Modeling Moving Target Defense strategies and attacks with SAN and ADVISE

Modeling Moving Target Defense strategies and attacks with SAN and ADVISE

Francesco Mariotti*, Lorenzo Manetti† and Paolo Lollini‡

*†‡Dipartimento di Matematica e Informatica ‘U. Dini’, University of Firenze — Firenze, Italy
Email: *francesco.mariotti@unifi.it, †lorenzo.manetti2@stud.unifi.it, ‡paolo.lollini@unifi.it

***Abstract*—Security evaluation can be used at the early stage of development to identify the security level of the system’s components and to guide the system’s development process. In previous works we extended the ontology of ADVISE Meta, an high-level security modeling framework, to integrate common attack patterns and standardized adversaries’ profiles, thus enabling wide-ranging security analyses. However, in such formalism, the active part is played only by the adversary, while the defense is only a passive aspect delegated to a few embedded attributes of the models. This work proposes a preliminary study on an approach to model active dynamic defense strategies, known as Moving Target Defense (MTD). We target one of them, the proactive obfuscation technique, which is modeled using Stochastic Activity Networks to represent the system’s dynamic defense and, we join it with an ADVISE model to represent the attack counterpart.**

***Index Terms*—ADVISE, modeling, Moving Target Defense, Petri nets, proactive obfuscation, security.**

I. Introduction

Model-based security analysis can be used at the early stage of a system’s development to obtain a preliminary assessment of the security level of the system. The challenge, at this stage, is to have little knowledge about the system, thus not knowing its vulnerabilities, the possible involved adversaries, and the possible attacks that might exploit such vulnerabilities.

ADVISE Meta [1] is an ontology framework for security analysis, which allows the automatic generation of complex, analyzable ADVISE [2] models starting from an architectural description of the system. In our two previous works [3], [4], we proposed a methodology that extends the ontology of ADVISE Meta with standardized adversaries’ profiles and attack patterns, in order to enable a broader set of early-stage security analyses.

In ADVISE Meta and, consequently, in the generated ADVISE formalism, the system is represented in a static way as a set of component instances and dependency relationships that connect component instances, and the active behavior is only played by the adversary attacking the system. The defense counterpart is static as well, delegated to some embedded elements of the models, e.g., the authentication level of a component of the system or the detection probability associated with a specific attack step.

Moving Target Defense (MTD) [5] is a dynamic strategy that aims to constantly change the attack surface of the system, thus confounding the adversary and reducing the time window available for attacks. In this work, we propose an exploratory modeling approach to capture both the behavior of the dynamic system’s defenses, using Stochastic Activity Networks (SAN) [6], and the behavior of the adversary, using ADVISE [2].

II. Basics of Moving Target Defense (MTD)

In cybersecuirity, the deterministic and static nature of network configurations advantages the adversary in identifying vulnerabilities [5]. Moving Target Defense (MTD) [5] is a modern active defense principle in which the static nature of a system is broken, as its attack surface is constantly moved and changed in a reactive and/or proactive way. Hence, the probability for the adversary to successfully complete an attack will be significantly decreased. MTD strategies have several characteristics which can be summarized as follows [5]: multi-candidate, diversity, randomness, limited timeliness, and attack surface reduction. Based on these characteristics, several MTD techniques have been proposed in the literature [5].

Proactive obfuscation [7] is a MTD technique that protects and diversifies the executable code of some redundant execution units (e.g., servers), called replicas, using an obfuscator. The obfuscator uses program transformations to automatically create diverse executable code on each replica, which is structurally different from the others, but with the same semantics. Periodic restarts are also applied to the replicas. After a restart, a replica is reset (totally or partially) using the obfuscator, nullifying the progress made by the adversary in trying to exploit the executable code. Hence, in order to be successful, the attack carried on by the adversary should be completed within the time window used to restart the replica.

III. Modeling MTD and Attacks

In this section, we propose an approach to model the proactive obfuscation MTD technique, using SAN, combined with the attacks carried on by the adversary, using ADVISE. SAN is a stochastic formalism that is commonly used for performability-focused analysis and it is capable of representing dynamic behaviors, while ADVISE has been developed for high-level security analysis. Both formalisms are available in the Möbius framework [8] and are relatively easy to combine

This work was partially supported by the project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union—NextGenerationEU.

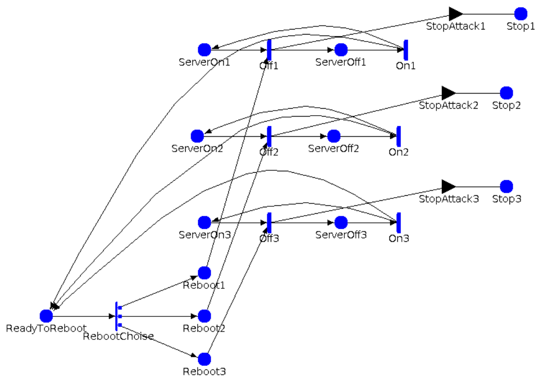

Fig. 1. SAN model of a generic system composed of three redundant servers, using the proactive obfuscation technique.

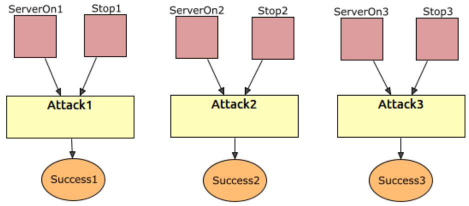

Fig. 2. ADVISE model of the attacks on the system. Each attack step (yellow rectangle) represents a generic attack on each of the three different servers. Red squares are attack preconditions variables, shared with the SAN model.

thanks to the embedded model composition formalisms (e.g., Replicate/Join).

Figure 1 shows the SAN model representing the proactive obfuscation technique applied to a generic system that makes use of three redundant servers. The servers can be on (*ServerOn*) or off (*ServerOff*). Initially, all servers are on and the *ReadyToReboot*'s marking is equal to 1. The server to be rebooted is randomly determined by the *RebootChoice* instantaneous activity (the cases' probabilities are equally distributed). The chosen server is turned off through the *Off* timed activity (with a deterministic rate). When the server is off we assume that it has terminated its service and it started its obfuscation procedure. In such case, possible attacks carried on by an adversary on that specific server are interrupted (i.e., the *Stop*'s marking is set to 1).

In Figure 2 the ADVISE model representing the adversary is shown. The model consists of three single attack steps, each of them representing a generic attack on one of the three servers. Each attack step is enabled only if the corresponding server is on and not in the reboot phase (*ServerOn* is equal to 1 and the *Stop* variable is not equal to 1). These elements are shared with the SAN model (i.e., with the SAN's homonymous places). We assume that each of the three attack steps has a different success probability. After one of the attack steps is completed the corresponding server is compromised and the adversary's goal is reached.

The SAN and ADVISE models have been composed together using the Join formalism available in Möbius, sharing *ServerOn* and *Stop* places.

We performed some preliminary experiments with the proposed models. In Figure 3 we show the probability of successfully attacking one of the three servers as time varies. Several configurations of time between switch-offs (*t_off*) were used, along with the configuration without the application of the proactive obfuscation technique (*NoMTD*), i.e., the system is composed only of a single server. Results confirm the efficacy of adopting the proactive obfuscation technique for decreasing the probability of being successfully attacked by an adversary. Moreover, it can be seen that choosing a shorter switch-off time is generally always beneficial, reducing the attack probability. However, a proper trade-off between periods of activity and inactivity should be defined so to not compromise the correct functioning of the system.

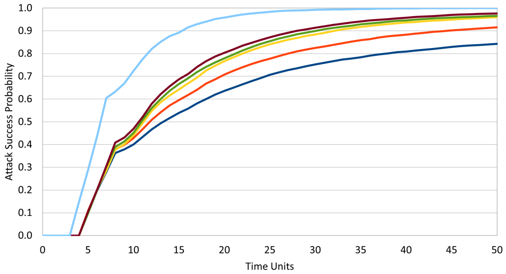

Fig. 3. Probability of successfully performing an attack on one of the three servers as time varies.

IV. Conclusions

In this work we proposed a preliminary approach for combining ADVISE models, to model adversary behavior, with SAN models for representing a specific MTD technique, the proactive obfuscation. Next steps concern the extension of the approach to model additional MTD strategies, its integration in the ADVISE Meta framework, and its application to a concrete case in the domain of future cyber-physical ecosystems, as those addressed in the SERICS project EcoCyber (Risk management for future cyber-physical ecosystems [9]).

References

[1] K. Keefe, B. Feddersen, M. Rausch, R. Wright, and W. H. Sanders, "An ontology framework for generating discrete-event stochastic models," in *Computer Performance Engineering*. Cham: Springer International Publishing, 2018, pp. 173–189.

[2] E. LeMay, M. D. Ford, K. Keefe, W. H. Sanders, and C. Muehrcke, "Model-based security metrics using ADversary VIew Security Evaluation (ADVISE)," in *2011 Eighth International Conference on Quantitative Evaluation of SysTems*, 2011, pp. 191–200.

[3] F. Mariotti, M. Tavanti, L. Montecchi, and P. Lollini, "Extending a security ontology framework to model capec attack paths and tal adversary profiles," in *2022 18th European Dependable Computing Conference (EDCC)*, 2022, pp. 25–32.

[4] F. Mariotti, A. Bondavalli, P. Lollini, L. Montecchi, and S. Nardi, "An extension of the advise meta modeling framework and its application for an early-stage security analysis of a public transport supervision system," *Journal of Reliable Intelligent Environments*, 2023.

[5] G.-l. Cai, B.-s. Wang, W. Hu, and T.-z. Wang, "Moving target defense: state of the art and characteristics," *Frontiers of Information Technology and Electronic Engineering*, vol. 17, no. 11, p. 1122 – 1153, 2016.

[6] W. H. Sanders and J. F. Meyer, "Stochastic activity networks: Formal definitions and concepts," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 2090, p. 315 – 343, 2001.

[7] T. Roeder and F. B. Schneider, "Proactive obfuscation," *ACM Transactions on Computer Systems*, vol. 28, no. 2, 2010.

[8] PERFORM Performability Engineering Research Group, "Möbius Website." [Online]. Available: https://www.mobius.illinois.edu/

[9] SERICS, "Risk management for future cyber-physical ecosystems (EcoCyber)." [Online]. Available: https://serics.eu/en/services/spoke-8-gestione-rischio-governance/