Testing techniques to assess impact and cascading effects

Valeria Valdés Ríos*‡, Ana Rosa Cavalli*†, Fatiha Zaïdi‡, Wissam Mallouli*
* Montimage EURL
Paris, France
valeria.valdes@montimage.com
wissam.mallouli@montimage.com
† Institut Politechnique, Telecom SudParis
Paris, France
ana.cavalli@it-sudparis.eu
‡ Université Paris-Saclay, CNRS, ENS Paris-Saclay, Laboratoire Méthodes Formelles
91190, Gif-sur-Yvette, France
fatiha.zaidi@universite-paris-saclay.fr

***Abstract*—The rapid evolution of digital environments and their integration into critical operations of our society have led to substantial challenges in advancing cybersecurity to ensure the proper functioning of these systems . In the face of over-evolving cyber threats and attacks, systems must be equipped with robust mechanisms for protection. In this context, resilience techniques aim to mitigate such treats. However, the evaluation of these techniques is a crucial process, enabling informed decision-making and proactive threat mitigation. This article introduces a methodology based on regression testing for evaluating the impact and cascading effects of resilience strategies. It delves into the methodology's adaptability across different scenarios and provides insights about the evaluation process.**

***Index Terms*—resilience, regression resting, moving target defense, cloud computing, IoT, resilience evaluation**

I. Introduction

In times characterized by the rapid evolution of digital environments, our interconnected society finds itself confronted with a wide range of cybersecurity challenges. These challenges extend to the analysis of cloud continuum and IoT platforms, where the demand for resilient solutions becomes more critical than ever. Over the years, the study of resilience techniques has witnessed significant growth [1], highlighting the critical need for evaluating such techniques and strategies.

This article introduces a novel methodology based on regression testing. It's primary aim is to comprehensively assess the impact and cascading effects of resilience techniques, with a specific focus on those leveraging Moving Target Defense (MTD) strategies. This methodology considers the impact from two distinct perspectives. Firstly, it analyses the repercussions that changes in one system component can produce on other interconnected components within the same system. Secondly, it extends its scope to encompass a broader landscape, delving into the potential cascading effects that changes in one system component could trigger in another interconnected system. By doing so, this methodology offers a systematic approach to the evaluation and understanding of resilience techniques within interconnected infrastructures or systems.

This work is partially supported by the European Union's Horizon Europe research and innovation program under grant agreement No 101070455 (DYNABIC)

The remainder of this paper is organized as follows. Section II presents the related work, Section III presents the proposed methodology with an illustrative example, Section IV presents a discussion, and Section V presents final remarks and conclusions.

II. Related Work

In the field of cybersecurity resilience, a strong background of research and methodologies can be found in the literature. This section provides a concise overview of related work, focusing on the assessment of resilience techniques. By surveying existing literature and methods, we establish the context for the proposed methodology.

Resilience refers to the ability to resist, absorb, recover or adapt to adversity or changing conditions [2]. Several approaches to achieve resilience can be found in the literature, an overview of these are described below:

- Dynamic adaptation: Strategies such like Moving Target Defense (MTD) involve dynamically changing the system components to reduce the attack surface and mitigate potential threats and attacks. In the literature, examples of self-adaptive architectures can be found in [3], [4], and [5].
- Data protection and access control: Safeguarding data confidentiality, integrity, and system availability is the objective of these techniques. For instance, a various range of encryption mechanisms for cloud computing have been developed [6].
- Incident detection: Several approaches of intrusion detection systems that continuously monitor traffic data and systems can be found, from using rule-based approaches to ones optimized with the use of machine learning

techniques [7]. These systems can be complemented with incident response plans [8] and threat intelligence [9].

In the field of cybersecurity, regression testing plays an important role in ensuring the resilience and security of software systems. It involves comparing two different versions of a system to provide confidence that new changes do not interfere with existing features [10]. Regression testing serves as a proactive measure to assess the security of software and systems, ensuring that security mechanisms do not introduce vulnerabilities. By incorporating regression testing into security practices, organizations can systematically evaluate the impact of modifications within the system, thereby enhancing cybersecurity resilience and maintaining the integrity of critical infrastructures and interconnected systems.

III. Testing Methodology

This section introduces the testing methodology, which is grounded in the principles of regression testing. The methodology is designed to evaluate the effectiveness of resilience techniques and mechanisms that dynamically adapt system at runtime, achieved by adding or removing system components, with a particular focus on Moving Target Defense (MTD).

The primary goal of this methodology is to comprehensively evaluate the impact of implementing changes within a system, with a particular focus on modifications introduced by MTD-based techniques. The assessment of impact encompasses two key perspectives. Firstly, it considers the repercussions that a change in one system component may induce in other unaffected system components that are interconnected with the modified one. Secondly, it examines the consequences that a system may trigger within another interconnected system when alterations are made. In this latter scenario, the interconnection of two systems is regarded as an unified entity, enabling a holistic evaluation of the consequences of changes across interconnected systems.

MTD-based techniques such as dynamic network reconfiguration, software diversity, and adaptive access control implement strategic modifications in systems based on events and system metrics. These changes are executed with the objective of minimizing a system's attack surface. They can be applied proactively, aiming to prevent potential threats before they are detected, or reactively, with the purpose of mitigating damage and containing potential attacks after their detection. This flexibility allows for a more comprehensive approach to cyber resilience in the face of evolving threats.

The testing methodology proposed in this study leverages the capability of regression testing, a method that involves comparing two versions of a software system. This inherent capability makes regression testing particularly well-suited for evaluating the effectiveness of MTD-based resilience techniques. To employ regression testing, a test suite must be established; this suite comprises the set of test cases to be executed within the system. However, executing the entire test suite can use a lot of resources and can be costly. This leads to challenges such as the need for test suite minimization, test case selection, and prioritization. These challenges aim to optimise the execution of the test suite while maintaining comprehensive coverage of the test cases.

The key concepts of the methodology are illustrated in figure 1 and it involves:

- **Resilience techniques**: Encompass a diverse set of strategies and mechanisms employed within a system to withstand and recover from cyber threats and attacks. This methodology places a particular emphasis on MTD-based techniques, which involve the deliberate introduction of dynamic changes within a system. these changes include adding or removing systems components, all with the objective of mitigating potential attacks and reducing the system's attack surface. Their effectiveness is evaluated through a series of comprehensive tests and assessments. By examining various metrics within the system, the methodology seeks to uncover insights into the landscape of cyber resilience in the system.
- **Test suite generation**: The foundation of the testing methodology lies in the creation of an initial test suite, a critical component in the evaluation process. This initial test suite can be sourced from existing datasets made available by organizations or it can be generated specifically for the system under testing. Test suites often encompass a mixture of elements, ranging from redundant test cases to reusable ones, and in some instances, obsolete test cases that may no longer align with the system's current configuration, functionalities, or requirements. As a result, the process of the test suite generation must contend with several challenges such as test suite minimization, test case selection, and test case prioritization.
- **Test execution engine**: Once the test suite is defined, the execution engine takes center stage in the evaluation process. This component is responsible for orchestrating the execution of the designated test cases within a controlled environment. The primary objective is to check whether the newly modified version of the system continues to meet the same requirements and standards as it did prior to the implementation of changes. The execution engine evaluate the system's response to various scenarios and conditions. It simulates real-world conditions in an isolated environment and assess how the system behaves in the face of dynamic alterations, safeguarding critical systems and data.
- **Metric Collector**: As the tests are executed, the metric collector assumes the responsibility of gathering a diverse array of pre-defined metrics about the system's behavior. These metrics serve as pieces of information useful to make an analysis of both performance and resilience. The metric collector operates as an observer, capturing data points of the system's response during the evaluation process. These metrics encompass a wide spectrum of system attributes, including response times, resource utilization, error rates, and security-related parameters. However, the evaluation conducted by the metric collector

goes beyond the boundaries of the modified system component. Recognizing the interconnected component and systems, it acquires metrics not only from the modified component but also from the interconnected ones. This holistic approach ensures that the assessment accounts for potential cascading effects and dependencies within the system.

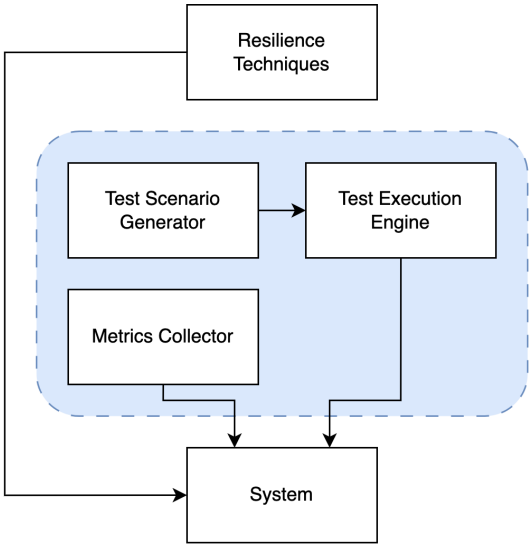

Fig. 1. High-level architecture of the testing methodology

This methodology seamlessly integrates into the software development lifecycle, offering flexibility and adaptability from design to production phases. During design time, its modular architecture allows for the proactive inclusion of resilience strategies, including MTD-based approaches. In production, the methodology becomes an integral part of the testing phase, enabling assessments of operational software's cyber resilience.

In the context of cybersecurity, this methodology proves to be versatile and applicable to a wide range of scenarios and use cases, several of which are described below:

- Cloud environments: The methodology excels in assessing cyber resilience of cloud-based services and infrastructure. This methodology can assess the impact of changes in cloud configurations, access control policies, and service availability.
- IoT environments: Evaluating security and resilience of IoT devices and their interconnections. It includes a evaluation of how changes in devices and configurations impact the overall system.
- Smart Cities: This methodology is a tool for evaluating the resilience of smart city infrastructure, including sensors, communication networks, and data processing systems. This can help identify vulnerabilities and quantifies the consequences of infrastructure changes, thus facilitating early mitigation of threats and attacks in interconnected systems.
- Network infrastructure: Evaluating the resilience of components such as routers, switches, and firewalls. Given the potential effect of resilience techniques such as MTD in network infrastructures, this methodology effectively assesses the impacts on other network components.
- Telecommunication networks: It is equally adept at evaluating the impact of alterations in network configurations and traffic patterns within telecommunication networks.
- Software applications: With its adaptability, the methodology is well-suited for assessing changes in web applications, mobile apps, and software applications. the evaluation ensures that system requirements continue to be met as changes are introduced.

A. Illustrative example: Electric Vehicle Charging Station

Electric vehicle charging stations (EVCS) serve as a good illustration of critical systems where MTD-based approaches can be applied. These stations encompass physical and virtual components within their architecture. The EVCS architecture includes several key components, as depicted in Figure 2 which provides a high-level model of an EVCS. These components include:

- Charging Stations (CS): Each station originates from different vendors, having distinct attributes and capacities. All charging stations are connected to the CSMS.
- Charging station management system (CSMS): This web platform is responsible of remotely maintaining and monitoring the CSs. It operates within a private cloud environment and utilizes the Open Charge Point Protocol (OCPP) to communicate with the charging stations.
- Network switch: This component delivers essential Ethernet connectivity to the CSs.
- Router: Serving as an intermediary network device, the router facilitates the connection of CSs to the Internet.
- WiFi Access Point (AP): Selected CSs benefit from WiFi connectivity provided by this component.
- Feeder Protection Relay (FPR): Holds responsibility for safeguarding CSs against overloading and circuit faults.
- GPS clock: Ensures precise time synchronization for the FPR.

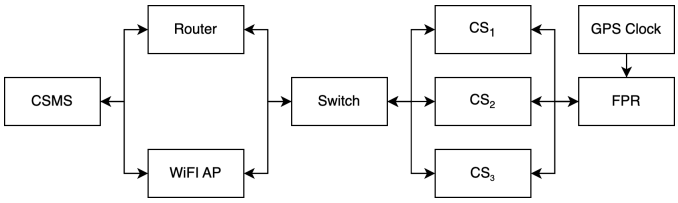

Fig. 2. EVCS architecture model

Figure 2 provides a visual representation of the interdependencies among components within the EVCS system. Of particular note is the integration between each CS and the CSMS. This inherent connectivity means that any change introduced to the CSMS has the potential of having an impact on the functioning of the CSs. Consequently, it becomes

imperative that each modification within the CSMS is properly executed to safeguard against adverse effects cascading down to the CSs.

For example, consider a scenario where the decision of replacing the existing CSMS with an alternative instance of the web application is made. Such transition implies that the CSs must establish new connections with this new CSMS instance. To ensure seamless and uninterrupted functionality, it becomes essential to update connection credentials and pertinent information in the CSs. This proactive step guarantees that the charging station network remains robust and dependable despite the architectural change.

Another important factor to consider is how much the EVCS relies on other external systems. One key example of this reliance is with the energy provider. The charging stations depend on a constant and reliable supply of electricity to operate. In the case of an unexpected event happening, like a power outage or disruption, it directly impact the functionality of the EVCS. These disruptions can lead to outages in the charging stations, which will affect EV users and potentially impact the charging network. Therefore, evaluating the resilience of the EVCS also involves assessing its ability to respond and recover from external event and disruptions.

Moreover, these examples highlight the importance of comprehensively testing and assessing the impact of changes within the EVCS system. The proposed methodology, which concentrates on evaluating resilience and conducting regression testing, provides a structured way to analyze scenarios like these. This approach helps the resilience mechanisms to make informed decisions and take proactive steps to prevent potential disruptions.

IV. Discussion

Regression testing emerges as a highly promising tool for the evaluation of MTD-based approaches. However, in the context of complex and large systems, the execution of an entire test suite can mean to spend a high amount of resources. This is the point where the use of test suite minimization, test case selection, and test prioritization strategies becomes imperative. These strategies are essential not only for reducing costs but also for ensuring that test coverage is maintained. Furthermore, they play a crucial role in verifying that all system requirements are assessed.

Some of these strategies rely on system models, such as graph models and transfer functions. Here we highlight the potential of incorporating emerging technologies, such as Digital Twins (DT), into these test suite minimization, test case selection, and prioritization strategies. DTs are defined as the virtual replica of a system created by merging models and data [11]. With their simulation and emulation capabilities, DTs offer an opportunity to optimize the resources required for regression testing. By leveraging the power of DTs, we can enhance the efficiency of regression testing processes.

V. Conclusion

In this article, we introduced a novel methodology based on regression testing, tailored for the evaluation of MTD-based resilience techniques. Our methodology demonstrates its adaptability across diverse environments encompassing domains like cloud computing, IoT, smart cities, network infrastructures, telecommunication networks, and software applications.

The methodology addressed various challenges inherit to regression testing including test suite minimization, test case selection, and prioritization. These considerations are crucial when ensuring the comprehensive evaluation of MTD-based approaches and their potential cascading effects.

As part of our future work, we plan to implement the testing methodology within the case study of Electric Vehicle Charging Stations, as introduced in Section III. Our goal is to delve deeper into understanding the impact of incorporating MTD-based resilience strategies within the system, while also analyzing the potential cascading effects on other critical infrastructures interconnected with it.

References

[1] B. Cassottana, M. M. Roomi, D. Mashima, and G. Sansavini, "Resilience analysis of cyber-physical systems: A review of models and methods," *Risk Analysis*, Jan. 2023. [Online]. Available: https://doi.org/10.1111/risa.14089

[2] D. R. S. Committee *et al.*, "Dhs risk lexicon," *Department of Homeland Security Tech. Rep*, 2008.

[3] I. Alfonso, K. Garcés, H. Castro, and J. Cabot, "Self-adaptive architectures in iot systems: a systematic literature review," *Journal of Internet Services and Applications*, vol. 12, no. 1, p. 14, Dec 2021. [Online]. Available: https://doi.org/10.1186/s13174-021-00145-8

[4] S. Y. Shin, S. Nejati, M. Sabetzadeh, L. C. Briand, C. Arora, and F. Zimmer, "Dynamic adaptation of software-defined networks for iot systems: A search-based approach," in *Proceedings of the IEEE/ACM 15th International Symposium on Software Engineering for Adaptive and Self-Managing Systems*, ser. SEAMS '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 137–148. [Online]. Available: https://doi.org/10.1145/3387939.3391603

[5] L. Ji, S. He, W. Wu, C. Gu, J. Bi, and Z. Shi, "Dynamic network slicing orchestration for remote adaptation and configuration in industrial iot," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 6, pp. 4297–4307, 2022.

[6] Y. Zhang, R. H. Deng, S. Xu, J. Sun, Q. Li, and D. Zheng, "Attribute-based encryption for cloud computing access control: A survey," *ACM Comput. Surv.*, vol. 53, no. 4, aug 2020. [Online]. Available: https://doi.org/10.1145/3398036

[7] M. Alkasassbeh and S. Al-Haj Baddar, "Intrusion detection systems: A state-of-the-art taxonomy and survey," *Arabian Journal for Science and Engineering*, vol. 48, no. 8, pp. 10 021–10 064, Aug 2023. [Online]. Available: https://doi.org/10.1007/s13369-022-07412-1

[8] G. Ahmadi-Assalemi, H. Al-Khateeb, G. Epiphaniou, and C. Maple, "Cyber resilience and incident response in smart cities: A systematic literature review," *Smart Cities*, vol. 3, no. 3, pp. 894–927, 2020. [Online]. Available: https://www.mdpi.com/2624-6511/3/3/46

[9] M. A. Althamir, J. Z. Boodai, and M. M. Hafizur Rahman, "A mini literature review on challenges and opportunity in threat intelligence," in *2023 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, 2023, pp. 558–563.

[10] S. Yoo and M. Harman, "Regression testing minimization, selection and prioritization: a survey," *Software Testing, Verification and Reliability*, vol. 22, no. 2, pp. 67–120, 2012. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/stvr.430

[11] D. Wagg, K. Worden, R. Barthorpe, and P. Gardner, "Digital twins: State-of-the-art future directions for modelling and simulation in engineering dynamics applications," *ASCE-ASME J Risk and Uncert in Engrg Sys Part B Mech Engrg*, vol. 6, 03 2020.