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

SECUWARE 2020
November 21, 2020 to November 25, 2020

Research Group Security in Mobility
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.
Introduction

Motivation and Purpose

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
Introduction

Related Work

- 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
Design of an Attack Model for a Model-Based Security Testing Framework

Overview

Figure 1. Components of the framework.
Design of an Attack Model for a Model-Based Security Testing Framework

Adversary Model

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.
Design of an Attack Model for a Model-Based Security Testing Framework

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
Design of an Attack Model for a Model-Based Security Testing Framework

Attack Characterization and Simulation

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

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“.
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


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

tina.volkersdorfer@carissma.eu