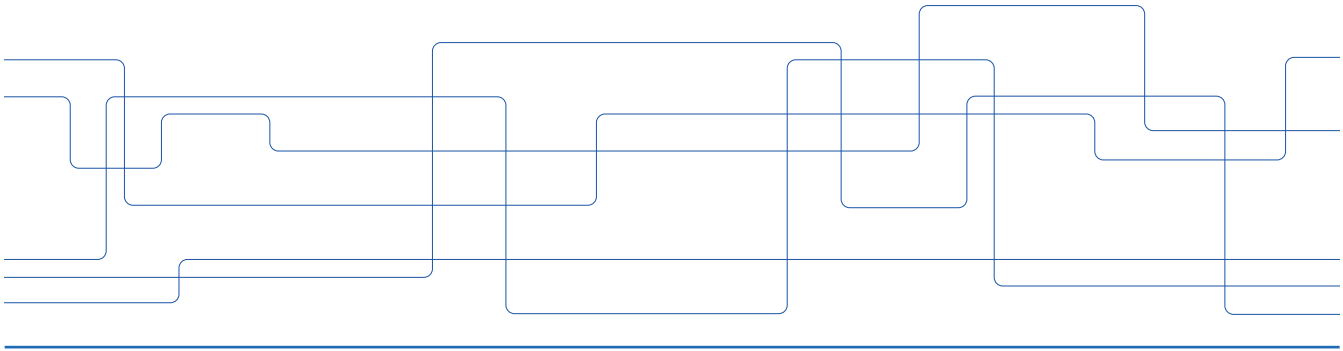
Threat Move in Focus

Results and impact

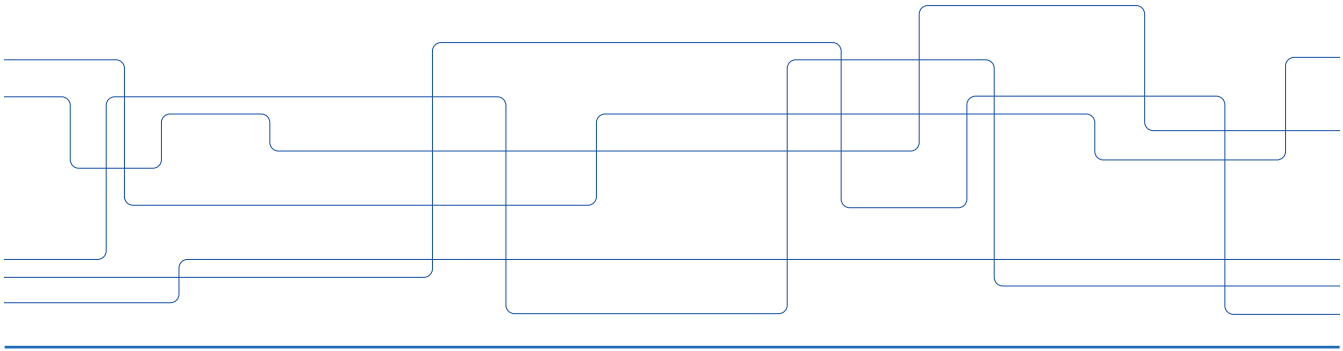
Robert Lagerström, KTH Royal Institute of Technology



KTH ROYAL INSTITUTE
OF TECHNOLOGY

Threat Modeling & Attack Simulations of Vehicle IT (THREAT MOVE)

KTH, Foreseeti, F-Secure, Scania, & Volvo Cars



Vehicle IT is a complex thing…

Hardware

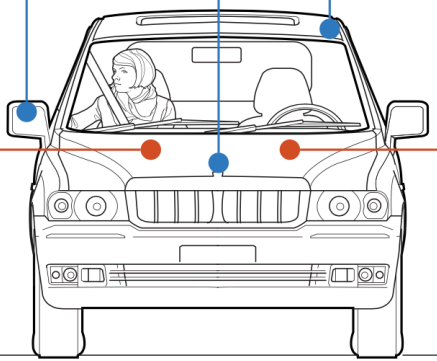
Corner modules, advanced sensors, etc

Drivetrain

Electric motors, power electronics, advanced batteries

Industrial design

Modular bodies, advanced user interfaces



Entertainment platform

Features and connectivity mirroring the home-entertainment experience

Autonomous drive/ operating system

Advanced central operating system with self-driving capability

Apps and services

Full library of applications from 3rd parties

Alternative business models

Autonomous vehicle sharing, new service offerings, etc

Data analytics

Fully connected cloud processing and data feeds for manufacturers

https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/how-the-convergence-of-automotive-and-tech-will-create-a-new-ecosystem

…making vehicles vulnerable to cyber attacks

CYBER SECURITY NEWS · 4 MIN READ

DAGENS NYHETER. Nyheter Ekonomi Kultur Sthlm Gbg Sport Ledare DN Debatt DN Åsikt ☰ Mer

Om våra annonser

Motor

Uppkoppling för äldre bil öppen för hackning

PUBLICERAD 2019-06-01

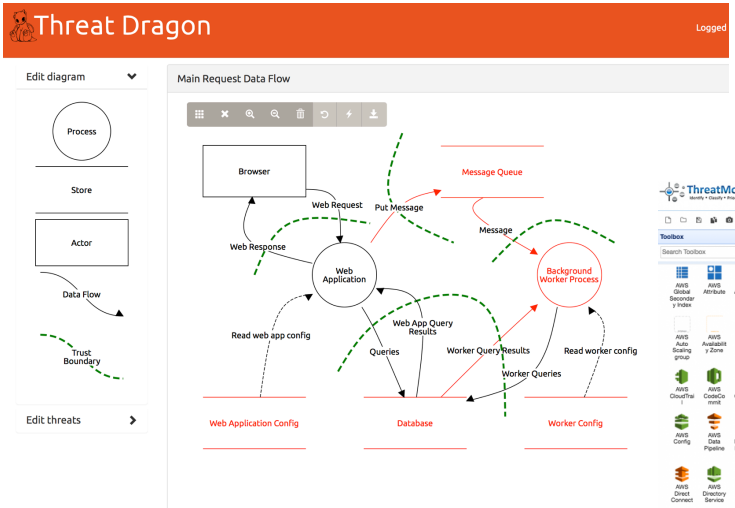
Enter -> threat modeling

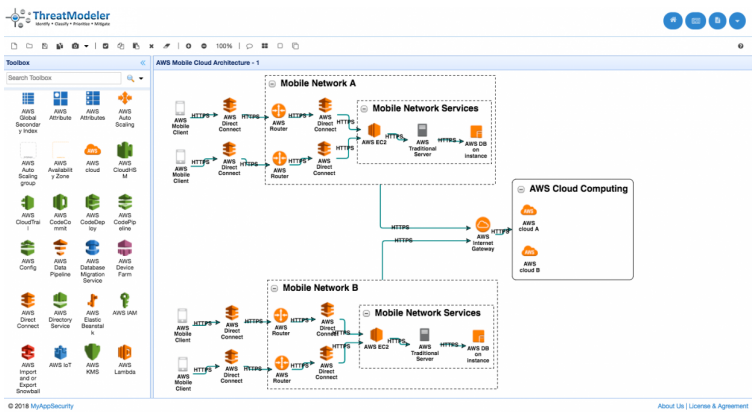
Secure app design

With for instance Microsoft Threat Modeling tool or OWASP Threat Dragon

System security analysis

With for instance Foreseeti securiCAD or ThreatModeler (ThreatModeler Software Inc.)





COMPUTERS & SECURITY 84 (2019) 53–69

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Threat modeling – A systematic literature review

*Wenjun Xiong, Robert Lagerström**

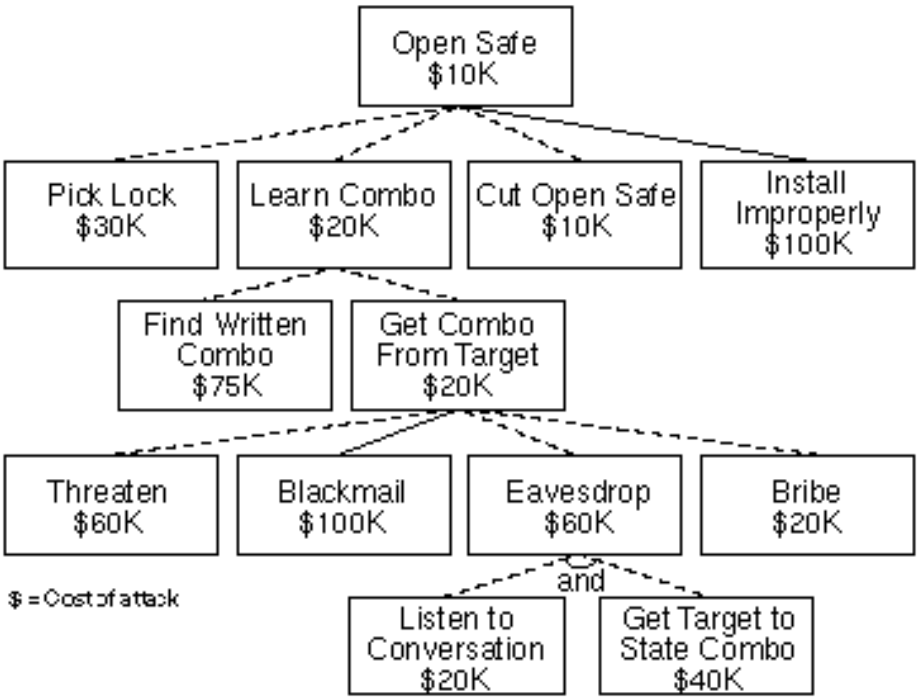
Division of Network and Systems Engineering, School of Electrical Engineering and Com Institute of Technology, Malvinas väg 6, SE-100 44 Stockholm, Sweden

Most approaches
=
manual modeling &
manual analysis
=
time consuming &
error prone

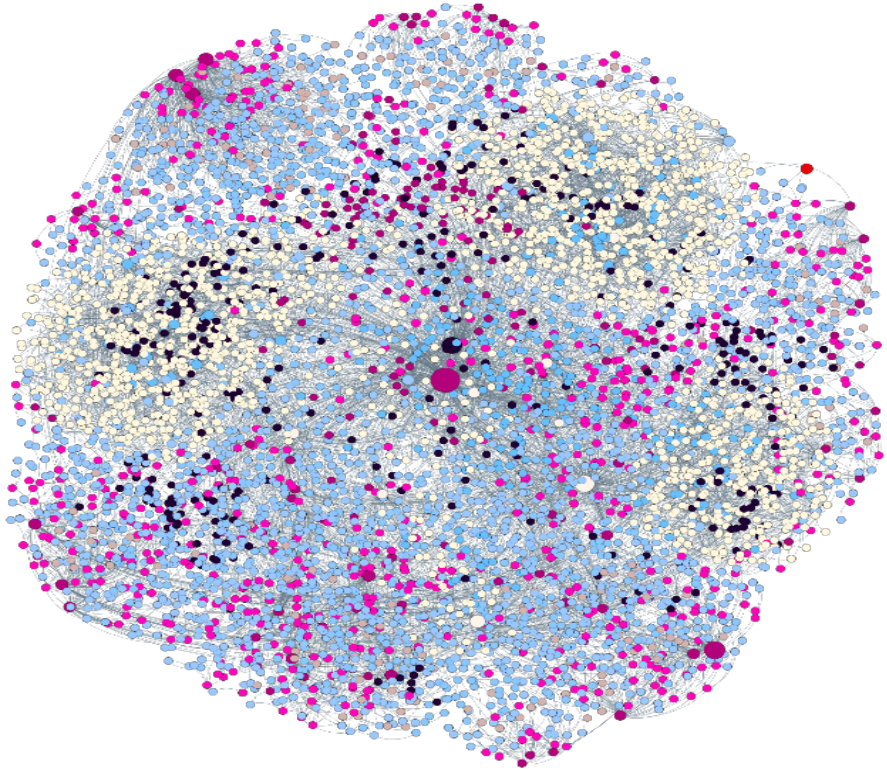
Table 4 – Type of threat modeling methods (C1).

Ref.	Manual	Automatic
Xu and Nygard (2006)	●	
Xu et al. (2012)	◗	●
Jiang et al. (2014)	●	
Yan et al. (2014)	●	
Pei et al. (2004)	●	
Liu et al. (2015)	●	
Hofmann and Kasseckert (2011)	●	
Cardenas et al. (2009)	●	
Arsac et al. (2011)	●	◗
Martina et al. (2015)	●	
Idziorek and Tannian (2012)	●	
Paladi et al. (2016)	●	
Meszaros and Buchalcevova (2017)	●	
Wu and Wei (2017)	●	
Bauer (2013)	●	
Seifert and Reza (2016)	●	
Lavrova and Pechenkin (2015)	●	
Baquero et al. (2015)		●
James and Prabakaran (2015)	●	
Dahbul et al. (2017)	●	
Chen et al. (2012)	●	
Musman and Turner (2018)		●
Kalinin and Konoplev (2014)	●	
Pendergrass et al. (2014)	●	
Al-Fedaghi and Alkandari (2011)	●	
Olawumi et al. (2017)	●	
Almulhem (2012)	●	
Bedi et al. (2013)	●	

Enter -> attack (tree/graph) simulations



Real life attack graphs, since IT is so complex



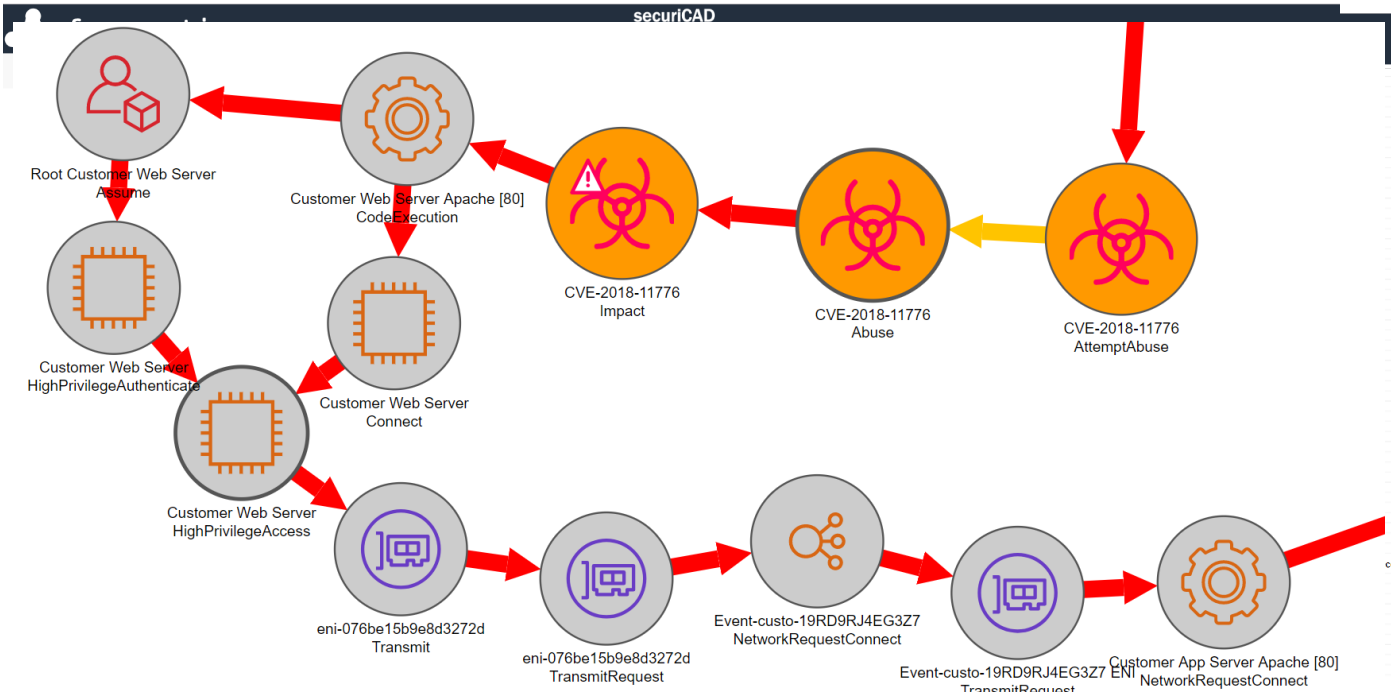
Enter -> automatic modeling

Generate Model

Simulate Attacks

Manage Risk Exposure

4. [illegible]tent


securiCAD
Root Customer Web Server
Assume
Customer Web Server Apache [80]
CodeExecution
CVE-2018-11776
Impact
CVE-2018-11776
Abuse
CVE-2018-11776
AttemptAbuse
Customer Web Server
HighPrivilegeAuthenticate
Customer Web Server
Connect
Customer Web Server
HighPrivilegeAccess
eni-076be15b9e8d3272d
Transmit
eni-076be15b9e8d3272d
TransmitRequest
Event-custo-19RD9RJ4EG3Z7
NetworkRequestConnect
Event-custo-19RD9RJ4EG3Z7 ENI
Customer App Server Apache [80]
NetworkRequestConnect

Meta Attack Language (MAL)

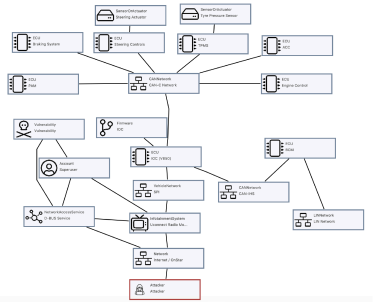
Language (framework) for creating threat modeling languages with attack simulations

```
asset ECU extends Machine
    info: "Specifies any ECU/MCU/controller in a vehicle."
    rationale: "Created as new parent class because the existing Machine had many unrelated attacks."
{
    | connect
            info: "Attackers can attempt to connect to the ECU and change the operation mode if they have access to the network, servic
            +>  attemptChangeOperationMode
                //firmwareUpdater.connect

    | maliciousFirmwareUpload
            info: "Maliciously upload a forged firmware leads to full access on the ECU and ability to inject messages on the previous
            ->  access,
                _firmwareUploadNetworkAccess

    & uploadFirmware
            info: "Updating the firmware leads to the ability to inject messages not only on the previous running services but also on
            ->  _firmwareUploadNetworkAccess

    | _firmwareUploadNetworkAccess
            info: "This a helper attack step because both above attack steps are leading to the same connections."
            ->  vehiclenetworks.messageInjection, // NOTE: I still think this is needed here, blame me!
                vehiclenetworks.j1939Attacks,
                vehiclenetworks._networkForwarding // This is left here because it might be needed! Or it might not...
```

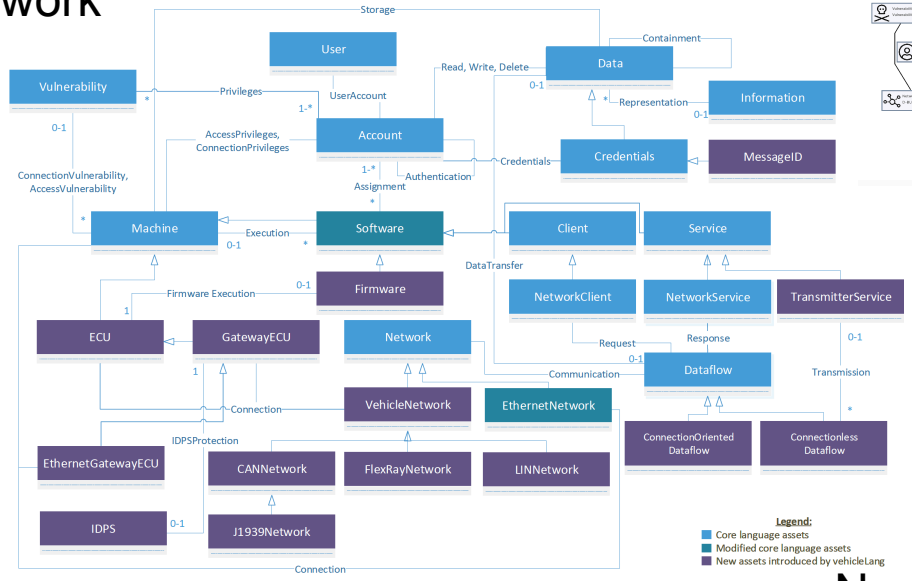
Being used in multiple projects e.g. for cloud, power, defense.

vehicleLang

Tested at Scania



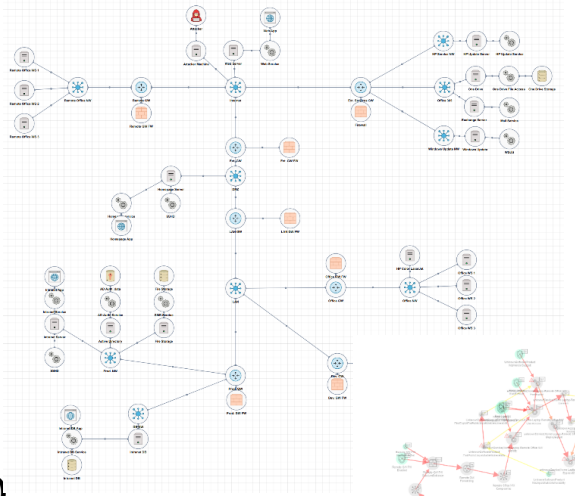
Based on the MAL framework



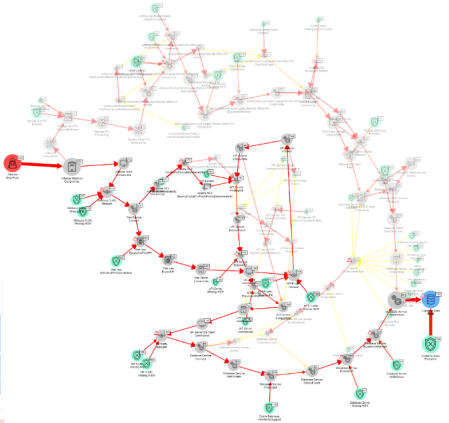
Vehicle specific assets (components), attacks, and defenses

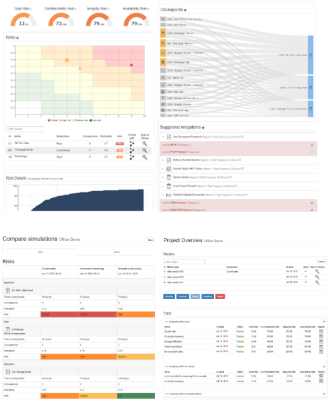
Next phase: more development, more validation/testing

Tool support



Make sure that securiCAD from foreseeti can model and analyze with MAL-based languages like vehicleLang





Tool chain integration

Like with AWS, find data sources that can feed the vehicle threat model

Also how can the output from vehicleLang/ securiCAD be used in other tools

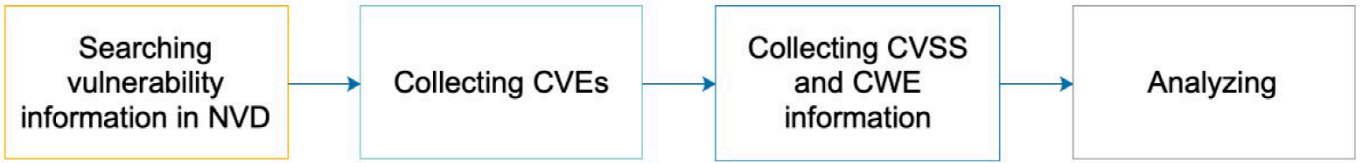
Vehicle specific security parameters

Investigate known attacks and vulnerabilities

Vuln ID	Summary	CVSS Severity
CVE-2018-9322	The Head Unit HU_NBT (aka Infotainment) component on BMW i Series, BMW X Series, BMW 3 Series, BMW 5 Series, and BMW 7 Series vehicles produced in 2012 through 2018 allows local attacks involving the USB or OBD-II interface. An attacker can bypass the code-signing protection mechanism for firmware updates, and consequently obtain a root shell. **Published:** May 31, 2018; 08:29:00 AM -04:00	*V3.0:* 7.8 HIGH *V2:* 7.2 HIGH
CVE-2018-9320	The Head Unit HU_NBT (aka Infotainment) component on BMW i Series, BMW X Series, BMW 3 Series, BMW 5 Series, and BMW 7 Series vehicles produced in 2012 through 2018 allows a local attack when a USB device is plugged in. **Published:** May 31, 2018; 08:29:00 AM -04:00	*V3.0:* 7.8 HIGH *V2:* 7.2 HIGH
CVE-2018-9318	The Telematics Control Unit (aka Telematic Communication Box or TCB), when present on BMW vehicles produced in 2012 through 2018, allows a remote attack via a cellular network. **Published:** May 31, 2018; 08:29:00 AM -04:00	*V3.0:* 9.8 CRITICAL *V2:* 10.0 HIGH
CVE-2018-9314	The Head Unit HU_NBT (aka Infotainment) component on BMW i Series, BMW X Series, BMW 3 Series, BMW 5 Series, and BMW 7 Series vehicles produced in 2012 through 2018 allows an attack by an attacker who has direct physical access. **Published:** May 31, 2018; 08:29:00 AM -04:00	*V3.0:* 6.8 MEDIUM *V2:* 7.2 HIGH
CVE-2018-9313	The Head Unit HU_NBT (aka Infotainment) component on BMW i Series, BMW X Series, BMW 3 Series, BMW 5 Series, and BMW 7 Series vehicles produced in 2012 through 2018 allows a remote attack via Bluetooth when in pairing mode, leading to a Head Unit reboot. **Published:** May 31, 2018; 08:29:00 AM -04:00	*V3.0:* 5.3 MEDIUM *V2:* 5.7 MEDIUM
CVE-2018-9312	The Head Unit HU_NBT (aka Infotainment) component on BMW i Series, BMW X Series, BMW 3 Series, BMW 5 Series, and BMW 7 Series vehicles produced in 2012 through 2018 allows a local attack when a USB device is plugged in. **Published:** May 31, 2018; 08:29:00 AM -04:00	*V3.0:* 7.8 HIGH *V2:* 7.2 HIGH
CVE-2018-9311	The Telematics Control Unit (aka Telematic Communication Box or TCB), when present on BMW vehicles produced in 2012 through 2018, allows a remote attack via a cellular network. **Published:** May 31, 2018; 08:29:00 AM -04:00	*V3.0:* 9.8 CRITICAL *V2:* 10.0 HIGH

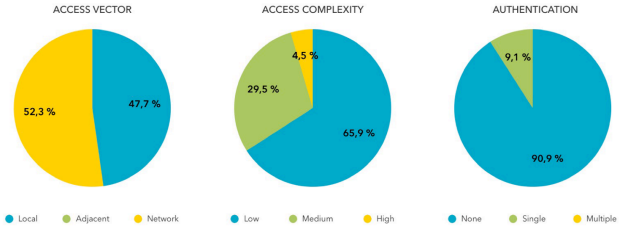
Hack stuff

NVD study



- `Part 1: Vehicle-Related Terms`
  vehicle, car, automotive.
- `Part 2: Common Vehicle Components and Networks`
  adaptive cruise control, adas, airbag, airbiquity, android auto, autoliv, bluetooth, braking system, carlink, carplay, collision prevention, control unit, cruise, drivesync, engine control, infotainment, keyless entry, lane keep assist, park assist, lidar, controller area network/CAN, local interconnect network/LIN, media oriented systems transport/MOST, flexray, OBD-II, aassive anti-theft system/PATS, radio data system, steering control, telematics, tire pressure/TPMS.
- `Part 3: Major OEMs`
  volkswagen, bmw, acura, audi, toyota, jeep, kia, mercedes-benz, skoda, renault, ford, peugeot, nissan, hyundai, opel, mazda, saab, seat, subaru, dacia, citroën, honda, great wall, cadillac, suzuki, land rover, rolls royce, porsche, jaguar, mitsubishi, chevrolet, mini, lexus, alfa romeo, lancia, snapdragon automobile, alpine, aston martin, bentley, bugatti, buick, changan, chrysler, daimler, dodge, dongfeng, ferrari, fiat, fisker, geely, general motors, infiniti, gmc, lamborghini, maserati, maclaren, tesla, pagani, ssangyong, tata motors.

Some results



CWE ID	Count	Description	Mitigations
CWE-693	7	Protection Mechanism Failure	Use intrusion detection systems; secure communications between ECUs
CWE-119	4	Buffer Errors	Use a language, or a vetted library, or a framework that does not allow this weakness to occur; use static analysis tools
CWE-200	4	Information Leak/Disclosure	Set trust boundaries. Use privacy mechanisms
CWE-310	3	Cryptographic Issues	Use strong cryptography and properly manage the private key
CWE-264	2	Permissions, Privileges, and Access Control	Design secure architecture
CWE-20	2	Input Validation	Use static and dynamic analysis tools to test the software

volkswagen	CVE_2018_1170
BMW	CVE_2018_9322
BMW	CVE_2018_9320
BMW	CVE_2018_9318
BMW	CVE_2018_9314
BMW	CVE_2018_9313
BMW	CVE_2018_9312
BMW	CVE_2018_9311
BMW	CVE_2017_9633
BMW	CVE_2017_9212
Toyota	CVE_2014_7128
Jeep	CVE_2015_5611
Benz/Mercedes	CVE_2018_18071
Benz/Mercedes	CVE_2018_18070
Ford	CVE_2017_9647
Ford	CVE_2017_9633
Nissan	CVE_2017_9647
Nissan	CVE_2017_9633
Hyundai	CVE_2017_6054
Hyundai	CVE_2017_6052
subaru	CVE_2018_18203
Chrysler	CVE_2015_5611
Daimler	CVE_2018_18071
Daimler	CVE_2018_18070
general motors	CVE_2017_9663
general motors	CVE_2017_12697
general motors	CVE_2017_12695
infiniti	CVE_2017_9647
infiniti	CVE_2017_9633
infiniti	CVE_2014_6746
Tesla	CVE_2019_9977
Tesla	CVE_2018_16806
Tesla	CVE_2016_9337
Tesla	CVE_2016_7389
Tesla	CVE_2016_7382
Tesla	CVE-2009-3277

Ethical hacking of vehicle components

DAGENS NYHETER. Nyheter Ekonomi Kultur Sthlm Gbg Sport Ledare DN Debatt DN Åsikt Mer

Motor

Uppkoppling för äldre bil öppen för hackning

PUBLICERAD 2019-06-01

Car dongles, car alarms, …

We have pentested three different car dongles

We are currently pentesting a car alarm

Vulnerabilities published

Arvid Viderberg, Pontus Johnson, and Robert Lagerström, CVE-2019-12943, Insecure permission, password reset function, in TTLock Open Platform.

Arvid Viderberg, Pontus Johnson, and Robert Lagerström, CVE-2019-12942, Insecure permission, account revocation mechanism, in TTLock Open Platform.

Theodor Olsson, Albin Larsson Forsberg, Pontus Johnson, and Robert Lagerström, CVE-2019-12821, Vulnerability in the app 2.0 of the Shenzhen Jisiwei i3 robot vacuum cleaner, while adding a device to the account using a QR-code.

Theodor Olsson, Albin Larsson Forsberg, Pontus Johnson, and Robert Lagerström, CVE-2019-12820, Vulnerability in the app 2.0 of the Shenzhen Jisiwei i3 robot vacuum cleaner, possible MiTM attack on http.

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.

We would like to pentest more/other types of vehicle components

Impact

- MAL and vehicleLang as Open source code on GitHub
- Tool support (securiCAD) for usability, performance, reporting etc
- Publishing discovered vulnerabilities (CVEs, NVD)
- Conferences (national/international, industry/academic)
- News (DagensNyheter, Sveriges Radio, NyTeknik, Computer Sweden)
- Podcasts, videos, popular science books
- Cross projects faciliatiation (vehicle and other security)

Visit https://autosec.se/threat-move-results/

Home About News Projects Events

Threat MOVE Results

Or
www.kth.se/nse/ssas for large than single project results and news