Identification and Modelling of Security and Privacy Threats in Connected Vehicles

Costas Lambrinoudakis
Christos Kalloniatis
Vasiliki Diamantopoulou

*University of Piraeus, Dept. of Digital Systems*

Prepared in collaboration with CCS–Airbus

27/5/2018
Threat vs Vulnerability vs Risk

- **Asset:** any tangible or intangible thing or characteristic that has value for an organization.

- **Threat:** potential cause of an unwanted incident, which may harm a system or an organization.

- **Vulnerability:** weakness of an asset or control that can be exploited by one or more threats.
Threat vs Vulnerability vs Risk

- The risk is a function of:
  - The value of the IS assets (A)
  - The nature and number of IS vulnerabilities (V)
  - The nature and occurrence probability of a threat (T)
  - The nature and extend of the consequences (impact) that the organisation will experience in case of a security incident (I)

- Thus, $R = f(A, T, V, I)$
Threat vs Vulnerability vs Risk

Asset has Vulnerabilities
Threat utilizes Calculates
Impact
Consequences reduces Risk
Countermeasure
Modelling Procedure

Scenario 1

In Car Components
- Hardware
  - Software
- Middleware

Car-attached Data Sources
- Sensors
  - Camera
  - etc.

External Data Sources
- Sensors
  - Traffic Lights
  - etc.

Safety Requirements
Security Requirements
Privacy Requirements
Modelling Procedure

Scenario 1

In Car Components
- Hardware
- Middleware
- Software

Car-attached Data Sources
- Sensors
- Camera
- etc.

External Data Sources
- Sensors
- Traffic Lights
- etc.

Risk Analysis

Modelling with EBIOS - SecureTROPOS - PriS

Safety Requirements
Security Requirements
Privacy Requirements
Modelling Procedure

Scenario 1

In Car Components
- Hardware
- Software
- Middleware

Car-attached Data Sources
- Sensors
- Camera
- etc.

External Data Sources
- Sensors
- Traffic Lights
- etc.

Risk Analysis

Data Valuation
- Threats
- Vulnerabilities

Modelling with EBIOS - SecureTROPOS - PriS

SPECIFY

Safety Requirements
Security Requirements
Privacy Requirements

DEDUCE

Attack Modelling
Threat Propagation
Modelling Procedure

Scenario 1

In Car Components
- Hardware
- Software
  - Middleware

Car-attached Data Sources
- Sensors
- Camera
- etc.

External Data Sources
- Sensors
- Traffic Lights
- etc.

Risk Analysis
- Data Valuation
- Threats
- Vulnerabilities

Specify

Safety Requirements
- Security Requirements
- Privacy Requirements

Derive

Attack Modelling

Threat Propagation

Derive

Security Measures

Protection Profiles

Modelling with EBIOS - SecureTROPOS - Pris
Modelling Procedure

Scenario 1

- In Car Components
  - Hardware
  - Software
- Car-attached Data Sources
  - Sensors
  - Camera
- External Data Sources
  - Sensors
  - Traffic Lights

Risk Analysis

- Data Valuation
- Threats
- Vulnerabilities

Modelling with EBIOS - SecureTROPOS - Pris

DERIVE

- Safety Requirements
- Security Requirements
- Privacy Requirements

DERIVE

- Assumptions
- Threats
- Attack Modelling
- Threat Propagation

DERIVE

- Security Measures
- Protection Profiles

Assurance Levels

Metrics & KPIs
T2.2 & T2.3 Methodology

Iterative process

Step 1: EBIOS assets identification

Step 2: Secure Tropos – PriS assets identification

Step 3: Objectives & constraint definition

Step 4: Threat, attack and vulnerabilities identification

Step 5: Security Objective & requirements definition

Step 6: Analysis & implementation techniques

D2.1: use case and main architecture
Expression des Besoins et Identification des Objectifs de Sécurité (Expression of Needs and Identification of Security Needs)

Five steps

- Circumstantial study
  - Target organization study
  - Target system study
  - Target scope definition

- Identification of security needs
  - complete the requirements sheets
  - requirements reports

- Threat study
  - Threats cause study,
  - vulnerabilities study
  - threats formalization

- Determination of security objectives
  - Matching between security
  - formalization of security goals
  - determination of security level

- Determination of security requirements
  - Functional requirements determination
  - assurance requirements determination
A Privacy Requirements Engineering Methodology
- adopts ideas from goal-based modelling
Models privacy requirements as privacy goals
Enables analysts to consider privacy issues from the early stages throughout the development process
1) Identify Privacy Requirements

Based on organizational goals, the stakeholders’ needs, the national and international legislation etc.

2) Analyze the impact on Privacy Processes

Locating the processes that realize privacy-oriented subgoals

3) Redesign of organisational processes

(Re)Design the aforementioned processes by applying respective privacy process patterns for satisfying privacy goals

4) Identify appropriate implementation techniques

Identify adequate implementation techniques for realising privacy related processes.
Secure Tropos

- A Secure Software Engineering Methodology that is strongly **Requirements Driven**
  - Adopts i*, modelling language suitable for an early phase of system modelling in order to understand the problem domain. **i* modelling language allows to model both as-is and to-be situations.**
  - It is an approach originally developed for modelling and reasoning about organizational environments and their information systems composed of heterogeneous actors with different, often competing, goals that depend on each other to undertake their tasks and achieve these goals.
  - offers actors, goals, and actor dependencies as primitive concepts for modelling during early requirements analysis
- Describes both the **organisational environment** of the system and the **system itself**
- Models security requirements as constraints
Secure Tropos process

1. Analyses the security needs of the stakeholders and the system, in terms of **security constraints** (e.g., keep info private)

2. Identifies **security objectives** that guarantee the satisfaction of the security constraints (e.g., ensure authorization)

3. Assigns **security mechanisms and resources** to the system to help towards the satisfaction of security objectives (e.g., role based access control)
EBIOS Alignment with Secure Tropos and PriS – Suggested Process (1/2)

SEQUENTIAL STAGES – STEPS

Stage 1: EBIOS
Output:
- 1.1 Identification of the respective Entities
- 1.2 Identification of the respective Essential Elements

Stage 2: Secure Tropos – PriS
Output:
- 2.1 Identify the list of Actors
- 2.2 Identify Existing Organisational Goals
- 2.3 Create the initial Organisational View Diagram

Stage 3: EBIOS – Secure Tropos – PriS
Output:
- 3.1 Identify the sensitivities (EBIOS)
- 3.2 Enhance the Security Constraints List (Secure Tropos)
- 3.3 Define the Privacy Constraint List (PriS)
EBIOS Alignment with Secure Tropos and PriS – Suggested Process (2/2)

Stage 4: EBIOS – Secure Tropos – PriS
Output:
- 4.1 Identify Threat Agents, Attack Methods and Vulnerabilities
- 4.2 Create the Threat related model Diagram
- 4.3 Create the Attack related model diagram

Stage 5: EBIOS – Secure Tropos – PriS
Output:
- 5.1 Define Security and Privacy Objectives (All three)
- 5.2 Define Security and Privacy Requirements (All three)
- 5.3 Define Security and Privacy Metrics (EBIOS-Secure Tropos)

Stage 6: Secure Tropos – PriS
Output:
- 6.1 Analyse Security and Privacy Requirements (Secure Tropos-PriS)
- 6.2 Identify possible Implementation Techniques (Secure Tropos-PriS)
Use Case – Optimal Speed Driving

V2X

Car

CAN / ETH

OBU

TT APP

CRF APP

TT Cloud/TTI

R–ITS–S

C–ITS–S

TMC

TLC

HMI (GLOSA)

HMI (GLOSA)

HMI (GLOSA)
Use Case Architecture

TLC → TMC → C-ITS-S → RSU → OBU

ESORICS / SECPRE – OSLO 2017

27/5/2018
Secure Tropos models – Organisational View
Secure Tropos models – Part of Requirements View
Secure Tropos models – Part of Attacks View
Thank you!
Any Questions?