ICMS Chair
Axis 6: Resilience By Design
PhD topic proposal
"Dynamic cybersecurity strategies for automotive CPS"

J. Leneutre, V. Malvone
(IP Paris, Télécom Paris, LTCI, ACES)

Keywords: Cybersecurity, Automotive CPS, Moving Target Defense, Threat Modelling, Security Game, Multi-agent system verification

Abstract

In cybersecurity, dynamic (or active) defense mechanisms such as "Moving Target Defense" (MTD) mechanisms, aim to disrupt the inherent advantage that an attacker possesses over the defender when targeting a system by making the system dynamic, thereby limiting the attackers' actions over time. Integrating such mechanisms into a classical security approach, which is usually based on static prevention or detection mechanisms, could enhance the resilience of an *automotive Cyber-Physical System* (*automotive CPS*) against new cyberattacks. However, these mechanisms are challenging to implement in practice as they can significantly impact system performances. The objective of this PhD is to provide methods, models, and tools to define and implement a cybersecurity strategy based on MTD mechanisms adapted to the context of automotive CPSs.

Context

Usual cybersecurity approaches based solely on static protection mechanisms introduce an asymmetry at the advantage of the attackers. On one hand, a defender must deploy a system incorporating security mechanisms at a given time, using state-of-the-art methods, tools, and implementations available at the time of deployment. On the other hand, the attacker can take their time to study the deployed system to find vulnerabilities (both known and unknown, such as zero-day vulnerabilities) and develop scenarios to compromise the system (possibly based on new attack methods). In the context of a "static" target system, given enough time, the attacker will eventually find vulnerabilities and exploit them. The question is not whether the system will be compromised but when. In other words, the attacker has the opportunity to learn the system's defense strategy, whereas for the defender, by the time they understand the attacker's strategy, it is often too late. This asymmetry is particularly pregnant when considering cybersecurity risks in the context of an automotive Cyber-Physical System (automotive CPS) as demonstrated by the Cherokee Jeep hack performed at Black Hat 2015 conference [MV2015]. A crucial challenge is therefore to anticipate unplanned future vulnerabilities and attacks in order improve the resilience of automotive CPS.

Dynamic (or active) cybersecurity approaches such as the *Moving Target Defense (MTD)* approach could be very helpful to answer to this challenge. The MTD approach is a relatively new cybersecurity paradigm that emerged in the late 2000s [GPS2009]. It aims at removing the inherent advantage that an attacker possesses over the defender, by enabling dynamic

reconfigurations of parts of the systems to limit the attack launch time interval. These reconfigurations may target the run-time environment, the software stack, the representation of the data, the network or the computing platform (see [CSA2020] for a general survey about MTDs). Recently, several works applied MTDs in the context of Automotive Cyber-Physical Systems [PZC2022]. For instance [WMY2019] proposes a Controller Area Network (CAN) protocol address shuffling technique that changes a sender ID whenever an *Electronic Control Unit (ECU)* transmits a data frame using one-time IDs. Another example is the work in [YCK2019], that proposes a Software Defined Networking (SDN) based in-vehicle network architecture to periodically change the IP addresses of ECUs.

Integrating dynamic defense mechanism such as MTDs in the cybersecurity policy seems to be promising approach to improve the resilience of automotive CPS. However, the relevance of its applicability to automotive domain requires to take into account specific constraints of this domain. First, MTD mechanisms that would require some specialized hardware, would increase the manufacturing costs of the end product, making it not as likely to be implemented from a business perspective. Secondly, most of MTD mechanisms depend on dynamic instrumentation to manipulate processes at runtime, and increase the performance overhead on systems: it may have a negative impact on real time or safety constraints. Transitioning from one configuration to another may require the defender to manage (i) downtime, (ii) ongoing legitimate requests that were directed to the previous configuration in a transparent manner, and/or (iii) maintaining different configurations running simultaneously to facilitate a quicker transition. A challenge is therefore to be able to select the relevant MTD mechanisms (the less invasive and most efficient) and use them sparingly in order to ensure an acceptable tradeoff between the security level and the impact on the system.

In this context, defining a defense strategy based on MTD mechanisms requires determining the set of possible configurations for the target (WHAT to move) as already described before, but also the movement function (HOW to move), and the timing function (WHEN to move). Examples of movement functions includes shuffling of configuration parameters (network address shuffling), diversification (modification of the implementation of an application), replication (use of several communication channels). The timing function may use a constant frequency (the configuration change occurs after a constant period of time) or a variable frequency (the period of time after which the configuration change occurs varies depending on the current state of the system. In the latter case the change can be reactive and based on a triggering event (such as the detection of an attack) or pro-active and based on a strategy.

Objectives

The objective of this thesis is to provide methods, models, and tools to define and implement a security strategy based on dynamic defense mechanisms that is well adapted to the context of automotive CPS. These dynamic defense strategies will have to delicately balance the tradeoff between cybersecurity and real time constraints, while maintaining the safety constraints of the systems.

To this end, this PhD proposes to study the integration of active defense mechanisms into the security architecture of the connected vehicle, right from the design phase, in order to improve its resilience. It will focus in particular on MTD mechanisms, which involve dynamically reconfiguring certain parts of the system.

The following challenges in particular will need to be addressed:

- On which part of the vehicle and when should these reconfigurations take place?
- How can we assess the efficiency of this type of mechanisms and their impacts on connected vehicle services?
- How to take into account "intelligent attackers" who adapt their strategy depending on the defense strategy?
- How can we find the right trade-off between the level of resistance to attacks and the impact on the services provided by the connected vehicle?
- How can we be sure of the deployment strategy chosen for these mechanisms?

Brief State of the Art

Most of the works on MTDs have focused on the WHAT and HOW questions, providing and evaluating new MTD mechanisms [TKB2016, XGZ2014]. More recently, some work has focused on the WHEN to reconfigure [LDZ2017, SVK2017, FZM2017, LZ2019], but these contributions focus on the domain of web applications, with requirements, choices of MTD mechanisms, and models that are not adapted to the context of automotive domain. The work in [AKB2022][1] is one of the few tackling this question in the context of automotive CPS. It uses non cooperative game theory to model the interactions between different types of attackers and the defender of the vehicle. The resolution of the game allows the defender to choose an optimal deployment strategy of MTD that secure the system in the best possible way against the different attackers. This optimal strategy is computed as the Nash Equilibrium of the game[2]. In order to be solvable, this work consider has to consider a simple abstract game model: it only considers one step attack scenarios (i.e. attack scenarios where the attacker performs only on action, and not a sequence of actions) and it does not take into account the vulnerability dependencies between the services in the vehicle. Furthermore, it does allow to reason fully on the game strategies in order to be able to prove other properties than the existence and unicity of Nash Equilibrium.

Method & Expected Results

In this PhD, we propose to study the definition of operational and optimal MTD defense strategies in the presence of multi-stage attack scenarios modelled realistically. To achieve this, we will rely on an explicit modelling formalism of complex attack scenarios, such as attack trees (or attack-defense trees) [KPS2014, WAF2019] or attack graphs [LI2005].

Furthermore, a prerequisite will be to identify the complete range of MTD techniques that can be used in a typical vehicle architecture. For each of these techniques, it will be necessary to evaluate and model its effectiveness as well as its impact on the functionalities of the vehicle's services.

We will then rely, on one hand, on the modelling of attack scenarios and, on the other hand, on the modelling of the selected MTD mechanisms to represent the interactions between the attacker and the defender in the form of an attack/defense game. This will take into account

[1] This work has been funded by the C3S chair.
[2] A Nash equilibrium is a situation where no player could gain by changing their own strategy (holding all other players' strategies are fixed).

"strategic attackers" who adapt their behaviors to the defender's actions (previous configuration changes).

Next, we aim to use model checking techniques for multi-agent systems [Jam2010] to analyze the previously defined game and find optimal strategies for the defender while taking the attack scenarios into account. For this, we will leverage a previous contribution from our team that proposed a novel temporal logic called *Obstruction Logic* [CLM2023, CLM2024]: this logic allows to reason both on the attacker strategies (trying to progress in the attack graph) and the defender strategies (trying to block the attacker by removing edges in the attack graph). An efficient model checking procedure to verify security properties specified in this logic has been designed and implemented.

The contributions of this thesis must be validated on an experimental platform demonstrating their relevance and effectiveness within the framework of one or more predefined realistic case studies in consultation with industrial partners. A typical case study will define a set of realistic attack scenarios (that could be executed on the eplatform) and a set of MTDs (that could be deployed on the platform).

References

[ADJ2012] E. Al-Shaer, Q. Duan, and J. H. Jafarian, "Random host mutation for moving target defense," in International Conference on Security and Privacy in Communication Systems. Springer, 2012, pp. 310–327.

[AKB2022] M. Ayrault, U. Kühne, E. Borde: Finding Optimal Moving Target Defense Strategies: A Resilience Booster for Connected Cars. Inf. 13(5): 242 (2022).

[CFK2012] Chen, T., Forejt, V., Kwiatkowska, M., Parker, D., & Simaitis, A. (2012). Automatic Verification of Competitive Stochastic Systems. *TACAS*.

[CLM2023] D. Catta, J. Leneutre, & V. Malvone. Obstruction Logic: A Strategic Temporal Logic to Reason About Dynamic Game Models. ECAI 2023: 365-372.

[CLM2024] D. Catta, J. Leneutre, V. Malvone, & A. Murano. Obstruction Alternating-time Temporal Logic: A Strategic Logic to Reason about Dynamic Models. AAMAS 2024: 271-280.

[CSA2020] J.-H. Cho, D. P. Sharma, H. Alavizadeh, S. Yoon, N. Ben-Asher, T. J. Moore, D. S. Kim, H. Lim, and F. F. Nelson. 2020. Toward Proactive, Adaptive Defense: A Survey on Moving Target Defense. Commun. Surveys Tuts. 22, 1 (Firstquarter 2020), 709–745.

[FZM2017] Feng, X., Zheng, Z., Mohapatra, P., & Cansever, D.H. (2017). A Stackelberg Game and Markov Modeling of Moving Target Defense. *GameSec*.

[GPS2009] GA. A.K. Ghosh, D. Pendarakis, and W. H. Sanders, "Moving target defense co-chair's report-national cyber Leap year summit 2009," Tech. Rep., Federal NITRD Program, 2009.

[HGL2015] B. Han, V. Gopalakrishnan, L. Ji, and S. Lee, "Network function virtualization: Challenges and opportunities for innovations," IEEE Communications Magazine, vol. 53, no. 2, pp. 90–97, 2015.

[HK2016] J. B. Hong, and D. S. Kim. Assessing the Effectiveness of Moving Target Defenses Using Security Models". In: IEEE Transactions on Dependable and Secure Computing 13.2 (2016), pp. 163-177.

[Jam2010] W. Jamroga. Modeling, Verification, and Strategic Reasoning in Multi-agent Systems. Universitätsbibliothek Clausthal, 2010.

[KPS2014] Kordy, B., Pietre-Cambacédes, L., & Schweitzer, P. (2014). DAG-based attack and defense modeling: Don't miss the forest for the attack trees. *Comput. Sci. Rev., 13-14*, 1-38.

[KRV2015] D. Kreutz, F. M. Ramos, P. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," Proceedings of the IEEE, vol. 103, no. 1, pp. 14–76, 2015.

[LDZ2017] C. Lei, D. Ma, and H. Zhang. "Optimal Strategy Selection for Moving Target Defense Based on Markov Game". In: IEEE Access 5 (2017), pp. 156–169.

[LI2005] R. P. Lippmann and K.W. Ingols. An annotated review of past papers on attack graphs. Technical report, MIT, 2005.

[LR2006] A. Lomuscio and F. Raimondi. MCMAS: A Model Checker for Multi-agent Systems". In: Tools and Algorithms for the Construction and Analysis of Systems. Ed. By Holger Hermanns and Jens Palsberg. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 450-454.

[LZ2019] Henger Li and Zizhan Zheng. "Optimal Timing of Moving Target Defense: A Stackelberg Game Model".

[MV2015] C. Miller, et C. Valasek, "Jeep Hacking 101", IEEE Spectrum, 6 août 2015, https://spectrum.ieee.org/jeep-hacking-101.

[NCN2021] R. E. Navas, F. Cuppens, N. Boulahia Cuppens, L. Toutain and G. Z. Papadopoulos, "MTD, Where Art Thou? A Systematic Review of Moving Target Defense Techniques for IoT," in *IEEE Internet of Things Journal*, vol. 8, no. 10, pp. 7818-7832, 15 May15, 2021.

[PMG2017] Papernot, N., Mcdaniel, P., Goodfellow, I.J., Jha, S., Celik, Z.B., & Swami, A. (2017). Practical Black-Box Attacks against Machine Learning. *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*.

[PZC2022] B. Potteiger, Z. Zhang, L. Cheng, et X. Koutsoukos. (2022). A Tutorial on Moving Target Defense Approaches Within Automotive Cyber-Physical Systems. Frontiers in Future Transportation. 2.

[SCS2020] S. Sengupta, A. Chowdhary, A. Sabur, A. Alshamrani, D. Huang and S. Kambhampati, "A Survey of Moving Target Defenses for Network Security," in IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1909-1941, thirdquarter 2020.

[SVK2017] Sengupta, S., Vadlamudi, S.G., Kambhampati, S., Doupé, A., Zhao, Z., Taguinod, M., & Ahn, G. (2017). A Game Theoretic Approach to Strategy Generation for Moving Target Defense in Web Applications. *AAMAS*.

[TKB2016] J. Taylor, K. Zaffarano, B. Koller, C. Bancroft, J. Syversen. "Automated Effectiveness Evaluation of Moving Target Defenses: Metrics for Missions and Attacks". In: Proceedings of the 2016 ACM Workshop on Moving Target Defense - MTD'16. the 2016 ACM Workshop. Vienna, Austria: ACM Press, 2016.

[WAF2019] W. Wideł, M. Audinot, B. Fila, and S. Pinchinat. 2019. Beyond 2014: Formal Methods for Attack Tree--based Security Modeling. ACM Comput. Surv. 52, 4, Article 75 (July 2020), 36 pages.

[WMY2019] S. Woo, D. Moon, T. Youn, Y. Lee, and Y. Kim. 2019. CAN ID shuffling technique (CIST): Moving target defense strategy for protecting in vehicle CAN. IEEE Access 7 (2019), 15521–15536.

[XGZ2014] J. Xu, P. Guo, M. Zhao, R. F. Erbacher, M. Zhu, P. Liu, "Comparing Different Moving Target Defense Techniques". en. In: Proceedings of the First ACM Workshop on Moving Target Defense - MTD '14. Scottsdale, Arizona, USA: ACM Press, 2014, pp. 97–107.

[YCK2019] S. Yoon, J.-H.Cho, D. Kim, T. Moore, F. Nelson, & H. Lim. (2019). Poster: Address Shuffling based Moving Target Defense for In-Vehicle Software-Defined Networks. 1-3.

[ZB2013] Q. Zhu, & T. Başar, (2013). Game-Theoretic Approach to Feedback-Driven Multi-stage Moving Target Defense. *GameSec*.