



WORLD SUMMIT ON  
THE INFORMATION SOCIETY

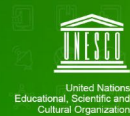
# WSIS FORUM 2021

Starting from January  
Final Week 17-21 May 2021

Coordinated by



Organized by



[www.wsis.org/forum](http://www.wsis.org/forum)

# Practice on Security Standards for Connected Vehicles Against Attacks

**Minrui Yan**

Head of Security Research  
Smart Car Security Business Unit  
360 Group

# Background

**Increasing Connectivity => Increasing Risks**



**Attack connected car**



**Lives**



**Personal assets**

**German Industry: estimated Euro 50B annual Damage from Hacking**

**China Development Commission: Annually increase 10 million connected cars by 2020**

# More Hacking Cases

**WIRED** Hackers Remotely Kill a Jeep on the Highway—With Me in It

ANDY GREENBERG SECURITY 07.21.15 6:00 AM

## HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

Technology iPhone Android

### BMW ConnectedDrive has... cars exposed to remote u...

News World Business Fintech Politics Technology Science Sport Entertainment

International Business

TESLA Patches Vulnerabilities that Allowed Remote Takeover of...

ANDY GREENBERG SECURITY 09.10.15 7:00 AM

## GM TOOK 5 YEARS TO FIX A FULL-TAKEOVER HACK IN MILLIONS OF ONSTAR CARS

TESLA RESPONDS TO CHINESE HACK WITH A MAJOR SECURITY UPGRADE

Technology CyberSecurity

### Hackers can control I...

DAIMLER Global Media Site

START COMPANY BRANDS & PRODUCTS TECHNOLOGY CLASSIC MOTORSPORTS SALES GERMANY

Mercedes-Benz and 360 Group to join forces: Mercedes-Benz and 360 Group with its Cyber Security Brain work together to strengthen car IT security for industry

16. December 2019 Beijing, Zhongguo

COMBITECH

# What We Are

- 360
  - The Biggest Security Company in China
  
- 360 Sky-Go Car Security Team
  - 82% market share on Cybersecurity of Connected Cars in China
  - Many Security Research Cases on Smart Cars
  - Vulnerability Discovery on Android, Linux, QNX, etc.
  - The Largest Malware Sample and Attack Behaviour Database



# What We Have Done



October 18, 2019



## Tesla Security Researcher Hall of Fame

Tesla appreciates and wants to recognize the contributions of security researchers. If you are the first researcher to identify a vulnerability, we will list your name in our Hall of Fame (unless you would prefer to remain anonymous). You may be awarded an award if you are the first researcher to report one of the top 3 confirmed vulnerabilities in a calendar quarter. Your Responsible Disclosure Guidelines (above) to be considered for our Hall of Fame and top 3 awards.

2018	UnicornTeam	Jun Li (@bravo_fighter), Qing Yang (@lrSmith), Yingtao Zeng, Chaoran Wang
2017	Keen Security Lab	Tencent for CVE-2017-9983 and CVE-2017-6261
2016	Keen Security Lab	Tencent
	Skygo Team, USSlab	Qihoo360, Zhejiang University
2014	Eusebiu Blindu	@testalways
	Muhammed Gazzaly	@gazy
	Jianhao Liu	Qihoo 360 Adlab
	Jiaheng Wang	Zhejiang University
	Yanqing Wu	Zhejiang University
	Wenyuan Xu	Zhejiang University

ATT:

Dear Mr. Yan,

Dear colleagues from Sky-Go team,

With this letter, we would like to thank you for the excellent cooperation and collaboration between our companies. Proactive identification of vulnerabilities is essential to protect our customers and their vehicles. Therefore, Mercedes-Benz has always attached great importance to the relevant work, and values the support and collaboration from industry experts such as Qihoo 360 with the Sky-Go team.

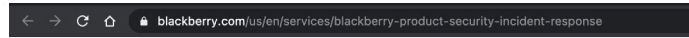
During our cooperation, we have always experienced your company as a valuable and inspiring partner. This applies especially to the field of vehicle cyber security led by your Sky-Go team.

Taking this opportunity, we would like to emphasize that we highly appreciate your expertise and the effort you have put to help further secure our vehicles and we look forward to our joint workshop and further discussions.

With my warmest regards,

Adi Ofek

CarIT Security Mandate, Mercedes-Benz Cars



## Acknowledgements

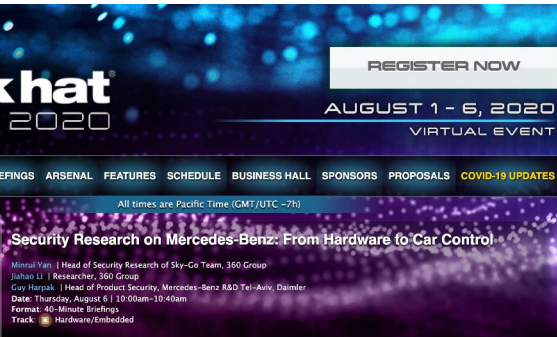
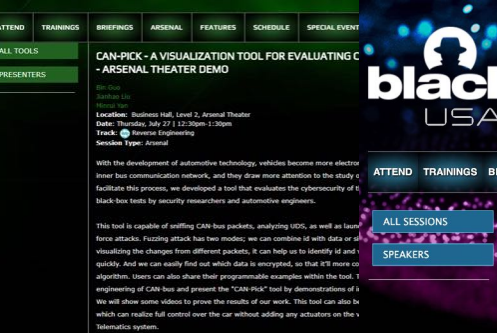
The BlackBerry PSIRT thanks the following people and organizations for reporting security issues under our customers.

\* - Identifies "Super Finder Status", signifying the finder has reported three or more security issues to the

⊕ Acknowledgements 2021

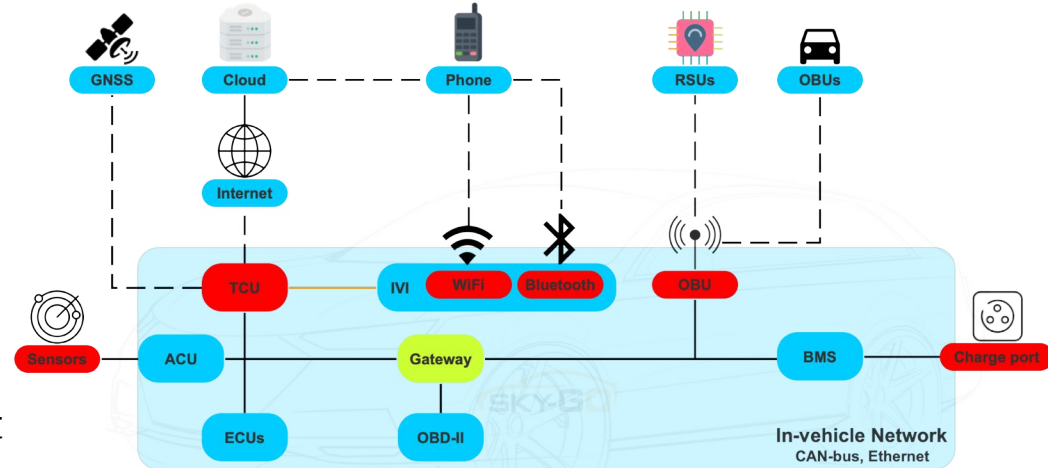
⊖ Acknowledgements 2020

- Harshal S. Sharma - <https://www.linkedin.com/in/harshalss-war10ck/>
- ahmad alassaf - <https://www.linkedin.com/mwite/in/ahmad-alassaf-638112184>
- Pritam Dash - <https://linkedin.com/in/pritam-dash-116931171/>
- Xie Ziming and Yan Minrui, 360 SkyGo Team
- Naveen Kumawat(nvk) - <https://twitter.com/nvkux>
- Jeya Seelan S - <https://www.linkedin.com/in/jeyaseelans>
- Omar Khaled Amin ( powerjacob1 )
- Nandigama Sai Shankar - <https://www.linkedin.com/in/nandigama-sai-shankar-38b562147>
- Kirtan Patel - <https://www.linkedin.com/in/kirtan-patel-02a239166>
- Talib Nadeem Usmani, Honeywell Cybersecurity CoE - HCE - <https://www.linkedin.com/in/talib>
- Pankaj Upadhyay\* - <https://pankajupadhyay.in/>
- Mohamed Saqib C - <https://www.linkedin.com/in/mohamed-saqib>
- Drew Green & Ken Smith, Bank of America



# What We Think The Attack Surfaces of Smart Car

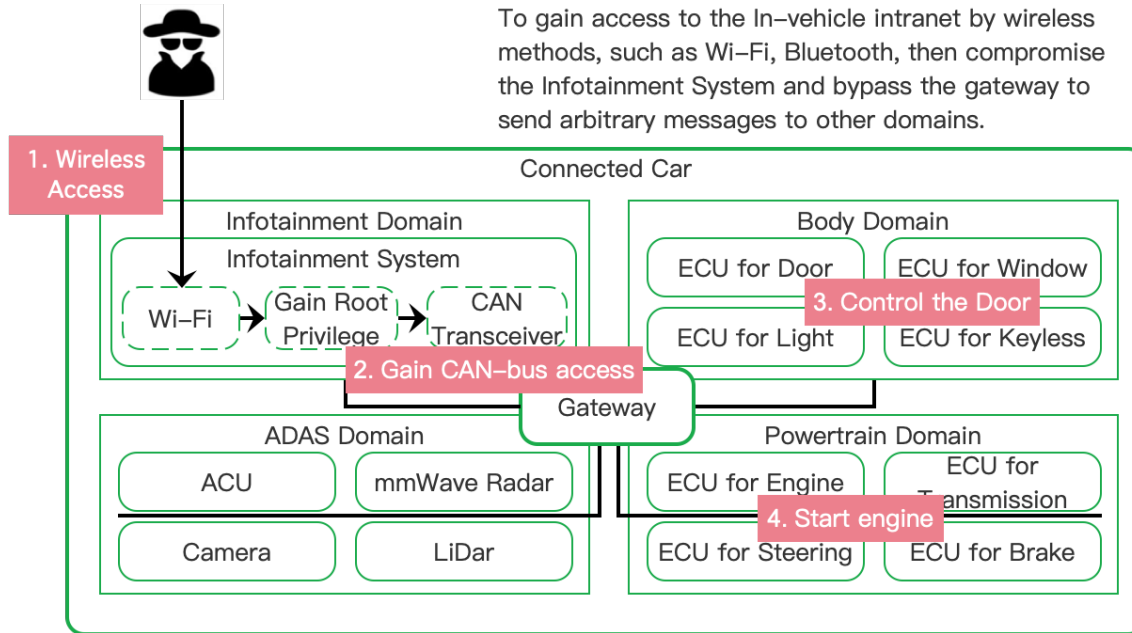
- **Cloud Side**
  - Car Backend Services
  - Communication Channel
- **Vehicle Side**
  - GNSS
  - Charging System
  - Smart ECUs
    - Infotainment System
    - Telematics Control Unit
  - Autonomous driving
    - Sensors
  - V2X
    - OBU
- **Road Side**
  - RSU



# What We Researched – Near Field Car Control

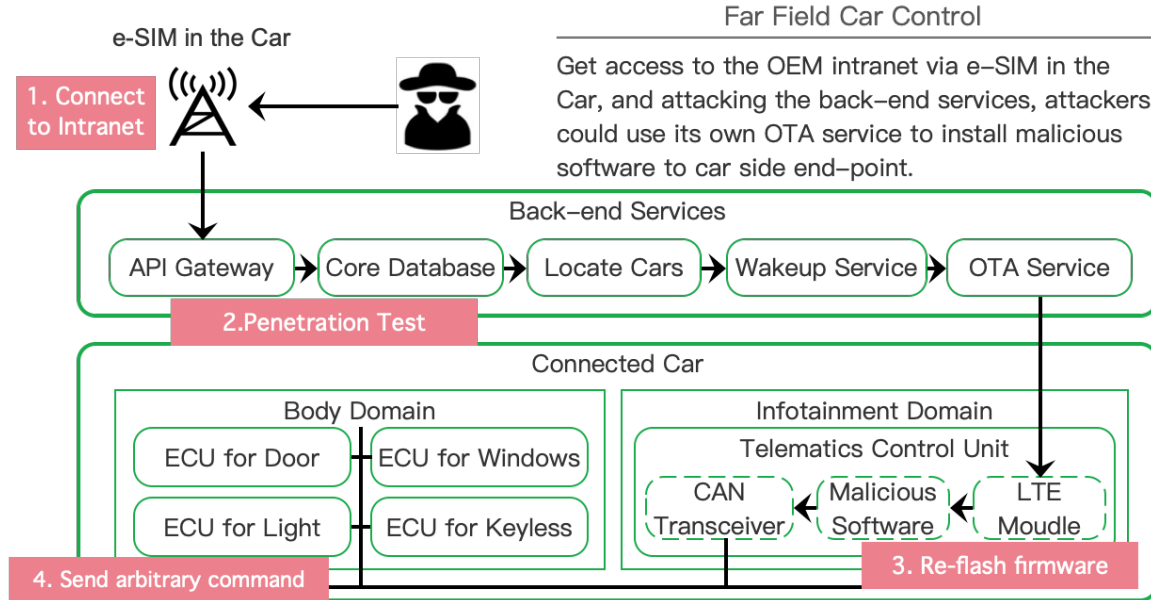
## Near Field Car Control

To gain access to the In-vehicle intranet by wireless methods, such as Wi-Fi, Bluetooth, then compromise the Infotainment System and bypass the gateway to send arbitrary messages to other domains.





# What We Researched – Far Field Car Control

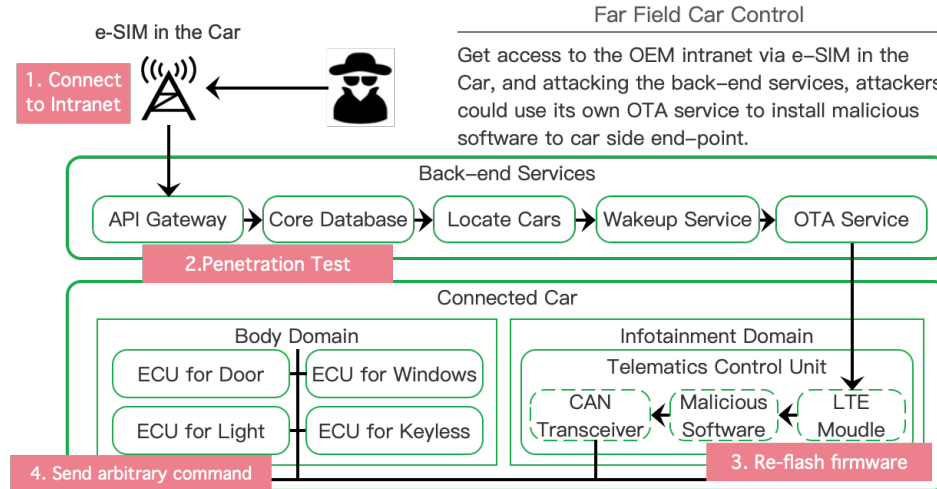


# How To Find Misbehaviour – Far Field Car Control

Normal Chain:

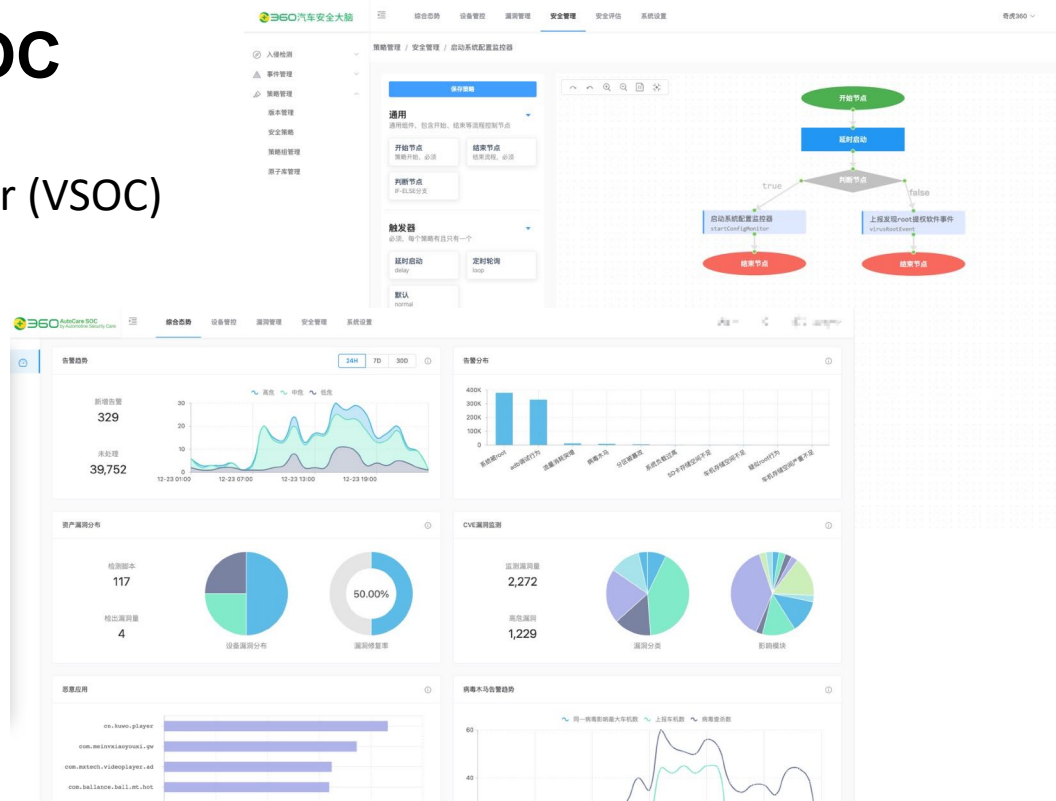


Attack Chain:



# What We Have Built - VSOC

- Smart Car Security Operations Center (VSOC)
  - Data Collection Module
  - Event Handling Module
  - Threat Intelligence Module
  - Misbehaviour Detection Module
  - SOAR
  - Response Center
    - Experts Team
    - Secure OTA

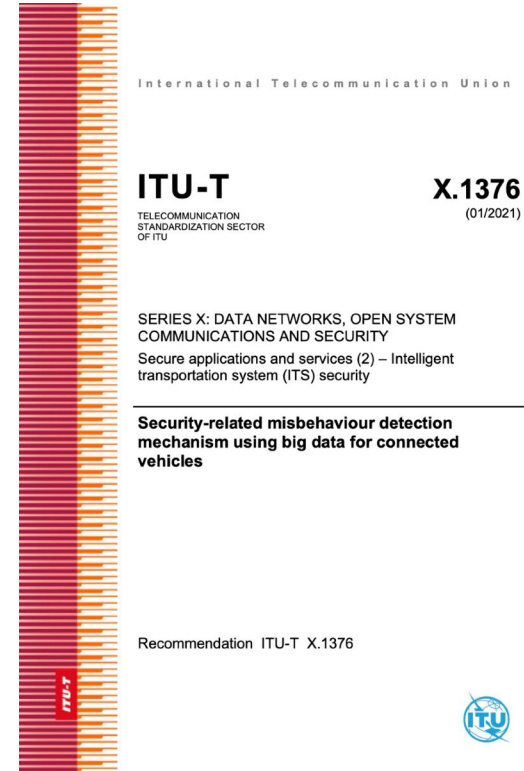


\*According to ITU-T X.1376, WP.29 CSMS

# ITU-T X.1376

*Security-related misbehaviour detection mechanism using big data for connected vehicles*

- Write this standard base on
  - Our Researches
  - Our Evaluation Cases
  - Our Attack Data
  - Our Virus Samples
  - Our Solution and Services



International Telecommunication Union

**ITU-T**  
TELECOMMUNICATION  
STANDARDIZATION SECTOR  
OF ITU


**X.1376**  
(01/2021)

SERIES X: DATA NETWORKS, OPEN SYSTEM  
COMMUNICATIONS AND SECURITY  
Secure applications and services (2) – Intelligent  
transportation system (ITS) security

---

**Security-related misbehaviour detection  
mechanism using big data for connected  
vehicles**

Recommendation ITU-T X.1376



# What We Contributed – International Standards

- ITU-T
  - ITU-T X.1376 *Security-related misbehaviour detection mechanism for connected vehicles*
- ISO
  - ISO/SAE 21434
  - PWI 5888 *Evaluation criteria for connected vehicle*

# What We Are Doing

- Still Working on New Technique Research
- Contribute Our Knowledge to the Industry
- Lower the Threshold of Car Security Research
- Help Industry to Improve Their Security Capability

# Thanks for Your Listening

Email: [minruiyan@gmail.com](mailto:minruiyan@gmail.com)

# WORLD SUMMIT ON THE INFORMATION SOCIETY



Coordinated by



Organized by

