Threat Move

Project Update September 2018

Agenda

foreseeti

THE THREAT MOVE PROJECT

- Overview & Summary
- Results to date

QUANTITATIVE THREAT MODELLING

- Concept
- securiCAD
- Demo

VEHICLELANG AND TOOLING

- MAL foundation
- Summary of capabilities
- Example and demo

FUTURE


The Project

Problem

foreseeti

Cyber security is costly

Ignoring cyber security in vehicles will also be very costly

- **Public trust and safety!**
- **Liabilities and risks for manufacturers**

Reactive cyber security common today. Putting out fires.

Proactive security and risk analysis is heavily dependent on manual approaches that are error prone, time consuming and subject to bias.

Solution

foreseeti

Threat modeling is an approach for proactive cyber security, however…

- **the tools available so far today are still dependent on human expertise (not efficient)**
- **automotive systems have features that are not supported in modeling tools today.**

We aim to develop a Threat Modeling approach that will automatically simulate attacks in vehicle systems, decreasing the risk of human error and increasing coverage and speed of analysis.

Goals

To develop a threat modelling and simulation language that:

- allows for real-world modeling and simulation of vehicle information system attacks
- is tested with real-world systems, and
- helps automotive IT security to be modeled and simulated in both design and operational phases, thus contributing to increased understanding of security challenges and risks
- is freely available to the automotive industry, academia and other interested parties

Tools and methodology support allowing:

- vehicle models to be created, simulated and analyzed through the foreseeti securiCAD product suite
- inclusion of quantitative threat modelling vehicle manufacturing toolchains, including document management and traceability of artifacts and decisions

Organization

MEMBERS

- foreseeti
- F-Secure
- KTH
- Scania
- Volvo Cars

PLANNED DURATION

- Oct 2017 – September 2021

WORK PACKAGES (ITERATIVE)

- WP1: Project Management
- WP2: Development of a framework for threat modelling DSLs
- WP3: Design of a domain specific modelling language for vehicle systems
- WP4: Implementation
- WP5: Iterative testing and validation of the domain-specific language
- WP6: Inclusion of Tool chain integration
- WP7: Vehicle security parameters
- WP8: Dissemination

Results

Continuously updated on https://autosec.se/threat-move-results/

foreseeti

Language framework - Meta Attack Language (MAL)

- Open (Apache 2.0) threat modelling language compiler on GitHub - https://github.com/pontusj101/MAL
- Paper "*A Meta Language for Threat Modeling and Attack Simulations*" presented in Proc. of the 13th International Conference on Availability, Reliability and Security (ARES), 2018.

Domain specific language - vehicleLang

- Master thesis: Sotirios Katsikeas, "*vehicleLang: a probabilistic modeling and simulation language for vehicular cyber attacks*", KTH Royal Institute of Technology, School of Electrical Engineering and Computer Science, Master Thesis, 2018.
- Open (Apache 2.0) language implementation on GitHub - https://github.com/pontusj101/vehicleLang
- Research tooling – Simulation and critical path rendering of vehicleLang models

Testing and validation

- Bachelor thesis: Fredrik Krantz, "*Modelling and Security Analysis of Internet Connected Cars*", KTH Royal Institute of Technology, School of Electrical Engineering and Computer Science, Bachelor Thesis, 2018.

Results (cont'd)

foreseeti

Vehicle specific security parameters

- Bachelor thesis: Simon Carlsson and Max Näf, "*Internet of Things Hacking*", KTH Royal Institute of Technology, School of Electrical Engineering and Computer Science, Bachelor Thesis, 2018.
- Bachelor thesis: Gustav Marstorp and Hannes Lindström, "*Security Testing of an OBD-II Connected IoT Device*", KTH Royal Institute of Technology, School of Electrical Engineering and Computer Science, Bachelor Thesis, 2018.

Outreach

- Video: Cybersecurity and ethical hacking of connected vehicles

Attack simulations and securiCAD

Challenge

WHAT IS YOUR TRUE RISK EXPOSURE?

CURRENT TECH

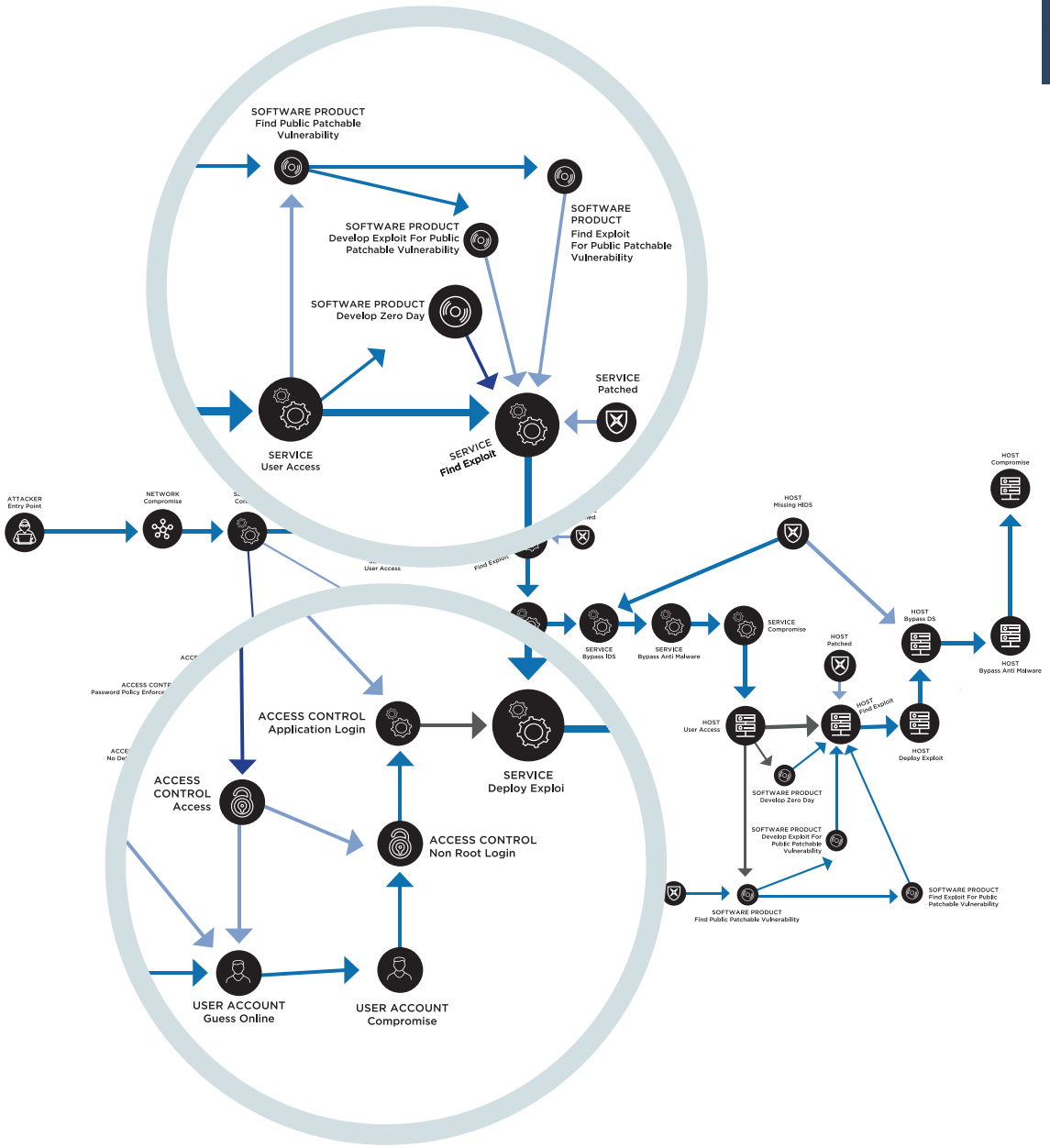
- FOCUS ON ISOLATED VULNERABILITIES
- FOCUS ON MICRO LEVEL
- GIVES A SNAPSHOT OF CURRENT STATUS

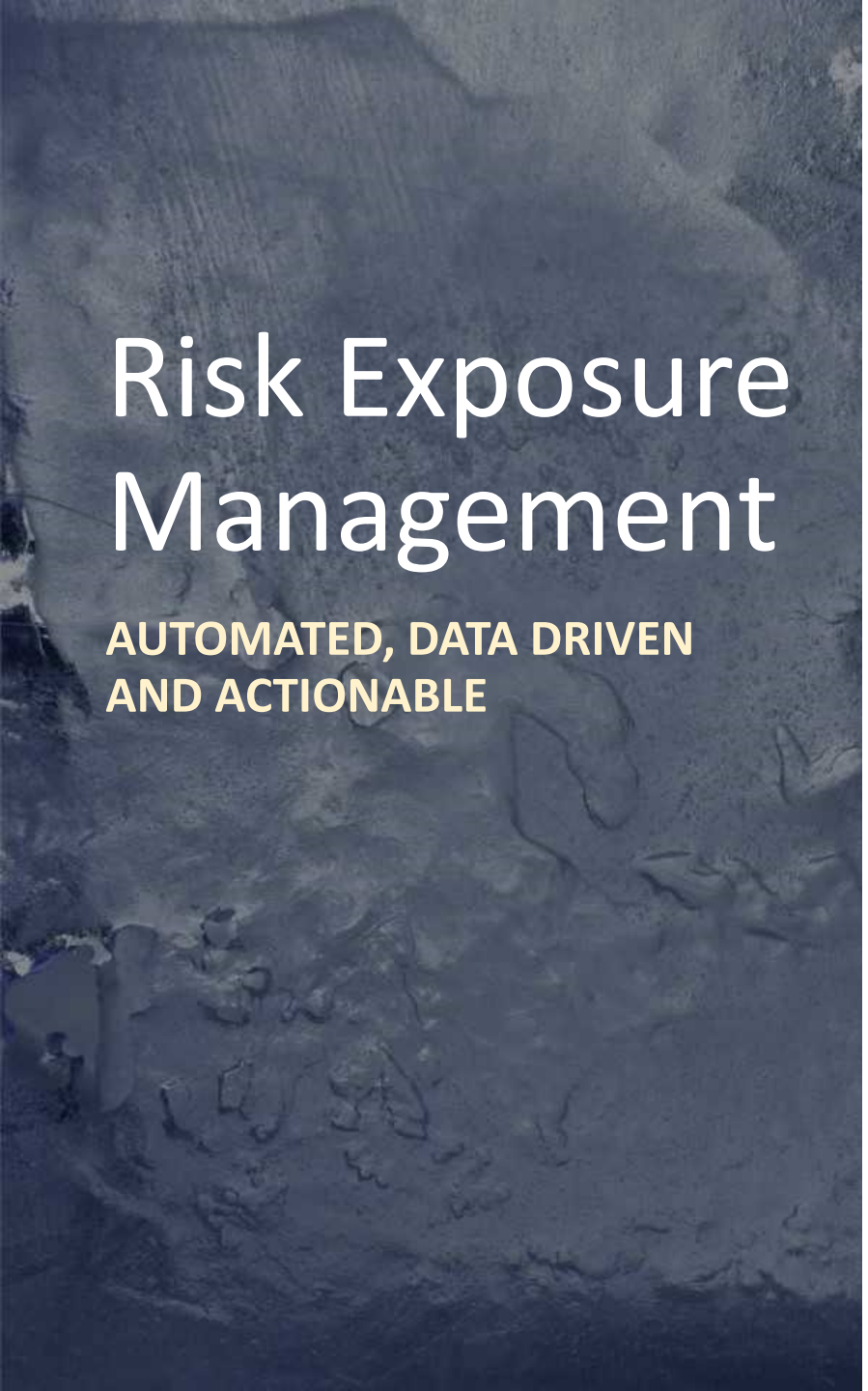
CURRENT CHALLENGE

- GROWING COMPLEXITY AND CONNECTIVITY
- NO ABILITY TO TEST POTENTIAL RISK LEVEL
- LACKING HOLISTIC RISK MEASUREMENT

Identify Weaknesses

STRUCTURAL VULNERABILITIES, CRITICAL PATHS TO HIGH VALUE ASSETS





Risk Exposure Management

AUTOMATED, DATA DRIVEN AND ACTIONABLE

foreseeti

NEW CAPABILITIES

- Holistic – at a structural level
- Quantitative and data driven
- Automated

PROACTIVE CONTROL

- Predict
- Design
- Track

BETTER EFFECT PER EURO

- Focus and prioritization
- Productivity
- Communication

foreseeti

securiCAD Concept

METHODOLOGY OVERVIEW

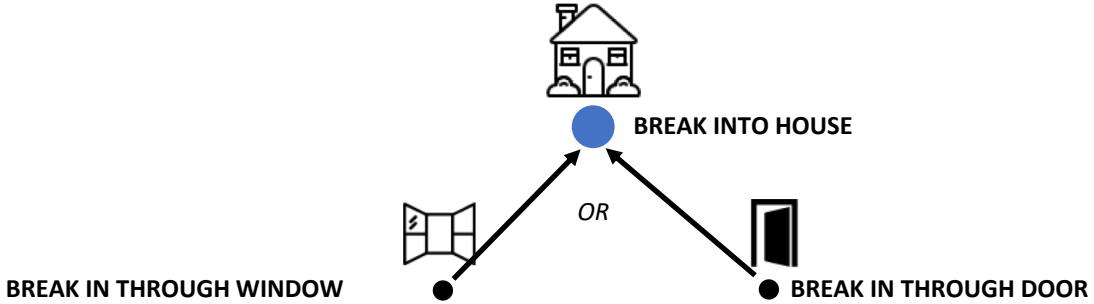
GENERATE A MODEL

SIMULATE ATTACKS

MANAGE RISK EXPOSURE

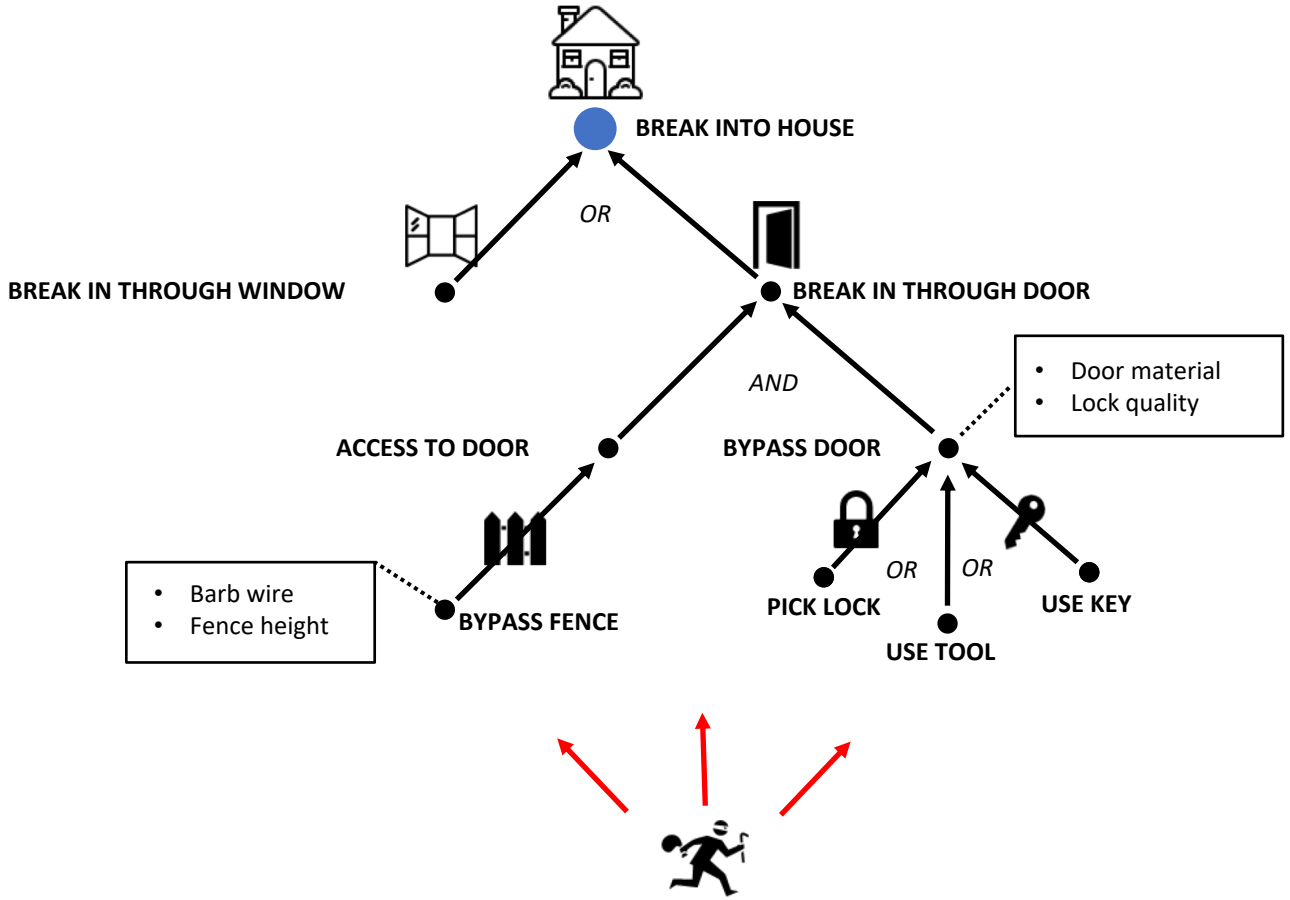
Simulate attacks with the securiCAD probabilistic simulation engine

ATTACK GRAPHS



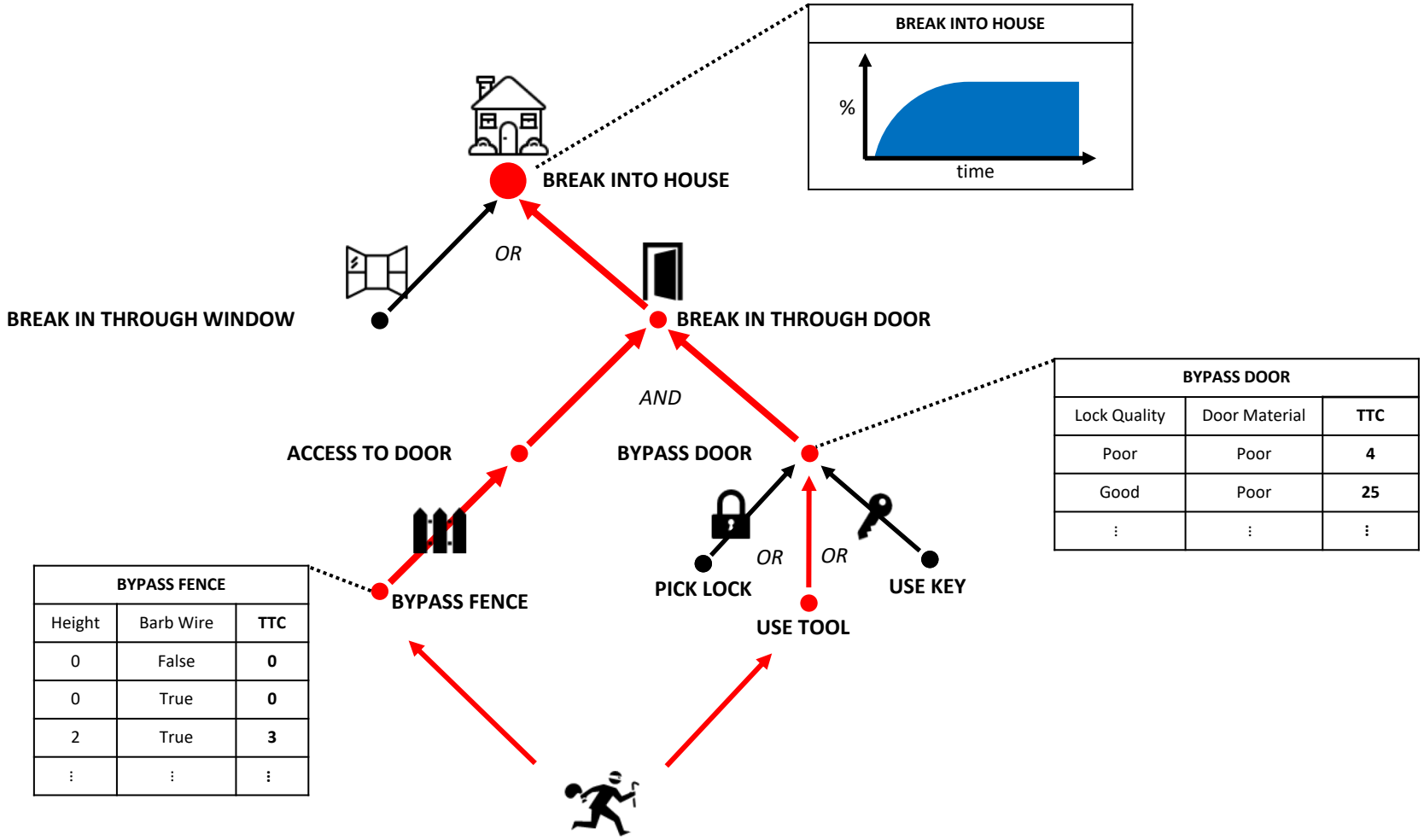
Simulate attacks with the securiCAD probabilistic simulation engine

ATTACK GRAPHS



Simulate attacks with the securiCAD probabilistic simulation engine

ATTACK GRAPHS

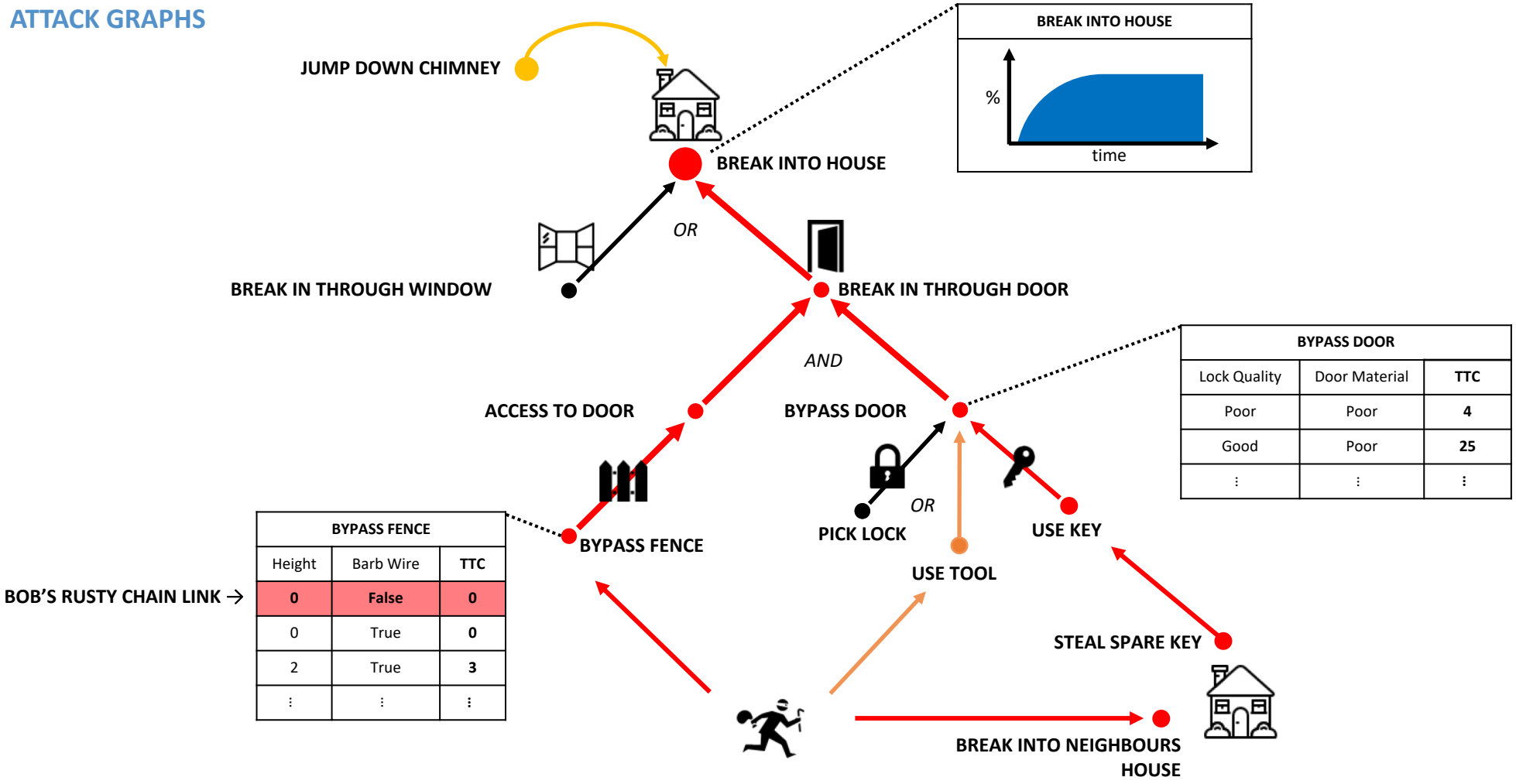


BYPASS DOOR		
Lock Quality	Door Material	TTC
Poor	Poor	**4**
Good	Poor	**25**
⋮	⋮	⋮

BYPASS FENCE		
Height	Barb Wire	TTC
0	False	**0**
0	True	**0**
2	True	**3**
⋮	⋮	⋮

Simulate attacks with the securiCAD probabilistic simulation engine

ATTACK GRAPHS



Simulate attacks with the securiCAD probabilistic simulation engine

ATTACK GRAPHS

Objects

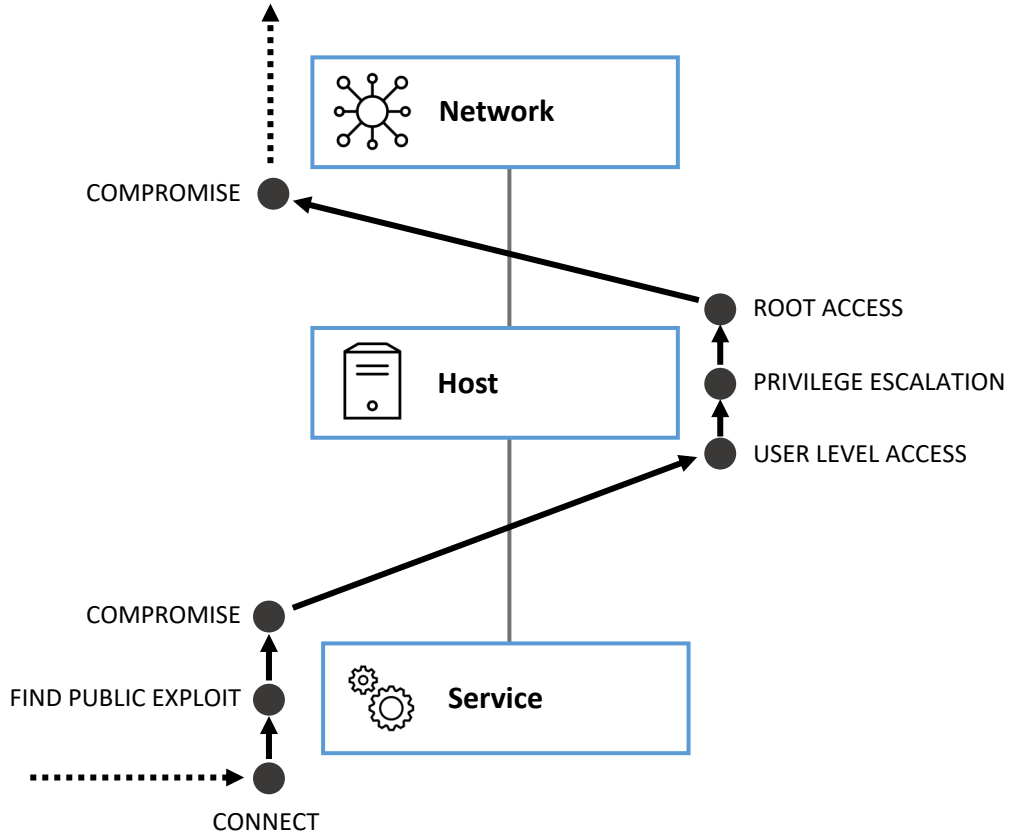
- Client
- Service
- Host
- Network
- User
- …

Attacks

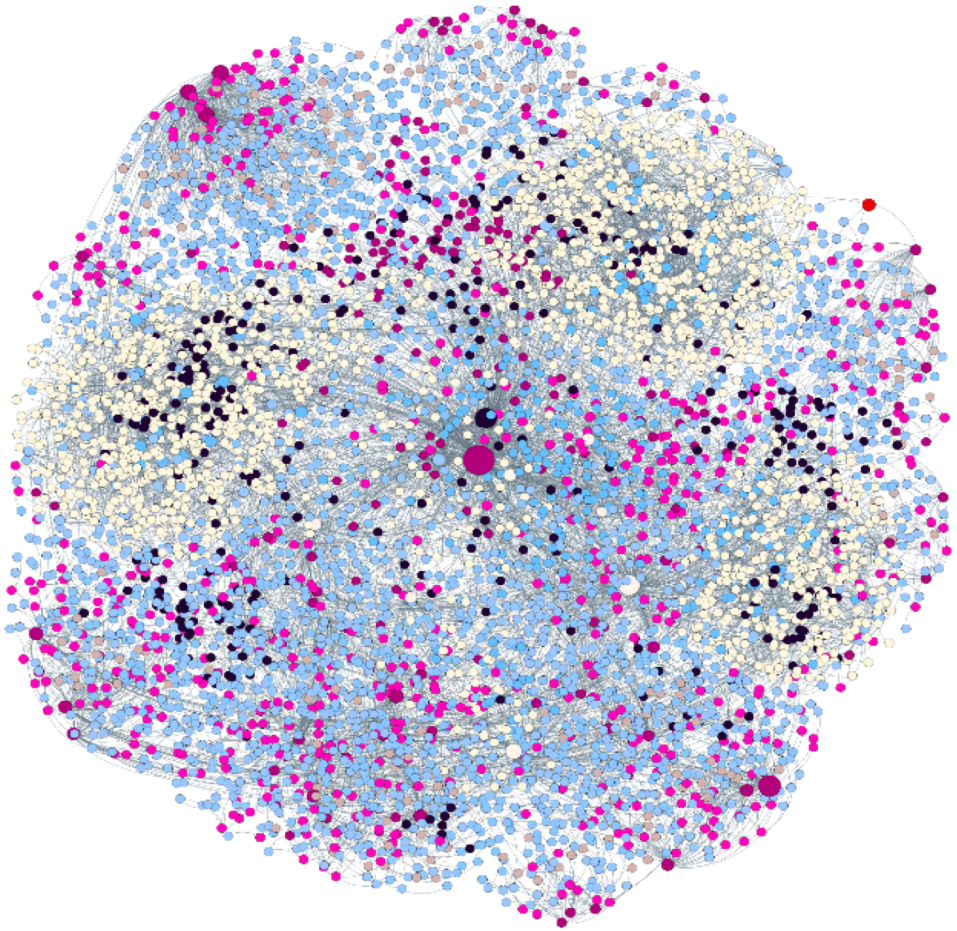
- DoS
- MiTM
- SQL injection
- Zero Day
- UserAccess
- **…**

Defences

- Patch level
- Encryption
- Hardening
- Security Awareness
- Architectural changes
- …



Real system



foreseeti

Demo

Jeep model from F. Krantz Bachelor's Thesis

securiCAD Community Edition:
http://www.foreseeti.com/community/

MAL & vehicleLang

Overview

Based on the Meta Attack Language framework:
https://github.com/pontusj101/MAL

Located in GitHub: https://github.com/pontusj101/vehicleLang

Models 43 attacks

- 7 attacks on ECUs
- 18 attacks on Vehicular Networks
- 3 attacks on Gateway ECUs
- 2 attacks on Infotainment system
- More attacks on dataflows, services, etc.

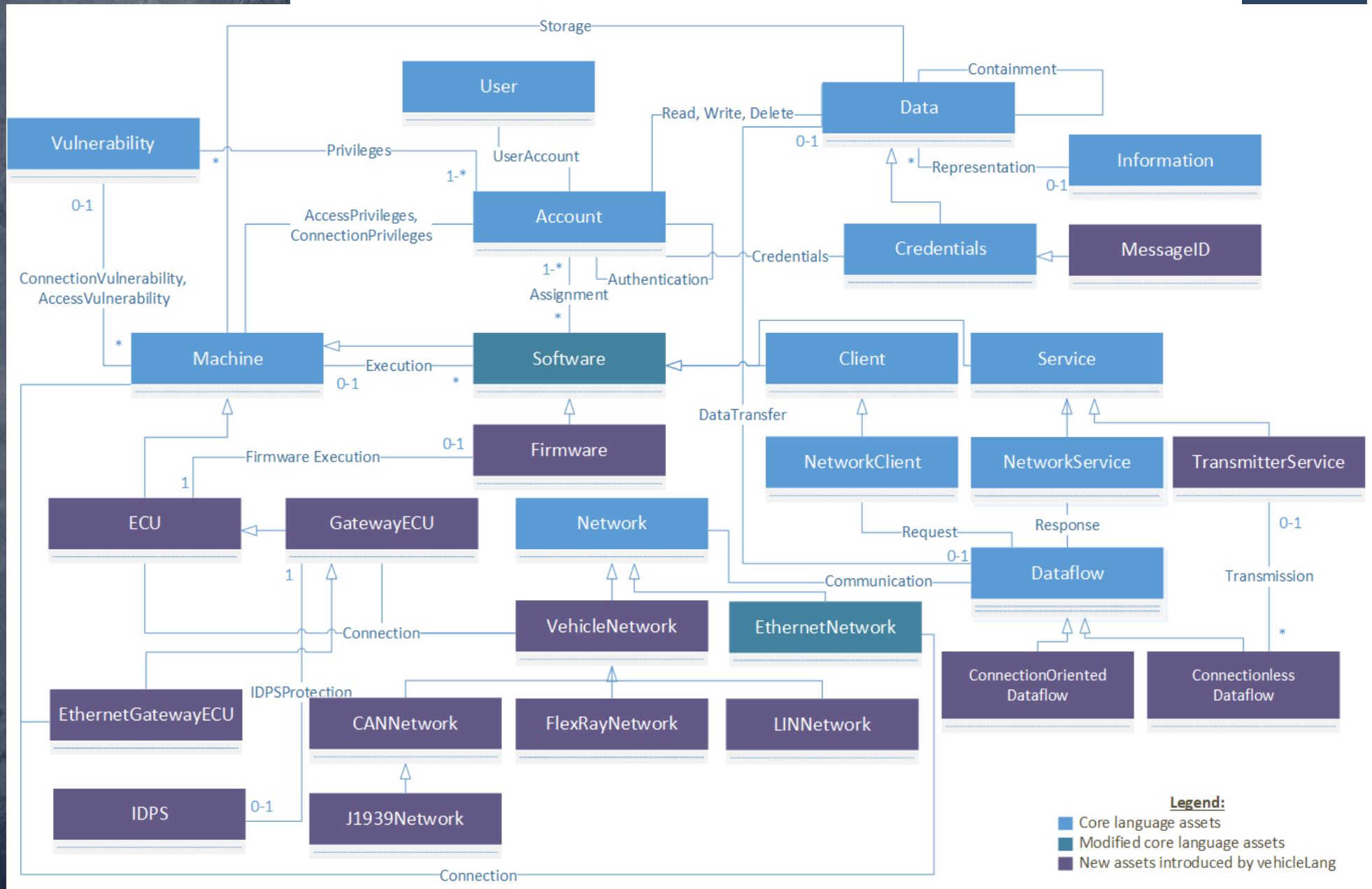
Modeled in 41 assets and more than 90 attack steps

More than 50 test cases were created

vehicleLang is comprised of 4 smaller files, in total more than 1000 lines of code

Focus on on-board networks and systems – e.g. MOST, Telematics, V2X currently out of scope

Assets


Storage
User
Containment
Vulnerability
Privileges
UserAccount
Read, Write, Delete
Data
0-1
Representation
Information
0-1
AccessPrivileges,
ConnectionPrivileges
Account
Credentials
Credentials
MessageID
1-*
Assignment
Authentication
ConnectionVulnerability,
AccessVulnerability
Machine
Execution
Software
Client
Service
DataTransfer
0-1
Firmware
NetworkClient
NetworkService
TransmitterService
Firmware Execution
1
ECU
GatewayECU
Network
Request
Response
0-1
Dataflow
0-1
Transmission
Communication
1
Connection
VehicleNetwork
EthernetNetwork
IDPSProtection
EthernetGatewayECU
CANNetwork
FlexRayNetwork
LINNetwork
ConnectionOriented
Dataflow
Connectionless
Dataflow
IDPS
0-1
J1939Network
Connection
Legend:
Core language assets
Modified core language assets
New assets introduced by vehicleLang

Example snippet

foreseeti

```
asset ECU extends Machine
          info: "Specifies any ECU/MCU/controller in a vehicle."
          {
                    | connect
                              -> _ecuConnect

                    | _ecuConnect
                              ->  _machineConnect,
                              attemptChangeOperationMode,
                              firmware.maliciousFirmwareModification

                    | access
                              -> _ecuAccess

                    | _ecuAccess
                              ->  _machineAccess,
                              physicalMachines.access,
                              changeOperationMode,
                              gainLINAccessFromCAN,
                              uploadFirmware,
                              bypassMessageConfliction

                    & attemptChangeOperationMode [ExponentialDistribution(10.0)]
                              ->  bypassMessageConfliction

                    # operationModeProtection
                              ->  changeOperationMode,
                                  attemptChangeOperationMode
                                        …
```

Research tooling

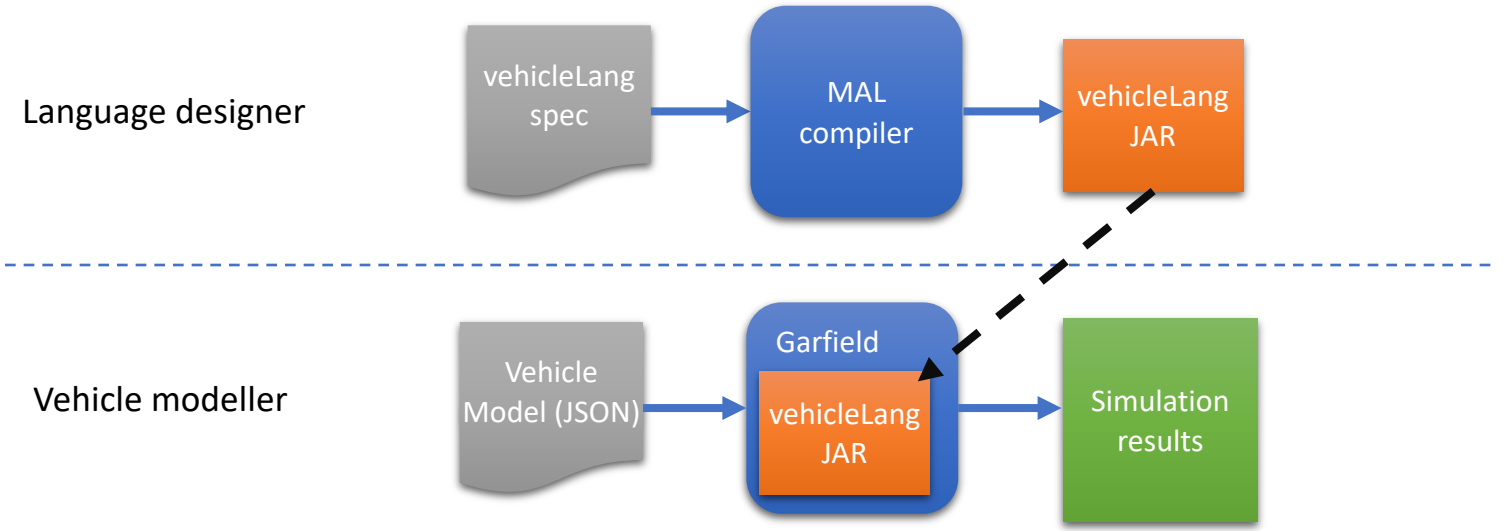
”Garfield”

Command line based simulator for vehicleLang (or any other MAL based threat modelling language)

Defines a JSON based model format

Full foreseeti simulation support, including GPU calculations

Support for web based Critical Path rendering and analysis



Going forward

Near term

2H2018

Two master thesis projects focusing in WP3 & WP5 – Test, validation and refinement of vehicleLang (2H2018)

- Modelling and expert validation of Scania systems
- Modelling and expert validation of Volvo Cars systems

One master thesis in context of WP7 (2H2018)

- Scania vehicle anomaly detection

Initiating work of WP6 – Toolchain integration

- Scania and foreseeti to explore requirements and needs to include threat modelling activities at design time and as traceable artifacts in production and change management workflows

Mid term

1H2019

foreseeti

Master thesis works Volvo Cars / Chalmers

- Likely in context of WP3 and WP5 but yet to be decided

Support for vehicleLang / MAL derivatives in securiCAD

- Remove the need for bespoke research tooling
- Full support for MAL langauges in all foreseeti products (securiCAD Professional and Enterprise Platform)