino, A. Guzzo, M. Ianni, F. Leotta, M. Mecella, Predicting activities of daily living via temporal point processes: Approaches and experimental results, Computers & Electrical Engineering 96 (2021) 107567.

[25] G. Fortino, C. Greco, A. Guzzo, M. Ianni, Neural network based temporal point processes for attack detection in industrial control systems, in: 2022 IEEE International Conference on Cyber Security and Resilience (CSR), 2022, pp. 221–226. doi:10.1109/CSR54599.2022.9850333.

[26] G. Fortino, C. Greco, A. Guzzo, M. Ianni, Identification and prediction of attacks to industrial control systems using temporal point processes, Journal of Ambient Intelligence and Humanized Computing (2022) 1–13.

[27] N. Corteggiani, G. Camurati, A. Francillon, Inception:{System-Wide} security testing of {Real-World} embedded systems software, in: 27th USENIX Security Symposium (USENIX Security 18), 2018, pp. 309–326.

[28] M. Kammerstetter, C. Platzer, W. Kastner, Prospect: peripheral proxying supported embedded code testing, in: Proceedings of the 9th ACM symposium on Information, computer and communications security, 2014, pp. 329–340.

[29] K. Koscher, T. Kohno, D. Molnar, {SURROGATES}: Enabling {Near-Real-Time} dynamic analyses of embedded systems, in: 9th USENIX Workshop on Offensive Technologies (WOOT 15), 2015.

[30] J. Zaddach, L. Bruno, A. Francillon, D. Balzarotti, et al., Avatar: A framework to support dynamic security analysis of embedded systems' firmwares., in: NDSS, volume 14, 2014,

pp. 1–16.

[31] M. Muench, D. Nisi, A. Francillon, D. Balzarotti, Avatar 2: A multi-target orchestration platform, in: Proc. Workshop Binary Anal. Res.(Colocated NDSS Symp.), volume 18, 2018, pp. 1–11.

[32] D. D. Chen, M. Woo, D. Brumley, M. Egele, Towards automated dynamic analysis for linux-based embedded firmware., in: NDSS, volume 1, 2016, pp. 1–1.

[33] A. Costin, A. Zarras, A. Francillon, Automated dynamic firmware analysis at scale: a case study on embedded web interfaces, in: Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, 2016, pp. 437–448.

[34] A. A. Clements, E. Gustafson, T. Scharnowski, P. Grosen, D. Fritz, C. Kruegel, G. Vigna, S. Bagchi, M. Payer, {HALucinator}: Firmware re-hosting through abstraction layer emulation, in: 29th USENIX Security Symposium (USENIX Security 20), 2020, pp. 1201–1218.

[35] E. Gustafson, M. Muench, C. Spensky, N. Redini, A. Machiry, Y. Fratantonio, D. Balzarotti, A. Francillon, Y. R. Choe, C. Kruegel, et al., Toward the analysis of embedded firmware through automated re-hosting, in: 22nd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2019), 2019, pp. 135–150.

[36] C. Spensky, A. Machiry, N. Redini, C. Unger, G. Foster, E. Blasband, H. Okhravi, C. Kruegel, G. Vigna, Conware: Automated modeling of hardware peripherals, in: Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security, 2021, pp. 95–109.

[37] G. Fortino, C. Greco, A. Guzzo, M. Ianni, Enabling faster security assessment of re-hosted firmware, in: 2022 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), 2022, pp. 1–6. doi:10.1109/DASC/PiCom/CBDCom/Cy55231.2022.9927780.