Physical security risk analysis for mobile access systems including uncertainty impact

Thomas Termin

Institute for Security Systems, University of Wuppertal, Germany. E-mail: termin@uni-wuppertal.de

Daniel Lichte

Institute for the Protection of Terrestrial Infrastructures, German Aerospace Center, Germany. E-mail: daniel.lichte@dlr.de

Kai-Dietrich Wolf

Institute for Security Systems, University of Wuppertal, Germany. E-mail: wolf@iss.uni-wuppertal.de

Protection against car theft, involving organized crime, is a growing threat for car owners as well as fleet management providers. This brings the use of security technologies into automotive industry. The evaluation of security and the justified use of measures to reduce vulnerability of car security systems is perceived as a special challenge for vendors and users of mobile access systems (MAS), as usually only limited resources for design and analysis are available. A lack of adequate reference works and specifications in the form of concrete recommendations for action, guidelines or standards often leads to proprietary security assessments heavily relying on compliance checks. These assessments often lack sufficiency regarding application-specificity and target-orientation in terms of a good cost benefit ratio. This is true for MAS in particular, as they are relatively new products with specific use cases and boundary conditions. The open-available Performance Risk-based Integrated Security Methodology (PRISM) allows a performance-based physical security assessment of critical infrastructures (CRITIS) and initiated a paradigm shift towards performance-based methods within this area. However, PRISM comprises semi-quantitative approaches only and thus does not allow for the consideration of uncertainty impact. Moreover, the approach has not been applied to mobile access systems (MAS) yet. This paper aims at applying the concept of PRISM to the use case of MAS by extending and optimizing it to enable a holistic risk assessment considering uncertainties.

Keywords: Mobile Access Systems, Security, Risk Analysis, PRISM, Uncertainty, Decision Making under Uncertainty.

1. Introduction

The evaluation of security and the justified use of measures to reduce the inherent vulnerability of car security systems is perceived as a special challenge for vendors and users of mobile access systems (MAS), as usually only limited resources are available (Termin et al. 2020). The concept of Performance Risk-based Integrated Security Methodology (PRISM) by the Harnser Group (2010) allows conducting a guided qualitative and semi-quantitative security analysis of physical infrastructures.

In contrast to common security assessment approaches, which are often compliance-based (Sowa 2011), PRISM analyzes and evaluates system and component performance. So far, this methodology has been used for critical infrastructures (CRITIS), but it shows great potential for application to other use cases, e.g. mobile access systems (MAS).

Being an example for cyber-physical systems, MAS not only introduce new opportunities, but also vulnerabilities that need to be considered in a security risk assessment (SRA) (Cardenas et al. 2009). Thus, an approach is necessary that can consider different perspectives and requirements.

As there are no particular performance-based standards for security risk assessment (SRA) of MAS yet (Schwerdtfeger 2018), PRISM - as an elaborated procedure – potentially can be applied to MAS.

The PRISM assessment model is linear, so vulnerabilities cannot be depicted as a sharp either/or (yes/no) relationship. For this reason, it is necessary to modify PRISM to be able to handle a sharp vulnerability criterion which clearly separates the defender's success (successful intervention) from the attacker's success (worst case: asset gets successfully attacked) (Lichte et al. 2016). Moreover, it needs to be assessed how uncertainties affect the residual probability that an attacker will still successfully reach the asset (Lichte et al. 2020). Here, an approach using quantitative metrics is reasonable but not yet applied within PRISM.

The focus of this paper is a description of how the PRISM scheme could be adapted and applied to MAS and the potential role of uncertainties in this process. Subsequently, it is explained how sharp vulnerability criteria can be used in SRA of MAS. The approach presented is explained using an exemplary automotive mobile access system.

Physical security, as often neglected in cyber-physical car security system design (Anderson 2001), is analyzed in detail within the scope of this paper.

Proceedings of the 31st European Safety and Reliability Conference
Edited by Bruno Castanier, Marko Cepin, David Bigaud, and Christophe Berenguer
Published by Research Publishing, Singapore.
ISBN: 978-981-18-2016-8; doi:10.3850/978-981-18-2016-8_175-cd

2. Background

Nowadays, original equipment manufacturers (OEM) and suppliers of the automotive industry are aiming to provide digital car access as a service (Winkelhake 2017).
The physical key is replaced by a virtual entity and a mobile device acts as the new user interface to the vehicle that is connected to the internet. In order to enable the digital car access service, different interfaces are needed between the systemic actors, e.g. backend, mobile device and locking device (Termin et al. 2020). If cars and its inventory are considered attractive for an attacker, a thorough risk analysis is required to protect the economic viability of the business model behind the MAS use case.
A simple and quick statement about security is, however, not possible due to different boundary conditions of the specific use cases (Cockburn 2015). Additionally, higher degrees of complexity need be considered as well, since different stakeholder perspectives need to be addressed in the course of the analysis (Berg 1995).
Due to lacks of adequate reference works for action, guidelines or standards, SRA suited for specific use cases are difficult to conduct (Kofler et al. 2018). Moreover, usually applied SRA are mostly proprietary and conduct a compliance analysis that does not allow an appropriate design for specific use cases (Sowa 2011).
The Harnser Group developed a new approach aiming at performance-based assessment of physical infrastructures using a well-defined Performance Risk-based Integrated Security Methodology (PRISM) (Harnser 2010). Although performance-based generally aim to assess the mechanisms of delay, detection and response of barriers with regard to different attack scenarios (Garcia 2005), PRISM does not consider the interaction of all three parameters yet.
PRISM integrates protection, detection, and intervention into analysis using a methodology similar to a very detailed and elementary Failure Mode and Effect Analysis (FMEA) known from safety applications. Despite the feasibility of holistic security evaluation of physical infrastructures using PRISM, its implementation is an elaborate task. PRISM is a multi-stage process in which various security criteria are ranked, filtered and aggregated to a holistic risk index. The overall identified risks are collected and ranked in a risk register that helps the provider in decision-making.
However, security risk assessment is a challenge for providers of cyber-physical systems (Ashibani et al. 2017) due to the often-occurring lack of evidence regarding attacks (Ingolsby 2016); (Zio et al. 2013). Moreover, the residual probability of attack success should be calculated with respect to uncertainty in the context of performance-based vulnerability analysis (VA). This uncertainty can have severe effects on system design because the probability of a successful intervention can scatter. (Lichte et al. 2018) So far, PRISM, being structured similar to FMEA does not allow for the mapping of real attacks.

3. Approach

While application of PRISM is generally advantageous in security analysis and assessment, the consideration of sharp use case specific vulnerability criteria is not possible. The presented approach modifies PRISM for use case specific SRA considering the impact of uncertainty using time-based metrics. The needed steps are illustrated using an exemplary use case of mobile access system (MAS).
At first, the topology of an exemplary MAS is defined. PRISM process steps are described and adapted for the SRA for MAS. Finally, results are summarized.

3.1. Exemplary MAS definition

The system considered exemplarily in this paper is a MAS that consists of the triplet of backend, mobile device and locking device (flinkey 2021). In the following, we investigate an exemplary MAS retrofit solution for keyless access to vehicles. The physical vehicle key is kept in a box located in the vehicle.
An application on the user smartphone enables communication with the box via Bluetooth Low Energy (BLE) in order to unlock the vehicle and gain access to the physical key or to lock the vehicle. A physical mechanism presses the buttons on the key to unlock the central locking. For this application, the provider uses a trusted service for encrypted authentication. As the used digital key remains valid for a defined time-period, offline authentication is also possible.
The challenge-response principle (CRP) and a locking control protocol (LCP) are implemented for encryption purposes (Kofler et al. 2018). Communication between smartphone and backend for authorization purposes is realized via a secure Hypertext Transfer Protocol (HTTPS) connection. The backend of the provider and the intermediate trusted service are operated in a cloud (see Figure 1).

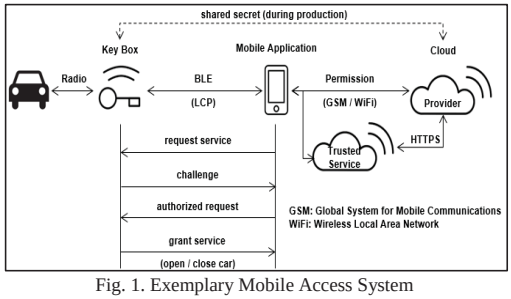

Fig. 1. Exemplary Mobile Access System

Fleet management, e.g. car sharing is a central use case of the exemplary MAS. The original key of the vehicle is stored in a secured drawer in the key box, i.e. if the vehicle is locked, the box is also locked. A manager initially assigns users via invitation. Alternatively, a driver can be defined as a team leader by the manager to be able to also assign users via the app. Only authorized users are allowed to unlock the key box and thus the vehicle.
However, MAS based fleet management faces practical problems regarding insurance coverage, because the physical key is placed inside the vehicle (Lohmann et al. 2018). For this reason, the stakeholder perspectives of insurance companies must particularly be considered here. Using the configuration space (CS) proposed by Termin et al. (2020), the exemplarily evaluated MAS can be classified (see Figure 2).

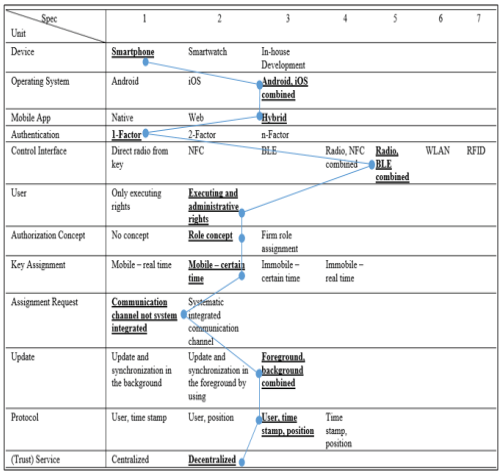

Fig. 2. Classification of the Exemplary MAS in the Configuration Space according to Termin et el. (2020)

3.2. PRISM definition

The modular Performance Risk-based Integrated Security Methodology (PRISM) is an essential part of the Harnser Reference Security Management Plan (RSMP) (Harnser 2010). Essentially, PRISM is a four steps procedure:

(i) Strategy and planning - context and scope definition
(ii) Risk assessment
(iii) Design - derivation of technical measures from the risk assessment
(iv) Implementation and testing - suitability verification in practice

After the fourth step, the PRISM process is restarted based on the continuous improvement Plan-Do-Check-Act (PDCA) (Syska 2006) cycle. Operators gain additional evidence over time, i.e. regarding efforts needed for implementation and reached effectiveness (Klipper 2015).
Within the general procedure of PRISM, resilience of infrastructures is assessed to further evaluate the consequences of successful attacks. In contrast, it is assumed for MAS use cases that there are no opportunities for recovery or rebuilding, i.e. resilience (how to deal with effects of attacks) is not assessed within this approach (see Figure 3).
The exclusion of resilience when applied to MAS is based on the fundamental consideration that if an attack is successful, users will lose confidence in the provider and the vehicle may be stolen after a successful attack. As described, PRISM consists of multiple analysis and assessment steps which are successively merged into an overall risk score.

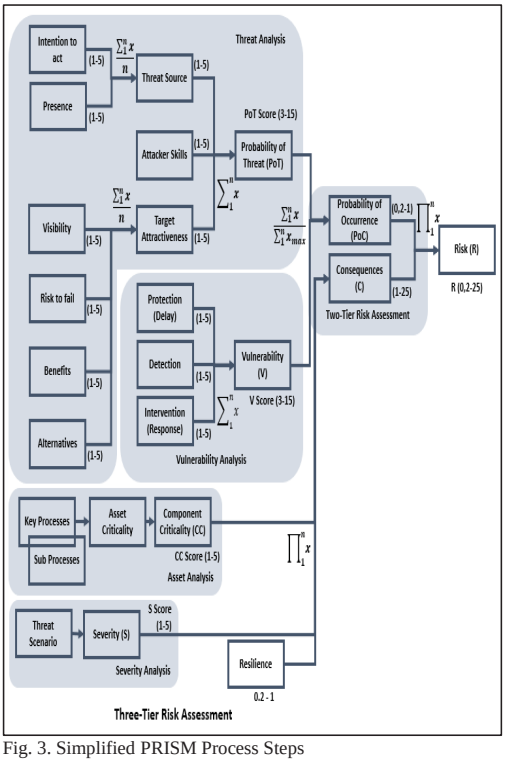

Fig. 3. Simplified PRISM Process Steps

Influencing parameters are first granulated, scored, filtered and then synthesized using a corresponding formula of multiplication, averaging and summation.
In PRISM, the relationships between individual parameters is linear. As a result, the resulting vulnerability score is of linear nature as well. However, this may be problematic for a purposeful design, since vulnerability in real-world attack scenarios is characterized by a binary outcome. In particular, the representation of vulnerability as the sum of protection, detection and intervention makes the estimation of the actual risk difficult. For security technologies to be effective, synergetic collaboration of all three mechanisms is needed in the context of specific threat scenarios for the respective use case (Lichte et al. 2016). Thus, the usual outcome of vulnerability studies is the probability of vulnerability to given scenarios.
When considering real-world performance of security measures, defining a sharp nonlinear time-based criterion is reasonable to distinguish between the binary outcome of attack scenarios: successful attack or secured asset. For example, the criterion may be that the intervention time must be shorter than the remaining time until an attacker reaches a target. If it is equal or longer, the attacker reaches the asset, otherwise not (Garcia 2005) (see Figure 4).

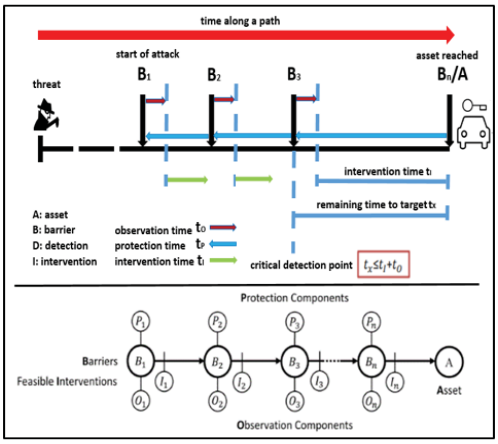

Fig. 4. Intervention Capability Model according to Garcia (2005) (below) applied to MAS (above)

In addition to a discrete consideration, variances can be defined and mathematically mapped using density functions (Lichte et al. 2018). In security, the focus is on technical measures that can prevent or sufficiently delay attacks, so that ideally– an intervention can take place (Lichte et al. 2016). Thus, these measures affect the residual probability whether an attacker reaches the asset. Use of a distribution-based approach is explained in the vulnerability analysis (VA) in this paper.

3.3. PRISM Phase B: Risk Assessment

The second phase of PRISM is the conduction of a SRA. This step is divided into seven sub-steps:

(i) Characterization of Assets
(ii) Characterization of Threats
(iii) Assessment of Consequences
(iv) Assessment of Vulnerabilities
(v) Assessment of Threat Probabilities
(vi) Risk Assessment
(vii) Definition of Protection Objectives

This paper explains procedures for MAS operators for conducting a SRA, but does not focus upon the details of the single sub-steps. These are briefly discussed in the context of SRA for MAS. A holistic risk assessment requires the evaluation of threat, vulnerability and consequences. The focus of this work is on the VA because a cost-benefit analysis supporting the operator in MAS optimization can be conducted based on the results of this sub step (iv).

3.3.1. Asset Characterization

For conducting this step, the exemplary four-tier MAS structure of provider, trusted service, locking device and user including mobile device is analyzed topologically. Figure 5 depicts the assumed MAS topology.

According to Harnser (2010), the "*what-if"* technique can be used for identification and evaluation of assets. This scenario-based approach is used to analyze and evaluate systems under different boundary conditions (Garcia 2005). The strategy is to conceptually remove a systemic function or an element of the system and then consider what effect this loss has on the overall functionality. If system functionality is restricted, the element is characterized as an asset. An asset can be a process, a component or a group of components (Garcia 2005).
In PRISM, asset criticality is scored using a value from one to five (Harnser 2010). Based on this rating, a ranking can be conducted to identify assets considered as critical points (CP). These assets with high criticality scores are further analyzed in detail, while low ranked assets are not considered during the SRA procedure.

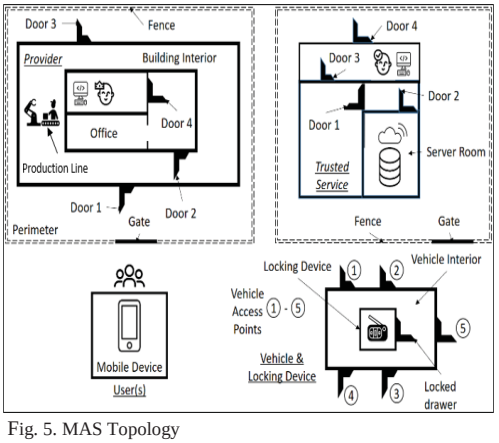

Fig. 5. MAS Topology

A number of MAS assets were already identified by Termin et al. (2020), namely:

(i) Locking Device
  (a) Access to the physical key, if available
  (b) Access to a vehicle
(ii) Mobile Device (hardware)
  (a) Access credentials for the user account
  (b) Access to cars via mobile application
(iii) Access credentials for the portal (manager account)
  (a) Access to permission management (e.g. definition of roles, assignment of users to cars)
  (b) Editing user or manager accounts or products or services
  (c) Stored user / product / service data
(iv) Access credentials for the key management system (trusted service)
  (a) Transmission of digital keys
  (b) Generation of digital keys
  (c) Stored user / product / service data

According to Harnser (2010), assets are generally divided between hardware, software and workforce (see Table 1). Hardware in this case are the key box including the physical key, the user device, the manager's computer and the physical entities of the backend or the cloud respectively (Klipper 2015).

Table 1. Exemplary High Level MAS Asset Characterization

Asset Type	**Asset Specification (Detailed Description)**
Hardware	Physical Vehicle Key
	Computer of Manager
	Mobile Device Storage Entity of Backend
	Production Line
Software	Transmission of Digital Keys
	Storage of Permissions & Access Data
	Processing of Data
Workforce (Human Entity)	User
	Company Manager (of Permissions)
	Trusted Service Manager (of Digital Keys)

Software assets refer to the storage, processing and transmission of data (Wheeler 2011). Workforce includes every human component, here e.g. the user or employees of the provider. The workforce component is not part of further analysis.
It is rational to conduct a detailed asset characterization to specify the specific role and task of MAS entities precisely (Klipper 2015). The physical description (geographical position, topological boundary conditions) and operation modes (operating hours, availability, etc.) with their interdependencies to other entities should also be cautiously analyzed in this step.
It should be noted that the assessment of the criticality of the specified assets is subjective due to an indifferent scoring process. In Table 1, the physical key, the transmission of the digital key, the mobile device of users and the physical storage entities of the backend are potential critical points (CP).

3.3.2. Threat Characterization

This step is used to screen and prioritize potential threat sources based on the intrinsic level of threat for MAS. The characterization is the starting point for the development, analysis and evaluation of scenarios. In this paper, only criminal activities are assumed. According to Harnser (2010), criminal threats are divided into five main categories:

(i) Terrorists
(ii) Economic criminals
(iii) Violent criminals
(iv) Subversives
(v) Petty criminals

Expert interviews are a feasible way to gather the needed information to be able to identify possible threats for a specific use case and to define their relevance (Klipper 2015). If matching data is available, extrapolation, the analysis of similar use cases (from other providers), statistical information from insurance companies and authorities, e.g. police or federal vehicle department can be applied or adapted to the MAS (Brezinski et al. 2013).
Extrapolation, e.g. based on burglary statistics, helps to estimate the threat likelihood. A main advantage of burglary statistics for the MAS use case is contained data regarding city, region and vehicle type or brand. For example, if a MAS use case involves a large number of vans from a particular original equipment manufacturer, the operator of the respective business model is able to check the rate of thefts of certain vehicles and identify burglary hotspots in the application area (see Figure 6).

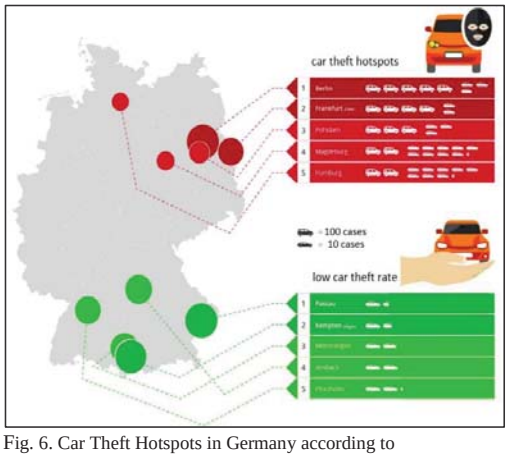

Fig. 6. Car Theft Hotspots in Germany according to FinanceScout24 (2021)

3.3.3. Consequence Characterization

This step deals with characterizing the severity of functional failures caused by theft or destruction of an asset. Severities can already be implicitly derived from asset characterization. Within the scope of consequence characterization, threat scenarios are related to specific CP (see Table 2). The severity scoring only considers primary consequences, i.e. those that directly affect system functionality.
According to Harnser (2010), three main pillars of primary consequences can be differentiated. The first pillar is loss of health or life due to a particular materialized threat scenario. The second pillar consists of loss of production (total or partial loss for any amount of time). The third pillar includes loss of security of the respective critical asset, i.e. uncontrolled exploitation or access. In the context of the threat scenarios considered, loss of human life is not to be expected.

The loss of production is a corner case that does not affect the actual performance of a MAS, but can have a monetary impact on the operator's business model. Depending on the assessment scope, buildings, facilities and related assets are considered within the VA as well. For the VA of MAS it is recommended to consider only the vehicle. Harnser (2010) uses a scoring range between 10 (insignificant consequences) and 100 (worst case, total loss, including 100k and more injured people). Graduations are recommended in intervals of ten.
In contrast to PRISM, loss of human life can be neglected here because in case of a theft of the car or a damage of the inventory, human health is not directly affected. Due to this, damage in the sense of unavailability of system functions is focused upon in the MAS SRA.

Table 2. MAS Risk Scenarios

Threat Source	**Scenario Description**	**Critical Points**
Economic criminal	Employee uses his access right to delete service-related data	Computer (of Manager), Mobile Device
	Hardware is sabotaged during production	Production Line
Violent Criminal	Theft of user device	User device
	Blackmailing provider	Company Manager
	Eavesdropping	Mobile Device Communication

In a further stage, consequences can not only be scored but also actually monetized, i.e. consequences can be represented in the form of monetary losses (Lichte et al. 2016). An operator can estimate the consequences of the damage or theft of physical units, e.g. for a stolen car.

3.3.4. Assessment of Vulnerabilities

In the previous steps, threat scenarios were set up that assign a threat to a concrete CP. This step evaluates how high the vulnerability, i.e. the likelihood of a successful attack is in each of the considered (worst case) scenarios.
There are different approaches to assess vulnerability, mainly compliance-based or performance-based assessments (Harnser 2010). The former corresponds to checklists controlling whether needed security measures are deployed and working. However, compliance checks by analysts and experts do not assess the quality of implementation of security measures. Additionally, compliance checks represent only an actual snapshot. Thus, they are rather unsuitable for the SRA of specific MAS use cases. Application is reasonable, when assuming large uncertainties regarding the capabilities of considered security measures (Klipper 2015); (Wheeler 2011).
In contrast, Garcia's (2005) performance-based approach evaluates the performance of security measures for specific attack scenarios using the capabilities protection, detection and intervention. It was adapted by Harnser (2010) without using quantification. To assess vulnerability in a scenario-based manner, PRISM recommends the use of an Adversary Sequence Diagram (ASD). This diagram shows each potential path of an attacker to the target (see Figure 7).

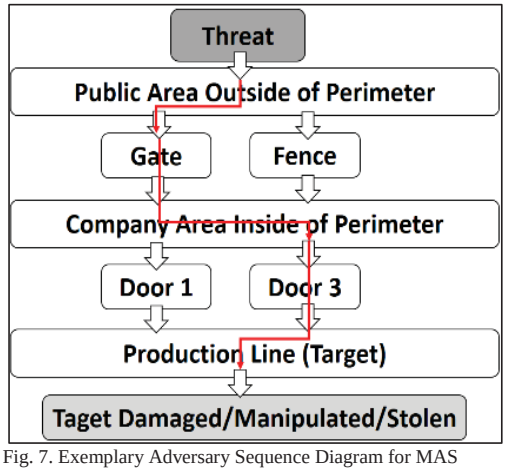

Fig. 7. Exemplary Adversary Sequence Diagram for MAS

Within PRISM, the VA assesses a vulnerability level by scoring protection, detection and intervention between 1 = high performance (low vulnerability) and 5 = low performance (high vulnerability) (see Table 3).
General scoring as conducted within the PRISM VA is not related to specific security measures. Better results can be achieved by using a quantitative approach to VA using e.g. a time-based metric.

Table 3. Performance Mechanism Scoring (for Protection, Detection & Intervention)

Score	Description	Vulnerability Level
1	High Degree of Capability to prevent occurrence of scenario x	Very Low
2	Significant Capability	Low
3	Moderate Capability	Moderate
4	Limited Capability	High
5	No Capability	Very High

3.3.5. Time-based Vulnerability Assessment

In a first step, the topological relations of the exemplary MAS entities need to be mapped based on the ASD shown in Figure 7. For a thoroughly conducted VA, all possible paths to an asset need to be considered. For the exemplary MAS, ten paths can be identified.
Then, the sequences need to be further described using both protection, observation and intervention as illustrated in Figure 4.

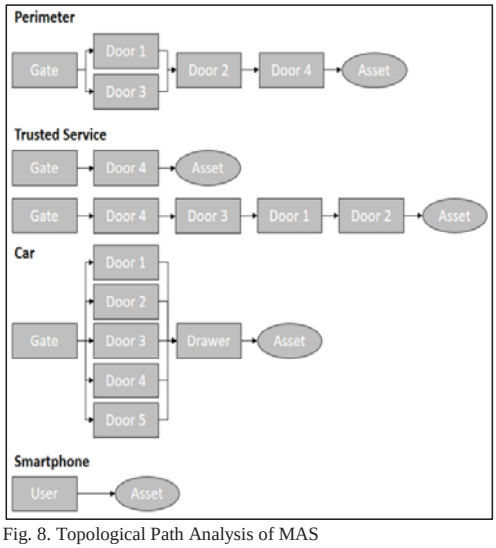

Fig. 8. Topological Path Analysis of MAS

An attacker must break through barriers that slow him down on his way to the asset. In the course of the attack process, observation is needed to detect an attacker. Probability of detection can be defined as Eq. (1).

$$D = P(t_p > t_o) \tag{1}$$

The respective probabilistic density functions (pdf) are assumed as normal distributions within the scope of a specific attack (see Figure 9). One way to assume parameters for distributions is to use the results of penetration tests performed, extrapolation as introduced in the threat characterization section or best-guesses by experts. The probability of successful detection corresponds to the area enclosed by the density functions of protection and observation. To obtain the cumulative probability, it is necessary to integrate over the corresponding time interval (see Eq. (2)).

$$D(t) = \int_0^t o(t_O) \times \left[\int_{t_O}^{\infty} p(\tau) d\tau\right] dt_O \tag{2}$$

t is the time of an attack and to represents the observation time. Once the attacker has been detected, the attack can be stopped by an intervention unit only if there is enough time available. Intervention probability thus is the inverted probability of a successful attack. Successful intervention at individual barriers is reached when the time to intervene is shorter than the residual protection time, as formulated in Eq. (3) and Eq. (4).

$$t_I < \sum_{x+1}^{n} t_{p,i} \tag{3}$$

$$T = P(t_X > t_I) \tag{4}$$

Herein residual protection time is the convolution of the protection density functions of the remaining barriers along an attack path (see Eq. (5)).

$$p_{Path,x}(t) = p_{x+1}(t) \times \ldots \times p_n(t) \tag{5}$$

Combining the pdf of intervention and residual protection leads to the probability of a timely intervention at the "*i-th*" barrier of the considered attack path (see Eq. (6)).

$$T(t) = \int_0^t i(t_I) \times \left[\int_t^{\infty} p_{Path,x}(\tau) d\tau\right] dt_I \tag{6}$$

As a result, vulnerability of individual barriers is calculated using Eq. (7):

$$V_i = 1 - S_i = 1 - D_i \times T_i \tag{7}$$

Herein, the strength of a barrier is combined with the probability of a timely intervention. Finally, total vulnerability can be calculated by multiplying the vulnerabilities of all barriers along the considered attack path (see Eq. (8)).

$$V_{path,j} = \prod_{i=1}^{n} V_i \tag{8}$$

Implementing the described approach enables analysis of sharp vulnerability criteria in the SRA of MAS.

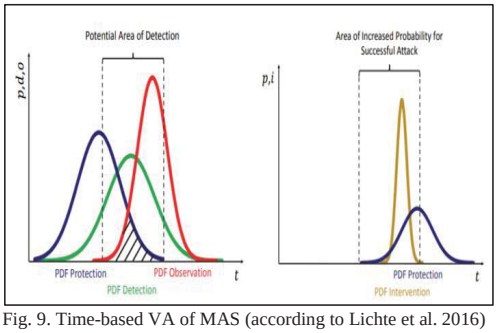

Fig. 9. Time-based VA of MAS (according to Lichte et al. 2016)

4. Conclusion and outlook

Within this paper, the approach of PRISM is adopted and optimized for the use case of MAS to analyze and assess threat scenarios using a time-based quantitative vulnerability metric. First, the methodology was explained, challenges and limits were highlighted.

Although PRISM is successfully applied in security analysis and assessment of CRITIS, there is no adoption of this elaborated procedure in other security-related use cases yet. The presented approach outlines first steps to fill the gap regarding adequate MAS SRA frameworks by adopting relevant parts of PRISM.

The analysis and evaluation of various risk parameters is a particular challenge within the extensive PRISM framework. Additionally, the semi-quantitative approach does not consider the interaction between performance

mechanisms and the impact of parameter inherent uncertainties that are a result of different information gaps. Within this paper, a PRISM modification is proposed, that allows conducting VA for specific MAS use cases based on defined threat scenarios. The performance-based VA enables more specific insights regarding vulnerabilities. Usage of probability density functions within this approach enables the consideration of lacking information.
However, the presented approach only covers the related to physical security risk of MAS. Eventually, the assessment of the comprehensive security risk of an individually configured MAS requires the consideration of cyber security aspects. At this point, a holistic vulnerability metric used for analyzing and assessing the interaction of physical and IT scenarios is strongly needed. Enabling the alignment of different risks within one procedure in this way could be an important milestone for completing a holistic assessment of MAS risks.

References

Anderson, R. (2001). Security engineering: a guide to building dependable distributed systems. John Wiley & Sons.

Ashibani, Y. and Q. H. Mahmoud (2017). Cyber physical systems security. Analysis, challenges and solutions. Computers & Security. 68. Jg. Pp. 81-97.

Berg, M. (1995). Risikobewertung im Energiebereich. Vdf Hochschulverlag AG.

Brezinski, C., M. Zaglia and M. Redivo (2013). Extrapolation methods: theory and practice. Elsevier.

Briggs, A. and P. Fenn. (1998). Confidence intervals or surfaces? Uncertainty on the cost-effectiveness plane. Health economics. 7. Jg. Nr. 8. pp. 723-740.

Cardenas, A. et al. (2009). Challenges for securing cyber physical systems. In: Workshop on future directions in cyber-physical systems security.

CCC (2020). https://carconnectivity.org/.

FinanceScout24 (2021). https://www.financescout24.de/wissen/studien/autodiebstaehle-statistik.

FIRST (2020). https://www.first.org/.

Flinkey (2021). https://www.flinkey.de/.

Garcia, M. L. (2005). Vulnerability Assessment of Physical Protection Systems. Sandia National Laboratories, Burlington, Elsevier.

Harnser Group (2010). A Reference Security Management Plan for Energy Infrastructure. European Commission.

Hoffmeister, C. (2015). Digital Business Modelling. Digitale Geschäftsmodelle entwickeln und strategisch verankern. Hanser, München.

Ingolsby, T. R. (2016). Attack Tree-based Threat Risk Analysis. Amenaza Technologies Limited, a vendor whitepaper.

Klipper, S. (2015). Information Security Risk Management: Risikomanagement mit ISO/IEC 27001, 27005 und 31010, 2nd Edition, Wiesbaden, Springer-Verlag.

Kofler, B, A. Zingsheim, K. Gebeshuber, M. Widl, R. Aigner, T. Hackner, S. Kania, P. Kloep and F. Neugebauer (2018). Hacking & Security: Das umfassende Handbuch, Bonn, Rheinwerk-Verlag.

Lichte, D. and K.-D. Wolf (2018). A Study on the Influence on Uncertainties on Physical Security Risk Management, In: Proceedings of ESREL 2018: Safety and Reliability – Safe Societies in a Changing World (Haugen, S. et al.), CRC Press.

Lichte, D., S. Marchlewitz and K.-D. Wolf (2016). A Quantitative Approach to Vulnerability Assessment of Critical Infrastructures With Respect to Multiple Physical Attack Scenarios. In: Future Security 2016, Proc. intern. conf., Berlin, Germany.

Lichte, D., T. Termin and K-D. Wolf (2020). On the Impact of Uncertainty on Quantitative Risk Assessment. In: Proceedings of the 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference.

Lohmann, M. F. and A. Rusch (2015). Fahrassistenzsysteme und selbstfahrende Fahrzeuge im Lichte von Haftpflicht und Versicherung. HAVE-Haftung und Versicherung. 4. Jg. pp. 349-355.

Saltelli, A., P. Annoni, I. Azzini, F. Campolongo, M. Ratto and S. Tarantola (2010). Variance based sensitivity analysis of model output. Design and estimator for the total sensitivity index, Joint Research Centre of the European Commission.

Schwerdtfeger, A. (2018). Konzeption und Evaluierung eines Prozesses zur ganzheitlichen Sicherheitsbewertung von Mobile-Access-Systemen, Wuppertal, Bergische Universität Wuppertal.

Sowa, A. (2011). Metriken - der Schlüssel zum erfolgreichen Security und Compliance Monitoring. Wiesbaden: Vieweg and+ Teubner Verlag.

Stamatis, D. H. (2003). Failure mode and effect analysis: FMEA from theory to execution. Quality Press.

Syska, A. (2006). PDCA-Zyklus. Produktionsmanagement: Das A—Z wichtiger Methoden und Konzepte für die Produktion von heute. 2006.

Termin, T., D. Lichte and K.-D. Wolf (2020). Approach to Generic Multilevel Risk Assessment of Automotive Mobile Access Systems. In: Proceedings of the 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference.

Wheeler, E. (2011). Security Risk Management: Building an Information Security Risk Management Program.

Winkelhake, U. (2017). Die digitale Transformation der Automobilindustrie: Treiber-Roadmap-Praxis. Springer-Verlag.

Zio, E. and T. Aven (2013). Model output uncertainty in risk assessment. International Journal of Performability Engineering. 29. Jg. Nr. 5. pp. 475-486.