SECURING THE FUTURE OF MOBILITY: IS YOUR CONNECTED CAR UNHACKABLE?

Sergey Kravchenko
Senior Business Development Manager
Kaspersky Lab
@propulsivo
Vulnerabilities and their exploits in cars
Navigation: CD era
Vulnerabilities and their exploits in cars
Navigation: CD era

SECURITY

FREE NAVIGATION

HACKED
Vulnerabilities and their exploits in cars
Navigation: Flash drive era

+ activation code = SECURED

Key generator
Vulnerabilities and their exploits in cars
Navigation: Flash drive era

You can find different key generators with instructions on how to implement them by entering a simple search request:

https://www.youtube.com/results?search_query=CARBRAND+map+key+generator
Vulnerabilities and their exploits in cars
Modern times

- NAV
- Voice control (via cloud)
- Text to speech
- Map updates
- Satellite Radio
- RTTI (Traffic)
- CarPlay
Vulnerabilities and their exploits in cars

Digital signature security system also implemented in:

- External car cameras
- Engine
- New services (ride sharing, car sharing)
- etc...

All of them have already been hacked and monetized by ‘grey garage’ businesses.
Vulnerabilities and their exploits in cars

http://fscmap.com/ (there are not only USB solutions, they sell chiptuning technology based on TriCore vulnerability)
http://cartechnology.co.uk/showthread.php (this forum itself covers many brands, have a look around)
http://cartechnology.co.uk/showthread.php (DIY USB stick thread for CIC HU)
http://audi-rus.ru (tuning solutions for audi cars)
http://tokenmaster.blogspot.ru/ (change log Esys tool modification for using with modified EST or without it at all)
http://www.obdiigroup.com/ (different tools for many cars)
https://www.fxxtokenmaster.com/ (main address for Esys launcher)
http://www.bimmerfest.com/forums/forum (very well-known BMW forum)
http://auto-explorer.com/ (mileage reset and ECU explorer)
http://www.abrites.com/home (VW/Toyota/Lexus services and solutions like Vehicle Diagnostics Interface)
http://apg.org.ua
https://mbworld.org/forums/c63-c63s-amg/633163-dealer-mode.html
http://mozy.org/w205/srm.htm
http://www.boostedautos.net/
New business opportunity

Autostart module allows you to bypass immobilizers and engage the engine autostart option, providing additional security measures and improving the security of your car.

*https://author-alarm.ru/informatsiya/novosti/autostart-my-uvelichili-kolichestvo-podderzhivaemyh-modeley
Standard attack schema exploiting vulnerabilities in the USB stack

Reboot HU
Anatomy of attack

upd00000000.bin is a **TAR** archive

- **DO WHAT YOU WANT**
  - Reboot HU
  - Autostart script substitutes Bootloader

- **HU**
  - Activates internal process `**Car**`
    - spawns `bin\sh`
    - spawns `bin\bsdtar`

- Inside the package, a symlink to an absolute path to a closed area

- After symlink opened, all files are copied from archive to the autostart area
Is your car secure?
Standard attack schema exploiting vulnerabilities in the USB stack

- Backdoor
- Data leakage
- Malware
- Ransomware
- Tracking via GPS or internet
- Espionage via microphone & cameras

- Car theft
- VPN channel to the car
- SSH
- Manipulation with any car ECUs
- Full remote control
Why this problem still exists

- OEMs have a long development cycle (5-7 years)
- Large number of suppliers
- Cyber-security not seen to be a major issue
- New tech solutions outperform 5 years old solutions
- Lack of holistic cyber-security approach
In 2016 Kaspersky Lab researchers tested 9 car apps for resistance to several cyber attack vectors. NONE OF THEM WERE SECURE.

1 year after, the researchers tested 13 applications. THE ORIGINAL NINE TESTED WERE STILL NOT SECURE.

Of the 4 new applications tested ONLY ONE APP WAS PROTECTED AGAINST JUST ONE ATTACK.
Is there a cure?

- Cyber-security should be considered as important as safety
  Safety features can currently be switched off with software commands. So if your system is not secure – it’s not safe.

- Secure by design systems and solutions (Secure Communication Unit)
  This is when security measures are applied at the architecture level allowing manufacturers to avoid most post-applied security gaps.

- Isolation
  It is necessary to isolate the security and safety critical functions from other functionality with multiple access checks.
Is there a cure?

- **Secure Operating System**
  Most operating systems in automotive and transportation contain tons of known vulnerabilities and ready exploits for kernels, drivers or stacks. Secure Operating Systems are designed to be immune to any malicious interference and exploits, following a "security is first" paradigm.

- **TPM and HSM modules support**
  Hardware support for safe storage, digital signature and cryptoprocessing.

- **Collaboration (not acquisition) between automotive and cyber-security industries**
  Professional expertise collaboration allows automotive security teams to apply technologies and products developed by dedicated cyber-security companies to build incredible products with all the benefits from both sides.