Biljeske 4.11. - 10.11.2023

Koje komponente automobila i sustava oko automobila je potrebno emulirati/simulirati za uspješno repliciranje nekih od poznatijih stvarnih napada?

Miller, Charlie, and Chris Valasek. "Remote exploitation of an unaltered passenger vehicle." Black Hat USA 2015.S 91 (2015): 1-91. (Jeep)

Lanac ranjivosti:

- anonimni login na dbus servise preko mobilne mreze ili wi-fi mreze automobila
  "we've found several that permit direct interaction with
  the head unit, such as adjusting the volume of the radio, accessing PPS data, and others
  that provide lower levels of access"
  ili
- flashanje modificiranog firmwarea preko USB-a
  - ranjiva lua skripta NavTrailService dbus servisa koja omogucava slanje naredbi kao root
  - pokretanje ssh servisa i ssh login
  - za upravljanje GPS-om, radijem, HVAC-om itd postoje lua skripte
  - reverzanje firmwarea Renesas V850/Fx3 cipa
  - flashanje malicioznog firmwarea na čip Renesas V850/Fx3 koristen za komunikaciju s CAN-om koji omogucava slanje CAN poruka preko SPI-a
  - slanje CAN poruka preko SPI-a

Web hackers vs the auto industry

https://samcurry.net/web-hackers-vs-the-auto-industry/

- vecinom banalne ranjivosti API-ja koji ne zahtjevaju autentifikaciju

BMW

- otvoreni API endpoint za pretrazivanje usera, vraca id, ime i prezime i korisnicko ime korisnika
- otvoreni TOTP API koji vraca OTP za korisnikov id
- password reset pomocu dobivenog OTP-a

To demonstrate the impact of the vulnerability, we simply Googled "BMW dealer portal" and used our account to access the dealer portal used by sales associates working at physical BMW and Rolls Royce dealerships.
After logging in, we observed that the demo account we took over was tied to an actual dealership, and we could access all of the functionality that the dealers themselves had access to. This included the ability to query a specific VIN number and retrieve sales documents for the vehicle.
With our level of access, there was a huge amount of functionality we could've performed against BMW and Rolls Royce customer accounts and customer vehicles. We stopped testing at this point and reported the vulnerability.

Mercedes

After fuzzing random sites for a while, we eventually found the "umas.mercedes-benz.com" website which was built for vehicle repair shops to request specific tools access from Mercedes-Benz. The website had public registration enabled as it was built for repair shops and appeared to write to the same database as the core employee LDAP system.

- fuzzing web stranica
- koristeci credentialse dobivene s portala za autoservise, prijava na razno razne interne servise
  - git, teams, sonarqube, mattermost
  - Multiple employee-only Githubs with sensitive information containing documentation and configuration files for multiple applications across the Mercedes-Benz infrastructure

- Spring boot actuators which lead to remote code execution, information disclosure, on sensitive employee and customer facing applications Jenkins instances
- AWS and cloud-computing control panels where we could request, manage, and access various internal systems
- XENTRY systems used to communicate with customer vehicles
- Internal OAuth and application-management related functionality for configuring and managing internal apps
- Hundreds of miscellaneous internal services

ne rezultira upravljanjem automobilom, ali omogucuje pristup izvorima koji bi potencijalno mogli sadržavati informacije o ranjivostim

Ferrari

- pronalazak API endpointova i API kljuca u javascript kodu web portala za autoservisere
- modifikacija korisnickih racuna i podizanje korisnickih prava za napadaca,

ne rezultira upravljanjem automobilom

Spireon

- SQL injection na admin login panelu
- admin login
- The administrator user had access to all Spireon devices, including those of OnStar, GoldStar, and FleetLocate. We could query these devices and retrieve the live location of whatever the devices were installed on, and additionally send arbitrary commands to these devices.

Reviver

- mass assignment, promjena korisnicke role -> priv esc ->
  - Overwrite the Virtual License Plates for All Reviver Customers, Track and Administrate Reviver Fleets, and Access, Modify, and Delete All User Information

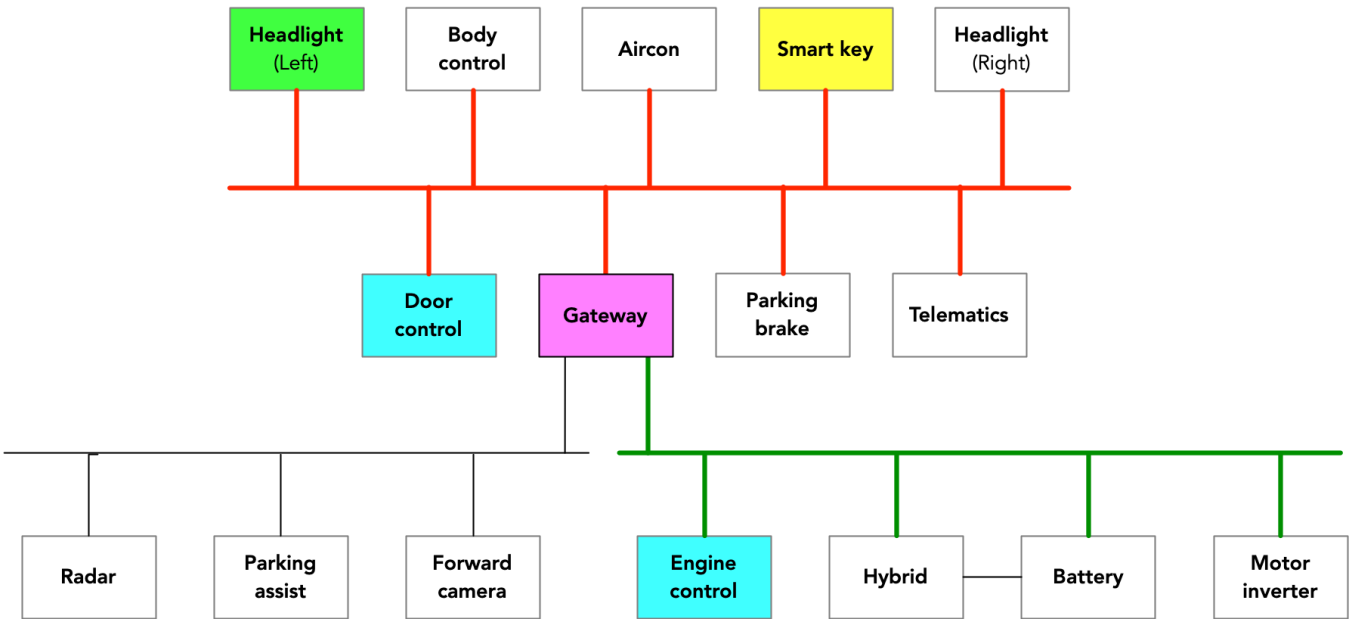
Honda

https://x.com/samwcyo/status/1597792097175674880?s=20

- **neautentificirano** slanje naredbi automobilu putem API-ja pomocu VIN-a

CAN injection: keyless car theft

CAN Injection: keyless car theft



- CAN injection tehnika

    - koristi modifcirani CAN čip koji poteze sabirnicu u recesivno stanje, onemogucavajuci slanje svih poruka osim njegovih
- preko ECU-a za upravljanje prednjim svjetlima salje se poruka za otkljucavanje vrata i omogucavanje paljenja motora
- ovako nesto **nije moguce simulirati virtualno**, obzirom da se koriste fizicka svojstva sabirnice

Nie, Sen, et al. "Over-the-air: How we remotely compromised the gateway, BCM, and autopilot ECUs of Tesla cars." *Briefing, Black Hawt USA* (2018): 1-19.

Nie, Sen, Ling Liu, and Yuefeng Du. "Free-fall: Hacking tesla from wireless to can bus." Briefing, Black Hat USA 25 (2017): 1-16.

- Wi-Fi -> WebKit -> priv. esc. glavne jedinice (Linux) -> pristup CAN-u i modificiranje firmware-a
- iskoristavanje ranjivosti u web rendering engineu Infotainmenta

Cai, Zhiqiang, et al. "0-days & mitigations: roadways to exploit and secure connected BMW cars." Black Hat USA 2019 (2019): 39.

Lennert Wouters - Passive Keyless Entry and Start Systems - DEF CON 27 Car Hacking Village

- opisano u biljeskama od 27.10.

KES relay i jam napadi

https://www.youtube.com/watch?v=rcPZi5-OJrI&pp=ygUYYXV0b21vdGl2ZSByZWxheSBhdHRhY2tz

Izvedba sustava za CTF/Edukacijske materijale :

- KES, za emulaciju potreban bi bio mikrokontroler ili SBC koji podrzava RF, opisano u DEFCON 27 talku
- cloud/web servisi (API-ji), najlaksi za izvest, kao u klasicnim CTF scenarijima, s mogucom integracijom s ostalim sustavima specificnijim za kiberneticku sigurnost automobila
- za slucaj Jeep-a, odnosno iskoristavanje dbus servisa preko wifi-a ili mobilne mreze potrebna je virtualna masina ili kontenjer s takvom vrstom povezivosti i nekom linux distribucijom
- za emulaciju/simulaciju CAN-a,
    - napisati softverske ECU-ove koji koriste socketcan ili neko drugo rucno rjesenje
    - umrezavanje i lakse podizanje i konfiguracija CAN "mreze" bi se moglo rjesiti i nekom vrstom kontenjera (prvo mi na pamet pada docker network)
      ili
    - napraviti jednostavniji fizicki lab poput Toyota PASTA (prednost je sto se mogu iskoristiti ranjivosti u fizickom sloju (Can injection))
- napadi putem USB-a, fizicki USB prikljucak i ili virtualni uredjaj https://github.com/jtornosm/USBIP-Virtual-USB-Device

Sve ovo bi se moglo obuhvatiti jednim SBC-om ili kombinacijom korisnickog racunala skupa s dodatnim mikrokontrolerom koji bi omogucavao RF, USB, Wi-fi i bluetooth napade. U to se moze ukljuciti i potencijalni cloud servisi/API-ji za "upravljanje" vozilom