

RSA®Conference2018

San Francisco | April 16 – 20 | Moscone Center

SESSION ID: SBX3-W3

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

Sergey Kravchenko

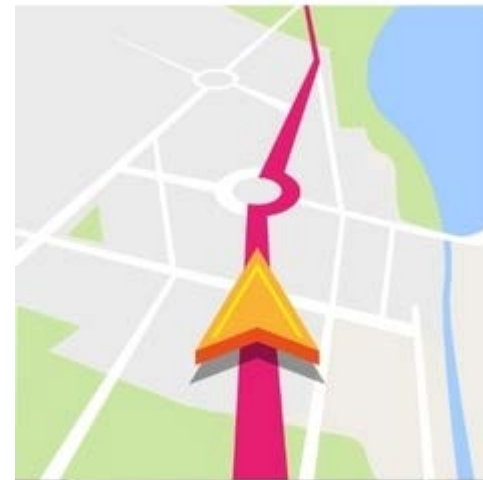
Senior Business Development Manager
Kaspersky Lab
@propulsivo



#RSAC

Vulnerabilities and their exploits in cars

Navigation: CD era



Vulnerabilities and their exploits in cars

Navigation: CD era



SECURITY

HACKED



#RSAC



+ activation code = SECURED

[illegible]

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=CARBAND+map+key+generator

The image shows a collage of YouTube search results for car-related key and map generators. The primary focus is on 'toyota ERC key generator' with 372 results. Visible video thumbnails include:

- bmw map key generator**: About 1,010 results. Videos show car interiors and navigation screens.
- mercedes map key generator**: Videos show car interiors and navigation screens.
- toyota ERC key generator**: About 372 results. Videos include:
 - Toyota ERC Solution** by Mira Auto (15 views): A red screen with 'Enter Erc Number' and 'Unlock Code' fields. A disclaimer states: 'This product is designed for professional purpose only. We do not take any responsibility or liability for the use of our product that may be considered illegal. All feedback for comments, queries and bugs are the property of the creator.' Duration: 1:08.
 - Toyota ERC GamingMonst**: A video showing a car's infotainment screen with a map. Duration: 0:23.
 - TOYOTA E** by Leo Samsung: A video showing a car's infotainment screen. Duration: 2:33.
 - TOYOTA JAPA** by PAKISTAN CAI: A video showing a car's infotainment screen. Duration: 2:33.
- ford map key generator**: Videos include:
 - Add Navigation to Sync 3** by OEMRadio Solutions (40K views, 1 year ago): A video showing a Ford truck's infotainment screen. Duration: 6:04.
 - How to connect a Ford vehicle to WiFi for SYNC3 Updates - FYF Episode 9** by Lacombe Ford (46K views, 1 year ago): A video showing a Ford's infotainment screen. Duration: 6:13.
 - Ford SYNC 3 Apple CarPlay Demonstration Using Maps & iTunes** by Lasco Ford (16K views, 1 year ago): A video showing a Ford's infotainment screen with CarPlay. Duration: 2:00.

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 USE
<http://cartechnology.co.uk/showthread.php>
<http://cartechnology.co.uk/showthread.php>
<http://audi-rus.ru> (tuning solutions for audi
<http://tokenmaster.blogspot.ru/> change log
<http://www.obdiigroup.com/> (different too
<https://www.fxxtokenmaster.com/> (main ac
<http://www.bimmerfest.com/forums/forum>
<http://auto-explorer.com/> (mileage reset ar
<http://www.abrites.com/home> (VW/Toyota
<http://apg.org.ua>
<https://mbworld.org/forums/c63-c63s-amg>
<http://mozy.org/w205/srm.htm>
<http://forums.vwvortex.com/showthread.p>
<http://www.boostedautos.net/>

All Categories	
 Distributors Price (4)	
 CDP and DS150E (44)	
 Brands (170)	
 Auto Tools Center (281)	
 OBD Code Scanner (2)	
 Truck / Heavy Duty Tool (47)	
 Auto ECU Programmer (167)	
 Auto Emulator (74)	
 Mileage Reset (47)	
 Auto Locksmith Center (110)	
 Airbag Reset Tool (12)	
 Garage Equipment (17)	
 Auto Tools Accessories (77)	
 Motorcycle Tools (22)	
 Diagnostic software (100)	
 Automotive Electrical Testers &	

ning technology based on TriCore vulnerability)
self covers many brands, have a look around)
thread for CIC HU)

using with modified EST or without it at all

well-known BMW forum)

ons like Vehicle Diagnostics Interface)

al

-Hack-may-be-possible&p=93910297

New business opportunity



Модуль AUTOSTART — автозапуск двигателя и бесключевой цифровой обходчик штатного иммобилайзера в одном устройстве. Успешно работает на самых популярных автомобилях, и список поддерживаемых моделей постоянно растет. Усилиями инженеров ГК «АВТОР» модуль AUTOSTART заработал на новых моделях «Тойот» и «Лексусов».

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

TOYOTA:

- Toyota Highlander
- Toyota Hilux
- Toyota Alphard
- Toyota Land Cruiser 200
- Toyota Land Cruiser Prado 2018

– Toyota Camry 2012-2018

– Toyota Rav-4 2012-2018

– Toyota Auris 2012-2018

– Toyota Corolla 2012-2018

– Toyota Prius C 2012-2018

LEXUS:

- Lexus LX 450 / 570
- Lexus NX 200 / 200t / 300h
- Lexus RX 200t / 270 / 350 / 450h
- Lexus IS 250 / 350

– Lexus ES 2012-2018

– Lexus GS 2012-2018

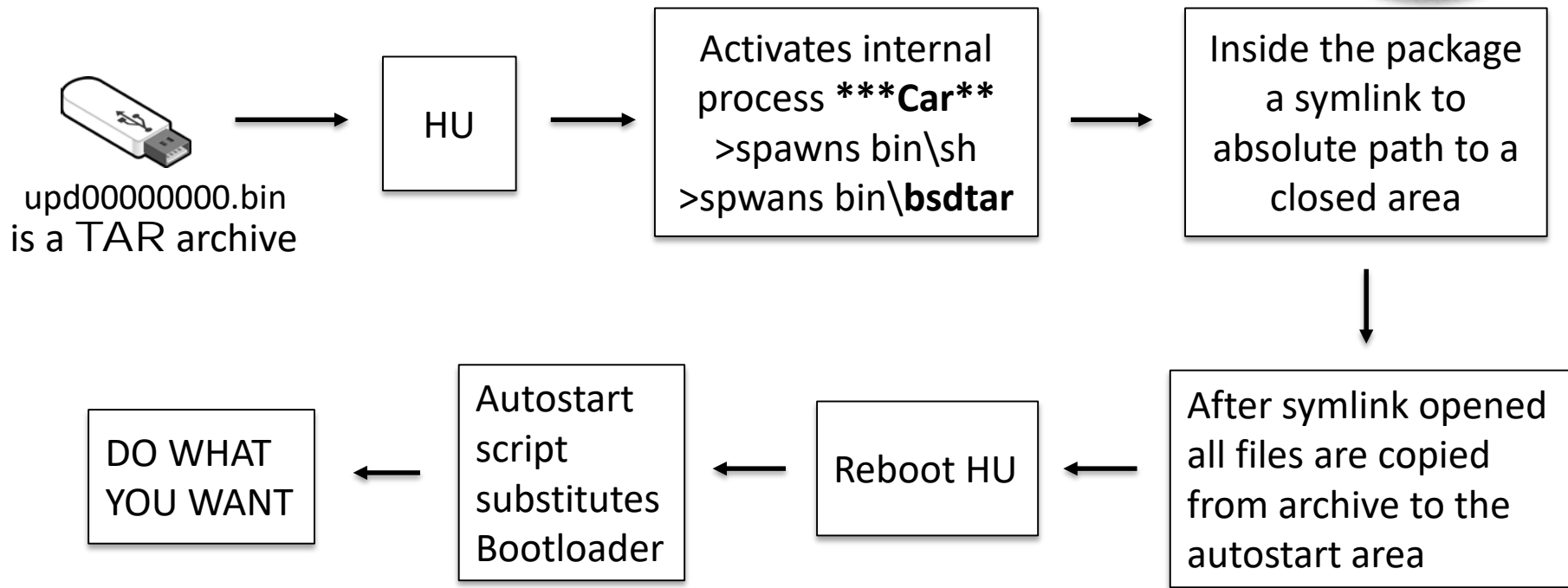
*<https://author-alarm.ru/informatsiya/novosti/autostart-my-uvelichili-kolichestvo-podderzhivaemyh-modelej>

Standard attack schema exploiting vulnerabilities in the USB stack



Reboot HU

Anatomy of attack



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

Example



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.