Overcoming New Technologies Challenges in IoT Security Labs: Strategies for Effective Adaptation

Dimitrios Simopoulos
Medical Informatics Laboratory, Department of Medicine
Democritus University of Thrace
Alexandroupolis, Greece
0000-0002-4311-3449

Andreas Wolf
IT Digital Solutions
Akkodis Germany
Sindelfingen, Germany
Andreas.WOLF@akkodis.com

***Abstract*—With IoT technology being widely implemented in crucial domains such as personal activity and health tracking or monitoring of critical technical processes, awareness for security risks has risen. First solutions for DevSecOps in IoT have been introduced in the past to detect typical programming flaws and the vulnerabilities they impose. With the increasing power and cheap availability of unlimited cloud resources, high speed networks and AI, new and more complex attacks seem feasible. In this paper we highlight these new threats and elaborate whether known approaches to IoT security are still sufficient or new strategies to fight the threats have to be developed. Furthermore, we present our approach to use the new technological possibilities in order to increase the power of security assessment and security tests for IoT.**

***Index Terms*—Internet of Things, Artificial Intelligence, 6G, DevSecOps, Cyber-Security, Threat Modeling, Security Testing**

I. Introduction

Internet of Things (IoT) is one of the rapid-expanding fields that attracts researchers' interest, given the profound changes it has brought in industry, business, and personal environments. Since one of its key success factors is simplifying work and life with cheap and easy-to-use devices, development of IoT devices has placed a greater emphasis on convenience features like Plug and Play, while often overlooking critical safety and security measures such as strong password enforcement. IoT technology was intended to add low-cost electronic features to commonly used devices to increase their intelligence. This has led many new players in entering the electronics and communication industry, including startups, who may not have had the experience or the resources to prioritize security concerns. Also the fact that the low-power devices usually could not just use the CPU and energy consuming security algorithms and methods of standard computing and networking like encryption, signing and certificates or authentication and authorization handshakes added to the increasing insecurity of the IoT solutions.

Huge improvements have been made by introducing encryption supporting instructions in modern micro-controller units (MCUs), such as ARMv8 architecture [1]. However, due to the very nature of IoT devices of being small and working off-grid for many years, CPU and energy put a limit to the security efforts. Risk models that included specific threats for IoT devices and systems, like [2], have been developed and increased the awareness of IoT-specific security risks. Different Test-Lab developments like [3] and [4], have shown that adding IoT-specific security tests into an IoT DevSecOps development cycle [12] can be achieved with low and almost negligible invest.

ISBN 978-3-903176-57-7 © 2023 IFIP

While awareness and possibilities for secure IoT devices are increasing, new developments in the IT industry have also increased the available resources for attacks.

The adoption of 5G and the upcoming 6G networks, along with the emergence of cheaper and more powerful computers equipped with dedicated multi-core compute units derived from graphics cards, could be exploited by attackers to increase their chances of detecting and exploiting vulnerabilities. Moreover, the unlimited cloud computing power and the ever increasing capabilities of AI could pose a significant threat.

In this paper, we look into those developments and how they could or already have been used to threaten IoT security. We analyze how established methods for risk assessment and threat analysis have to be adapted to cope with those new threats. We also examine if the small footprint design approaches for IoT Security Test Labs, like our SecLab, still hold in those new scenarios or if they have significant limitations. Finally, we sketch research and development tasks that we will follow to verify the proposed measures and to close potential gaps.

II. Previous Work

The broad usage and exponential growth of IoT devices have led to vast technological improvements and advancements over the past years. More and more devices are incorporated into a variety of fields, ranging from Healthcare and medical devices to Smart Cities. These devices play a significant role as they affect our daily routine in multiple ways. Indicatively, they enable remote patient monitoring, leading to significant and crucial healthcare outcomes.

However, that leads to analogous expansion of security risks, flaws and challenges. Therefore, security plays a significant role in IoT and its research interest on the aforementioned sector remains high, as it is imperative to guarantee the security of these devices to ensure their continued successful integration into our daily life.

The insufficiency of proper security testing in IoT devices and their security vulnerabilities as an effect have been presented in multiple studies. Namely, most medical IoT devices come with security risks and vulnerabilities [13]. Therefore, the need for vast and advanced security measures increases exponentially. While there have been several studies proposing specific tools and approaches for security testing in different domains and sectors [14], the main challenge remains to develop a robust and coherent solution for the majority of those devices. That underlines the significance of a universal but adaptable approach for security testing in IoT devices.

In our previous work [2], we addressed the security risks of IoT by adapting the PASTA (Process for Attack Simulation and Threat Analysis) threat model to optimize threat analysis based on domain knowledge and specific needs of IoT. With the integration of the PASTA results into the IoT software development life cycle, we identified and reduced security risks by using and adapting a prototype DevSecOps toolchain. Our approach provided a framework ensuring the safe and secure deployment of IoT devices and systems.

In continuation of that, we identified that security testing for these systems can be both costly and complex, often leading developers to overlook or skip security measures in total. To address this issue, we developed *SecLab*, a security testing laboratory that utilizes a lightweight and adaptable architecture, making it more accessible and user-friendly for developers and IoT security experts [4]. Our open architecture design allowed integrating existing external security test libraries and supported scalability for assessing complex IoT networks. In order to demonstrate the practical application of our approach, we implemented security tests in a realistic IoT application scenario, which served as a validation of *SecLab*'s effectiveness.

With the aforementioned lab architecture, we were able to prove that security testing for IoT devices with low-end hardware is feasible. More specifically, we achieved that with mini PC-level hardware. However, we also identified various discrete security vulnerabilities in typical IoT platforms with moderate effort. The reason is that most IoT devices in the market come with low-security standards. The results of our research underlined the significance of in-depth security testing in the aforementioned devices, ensuring their secure deployment. Moreover, our results showcased the feasibility to recognize and identify IoT vulnerabilities using a specific framework, even with resource-constrained conditions.

III. Limitations and Challenges

A. *Cheap "unlimited" computing power*

The rapid increase of computing power over the years has lead to both benefits and challenges in the cyber-security field. The availability of cheap and unlimited computing power has provided attackers with more opportunities to launch complex attacks and decrypt sensitive information.

As a derivative, dictionary attack efficiency has also increased, as larger dictionaries can now be handled with ease [5]. Although the benefits of cheap computing power are undeniable, it cannot be ignored this has a negative impact on cyber-security [6].

Sensitive data exchange of IoT devices over the Internet is constantly increasing. Therefore, it is crucial to consider the aforementioned impact on the security of these systems. The reason is that it elevates simultaneously both opportunities and challenges in the IoT cyber-security sector. It is of high importance to ensure that already existing universal frameworks and tools can be adjusted to cover and detect possible future threats.

Without sufficient security measures, the aforementioned powerful computing resources will allow upcoming threats and attacks to identify and exploit even more IoT device vulnerabilities in shorter time frames. Therefore, the need of modern and adaptable security testing frameworks arises, in order to effectively address these risks for both existing and upcoming devices.

B. *High-speed networks*

The constant network throughput increase along the last decades has lead to specific attack types, such as flooding. These discrete types of cyber-attack have become more complex and efficient over time. This is because they are based on overloading a target device with high traffic, which is achieved when reaching the target's resource limitations. In that way, attackers can make use of increased network throughput to execute successfully discrete attacks into more targets.

In addition, increased computing power enables attackers to execute more complicated and better designed attacks that require precise timing [7]. Low latency in networks provides an opportunity for orchestrating steps and tasks during attacks, making the challenging implementation of complex timing more reliable and successful. As a result, potential attackers can take advantage of it and exploit vulnerabilities, by creating more sophisticated and difficult to identify attacks.

Nowadays, one of the major IoT challenges is securing the increased amount of data and the ways to protect such sensitive data. To mitigate this, specific measures have to be taken into consideration, which are able to detect any type of possible anomalies and indicate potential threats or even attacks. This challenge becomes more critical when dealing with personal or health-related data, as the potential consequences of a security breach can be severe.

IoT devices often present significant security challenges due to their design and architecture. Most of these devices have in general limited resources, which implies the hardening of these systems becomes more challenging. Additionally, the environments and ecosystems in which IoT devices operate, can pose a variety of threats and security challenges.

In general, such IoT-related security limitations and challenges underline the importance and need for developing and implementing specific cyber-security countermeasures. That occurs in order to act more effectively against threats and attacks, based on both increased computing power and high network throughput.

To ensure the protection of IoT data generation and transfer, it is essential to develop adaptable testing frameworks, able to cope with these challenges. These frameworks should be capable of identifying and addressing potential cyber-security threats and risks, in order to implement and deploy in a short period of time the respective security patches and measures. That can safeguard such sensitive devices not only from existing but also from potentially coming threats.

C. Extended architectures

The evolution of IoT networks has been associated with complexity and diversity in terms of device communication. And that has played a significant role in the development of more complex security tests and countermeasures, especially for DevSecOps processes.

Initially, the first IoT networks were characterized by simple hubs and sensors -sometimes with hub hierarchies-, resulting to analogously simple security tests and attack surfaces [8]. As a result, the respective security measure requirements were also significantly simpler and superficial. However, a simple network architecture could not allow a network to be adjusted and adapted accordingly, while being developed. Although, security tests were still necessary covering simple but vital countermeasures against basic and non-sophisticated security vulnerabilities and risks. The first IoT network generation set up the foundation for the development of the upcoming generations, providing more complex and combined architectures.

The next generation of IoT networks introduced mesh configurations with dynamic reconfiguration capabilities [9]. As a result, that allowed introducing adaptable networks with efficient network performance but on the other hand that brought increased risks. Mesh networks introduced a different philosophy than their predecessors. Therefore, new threats were accompanied by higher complexity. That is, security measures should be built for both the discrete IoT devices and the network in total.

The technology advancement brought a variety of features and advantages. As a consequence, the edge computing concept [10] was introduced to the already existing IoT networks, posing a new approach and presenting a new level of complexity to the former network architectures. However, it broadened the prism of potential upcoming threats, focusing on a specific edge-computing area or on the network as a whole. In that way, effective security tests were needed to be developed, adaptable enough and capable of identifying and mitigating such vulnerabilities. As a result, with that generation of IoT networks, DevSecOps started playing a more crucial role in the design, architecture, and deployment phases in the software life-cycle.

The current generation of IoT networks has seen significant improvements and additions in terms of end devices. Intelligent sensors are equipped with operating systems, able to receive updates [11]. However, that comes with an additional cost. The increased capabilities and functionalities of the aforementioned devices have also increased the complexity of even more sophisticated threats and attacks. That happens because the attack surfaces become larger and the operating systems and their updates come with an extra layer of potential vulnerabilities to be exploited. Thus, effective security testing should be part of the design and implementation process of an IoT device. A comprehensive approach is required to ensure the robustness and security of the new IoT networks. That should take into account the whole network structure, including the smart actuators and sensors, as well as the communication protocols used.

D. AI and Attack generation

The rapid advancement of Artificial Intelligence (AI) has brought a wide variety of benefits and drawbacks in the fields it is applied. Whereas the advantages may be obvious, there are also concerns derived from potential misuse. Thus, AI can contribute to the development of malicious attacks. Attack creation or complete attack scenarios for identification and exploitation of vulnerabilities are two of the aforementioned concerns. In recent years, AI-generated malicious code raised concerns in the cyber-security community.

In December 2022 and early 2023, there were reports posing that ChatGPT [15] was able to produce malicious code, ready to be used. This indicated the capabilities and potentials of complicated and sophisticated AI-based attack generation, raising significant concerns. Check Point Research published an example [16] demonstrating a process how a complete attack scenario could be set up using a combination of ChatGPT and CODEX [17].

To prevent that misuse, OpenAI applied some countermeasures and restrictions in order to avoid generation of such answers. However, these additional security measures were not sufficient to prevent some users bypassing them within weeks [18]. That incident underlined the importance of defining clear guidelines, referring to ethical and security matters and handled by AI systems.

The development of efficient malicious code and attacks projects a challenge, especially when the target systems are located inside an unknown IoT device, and the respective technical documentation is not available. Although, side-channel attacks are capable of detecting patterns and collecting information during data exchange. In that way, they can be used during compressed or even encrypted communication. To illustrate, [19] showed how to use patterns in that kind of communication to extract meaningful insights from collected data transferred by smart meters.

Side-channel attacks deal with great challenges, though. One of them is to maintain their efficiency in large data volumes. With the help of AI, finding patterns and analyzing monitored communication, output, or any other accessible system resources has become more feasible. These methods have been broadly used in a variety of fields, including cryptography. As a result, usage of side-channel attacks has been well described and documented [20]. Nevertheless, such attack types get constantly improved as AI systems do not stop evolving. That emphasizes the need to develop further security measures and tests to prevent not only known but also unexpected threats and attacks.

IV. Solution Approach

A. AI in Threat analysis

Static code analysis is a common tool identifying potential threats and vulnerabilities in source code [21]. However, this technique is limited to examining already defined patterns without demanding complexity. As a consequence, these patterns can be detected and bypassed from attackers who can adapt their vulnerable code accordingly.

AI can address that matter, as it could be trained with already known exploits and vulnerable code. Training such a model in large data sets of vulnerable code is the key to develop an AI system detecting new and hidden patterns, potentially missed by traditional security tools. That improves threat detection, prevents security risks, and allows detecting more sophisticated but also unknown attacks.

Moreover, exploited executable files could be used for training the respective AI model. With methods such as decompiling [22], security tests can be effective even when the source code is not available. Namely, libraries or third-party components are often used without examining their source code first. In these scenarios, AI systems can prevent potential risks and threats when trained on such vulnerable executable files. In that way, AI systems can contribute on further hardening and securing developed systems and devices by detecting vulnerabilities that may have been overlooked or undiscovered.

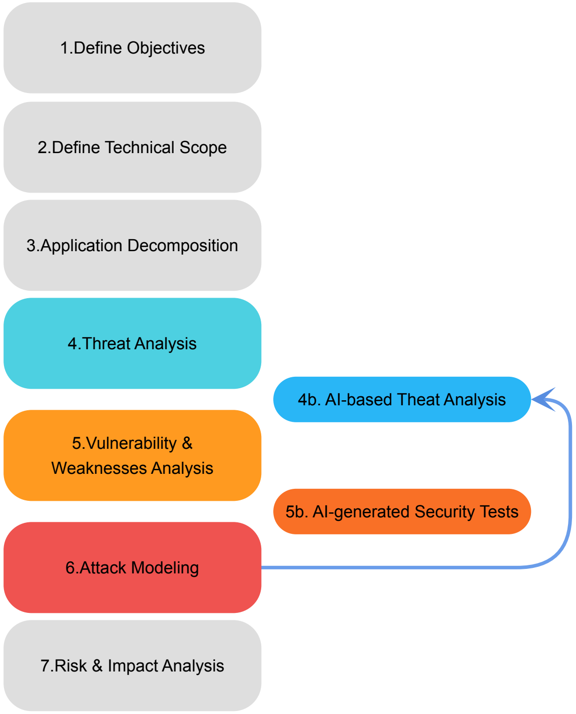
1.Define Objectives
2.Define Technical Scope
3.Application Decomposition
4.Threat Analysis
4b. AI-based Theat Analysis
5.Vulnerability & Weaknesses Analysis
5b. AI-generated Security Tests
6.Attack Modeling
7.Risk & Impact Analysis

Fig. 1. PASTA Model with ‘CT’ Concept: Overview and Additional Stages.

PASTA is a threat modeling framework, proposed by Tony UcedaVélez in 2015 [23]. To incorporate AI-based risk assessment on the aforementioned model, an additional layer between the ‘Threat Analysis’ and the ‘Vulnerability & Weaknesses Analysis’ stages has to be added, as shown in Fig. 1. In that way, the new addition can give a better overview to the analysts, regarding the countermeasures needed to be taken. That is, recommending mitigation strategies in design, developing respective security tests and continuously monitoring the developed systems and devices as discrete entities, but also as part of an ecosystem. This adaption can enhance the effectiveness of PASTA in terms of risk analysis.

B. AI in Test generation

The use of AI in DevSecOps has gained a lot of attention in recent years. Its integration can bring added value and deliver higher efficiency in the security stage of the aforementioned framework. As mentioned, an approach could be training a model based on given vulnerable source code or executable files in order to identify possible threats.

However, there are potential risks when it comes to training AI models in generating test code on a wider and unfiltered source code dataset. This is because arbitrary code could lead to accidental learning of attack methodologies by allowing other AI models to create attacks not previously known and posing a significant threat to the security aspects of a system or device. To address that matter, it has been proposed that training AI systems with successful vulnerable code could simplify test generation and increase the quality of security testing in DevSecOps.

It is clear that AI-based risk assessment has been established as an essential tool for further AI-based test generation. Therefore, it is important to prioritize security tests based on the ease of attack and their impact to expedite the detection of any critical vulnerabilities and exploits. That could be particularly meaningful in large systems and environments, where manual testing be insufficient to cover all possible test scenarios.

To fully take advantage of AI in the DevSecOps framework, it is recommended to integrate it in the respective CI/CD (Continuous Integration/Continuous Delivery) pipeline. Similar to the SiL (Software in the Loop) concept, the implementation of CT (Continuous Training) can be proposed, as outlined by [24]. In that way, developers and analysts can use robust and mature security testing tools to evaluate their code. Nevertheless, this approach allows such tools to gain awareness of attack scenarios that are more complex, sophisticated, and even unknown or unseen so far.

By integrating AI-based test generation as an intermediate layer between the ‘Vulnerability & Weaknesses Analysis’ and ‘Attack Modeling’ PASTA threat model stages, security testing in DevSecOps can be improved, as depicted in Fig. 1. This addition can provide a more resilient framework, corresponding to the increased challenges posed by the exponential growth of network throughput and device computing power. In summary, incorporating AI test generation in such a way can help to stay ahead of potential threats and achieve faster, more accurate and effective security testing.

V. Conclusion

Analyzing the threats imposed by new IT technologies, has shown that most changes have to be made in the risk analysis steps of the threat model. This starts with combining multiple code vulnerability analysis techniques to keep up with the wider spectrum of attacks. It also includes a better assessment of network infrastructure and protocols to identify possible leaks that can be exploited based on specific timing. A second part of the threat model affected is the complexity and size of the test library that has to be built and maintained for a thorough coverage of the detected threats. A focus shift from device-related attacks, like flooding or manipulated payload, to complex infrastructure-related tests for protocols and timing is to be expected. At last, the increase in test scenarios and cases requires a more sophisticated test strategy in the DevSecOps cycle because a full coverage at any time cannot be achieved. Therefore, effect-chain analysis of changes has to be combined with risk-based prioritization to detect tests that are always run, regularly run or only run in a full check before release.

When analyzing the changes in the type of tests to be performed in a DevSecOps cycle, the SecLab architecture has been proven flexible enough to cope with the new scenarios.

There is however one major change that has an impact on the SecLab architecture. When a System under Test relies on 4G/5G and later 6G and exploits rely on features of those networks, such as low latency based time-critical attack steps over the network, the attack technically runs over a public network. This has to be carefully validated in order to avoid negative effects on the public infrastructure and it also has to be agreed on with the providers that are affected. Thus, tests have to be separated in those that do not need the public components and therefore can make use of the isolation of the lab and run unrestricted tests, and those that need the public infrastructure and have to conform to the rules of the providers.

Our further research will concentrate on the systematic use of AI in vulnerability detection in two directions. First, we will use AI models trained with known exploits and vulnerable code patterns to detect possible vulnerabilities on both source code and binary code level. In parallel, we will analyze how effective AI can be used to select / create possible attack code based on an IoT system model to efficiently create effective test scenarios for IoT development.

References

[1] Limited, A. Arm Architecture Reference Manual. (Arm Limited,2013), https://developer.arm.com/documentation/ddi0487/latest/, Accessed: March 17, 2023

[2] Wolf, A., Simopoulos, D., D'Avino, L. & Schwaiger, P. The PASTA threat model implementation in the IoT development life cycle. *INFORMATIK 2020*. (2021)

[3] Adjih, C., Baccelli, E., Fleury, E., Harter, G., Mitton, N., Noel, T., Pissard-Gibollet, R., Saint-Marcel, F., Schreiner, G., Vandaele, J. & Watteyne, T. FIT IoT-LAB: A Large Scale Open Experimental IoT Testbed. *IEEE World Forum On Internet Of Things (IEEE WF-IoT)*. (2015,12), https://hal.inria.fr/hal-01213938

[4] Schwaiger, P., Simopoulos, D. & Wolf, A. Automated IoT security testing with SecLab. *NOMS 2022-2022 IEEE/IFIP Network Operations And Management Symposium*. pp. 1-6 (2022)

[5] Bošnjak, L., Sreš, J. & Brumen, B. Brute-force and dictionary attack on hashed real-world passwords. *2018 41st International Convention On Information And Communication Technology, Electronics And Microelectronics (mipro)*. pp. 1161-1166 (2018)

[6] Raheman, F. The Future of Cybersecurity in the Age of Quantum Computers. *Future Internet*. **14**, 335 (2022)

[7] Barreto, S., Suresh, A. & Le Boudec, J. Cyber-attack on packet-based time synchronization protocols: The undetectable delay box. *2016 IEEE International Instrumentation And Measurement Technology Conference Proceedings*. pp. 1-6 (2016)

[8] Van Kranenburg, R. The Internet of Things. A critique of ambient technology and the all-seeing network of RFID. (Institute of Network Cultures, 2007)

[9] Hortelano, D., Olivares, T., Ruiz, M., Garrido-Hidalgo, C. & López, V. From sensor networks to internet of things. Bluetooth low energy, a standard for this evolution. *Sensors*. **17**, 372 (2017)

[10] Pan, J. & McElhannon, J. Future edge cloud and edge computing for internet of things applications. *IEEE Internet Of Things Journal*. **5**, 439-449 (2017)

[11] Zikria, Y., Kim, S., Hahm, O., Afzal, M. & Aalsalem, M. Internet of Things (IoT) operating systems management: Opportunities, challenges, and solution. *Sensors*. **19**, 1793 (2019)

[12] Myrbakken, H. & Colomo-Palacios, R. DevSecOps: a multivocal literature review. *Software Process Improvement And Capability Determination: 17th International Conference, SPICE 2017, Palma De Mallorca, Spain, October 4–5, 2017, Proceedings*. pp. 17-29 (2017)

[13] Yaqoob, T., Abbas, H. & Atiquzzaman, M. Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—A review. *IEEE Communications Surveys & Tutorials*. **21**, 3723-3768 (2019)

[14] Hamid, B., Jhanjhi, N., Humayun, M., Khan, A. & Alsayat, A. Cyber security issues and challenges for smart cities: A survey. *2019 13th International Conference On Mathematics, Actuarial Science, Computer Science And Statistics (MACS)*. pp. 1-7 (2019)

[15] OpenAI Introducing ChatGPT. (https://openai.com/blog/chatgpt/,2021), Accessed: March 16, 2023

[16] Ben-Moshe, S., Gekker, G. & Cohen, G. Etal OpwnAI: AI that can save the day or hack it away. *Check Point Research*. (2023,1), https://research.checkpoint.com/2022/opwnai-ai-that-can-save-the-day-or-hack-it-away/

[17] OpenAI Codex. (https://openai.com/blog/codex/,2021), Accessed: March 16, 2023

[18] Cybercriminals Bypass CHATGPT restrictions to generate malicious content. *Check Point Software*. (2023,2), https://blog.checkpoint.com/2023/02/07/cybercriminals-bypass-chatgpt-restrictions-to-generate-malicious-content

[19] Fehér, M., Lucani, D., Hansen, M. & Vester, F. Exploiting DLMS/COSEM Data Compression To Learn Power Consumption Patterns. *2021 IEEE International Conference On Communications, Control, And Computing Technologies For Smart Grids (SmartGridComm)*. pp. 346-351 (2021)

[20] Kocher, P., Jaffe, J. & Jun, B. Differential power analysis. *Advances In Cryptology—CRYPTO'99: 19th Annual International Cryptology Conference Santa Barbara, California, USA, August 15–19, 1999 Proceedings 19*. pp. 388-397 (1999)

[21] Huuck, R. Iot: The internet of threats and static program analysis defense. *EmbeddedWorld 2015: Exibition & Conferences*. pp. 493 (2015)

[22] Cifuentes, C. & Gough, K. Decompilation of binary programs. *Software: Practice And Experience*. **25**, 811-829 (1995)

[23] UcedaVélez, T. & Morana, M. Risk Centric Threat Modeling: process for attack simulation and threat analysis. (John Wiley & Sons,2015)

[24] Prapas, I., Derakhshan, B., Mahdiraji, A. & Markl, V. Continuous training and deployment of deep learning models. *Datenbank-Spektrum*. **21**, 203-212 (2021)