Biljeske 18.11. - 8.12.2023

Sommer, Florian, Jürgen Dürrwang, and Reiner Kriesten. "Survey and classification of automotive security attacks." Information 10.4 (2019): 148.

- https://www.mdpi.com/2078-2489/10/4/148/pdf
- koristan izvor za stvaranje ctf izazova iz pravih napada
  - https://github.com/IEEM-HsKA/AAD
- njihov nacin klasifikacije napada

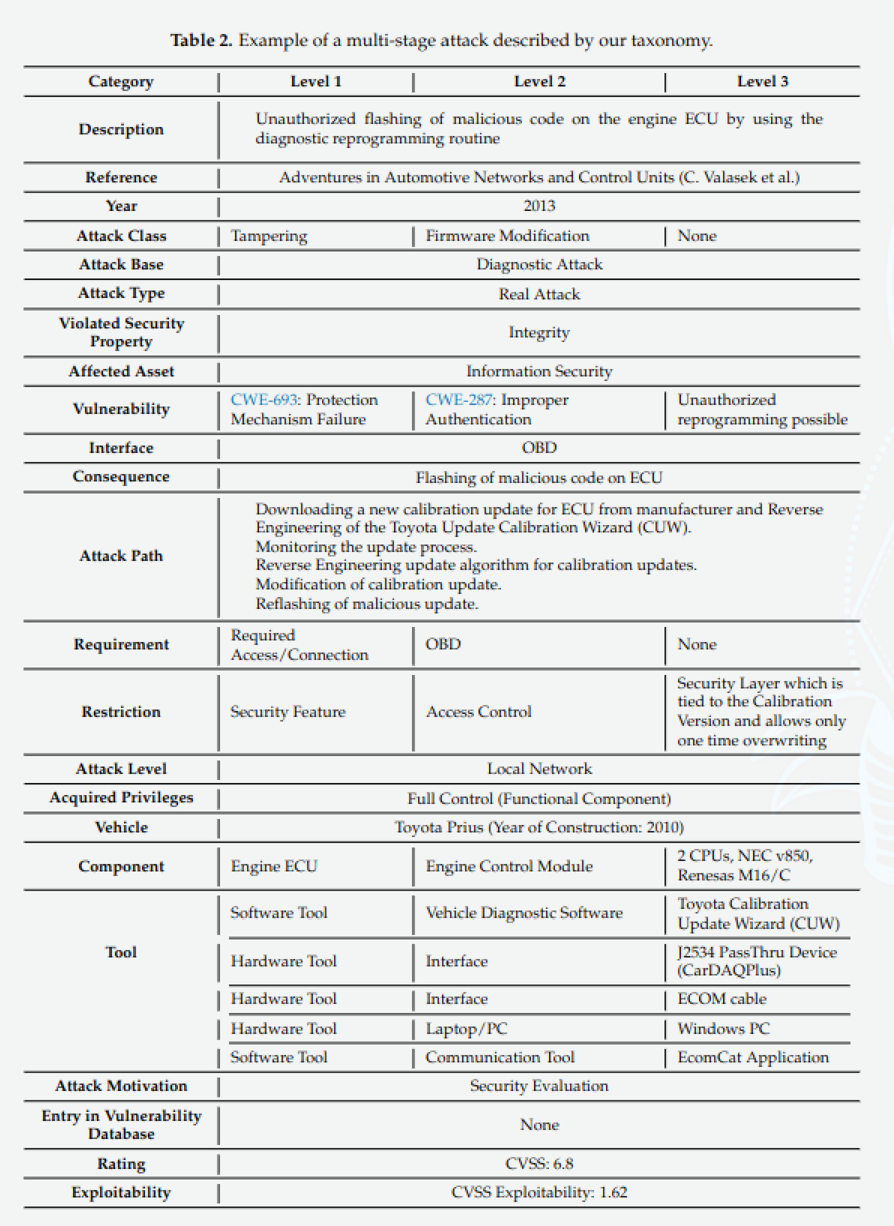


Table 2. Example of a multi-stage attack described by our taxonomy.

Category	Level 1	Level 2	Level 3
Description	Unauthorized flashing of malicious code on the engine ECU by using the diagnostic reprogramming routine		
Reference	Adventures in Automotive Networks and Control Units (C. Valasek et al.)		
Year	2013		
Attack Class	Tampering	Firmware Modification	None
Attack Base	Diagnostic Attack		
Attack Type	Real Attack		
Violated Security Property	Integrity		
Affected Asset	Information Security		
Vulnerability	CWE-693: Protection Mechanism Failure	CWE-287: Improper Authentication	Unauthorized reprogramming possible
Interface	OBD		
Consequence	Flashing of malicious code on ECU		
Attack Path	Downloading a new calibration update for ECU from manufacturer and Reverse Engineering of the Toyota Update Calibration Wizard (CUW). Monitoring the update process. Reverse Engineering update algorithm for calibration updates. Modification of calibration update. Reflashing of malicious update.		
Requirement	Required Access/Connection	OBD	None
Restriction	Security Feature	Access Control	Security Layer which is tied to the Calibration Version and allows only one time overwriting
Attack Level	Local Network		
Acquired Privileges	Full Control (Functional Component)		
Vehicle	Toyota Prius (Year of Construction: 2010)		
Component	Engine ECU	Engine Control Module	2 CPUs, NEC v850, Renesas M16/C
Tool	Software Tool	Vehicle Diagnostic Software	Toyota Calibration Update Wizard (CUW)
	Hardware Tool	Interface	J2534 PassThru Device (CarDAQPlus)
	Hardware Tool	Interface	ECOM cable
	Hardware Tool	Laptop/PC	Windows PC
	Software Tool	Communication Tool	EcomCat Application
Attack Motivation	Security Evaluation		
Entry in Vulnerability Database	None		
Rating	CVSS: 6.8		
Exploitability	CVSS Exploitability: 1.62		

candevstudio

https://github.com/GENIVI/CANdevStudio

- alat za testiranje i simuliranje CAN mreza
- moze raditi direktno s adapterima i CAN uredjajima poznatih proizvodjaca (vector, PEAK) ili sa socketcan-om

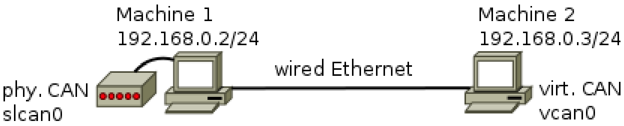
- omogucava izradu vlastitih QML komponenti koje mogu stvarati ili regirati na CAN promet (https://www.youtube.com/watch?v=1TfAyg6DG04)
- mogao bi se koristiti kao baza za CTF platformu
- CAN komunikacija se vrsi pomocu Qt CAN bus biblioteke

Qt CAN bus (C++ biblioteka)

https://doc.qt.io/qt-6/qtcanbus-backends.html

canelloni

https://github.com/mguentner/cannelloni



a SocketCAN over Ethernet tunnel

- moglo bi biti od koristi

socketcan demo

https://www.kernel.org/doc/html/next/networking/can.html

Stvaranje i podizanje virtualnog can sucelja putem naredbenog retka:

```
ip link add dev vcan0 type vcan
ip link set dev vcan0 up
```

Spustanje i brisanje virtualnog can sucelja putem naredbenog retka:

```
ip link set dev vcan0 up
ip link delete dev vcan0
```

Isprobani C example primjeri
https://github.com/craigpeacock/CAN-Examples

Skoro svaki jezik ima svoju biblioteku za socketcan pa tako i python i Golang:
https://python-can.readthedocs.io/en/stable/interfaces/socketcan.html
https://pkg.go.dev/go.einride.tech/can/pkg/socketcan

Za pogledati

mazda ECUs

https://youtu.be/3NhGoU-BToQ?si=YewlASVBJZsJM720

can analysis using wireshark

https://youtu.be/1nkgTtTWnPM?si=UtL0KPef3wQ-CIBp

Jmaxxz - Your Car is My Car - DEF CON 27 Conference

https://www.youtube.com/watch?v=w8SG2V3n4-U

DEF CON 27: Car Hacking Deconstructed

https://www.youtube.com/watch?v=gzav1K5KSI4

dbc-ovi CAN signala poznatih proizvodjaca

https://github.com/commaai/opendbc