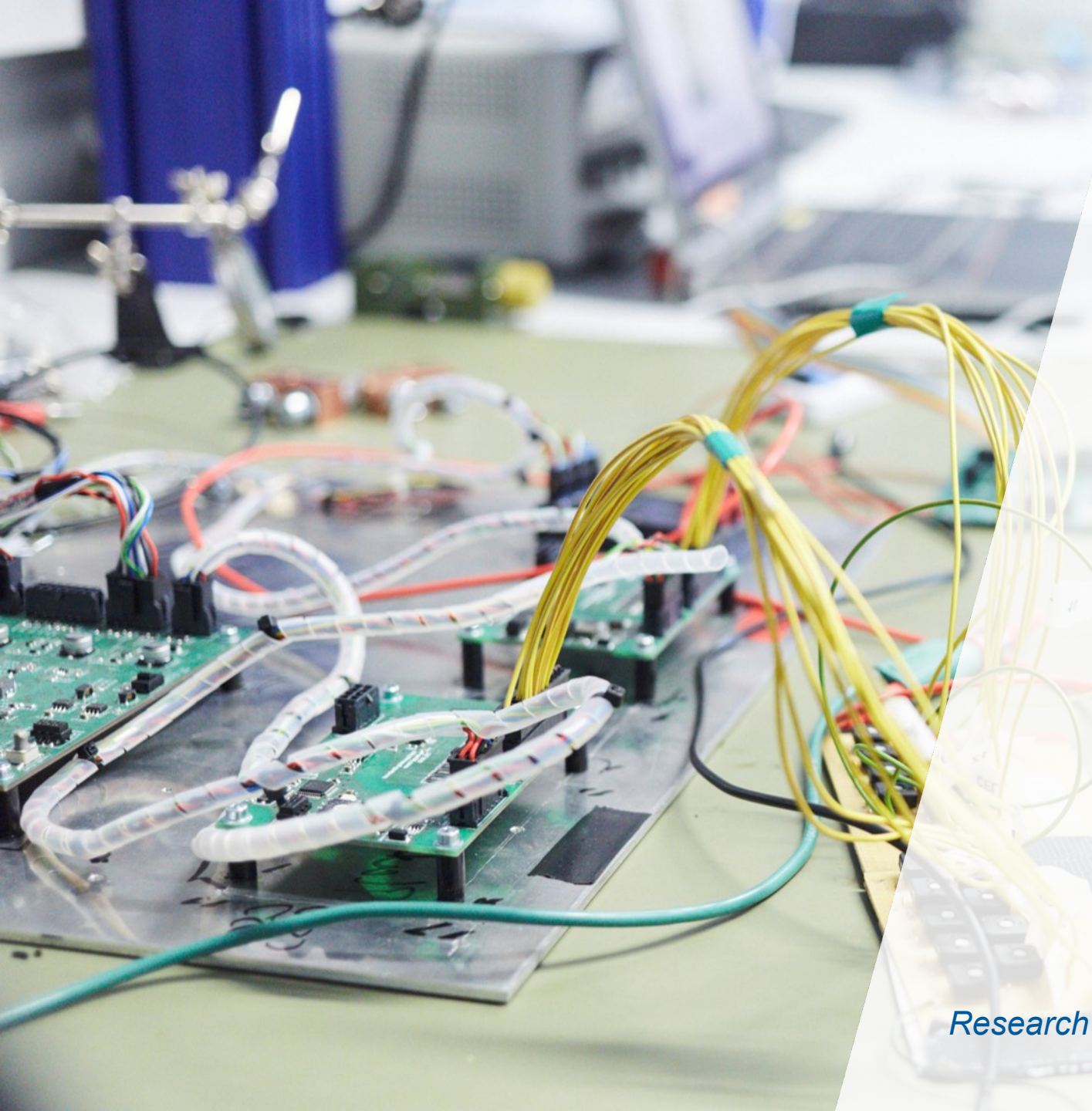


A Concept of an Attack Model for a Model-Based Security Testing Framework

Tina Volkersdorfer
tina.volkersdorfer@carissma.eu

Hans-Joachim Hof
hans-joachim.hof@thi.de

SECURWARE 2020
November 21, 2020 to November 25, 2020

Research Group Security in Mobility

Technische Hochschule Ingolstadt

Virtual Session Chair

Resume of the presenter

Tina Volkersdorfer received the M.S. degree at Technische Hochschule Ingolstadt (THI). She is a research assistant in the team „Security in Mobility“ of CARISSMA, the THI research and test centre. In context of automotive security, the group addresses the automated identification of vulnerabilities within all phases of software development (e.g., anti-patterns, forensics). Based on this, a complement generation of security advices is the purpose.

Her focus is on the security modelling and generation of security test cases, including attack, adversary and target models. She works on the current project “MASSiF” that addresses model-based security and safety assurance for automotive safety systems. “MASSiF” is supported by the BMBF under the KMU-innovative program.

Federal Ministry of Education and Research

Automotive domain

- Using different models (time-consuming; inconsistent and untraceable security)

⇨ Holistic modelling framework for attacks

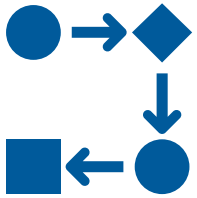
Penetration testing [1]

- Expensive solving of security problems
- Depending on the skills of the tester

⇨ Complement for penetration tests

⇨ Automatable test execution in the early design phase

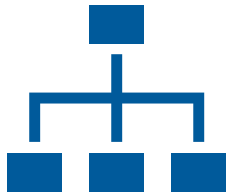
Focus is on identifying the necessary conceptional elements for a suitable holistic attack modelling framework



Process Modelling

⇨ Lockheed Martin Cyber Kill Chain [2]

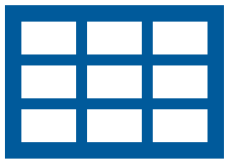
- Phases
- Linear



Graph-Based Modelling

⇨ Attack Tree [3]

- Reuse, combination
- Multiple paths
- No adversary information
- No adversary behaviour



Classification Modelling

⇨ MITRE ATT&CK [4]

- Abstraction level
- Adversary behaviour
- Late usage
- No Adversary Strategy

Holistic Modelling

⇨ ADVISE [5]

- Security Analysis Method
- Late usage
- Abstract adversary decision function

The proposed framework is intended to be used to decide on the next steps during testing activities with the following requirements (derived from [6]):

- Model-based
- Expressive
- Reusable
- Systematic
- Consistent
- Visualizable
- Understandable

Overview

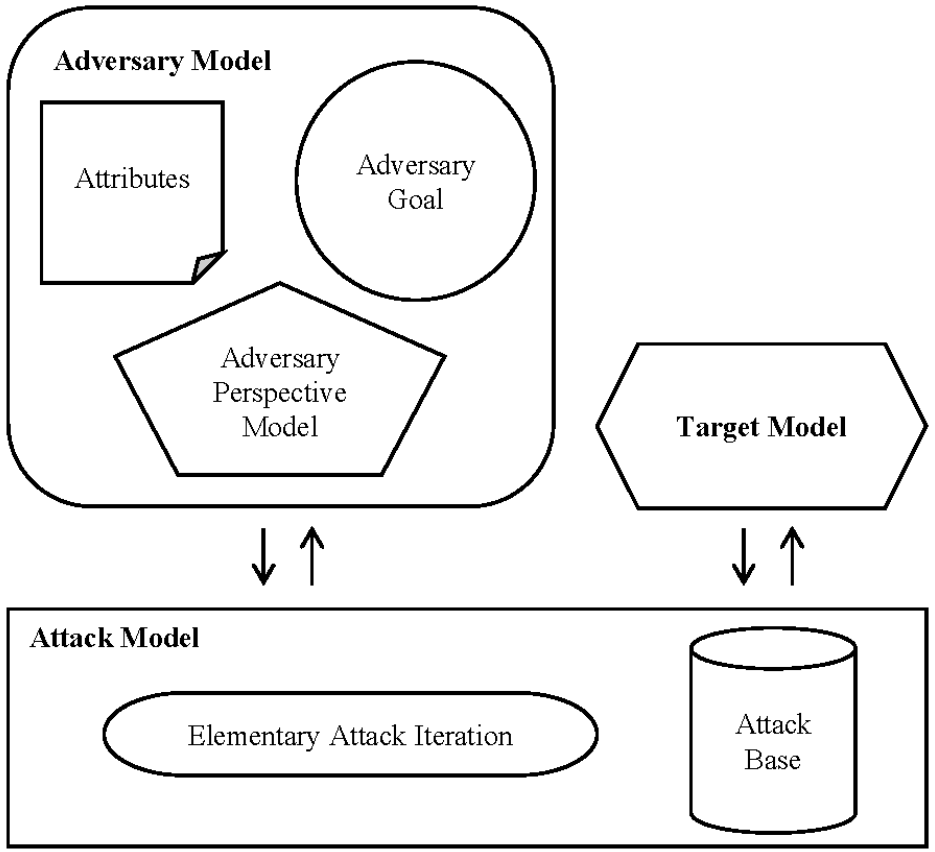


Figure 1. Components of the framework.

Attributes

⇨ Characterize each adversary

Adversary Goal

⇨ To derive the adversary's behaviour during an attack simulation

Adversary Perspective Model

⇨ Represents the adversary's knowledge about the target at a given time

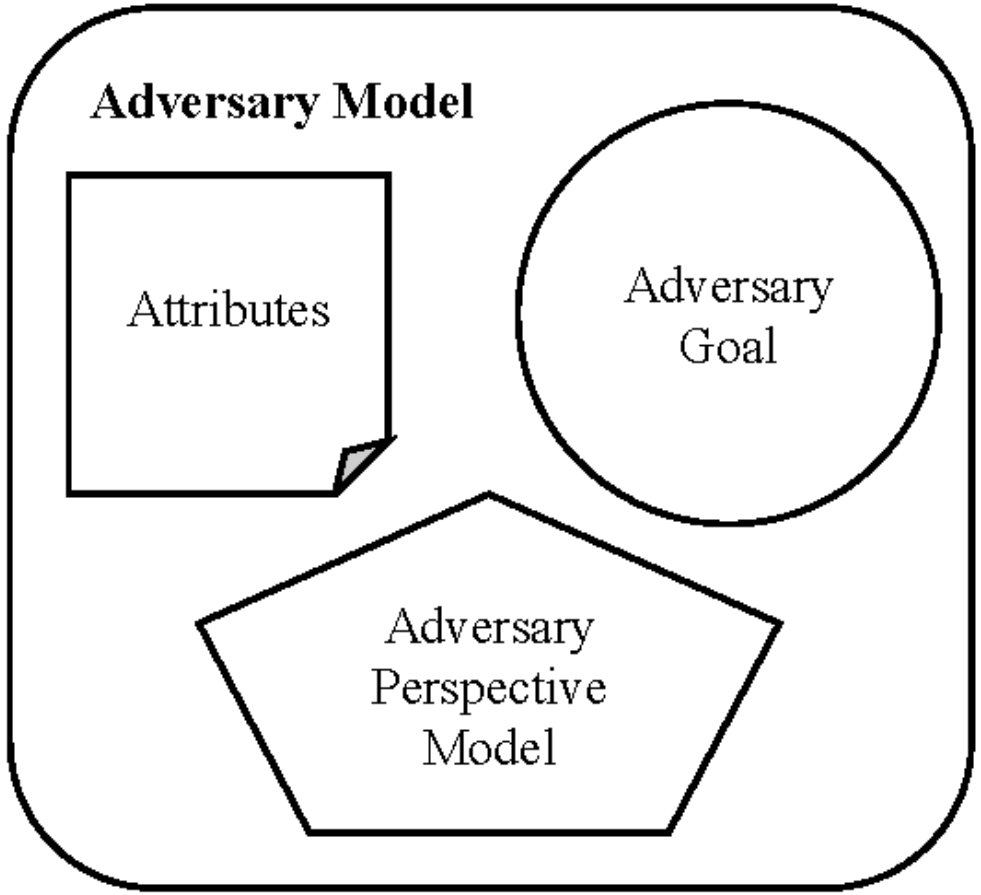


Figure 2. Components of the Adversary Model.

Target Model

Figure 3. Target Model.

- Represents one or more cyber-enabled capabilities [7], that an adversary wants to attack
- Holds all necessary, correct information (e.g., available access points [8])
- Allows executing attacks on systems that do not yet exist

Process perspective

- Elementary Attack Iteration
  1) Identify available access points
  2) Select one access point
  3) Probe the target
  4) Update the adversary's knowledge

Technical perspective

- Exploit [9] tagged with preconditions [10]

Strategic perspective

- Simulation of the adversary's strategical behaviour

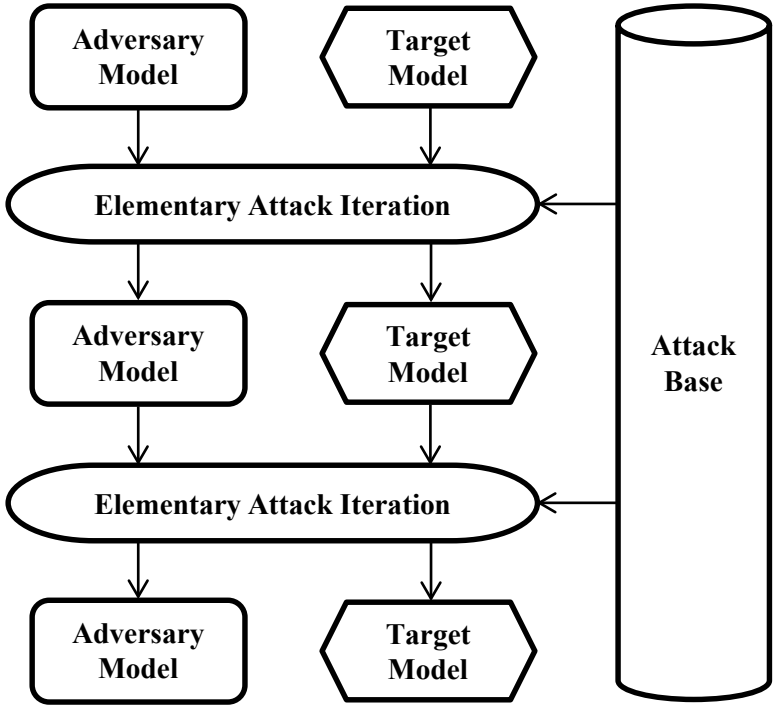


Figure 4. Interaction of the components regarding the elementary attack iteration.

Preliminary Evaluation

- Attack Scenario 1: Identity theft attack on a social media platform [11]
- Focus on step (3) “Probe the target” (of one Elementary Attack Iteration)

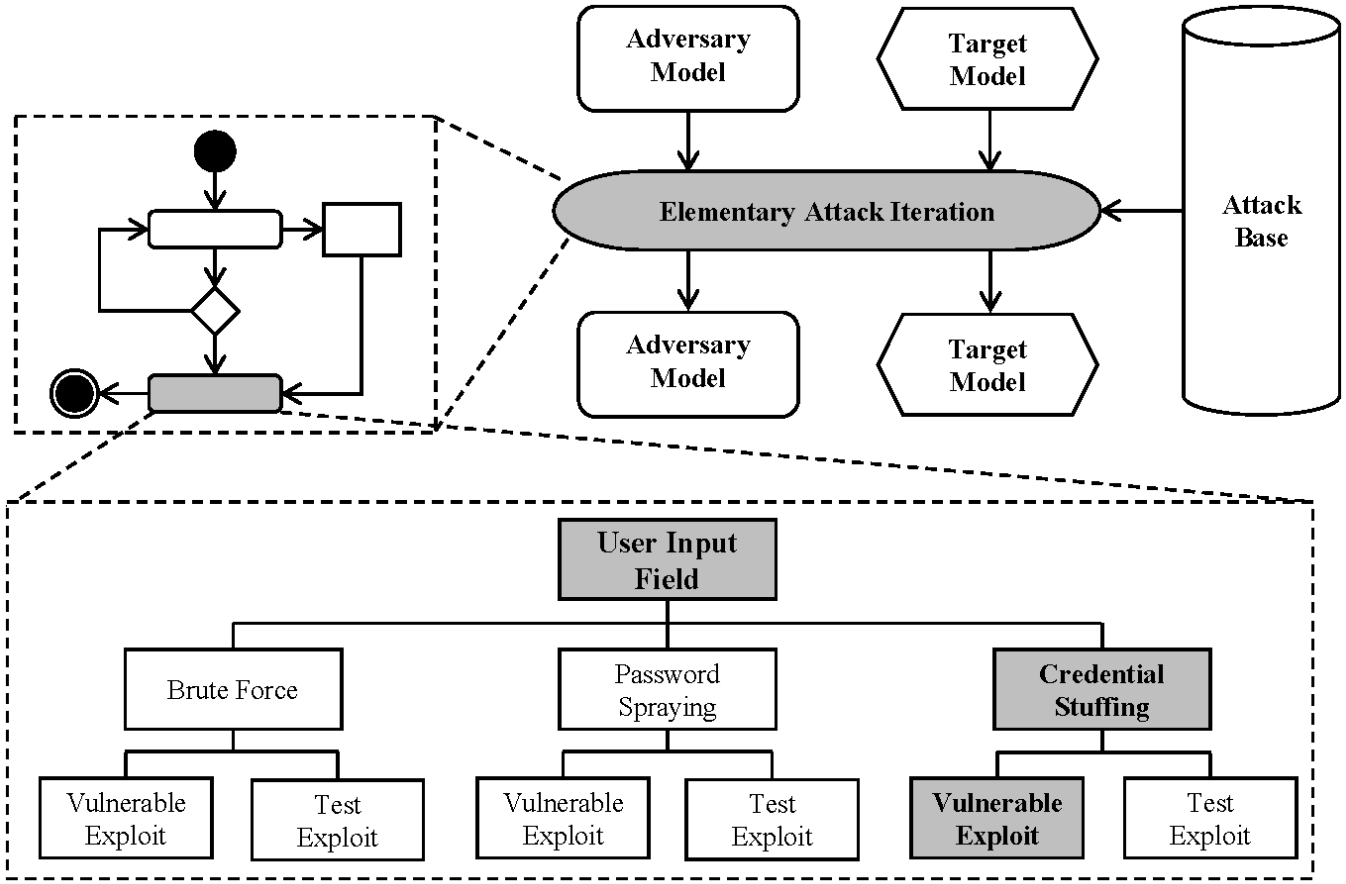


Figure 5. Findings in context of attack scenario „Identity theft“.

- ✓ **Model-based:** Suitable foundation for different modelling approaches
- ✓ **Relevant attacks:** Representative examples
- ✓ **Application domain independence:** Examples from very different application domains
- ✓ **Reusable elements:** E.g., Content of attack base, Elementary Attack Iteration
- ✓ **Systematic structures:** E.g., Elementary Attack Iteration, Adversary Model, Target Model
- ✓ **Visual elements:** Suitable foundation for the integration of graphical model elements

- Proposed attack modelling concept meets the requirements model-based, expressive, reusable, systematic and visualizable.
- In a later stage of the research project MASSiF the requirements, including the omitted requirements “consistent” and “understandable”, can be meaningfully evaluated.

Conclusion and Future Work

- Concept of an attack modelling framework for model-based security testing
  - Addresses security throughout the software engineering
  - Offers several perspectives on attacks

- **Purpose:** Support the automation of security tests, especially in early phases
- **Preliminary evaluation:** Model-based, expressive, reusable, systematic, and visualizable
- **Future work:** Detailed specification and implementation

References

[1] K. Scarfone, M. Souppaya, A. Cody, and A. Orebaugh, Technical Guide to Information Security Testing and Assessment, 800-115 ed., Gaithersburg, MD 20899-8930: National Institue of Standards and Technology, 2008.

[2] E. Hutchins, M. Cloppert, and R. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis," Leading Issues in Information Warfare & Security Research, vol. 1, pp. 80-106, January 2011.

[3] B. Schneier, "Attack Trees," Dr. Dobb's Journal, vol. 24, no. 12, pp. 21-29, 1999.

[4] B. E. Strom et al., "MITRE ATT&CK: Design and Philosophy," July 2018. [Online]. Available: https://www.mitre.org/sites/default/files/publications/pr-18-0944-11-mitre-attack-design-and-philosophy.pdf. [retrieved: 2020.09.25].

[5] E. LeMay et al., "Adversary-Driven State-Based System Security Evaluation," in Proceedings of the 6th International Workshop on Security Measurements and Metrics, New York, NY, USA, Association for Computing Machinery, 2010, pp. 1-9.

[6] A. Drescher, A. Koschmider, and A. Oberweis, Modellierung und Analyse von Geschäftsprozessen [Modelling and Analysis of Business Processes], Berlin, Boston: De Gruyter Oldenbourg, 2017.

[7] The MITRE Corporation, "CAPEC Glossary," 4 April 2019. [Online]. Available: https://capec.mitre.org/about/glossary.html. [retrieved: 2020.08.07].

[8] J. Bryans et al., "A Template-Based Method for the Generation of Attack Trees," in Information Security Theory and Practice, Cham, Springer International Publishing, 2020, pp. 155-165.

[9] H. Siller, "Exploit," Springer Gabler, 19 February 2018. [Online]. Available: https://wirtschaftslexikon.gabler.de/definition/exploit-53419/version-276511. [retrieved: 2020.09.15].

[10] K. Kaynar, "A taxonomy for attack graph generation and usage in network security," Journal of Information Security and Applications, vol. 29, pp. 27-56, August 2016.

[11] The OWASP Foundation, "OWASP Top 10 - 2017: The ten most critical web application security risks," 2017. [Online]. Available: https://owasp.org/www-project-top-ten/. [retrieved: 2020.08.13].

Thanks for your attention!
If you have any questions, please email me!

tina.volkersdorfer@carissma.eu