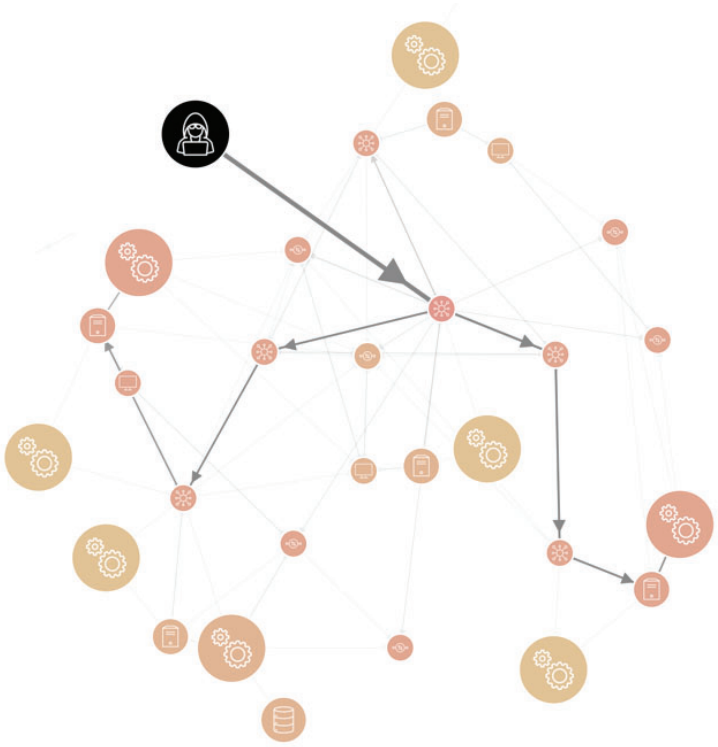
Threat modeling and simulation of vehicle IT

Public report



Project within Vinnova, FFI

Author Robert Lagerström, KTH, and project management team

Date 2022-10-25

Content

FFI in short

FFI is a partnership between the Swedish government and automotive industry for joint funding of research, innovation and development concentrating on Climate & Environment and Safety. FFI has R&D activities worth approx. €100 million per year, of which about €40 is governmental funding.

For more information: www.vinnova.se/ffi

1. Summary

The project "Threat Modeling and simulation of vehicle IT", for short called Threat MOVE, took place between 2017 and 2022 with the purpose to develop a method with tool support that can model and simulate the cyber security of internal IT environments in vehicles. The project was led by the Royal Institute of Technology (KTH) and was a collaboration between Foreseeti, WithSecure, Scania and Volvo Cars. It was very successful in bringing the entire value chain from research, via innovative companies, to end users. KTH and Foreseeti have previously developed a framework called the Meta Attack Language (MAL) which formed the basis for the work in this project. With the help of MAL, KTH and Foreseeti have developed a domain-specific threat modeling and attack simulation language for vehicle IT, also called vehicleLang. The language has been tested through both academic and practical activities. VehicleLang, the testing and validation of the language, are the main deliverables in the project. In addition to this, another focus has been on practical tests, so-called penetration tests, of vehicle equipment. That is, examine how resilient various components are against cyber attacks. These tests have both provided insights directly applicable to its developers and input to the modeling language and its simulations. Another important activity has been to communicate about IT security for vehicles in general and the project's results specifically.

2. Sammanfattning på svenska

Projektet “Threat Modeling and simulation of vehicle IT” kort kallat Threat MOVE som pågått mellan 2017 och 2022 handlade om att ta fram en metod med verktygsstöd som kan modellera och simulera de interna IT-miljöerna i fordon. Projektet leddes av Kungliga Tekniska Högskolan (KTH) och var ett samarbete mellan Foreseeti, WithSecure, Scania och Volvo Cars. Det var mycket lyckat att få med hela kedjan från forskning, via innovativa bolag, till slutanvändare. KTH och Foreseeti har tidigare tagit fram ett ramverk som heter the Meta Attack Language (MAL) som utgjorde grunden för arbetet i detta projekt. Med hjälp av MAL har KTH och Foreseeti inom ramen för Threat MOVE utvecklat ett domänspecifikt hotmodellerings- och attacksimuleringsspråk för fordons-IT, även kallat vehicleLang. Språket har testats både genom akademiska och praktiska aktiviteter. VehicleLang samt testning och validering av språket är huvudleverabeln i projektet. Utöver detta har ett annat fokus legat på praktiska tester, så kallade penetrationstester, av fordonsutrustning. Det vill säga undersöka hur motståndskraftiga olika komponenter är mot IT-attacker. Dessa tester har både gett insikter direkt applicerbara för dess utvecklare samt som indata till modelleringsspråket och dess simuleringar. En annan viktig aktivitet har varit att kommunicera kring IT-säkerhet för fordon generellt och projektets resultat specifikt.

3. Background

The increasing level of computerization makes modern vehicles vulnerable to cyber attacks. Software-based tools for threat modelling and simulation can be used to assess the probability that an attacker manages to reach different parts of the vehicle system. However, today there are no such tools for the transport domain. The goal was to develop a threat modelling and simulation language that allows for real-world modelling and simulation of vehicle information system attacks, as well as implementing and testing the language with real-world systems. This will help automotive IT security to be modelled and simulated in both design and operational phases, thus contributing to increased understanding of security challenges and risks. The proposed approach could well be a future best practice for the Swedish automotive industry.

4. Purpose and method

The main purpose is to develop a threat modelling and simulation language for vehicle IT. To achieve this the project has executed traditional engineering methodologies and design science research. In short; iteratively - based on previous research, on-going research, and expert knowledge develop an artefact, in our case the threat modelling and attack simulation language (vehicleLang), test and validate this language, communicate the results.

5. Objectives

The work had the following objectives;

- design the domain-specific modelling and analysis language for security in automotive IT,
- implement tool support,
- iteratively test and validate the domain-specific language,
- align with tool chain integration,
- collect vehicle security parameters, and
- disseminate the results.

6. Results and deliverables

Domain-specific language
Paper: Sotirios Katsikeas, Pontus Johnsson, Simon Hacks, Robert Lagerström, “VehicleLang: A probabilistic modeling and simulation language for modern vehicle IT infrastructures", in Computers & Security, Volume 117, 2022

Paper: Sotirios Katsikeas, Pontus Johnson, Simon Hacks, and Robert Lagerström, “Probabilistic Modeling and Simulation of Vehicular Cyber Attacks: An Application of the Meta Attack Language", in the Proc. of the 5th International Conference on Information Systems Security and Privacy (ICISSP), Feb. 2019.

Paper: Wenjun Xiong and Robert Lagerström, “Threat Modeling: A Systematic Literature Review", Computers & Security, 2019.

Paper: Wenjun Xiong and Robert Lagerström, “Threat Modeling of Connected Vehicles: A privacy analysis and extension of vehicleLang", in the Proc. of the IEEE Cyber Science conference, June 2019.

Master thesis: Sotirios Katsikeas, “vehicleLang: a probabilistic modelling and simulation language for vehicular cyber attacks”, KTH Royal Institute of Technology, School of Electrical Engineering and Computer Science, 2018.

Master thesis: Asmelash Girmay Mesele, AUTOSARLang: “Threat Modeling and Attack Simulation for Vehicle Cybersecurity”, KTH Royal Institute of Technology, School of Electrical Engineering and Computer Science, 2018.

Bachelor thesis: Nagy & K. Thai, “Investigating Traditional Software Testing Methods For Use With The Meta Attack Language”, KTH Royal Institute of Technology, School of Electrical Engineering and Computer Science, 2020.

Bachelor thesis: Love Almgren & Johan Holm Åström, ”Probabilistic modelling and attack simulations on AWS Connected Vehicle Solution: An Application of the Meta Attack Language”, KTH Royal Institute of Technology, 2019.

Language implementation: vechicleLang on GitHub

Language implementation: autosarLang on Github

Implementation
securiCAD (supporting MAL-based languages incl. vehicleLang)

Testing and validation
Paper: Wenjun Xiong, Fredrik Krantz, and Robert Lagerström, “Threat modelling and attack simulations of connected vehicles: a research outlook", in the Proc. of the 5th International Conference on Information Systems Security and Privacy (ICISSP), Feb. 2019.

Master thesis: Nedo Skobalj, “Validating vehicleLang for Domain-specific Threat Modelling of In-vehicle Network", KTH Royal Institute of Technology, School of Electrical Engineering and Computer Science, 2019.

Master thesis: Willem van der Schoot, “Validating vehicleLang, a domain-specific threat modelling language, from an attacker and industry perspective", KTH Royal Institute of Technology, School of Electrical Engineering and Computer Science, 2020.

Bachelor thesis: Fredrik Krantz (supervisor: Associate prof. Robert Lagerström), “Modelling and Security Analysis of Internet Connected Cars", KTH Royal Institute of Technology, School of Electrical Engineering and Computer Science, 2018.

Tool chain integration
Paper: Margus Välja, Fredrik Heiding, Robert Lagerström, and Ulrik Franke, “Automating threat modeling using an ontology framework", in Cybersecurity, Springer Open journal, 2020.

Technical report: Nikolaos Kakouros and Robert Lagerström, “ISO/SAE 21434 support in MAL/securiCAD", KTH Royal Institute of Technology, 2020.

Vehicle specific security parameters
Paper: Wenjun Xiong, Melek Gülsever, Koray Mustafa Kaya, and Robert Lagerström, “A Study of Security Vulnerabilities and Software Weaknesses in Vehicles", in the proceedings of the 24th Nordic Conference on Secure IT Systems (NordSec), 2019.

Paper: Joakim Loxdal, Måns Andersson, Simon Hacks, and Robert Lagerström, “Why Phishing Works on Smartphones: A Preliminary Study", IEEE Hawaii International Conference on System Sciences (HICSS-54), 2020.

Paper: Fredrik Heiding and Robert Lagerström, “Ethical Principles for conducting responsible offensive security training", IFIP Summer School on Privacy and Identity Management, 2020.

Master thesis: Madeleine Berner, “Where’s My Car? Ethical Hacking of a Smart Garage", KTH Royal Institute of Technology, School of Electrical Engineering and Computer Science, 2020.

Bachelor thesis: Simon Carlsson and Max Näf (supervisor: Prof. Pontus Johnson), “Internet of Things Hacking", KTH Royal Institute of Technology, School of Electrical Engineering and Computer Science, 2018.

Bachelor thesis: Gustav Marstorp and Hannes Lindström (supervisor: Prof. Pontus Johnson), “Security Testing of an OBD-II Connected IoT Device", KTH Royal Institute of Technology, School of Electrical Engineering and Computer Science, 2018.

Bachelor thesis: Ludvig Christensen and Daniel Dannberg, ”Ethical hacking of IoT devices: OBD-II dongles", KTH Royal Institute of Technology, 2019.

Bachelor thesis: Aldin Burdzovic and Jonathan Matsson, ” IoT Penetration Testing: Security analysis of a car dongle", KTH Royal Institute of Technology, 2019.

Bachelor thesis: Koray Kaya, ”A Study of Vulnerabilities and Weaknesses in Connected Cars", KTH Royal Institute of Technology, 2019.

Bachelor thesis: Melek Gülsever, ”A Study on Vulnerabilities in Connected Cars", KTH Royal Institute of Technology, 2019.

Bachelor thesis: S. Berglund & O. Eklund, “Spreading a computer worm over connected cars", KTH Royal Institute of Technology, School of Electrical Engineering and Computer Science, 2020.

Bachelor thesis: J. Loxdal & M. Andersson, “Why Phishing Works on Smartphones", KTH Royal Institute of Technology, School of Electrical Engineering and Computer Science, 2020.

Master thesis: P. Andersson, “Penetration Testing of an In-Vehicle Infotainment System”, KTH Royal Institute of Technology, School of Electrical Engineering and Computer Science, 2022.

Bachelor thesis: D. Ismail & P. Aslan, “Attack Simulations and Threat Modeling of Volvo Cars’ Vehicle Infotainment System”, KTH Royal Institute of Technology, School of Electrical Engineering and Computer Science, 2022.

Master thesis: H. Zahid, “MACsec in Classic AUTOSAR”, KTH Royal Institute of Technology, School of Electrical Engineering and Computer Science, 2022.

Technical Report: WithSecure, “In-Vehicle Infotainment unit Security Assessment”, WithSecure, 2022.

Outreach

Vulnerabilities (CVEs):

Ludvig Christensen, Daniel Dannberg, Pontus Johnson, and Robert Lagerström, CVE-2019-12797, Vulnerability in a clone version of an ELM327 OBD2 Bluetooth device, hardcoded PIN leading to arbitrary commands to an OBD-II bus of a vehicle.

Aldin Burdzovic and Jonathan Matsson, CVE-2019-12941, AutoPi Wi-Fi/NB and 4G/LTE devices before 2019-10-15 allows an attacker to perform a brute-force attack or dictionary attack to gain access to the WiFi network, which provides root access to the device.

CVE-2020-13119 – ismartgate PRO 1.5.9 is vulnerable to clickjacking. Student: Madeleine Berner, Supervisor: Pontus Johnson, Examiner: Robert Lagerström.

CVE-2020-12843 – ismartgate PRO 1.5.9 is vulnerable to malicious file uploads via the form for uploading sounds to garage doors. The magic bytes for WAV must be used. Student: Madeleine Berner, Supervisor: Pontus Johnson, Examiner: Robert Lagerström.

CVE-2020-12842 – ismartgate PRO 1.5.9 is vulnerable to privilege escalation by appending PHP code to /cron/checkUserExpirationDate.php. Student: Madeleine Berner, Supervisor: Pontus Johnson, Examiner: Robert Lagerström.

CVE-2020-12841 – ismartgate PRO 1.5.9 is vulnerable to CSRF that allows remote attackers to upload imae files via /index.php Student: Madeleine Berner, Supervisor: Pontus Johnson, Examiner: Robert Lagerström.

CVE-2020-12840 – ismartgate PRO 1.5.9 is vulnerable to CSRF that allows remote attackers to upload sound files via /index.php Student: Madeleine Berner, Supervisor: Pontus Johnson, Examiner: Robert Lagerström.

CVE-2020-12839 – ismartgate PRO 1.5.9 is vulnerable to privilege escalation by appending PHP code to /cron/checkExpirationDate.php. Student: Madeleine Berner, Supervisor: Pontus Johnson, Examiner: Robert Lagerström.

CVE-2020-12838 – ismartgate PRO 1.5.9 is vulnerable to privilege escalation by appending PHP code to /cron/mailAdmin.php. Student: Madeleine Berner, Supervisor: Pontus Johnson, Examiner: Robert Lagerström.

CVE-2020-12837 – ismartgate PRO 1.5.9 is vulnerable to malicious file uploads via the form for uploading images to garage doors. The magic bytes of PNG must be used. Student: Madeleine Berner, Supervisor: Pontus Johnson, Examiner: Robert Lagerström.

CVE-2020-12282 – iSmartgate PRO 1.5.9 is vulnerable to CSRF via the busca parameter in the form used for searching for users, accessible via /index.php. (This can be combined

with reflected XSS.) Student: Madeleine Berner, Supervisor: Pontus Johnson, Examiner: Robert Lagerström.

CVE-2020-12281 – iSmartgate PRO 1.5.9 is vulnerable to CSRF that allows remote attackers to create a new user via /index.php. Student: Madeleine Berner, Supervisor: Pontus Johnson, Examiner: Robert Lagerström.

CVE-2020-12280 – iSmartgate PRO 1.5.9 is vulnerable to CSRF that allows remote attackers to open/close a specified garage door/gate via /isg/opendoor.php. Student: Madeleine Berner, Supervisor: Pontus Johnson, Examiner: Robert Lagerström.

News:
Svt https://www.svt.se/nyheter/vetenskap/din-garageport-blir-kriminell

Svt https://www.svt.se/nyheter/varningen-uppkopplade-bilar-kan-hackas-och-tas-over

KTH News www.kth.se/aktuellt/nyheter/kth-utbildar-skolelever-i-it-sakerhet-1.1010356

Expressen https://www.expressen.se/dinapengar/sa-stor-ar-risken-att-din-bil-hackas/

Dagens Industri TV Motor
https://www.di.se/ditv/motor/di-tv-motor-21-november—se-hela-programmet/

DagensNyheter
https://www.dn.se/ekonomi/motor/uppkopplingen-gor-bilen-smartare-men-hackare-kan-ta-kontroll-over-ratten/

DagensNyheter
https://www.dn.se/ekonomi/motor/uppkoppling-for-aldre-bil-oppen-for-hackning/

Metro
https://www.metro.se/nyheter/forskaren:-dina-hushallsprylar-kan-hackas-och-anvandas-emot-dig-DffDLf8e2

KTH News
https://www.kth.se/aktuellt/nyheter/nar-robotdammsugaren-spionerar-pa-dig-1.898460

SR Studio 1 https://sverigesradio.se/sida/artikel.aspx?programid=1637&artikel=7293986

NyTeknik om Threat MOVE
https://www.nyteknik.se/digitalisering/foreseetis-kod-ska-skydda-uppkopplade-bilar-fran-hackare-6892180

Meetings and conferences:
Robert Lagerström presented threat modeling and ethical hacking at Stora Elektronikdagen (www.smartareelektroniksystem.se/event/summit-2020/) 2020-09-10.

PhD student Sotirios Katsikeas presented a threat modeling language at GraMSec (https://www.gramsec.uni.lu) 2020-06-22.

PhD student Fredrik Heiding presented Ethical principles for hacking education at the IFIP summer school (https://www.ifip-summerschool.org) 2020-09-21

Foreseeti and/or KTH have been presenting vehicleLang and securiCADCar for several non ThreatMOVE participants during the spring 2020, incl. Daimler, AB Volvo, and Copperhorse.

PhD student Wenjun Xiong presented a paper at the 24th Nordic Conference on Secure IT Systems in Aalborg Denmark, 2019-11-19.

Autosec FFI conference in Stockholm at RISE, Threat MOVE presented by Robert Lagerström (KTH), Niklas Wiberg (Scania, and Per Eliasson (foreseeti), 2019-10-10.

PhD student Wenjun Xiong presented a paper at the IEEE Cyber Science conference in Oxford UK, 2019-06-03.

Car security seminar at KTH, arranged by Dex, Robert Lagerström (KTH) and Per Eliasson (foreseeti) presented Threat MOVE, 2019-05-20.

KTH PhD students Sotirios Katsikeas and Wenjun Xiong presented Threat MOVE work at the 5th International Conference on Information Systems Security and Privacy (ICISSP) in February 2019.

Robert Lagerström presented at the Hawaii International Conference on System Sciences (HICSS) January 2019.

Niclas Wiberg participated in the podcast “Uppkopplad” and the episode on “Kina på väg”, 2018. https://sverigesradio.se/avsnitt/1114577

Threat MOVE presented by Per Eliasson (Foreseeti) at the Autosec meeting in Gothenburg https://autosec.se/ffi-autosec-conference-2018/

Educational seminar on threat modeling at the eCrime congress in Frankfurt, 2018-01-24.

Per Eliason (foreseeti), Nikolaos Kakouros (KTH) and Niklas Wiberg (Scania) presented the Threat MOVE project at the annual AutoSec (DEx) conference.

The paper ”Why Phishing Works on Smartphones: A Preliminary Study” was presented at the 54th Hawaii International Conference on System Sciences (HICSS) 2021. (https://hicss.hawaii.edu)

The short paper “Detecting plagiarism in penetration testing education” was presented as a poster at Nordsec 2020. (https://nordsec2020.on.liu.se)

Podcasts:
Robert Lagerström, KTH, participated in a Podcast about communication – robots, cancer cells and cyber security, 2018-03-16.

Robert Lagerström, KTH, participated in a Podcast about IT security with RadioScience, 2018-04-20.

Video: Cybersecurity and ethical hacking of connected vehicles

Popular Science:
Young Academy of Sweden, Ett kalejdoskop av kunskap, Santérus Förlag, 2019.
– Robert Lagerström, “En stundande cyberepidemi?”

Young Academy of Sweden, Forskardrömmar – Berättelser för nyfikna barn, Fri Tanke, 2021. (https://fritanke.se/bocker/forskardrommar/)
Robert Lagerström, initiator and author.

7. Dissemination

How are the project results planned to be used and disseminated?	Mark with X	Comment
Increase knowledge in the field	X	This is the main dissemination part. A lot of the work is aimed to increase knowledge in the field in general. For instance, the found CVEs, the modelling language, the example models, et cetera.
Be passed on to other advanced technological development projects	X	vehicleLang can be further enhanced and tested. Specifically, tighter integration with other tools.
Be passed on to product development projects	X	Unclear at the moment. But there is definitely interest and opportunity to keep building on top of vehicleLang.
Introduced on the market		
Used in investigations / regulatory / licensing / political decisions		

8. Conclusions and future research

The Threat MOVE project is considered by the project participants to be a successful project. Although, the Covid pandemic put some delimitations to in-person meetings and trips for workshops and conferences. There have been many interesting bachelor and master thesis projects in collaboration between the project partners, the development and testing of the main deliverable has been executed in collaboration as well. The project participants have been active in media appearances discussing cyber security in general, threat modelling, attack simulations, penetration testing, and vehicle security more specifically.

The main deliverable, vehicleLang, is still in a prototype state. The main future activities to further improve it should be around more testing and validation, and more research into the tool chain integration.

9. Participating parties and contact persons

Robert Lagerström	Royal Institute of Technology (KTH)
Roy D'souza	Foreseeti AB
Emil Manninen	WithSecure
Niklas Wiberg	Scania
Henrik Broberg	Volvo Cars