Modern Car Security

Jun Li @bravo_fighter

Unicorn Team

360 Security Technology

JD-HITBSECCONF 2018 BEIJING

Who Am I ?

Member of

Founder of

Speaker of

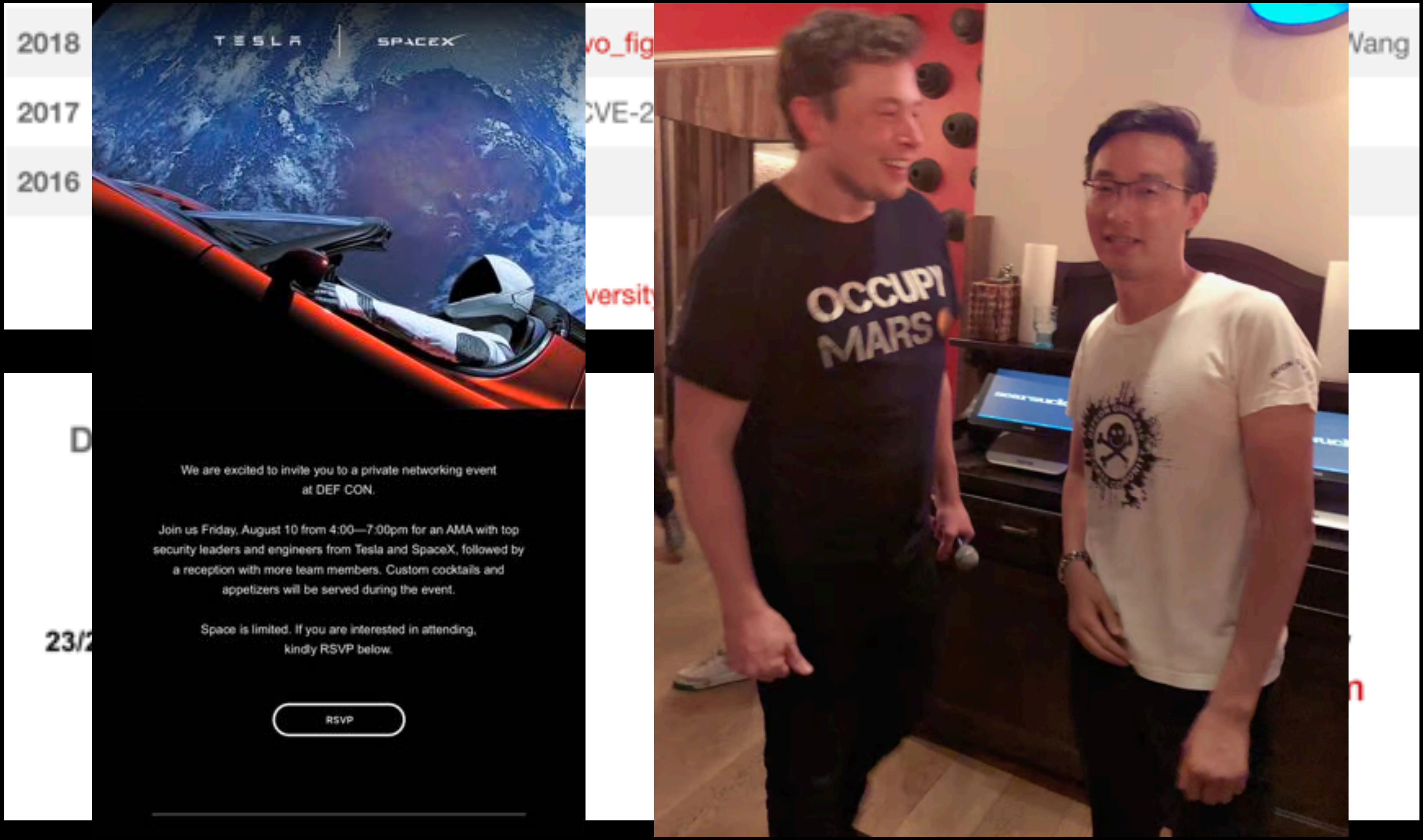
. . .

Who Am I ?

Author&Co-author of

Who Am I ?

Contributor of



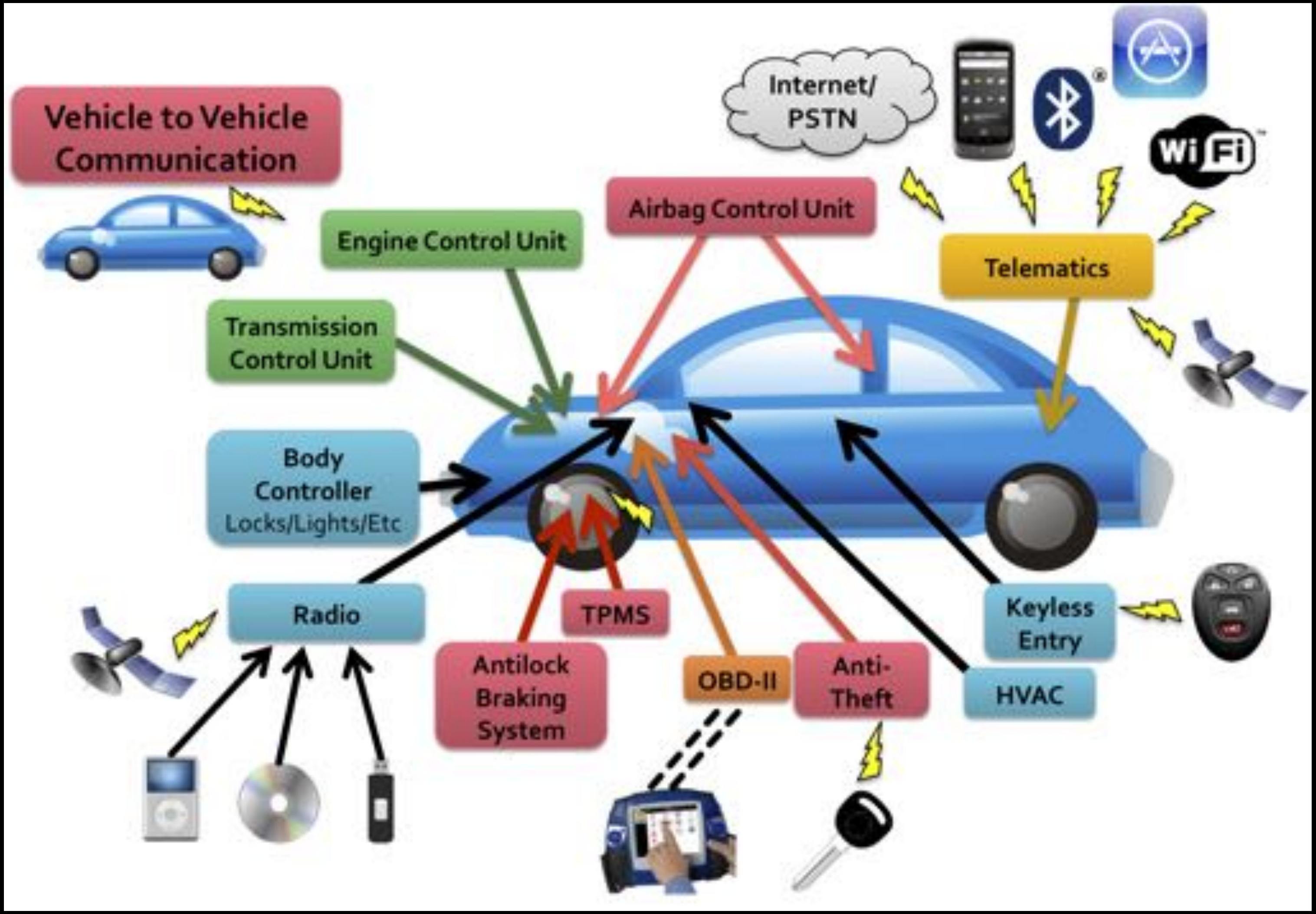
What I am going to talk ？

- Intro of Modern Cars
- Attack Surface of Modern Cars
- The Past：Some Vulnerabilities
- The Present： Some Remediations
- The Future：Some Suggestions

Intro of Modern Cars

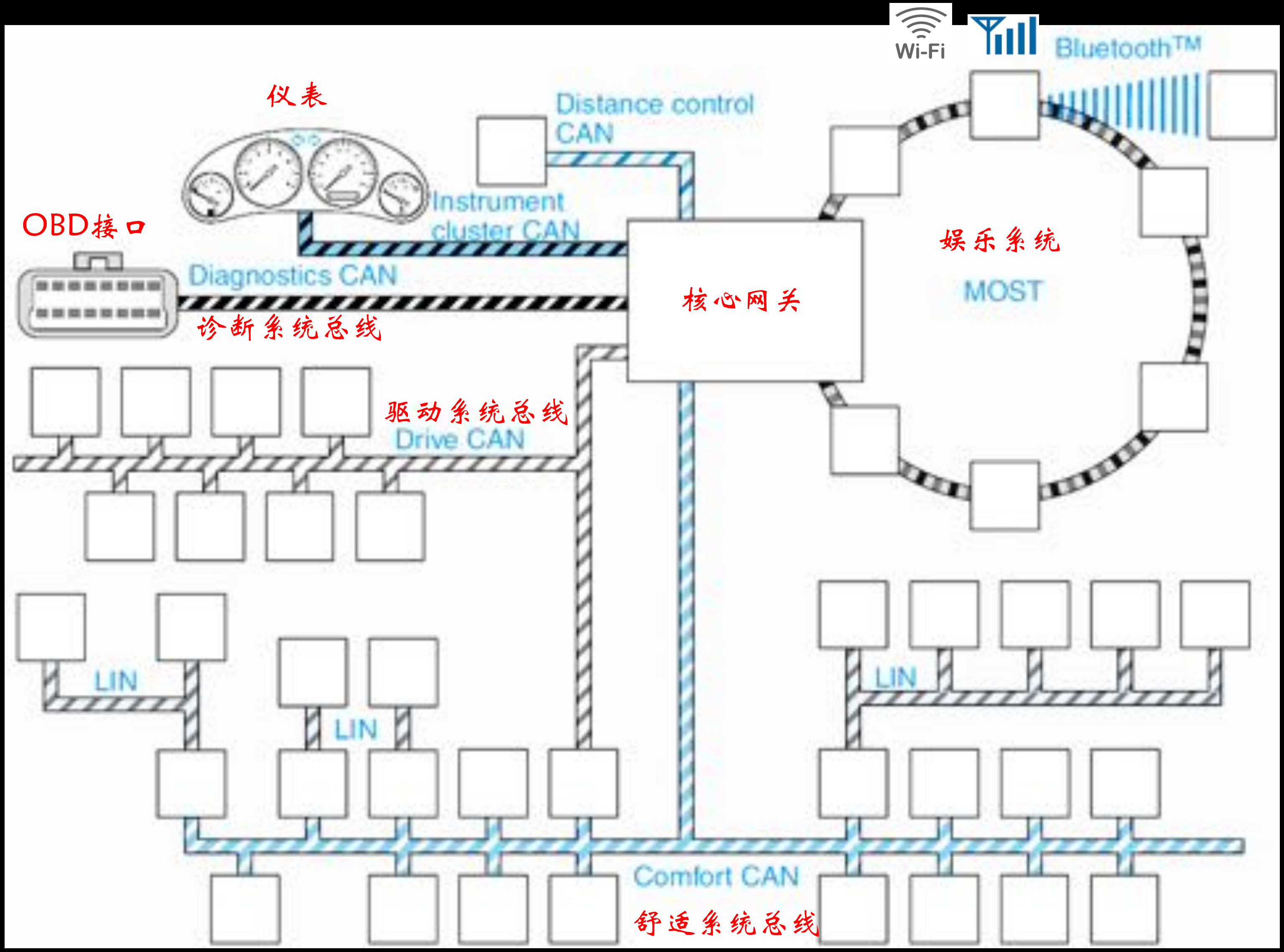
- Intro of Modern Cars
- Attack Surface of Modern Cars
- The Past：Some Vulnerabilities
- The Present： Some Remediations
- The Future：Some Suggestions

Modern Cars
Electronized & Connected



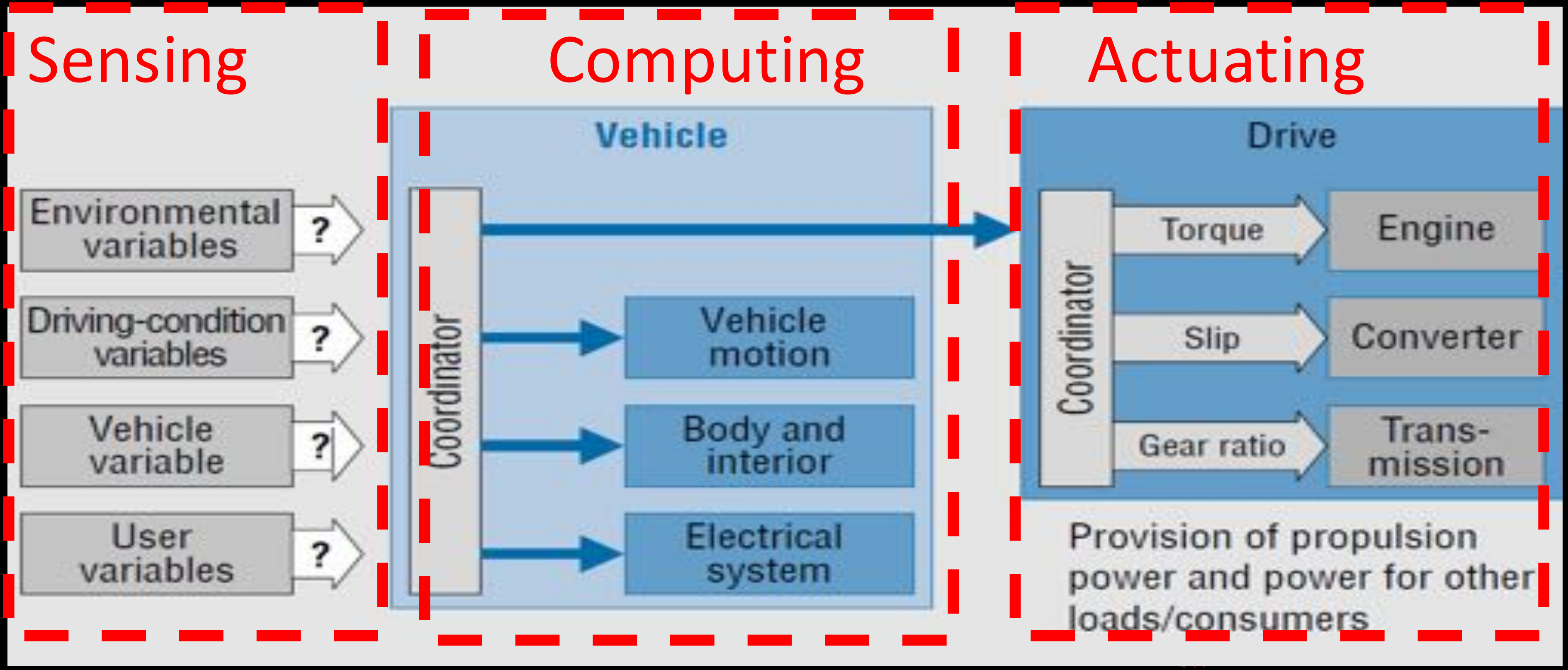
http://www.autosec.org/pubs/cars-usenixsec2011.pdf

Modern Cars
Electronized & Connected



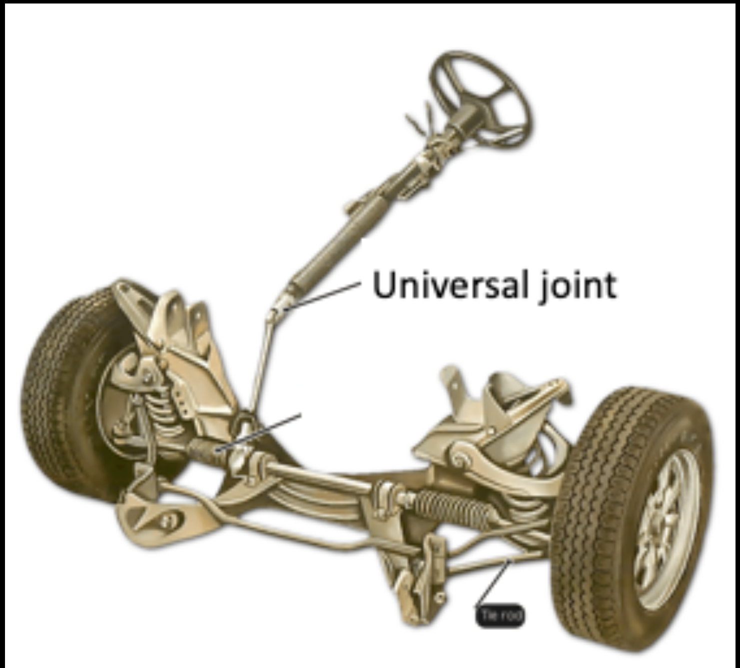
MOST
LIN
CAN
FlexRay
Bluetooth
Wifi
SubGHz

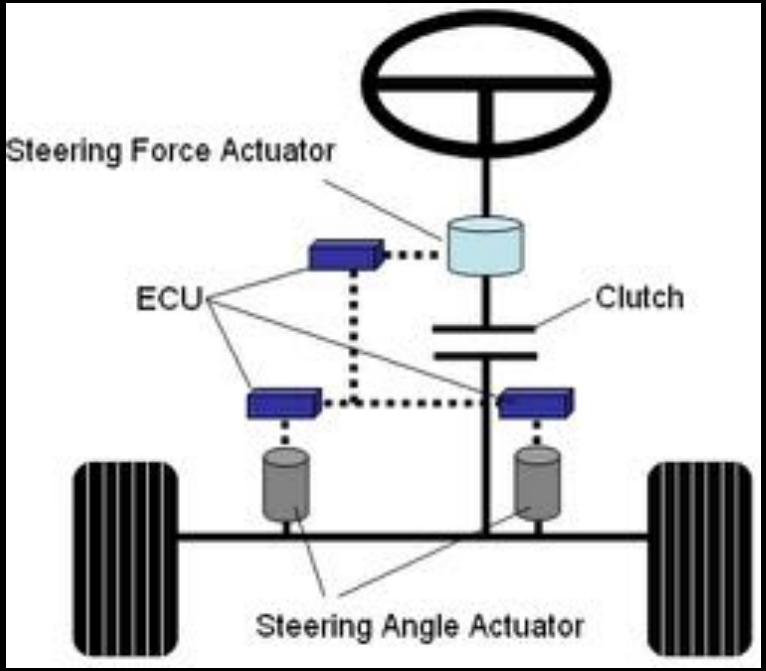
Modern Cars
Electronized & Connected



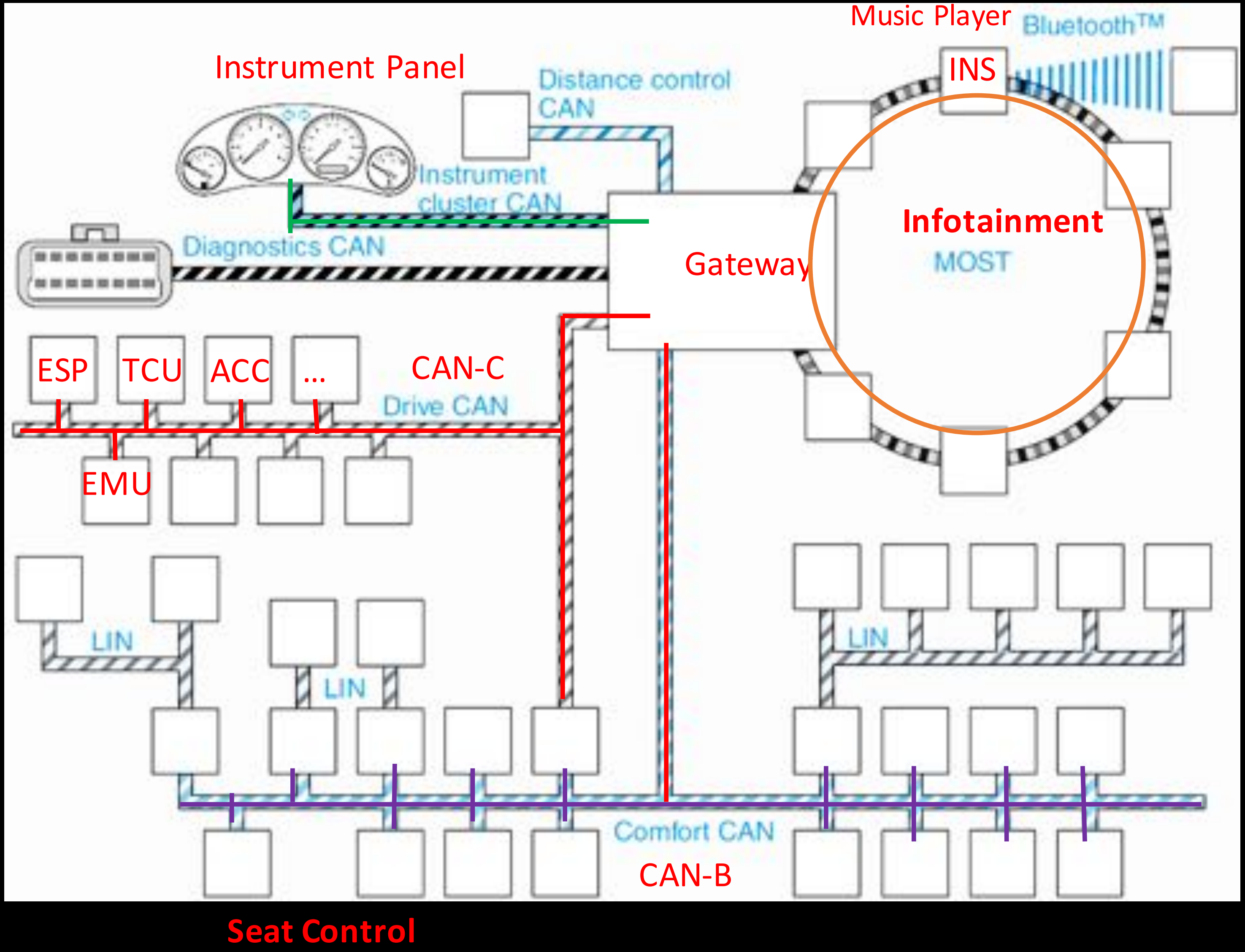
Modern Cars
Electronized & Connected

X-by –wire





Modern Cars
Electronized & Connected



ESP (electronic stability program)

EMU (engine management system)

TCU (transmission control unit)

ACC (adaptive cruise control)

INS (Inertial navigation system)

Modern Cars
Electronized & Connected

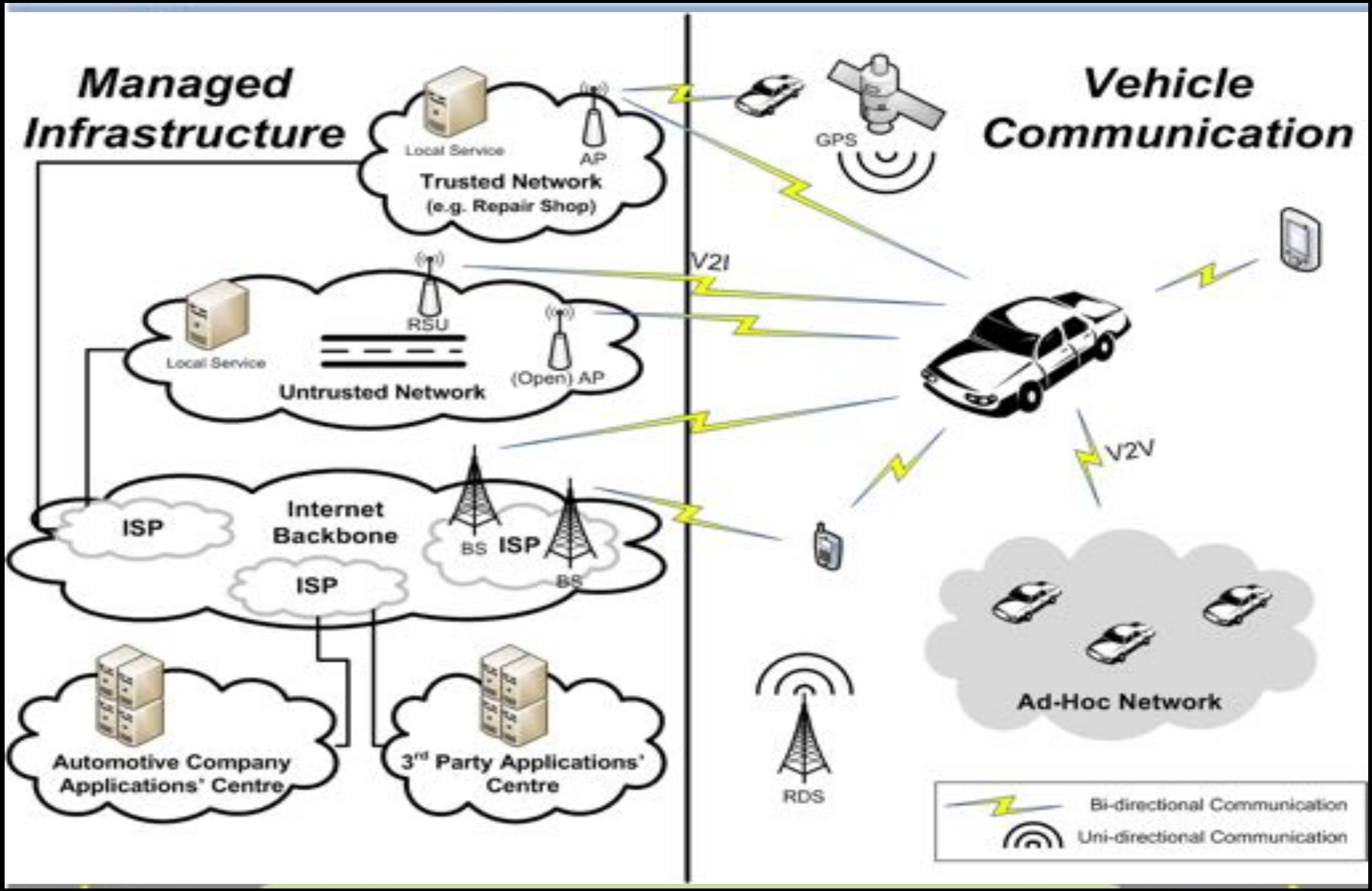
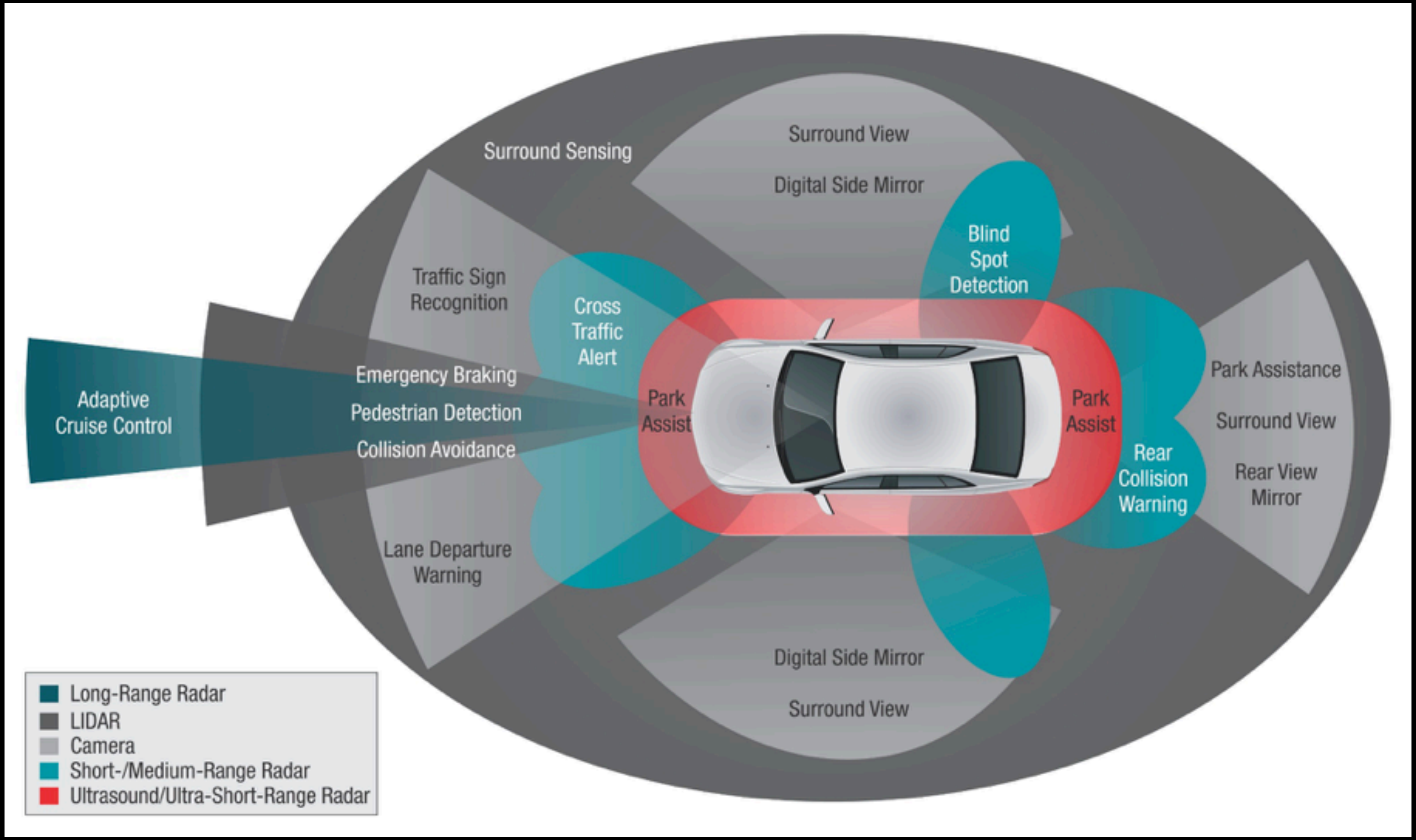


Image source :http://telematicswire.net/connected-cars-and-the-role-of-telematics-in-the-future-of-intelligent-transport/

Self-driving Cars
With Various Sensors



Self-driving Cars
With Various Sensors

Attack Surface of Modern Cars

- Intro of Modern Cars
- Attack Surface of Modern Cars
- The Past：Some Vulnerabilities
- The Present： Some Remediations
- The Future：Some Suggestions

Attack Surface of Modern Cars

Supply Chain Attack

eg.
Vulnerable Parts
Service Center Employee
Vulnerable Manufacture Backend
etc.

Local and Physical Attack

eg.
OBD Port
USB Port
SD Card Slots
etc.

Remote Attack

eg.
Bluetooth
Wifi
Celluar
Mobile APP
Cloud Platform
etc.

The Past：Some Vulnerabilities

- Intro of Modern Cars
- Attack Surface of Modern Cars
- The Past：Some Vulnerabilities
- The Present： Some Remediations
- The Future：Some Suggestions

Anti-theft System Security Vulnerabilities

Hitag2

DST40

Digital signature transponder
40bit key length

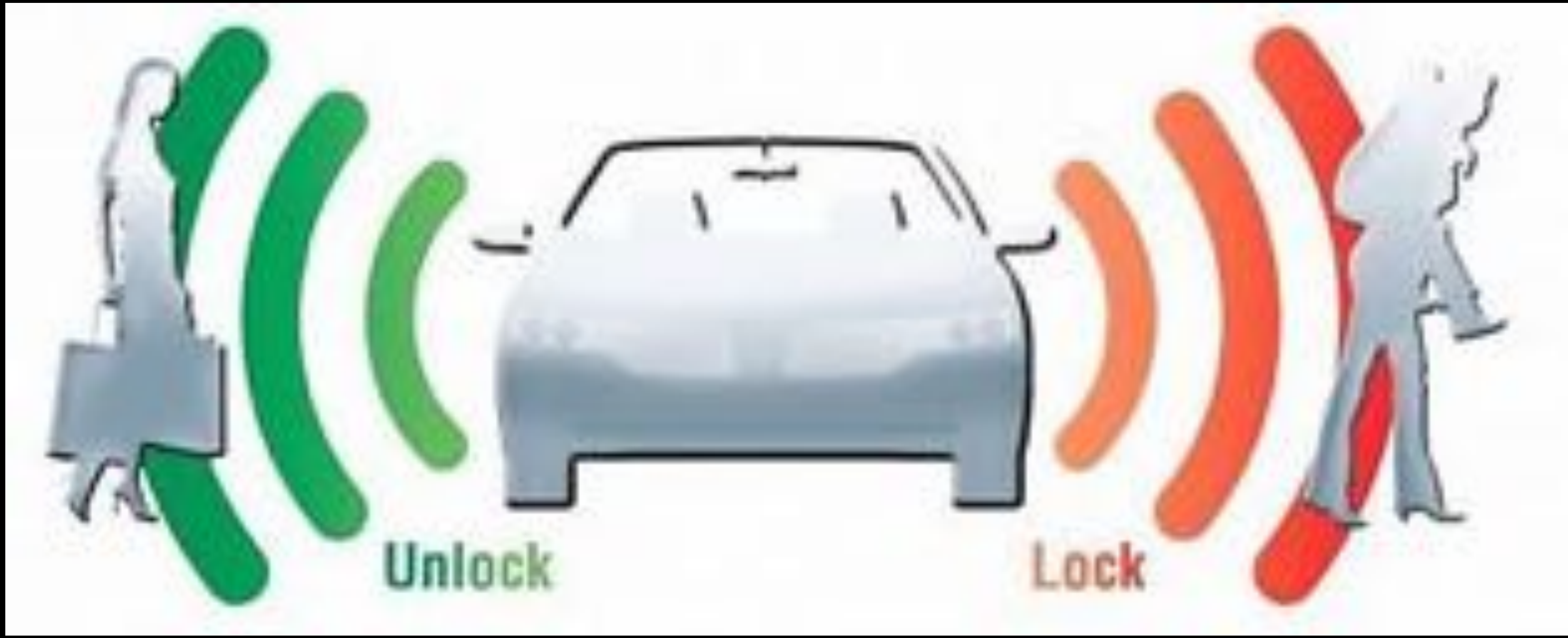
Mobile Phone (Bluetooth/Celluar)

Hitag2 is Vulnerable

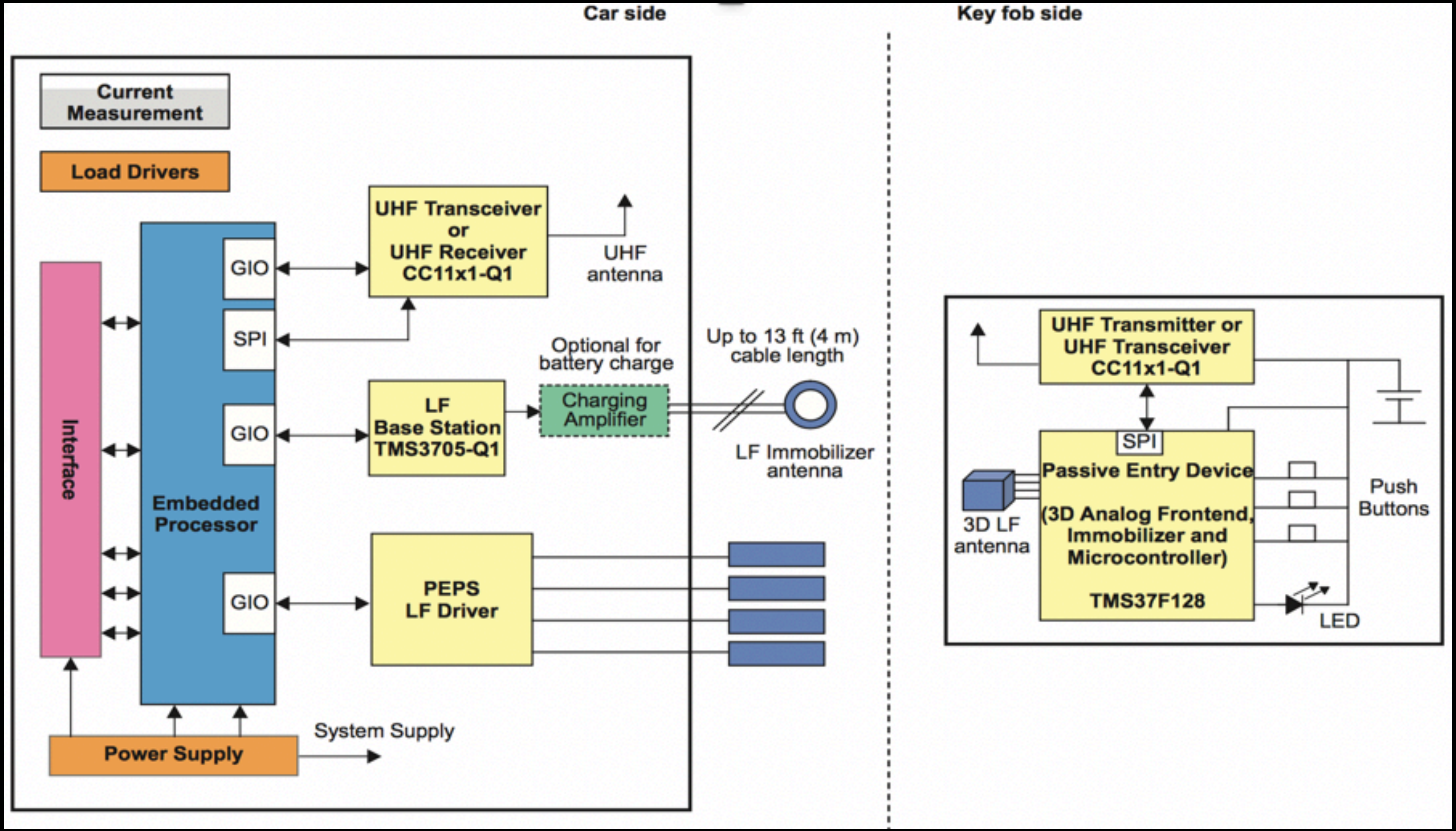
https://www.usenix.org/sites/default/files/conference/protected-files/verdult_usenixsecurity12_slides.pdf

https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final95.pdf

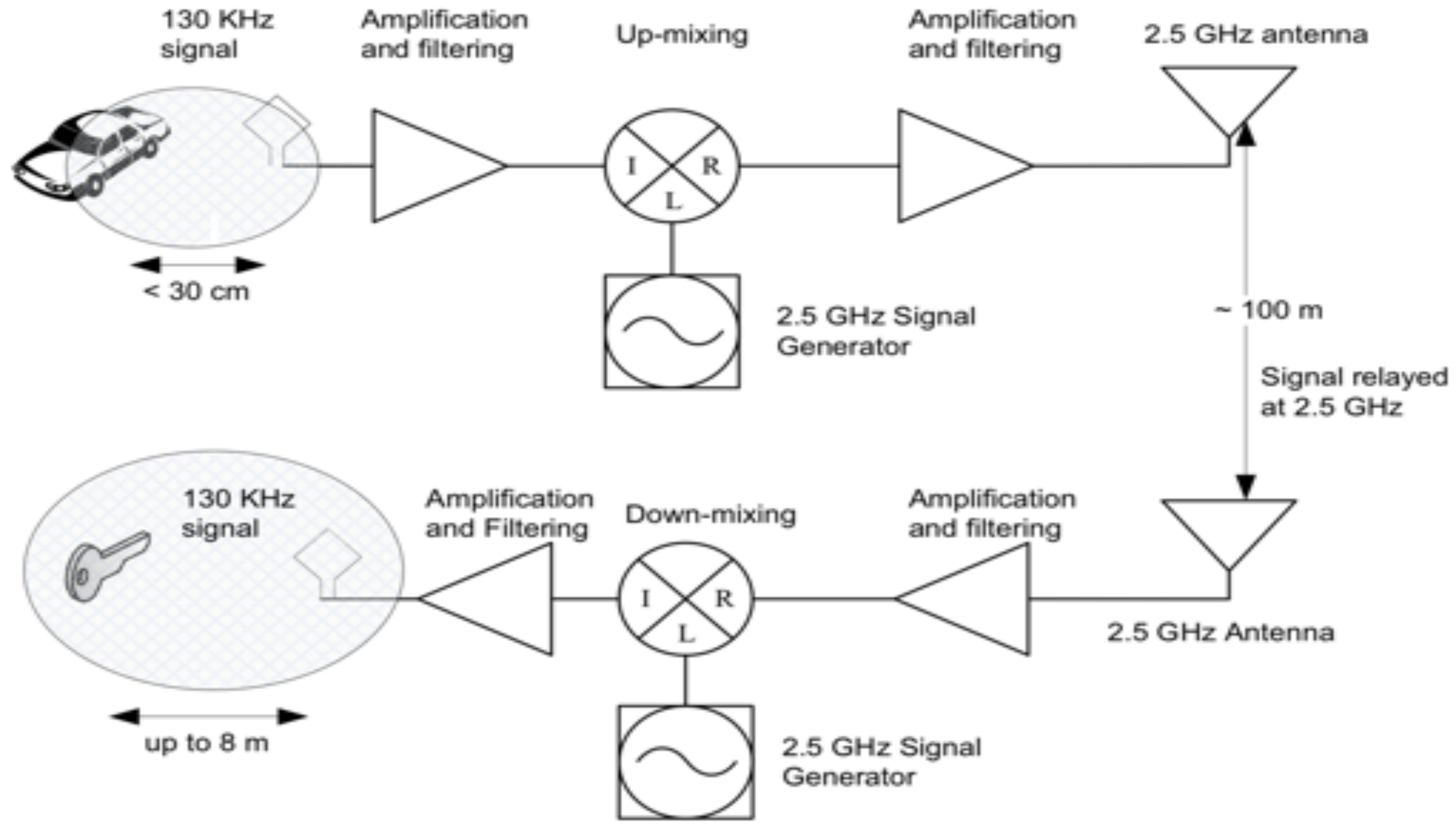
Passive Keyless Entry System
Relay Attack



Passive Keyless Entry System
Relay Attack



Passive Keyless Entry System
Relay Attack

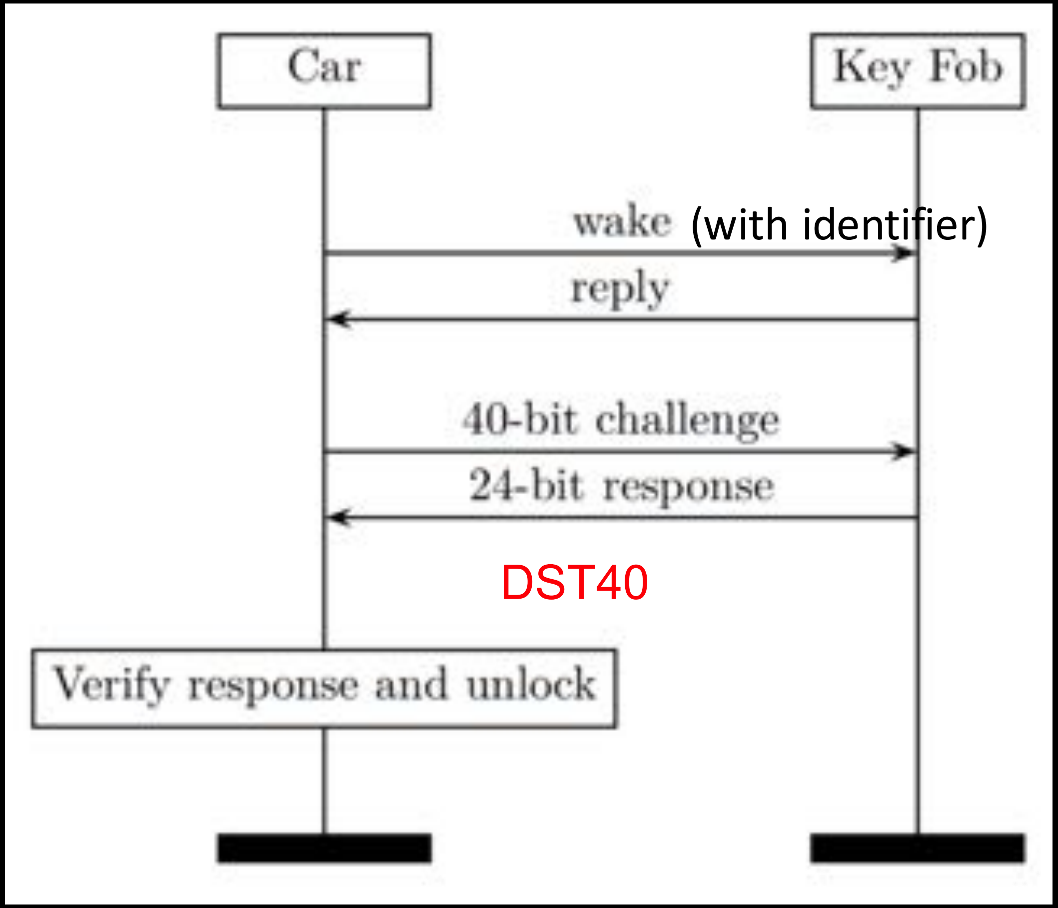


https://eprint.iacr.org/2010/332.pdf

Passive Keyless Entry System
Relay Attack

Passive Keyless Entry System Relay Attack

Passive Keyless Entry System
Key-fob Cloning Attack (DST40)



https://www.esat.kuleuven.be/cosic/fast-furious-and-insecure-passive-keyless-entry-and-start-in-modern-supercars/

Passive Keyless Entry System
Key-fob Cloning Attack (DST40)

Security Analysis of a Cryptographically-Enabled RFID Device

*Stephen C. Bono** *Matthew Green** *Adam Stubblefield** *Ari Juels*†
*Aviel D. Rubin** *Michael Szydlo*†

Abstract

We describe our success in defeating the security of an RFID device known as a Digital Signature Transponder (DST). Manufactured by Texas Instruments, DST (and variant) devices help secure millions of SpeedPass™ payment transponders and automobile ignition keys.

Our analysis of the DST involved three phases:

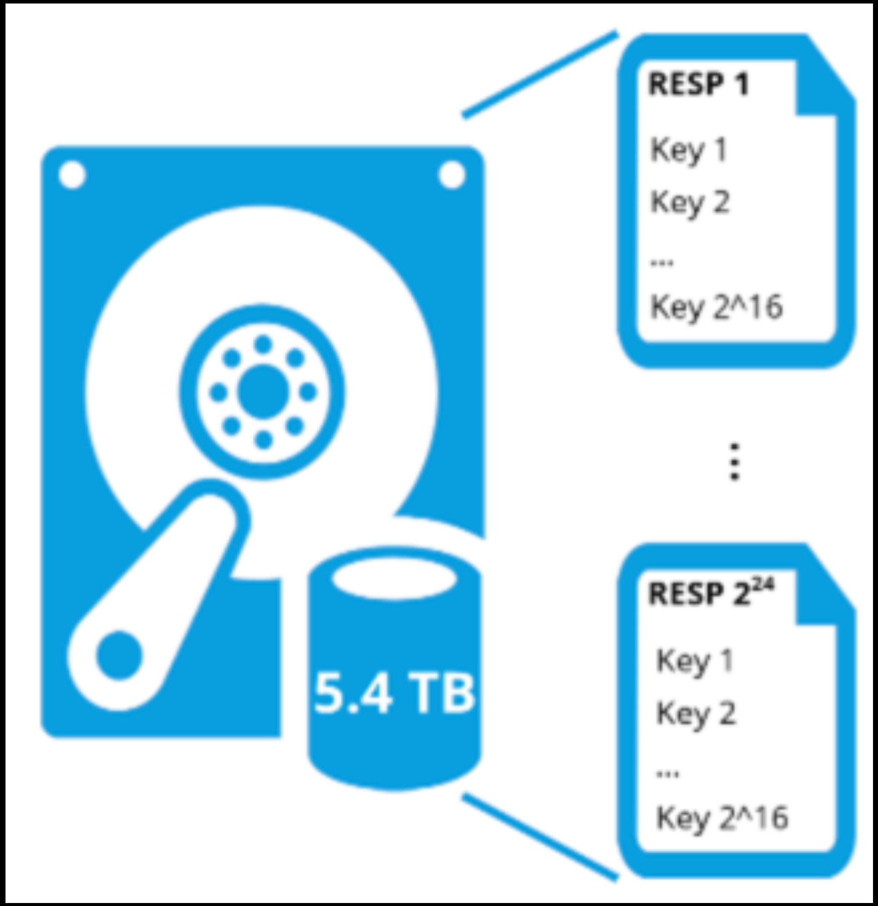
1 Introduction

Radio-Frequency IDentification (RFID) is a general term for small, wireless devices that emit unique identifiers upon interrogation by RFID readers. Ambitious deployment plans by Wal-mart and other large organizations over the next couple of years have prompted intense com-

Paper that REed DST40 in 2005 https://www.usenix.org/legacy/event/sec05/tech/bono/bono.pdf

Crypto Implementation on FPGA：https://github.com/jok40/dst40

Passive Keyless Entry System
Key-fob Cloning Attack (DST40)



https://www.esat.kuleuven.be/cosic/fast-furious-and-insecure-passive-keyless-entry-and-start-in-modern-supercars/

The Past : Some Vulnerabilities

Passive Keyless Entry System Key-fob Cloning Attack By Exploiting Vulnerable Crypto---DST40
Credit goes to Researchers from @CosicBe

Steal Cars Via Celluar Network

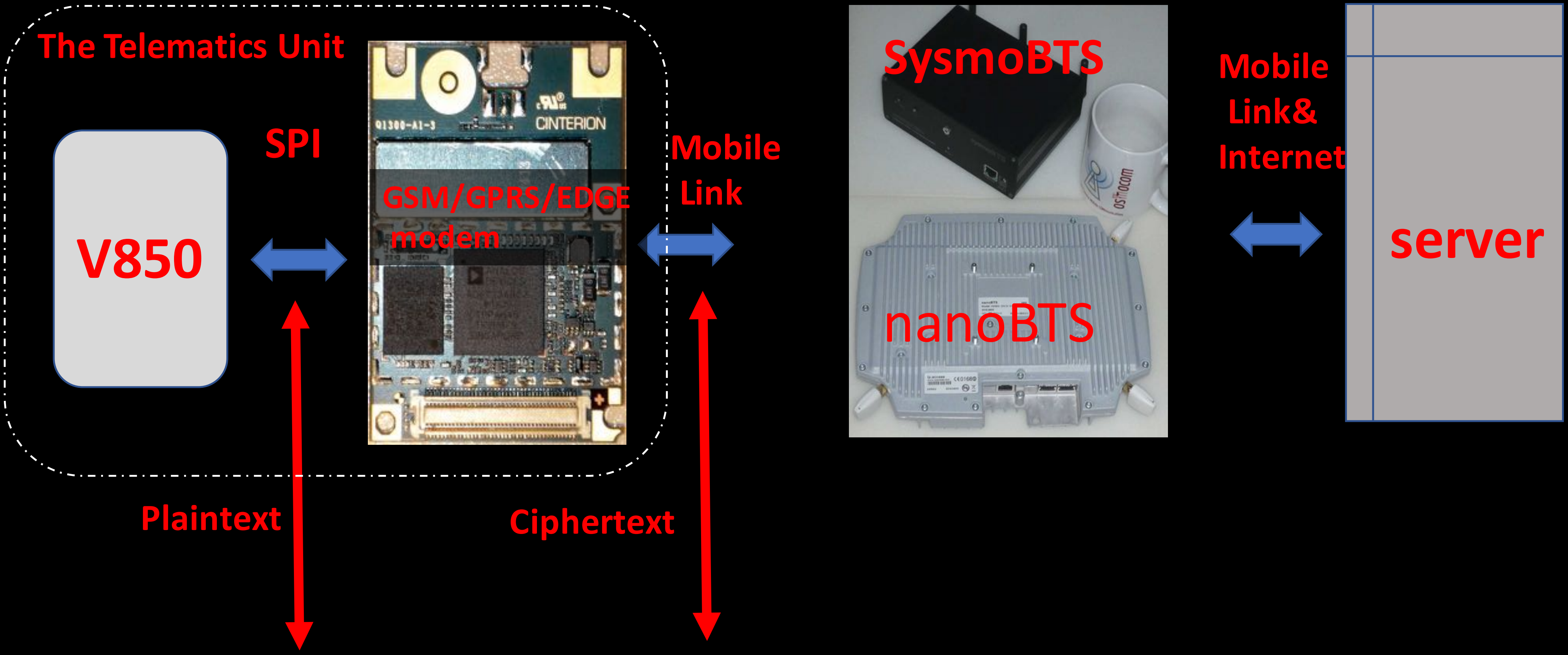
Beemer, Open Thyself! – Security vulnerabilities in BMW's ConnectedDrive

- *Deutsche Version dieses Artikels*

Cars with built-in modems are sending data to their manufacturers – German motorist's club ADAC wanted to know what exactly gets sent. c't connected ADAC with a specialist who analysed the data

https://www.heise.de/ct/artikel/Beemer-Open-Thyself-Security-vulnerabilities-in-BMW-s-ConnectedDrive-2540957.html

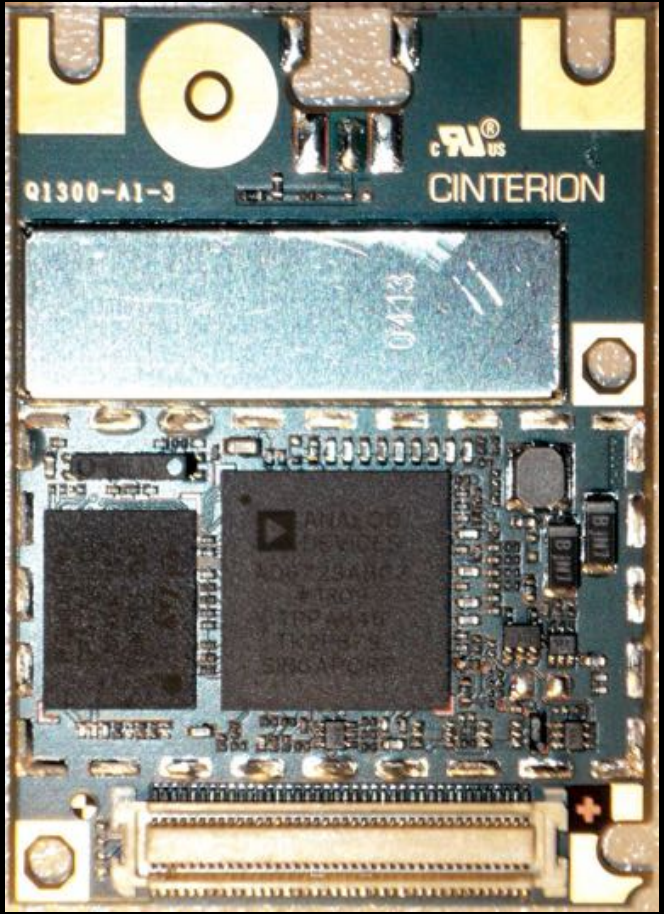
Steal Cars Via Celluar Network

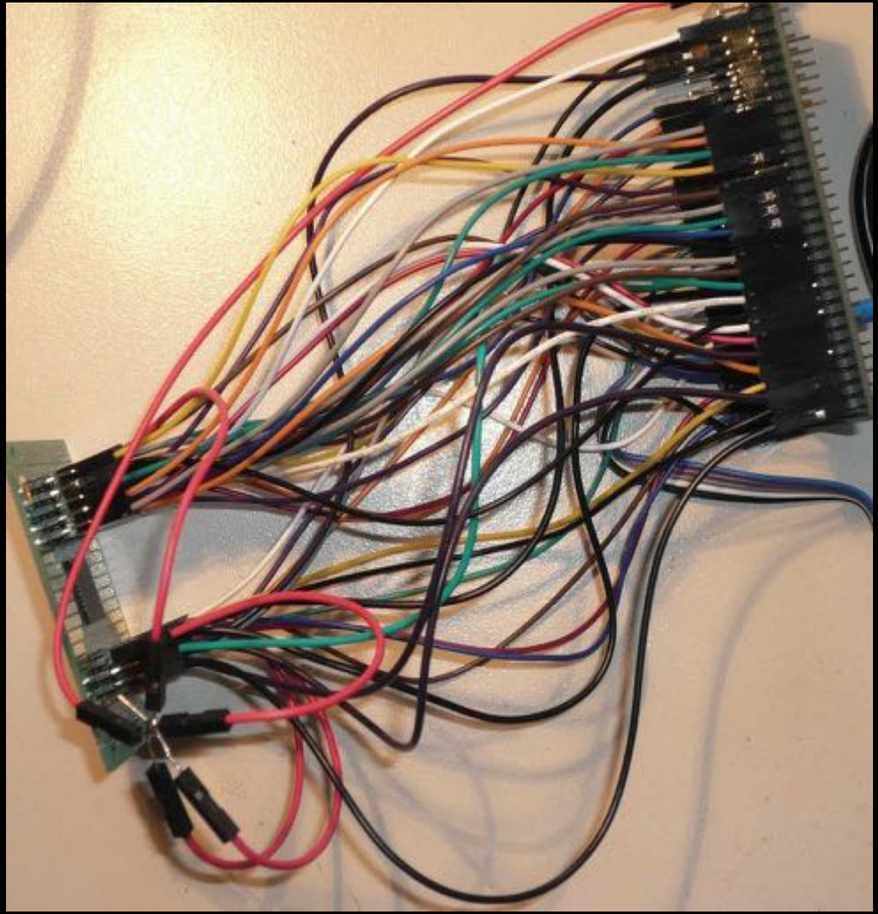


Traffic is encrypted by the modem ----> reverse engineer the modem

Steal Cars Via Celluar Network

Dump and Reverse Engineer the Firmware





Steal Cars Via Celluar Network

Discoveries in The Firmware

Encryption Algorithms：

- DES（56bit Key）
- AES128

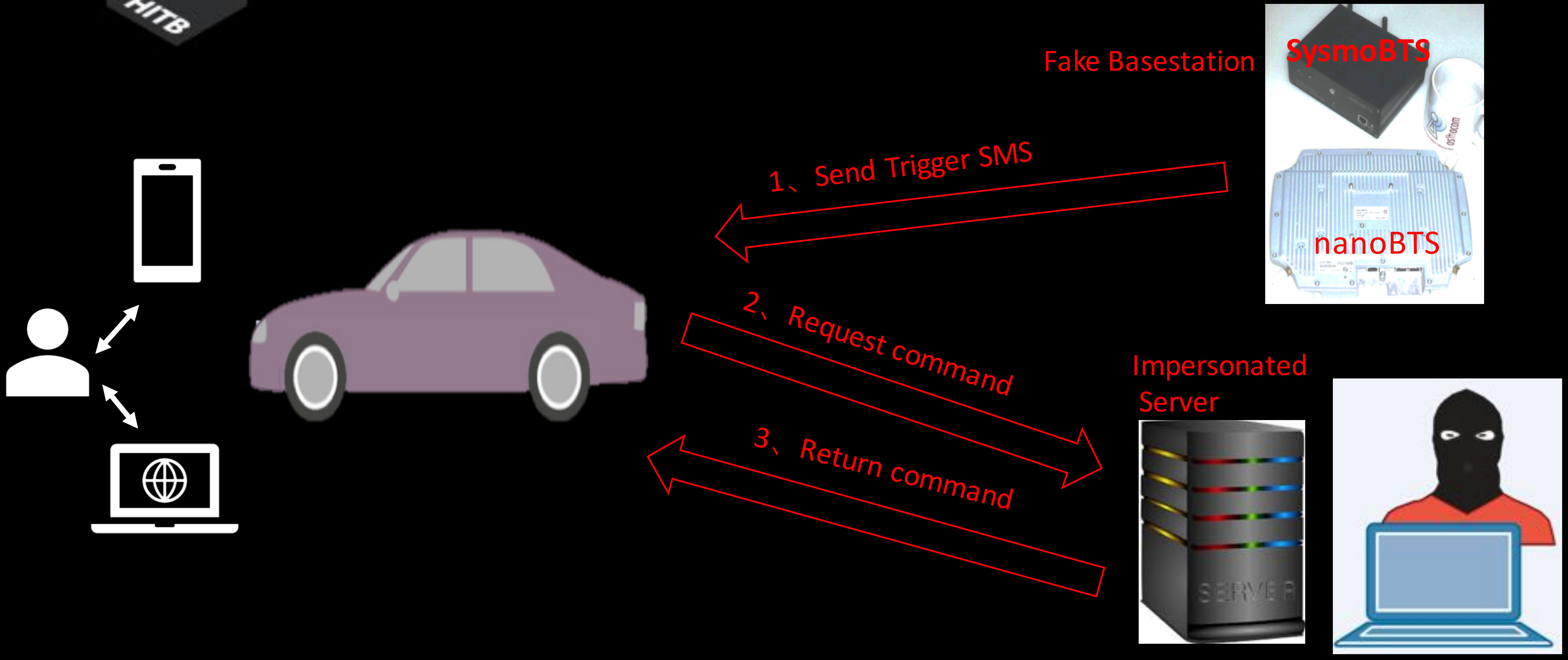
Message Signature Authentication Algorithms：

- DES CBC-MAC
- HMAC-SHA1
- HMAC-SHA256

Encryption Keys

16 Pairs of 64bit Keys

Steal Cars Via Celluar Network



Remote Physics Control

Experimental Security Analysis of a Modern Automobile

Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, and Tadayoshi Kohno
Department of Computer Science and Engineering
University of Washington
Seattle, Washington 98195–2350
Email: {supersat,aczeskis,franzi,shwetak,yoshi}@cs.washington.edu

Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage
Department of Computer Science and Engineering
University of California San Diego
La Jolla, California 92093–0404
Email: {s,dlmccoy,brian,d8anders,hovav,savage}@cs.ucsd.edu

2010

NSF

Comprehensive Experimental Analyses of Automotive Attack Surfaces

Stephen Checkoway, Damon McCoy, Brian Kantor,
Danny Anderson, Hovav Shacham, and Stefan Savage
University of California, San Diego

Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno
University of Washington

2011

Abstract

Modern automobiles are pervasively computerized, and hence potentially vulnerable to attack. However, while previous research has shown that the internal networks within some modern cars are insecure, the associated threat model — requiring prior physical access — has justifiably been viewed as unrealistic. Thus, it remains an open question if automobiles can also be susceptible to remote compromise. Our work seeks to put this question ... situation suggests a significant gap in knowledge, and one with considerable practical import. To what extent are external attacks possible, to what extent are they practical, and what vectors represent the greatest risks? Is the etiology of such vulnerabilities the same as for desktop software and can we think of defense in the same manner? Our research seeks to fill this knowledge gap through a systematic and empirical analysis of the remote attack surface of late model mass-production sedan.

Adventures in Automotive Networks and Control Units

By Dr. Charlie Miller & Chris Valasek

2012

DARPA

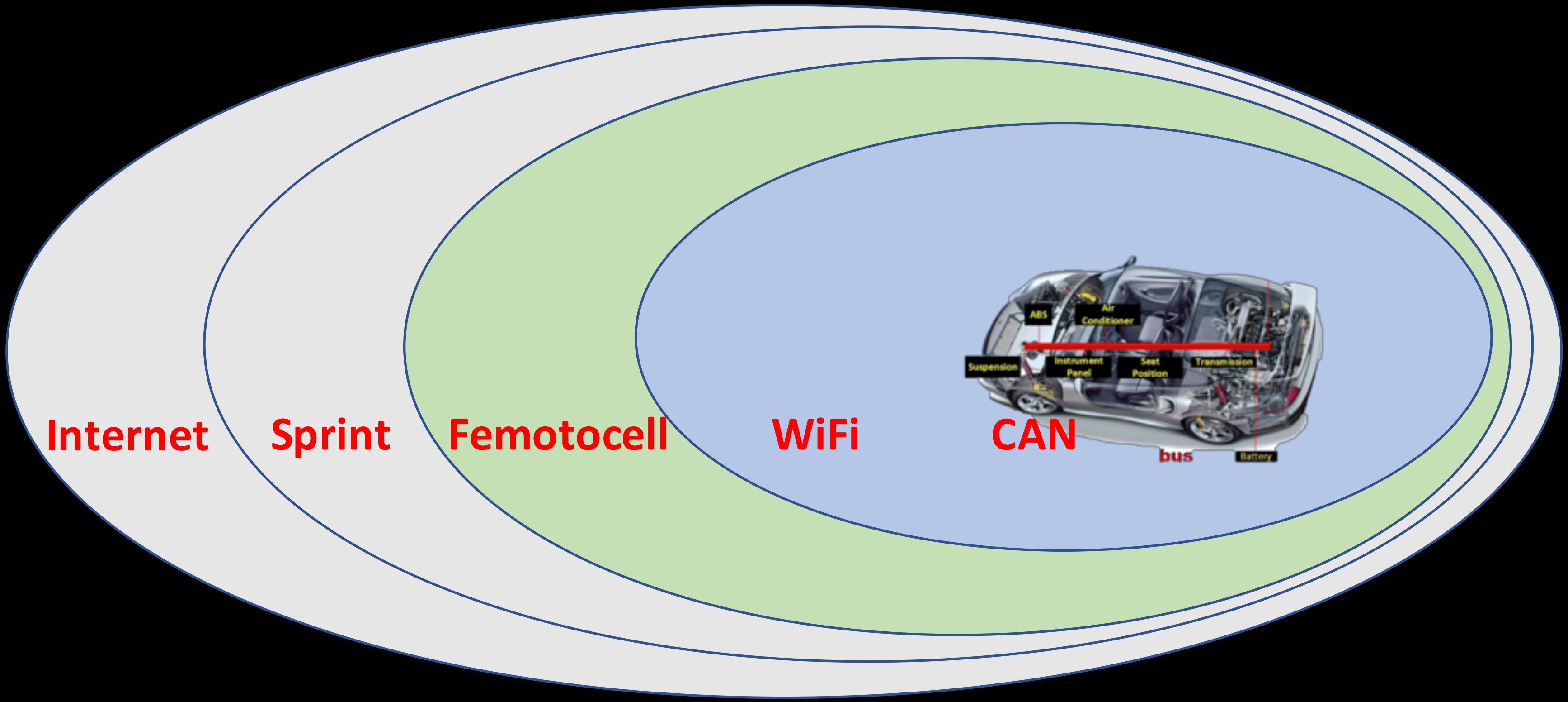
Remote Exploitation of an Unaltered Passenger Vehicle

Dr. Charlie Miller (cmiller@openrce.org)
Chris Valasek (cvalasek@gmail.com)

2015

Remote Physics Control

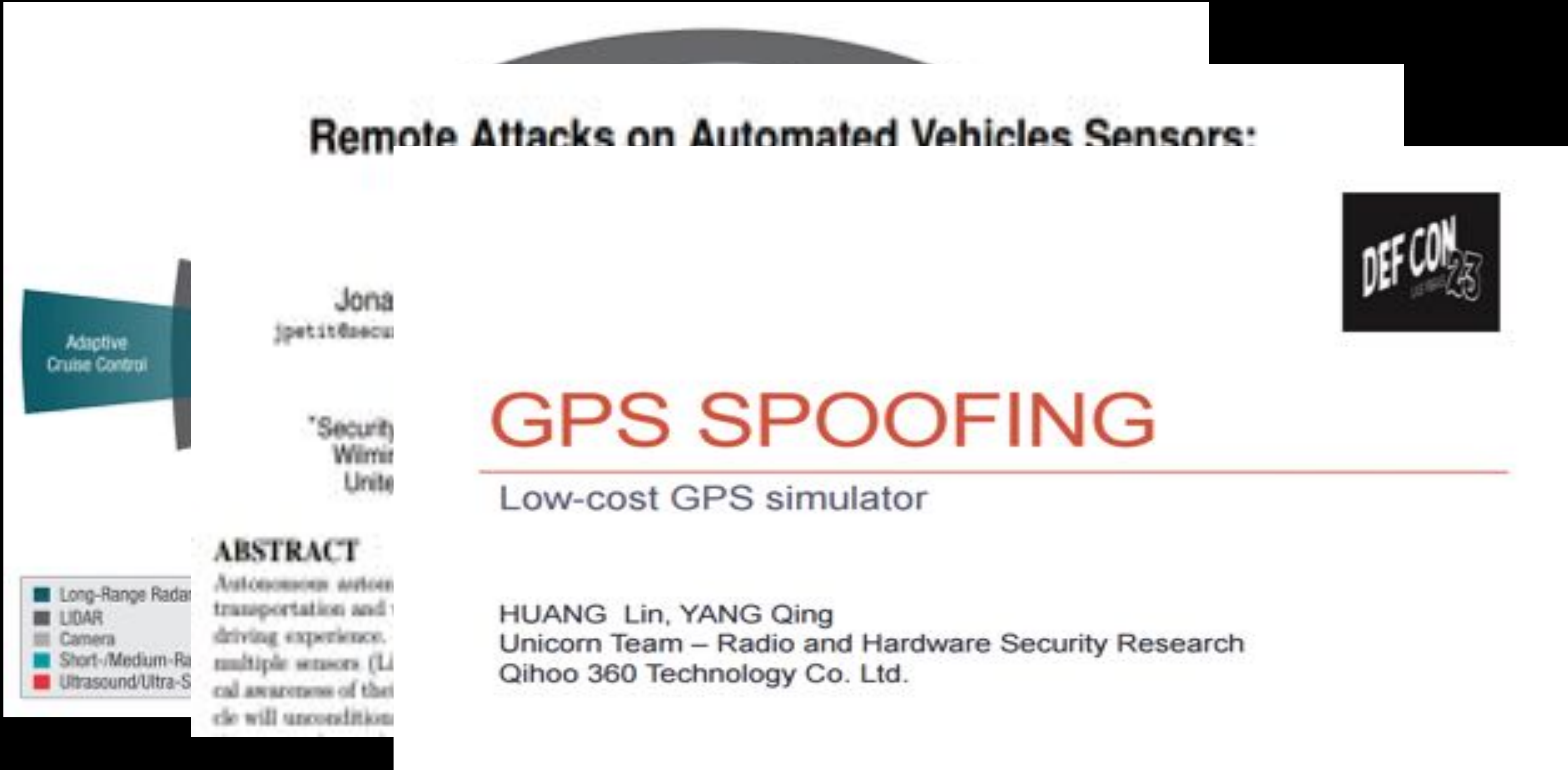
Epic eg. Jeep Uconnect Vulnerability



Jeep Uconnect Vulnerability was Discovered by Charlie Miller and Chris Valasek

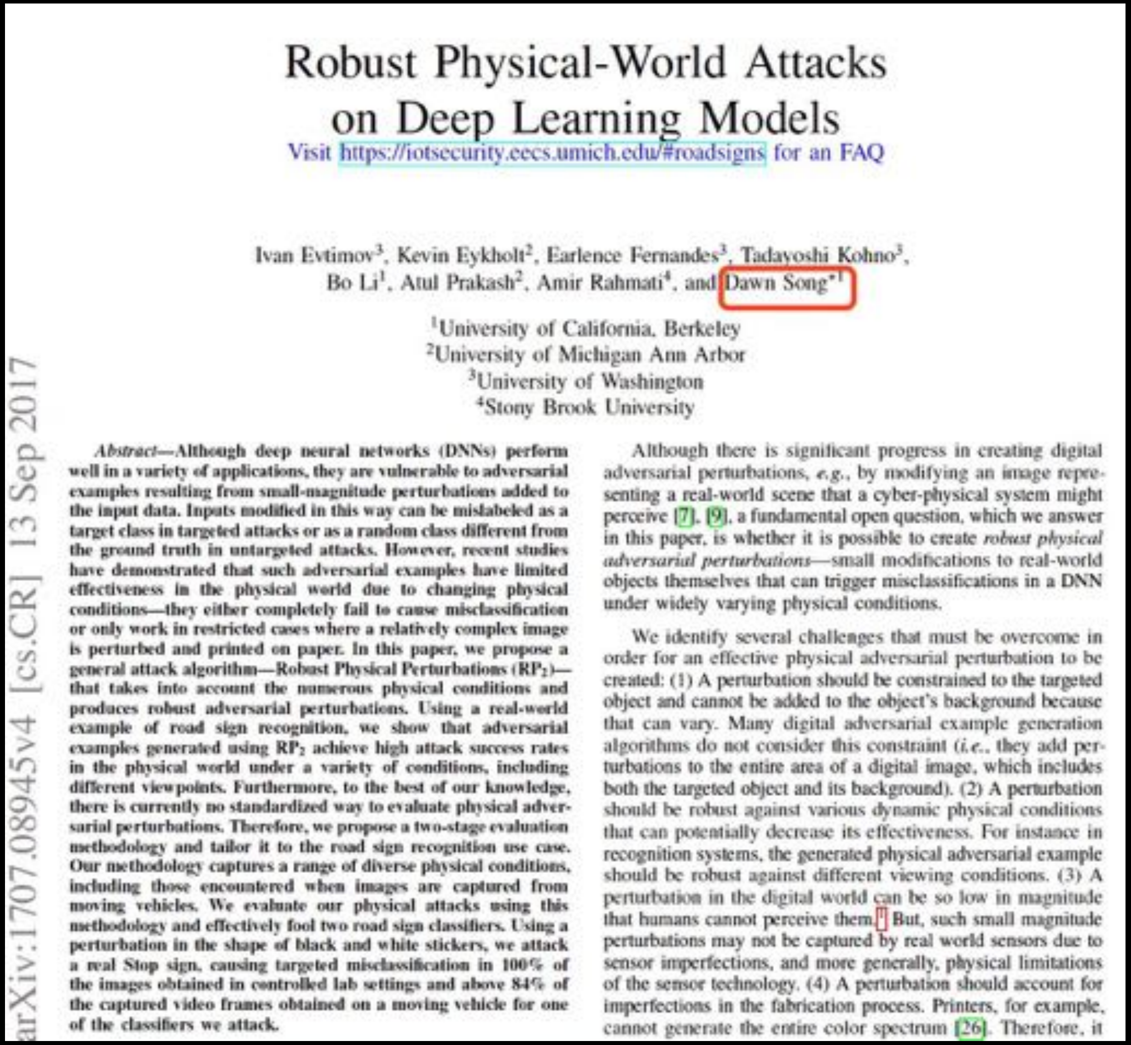
Vulnerabilities of Self-driving Cars

Vulnerable Perception



Vulnerabilities of Self-driving Cars

Vulnerable Perception



Robust Physical-World Attacks on Deep Learning Models

Visit https://iotsecurity.eecs.umich.edu/#roadsigns for an FAQ

Ivan Evtimov[3], Kevin Eykholt[2], Earlence Fernandes[3], Tadayoshi Kohno[3], Bo Li[1], Atul Prakash[2], Amir Rahmati[4], and Dawn Song*[1]

[1]University of California, Berkeley
[2]University of Michigan Ann Arbor
[3]University of Washington
[4]Stony Brook University

arXiv:1707.08945v4 [cs.CR] 13 Sep 2017

Abstract—Although deep neural networks (DNNs) perform well in a variety of applications, they are vulnerable to adversarial examples resulting from small-magnitude perturbations added to the input data. Inputs modified in this way can be mislabeled as a target class in targeted attacks or as a random class different from the ground truth in untargeted attacks. However, recent studies have demonstrated that such adversarial examples have limited effectiveness in the physical world due to changing physical conditions—they either completely fail to cause misclassification or only work in restricted cases where a relatively complex image is perturbed and printed on paper. In this paper, we propose a general attack algorithm—Robust Physical Perturbations (RP_2)—that takes into account the numerous physical conditions and produces robust adversarial perturbations. Using a real-world example of road sign recognition, we show that adversarial examples generated using RP_2 achieve high attack success rates in the physical world under a variety of conditions, including different viewpoints. Furthermore, to the best of our knowledge, there is currently no standardized way to evaluate physical adversarial perturbations. Therefore, we propose a two-stage evaluation methodology and tailor it to the road sign recognition use case. Our methodology captures a range of diverse physical conditions, including those encountered when images are captured from moving vehicles. We evaluate our physical attacks using this methodology and effectively fool two road sign classifiers. Using a perturbation in the shape of black and white stickers, we attack a real Stop sign, causing targeted misclassification in 100% of the images obtained in controlled lab settings and above 84% of the captured video frames obtained on a moving vehicle for one of the classifiers we attack.

Although there is significant progress in creating digital adversarial perturbations, *e.g.*, by modifying an image representing a real-world scene that a cyber-physical system might perceive [7], [9], a fundamental open question, which we answer in this paper, is whether it is possible to create *robust physical adversarial perturbations*—small modifications to real-world objects themselves that can trigger misclassifications in a DNN under widely varying physical conditions.

We identify several challenges that must be overcome in order for an effective physical adversarial perturbation to be created: (1) A perturbation should be constrained to the targeted object and cannot be added to the object's background because that can vary. Many digital adversarial example generation algorithms do not consider this constraint (*i.e.*, they add perturbations to the entire area of a digital image, which includes both the targeted object and its background). (2) A perturbation should be robust against various dynamic physical conditions that can potentially decrease its effectiveness. For instance in recognition systems, the generated physical adversarial example should be robust against different viewing conditions. (3) A perturbation in the digital world can be so low in magnitude that humans cannot perceive them.[1] But, such small magnitude perturbations may not be captured by real world sensors due to sensor imperfections, and more generally, physical limitations of the sensor technology. (4) A perturbation should account for imperfections in the fabrication process. Printers, for example, cannot generate the entire color spectrum [26]. Therefore, it

Privacy Leak of V2X

IEEE SPECTRUM
Follow on:
Engineering Topics Special Reports Blogs Multimedi
Cars That Think | Transportation | Advanced Cars

Researchers Prove Connected Cars Can Be Tracked

By Mark Harris
Posted 21 Oct 2015 | 18:00 GMT

surveillance mechanism. It's not yet clear how often connected vehicles will vary the unique wireless signatures that identify them, which could limit their use for tracking an individual car. But depending on how long those "pseudonyms" remain constant, Petit argues the connected vehicle protocol could offer a new, relatively cheap form of vehicle tracking that could bolster existing law enforcement tracking techniques like automatic license plate readers. Or, he imagines, hackers could collect and crowdsource data from the system to assemble a database of vehicle movements around entire cities.

The Present： Some Remediation

- Intro of Modern Cars
- Attack Surface of Modern Cars
- The Past：Some Vulnerabilities
- The Present： Some Remediations
- The Future：Some Suggestions

Hardware Security

- Secure Elements in ECUs
- Firmware Encryption&Verification
- Mutual Authentication Among ECUs
- …

Communication Security

Radio Distance Bounding

Realization of RF Distance Bounding

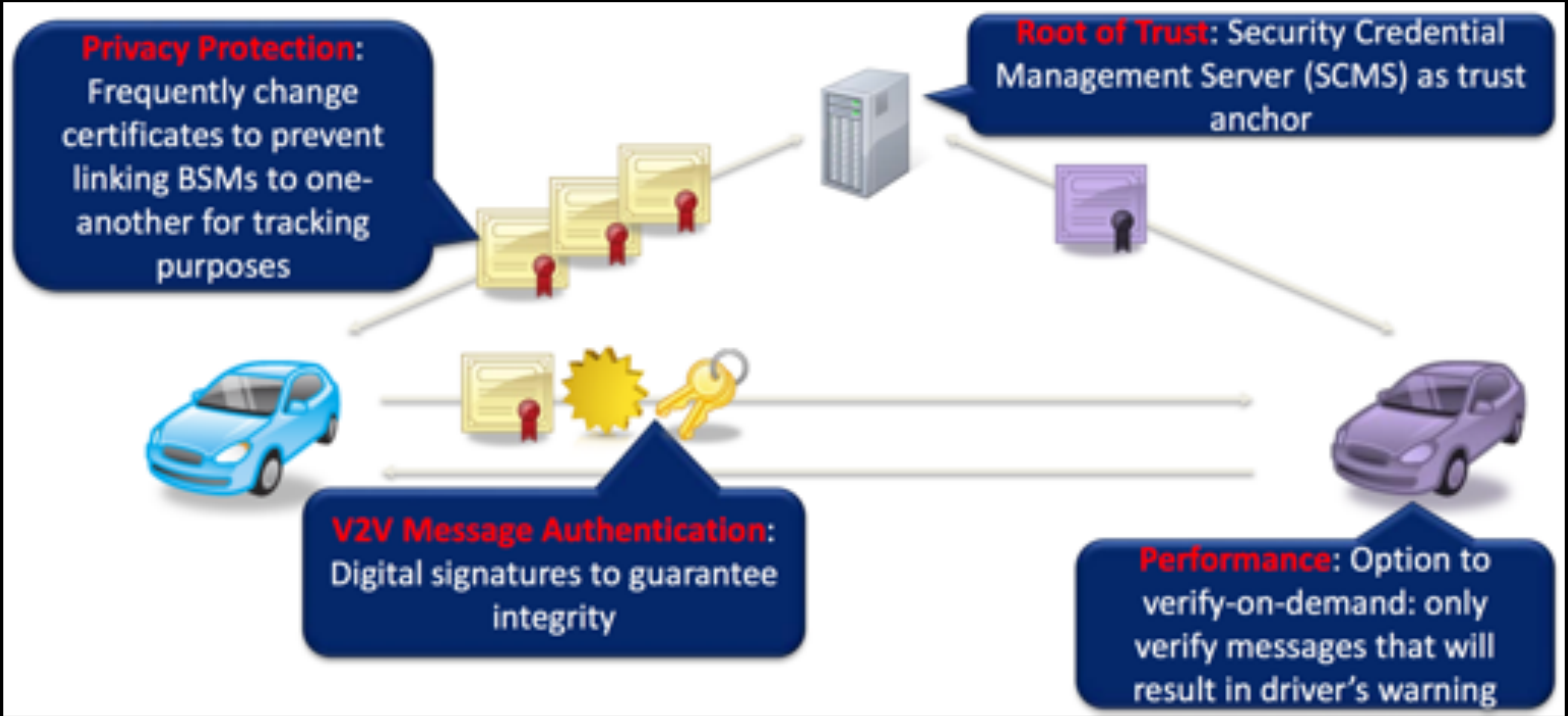
Kasper Bonne Rasmussen
Department of Computer Science
ETH Zurich
8092 Zurich, Switzerland
kasperr@inf.ethz.ch

Srdjan Čapkun
Department of Computer Science
ETH Zurich
8092 Zurich, Switzerland
capkuns@inf.ethz.ch

https://www.usenix.org/legacy/event/sec10/tech/full_papers/Rasmussen.pdf

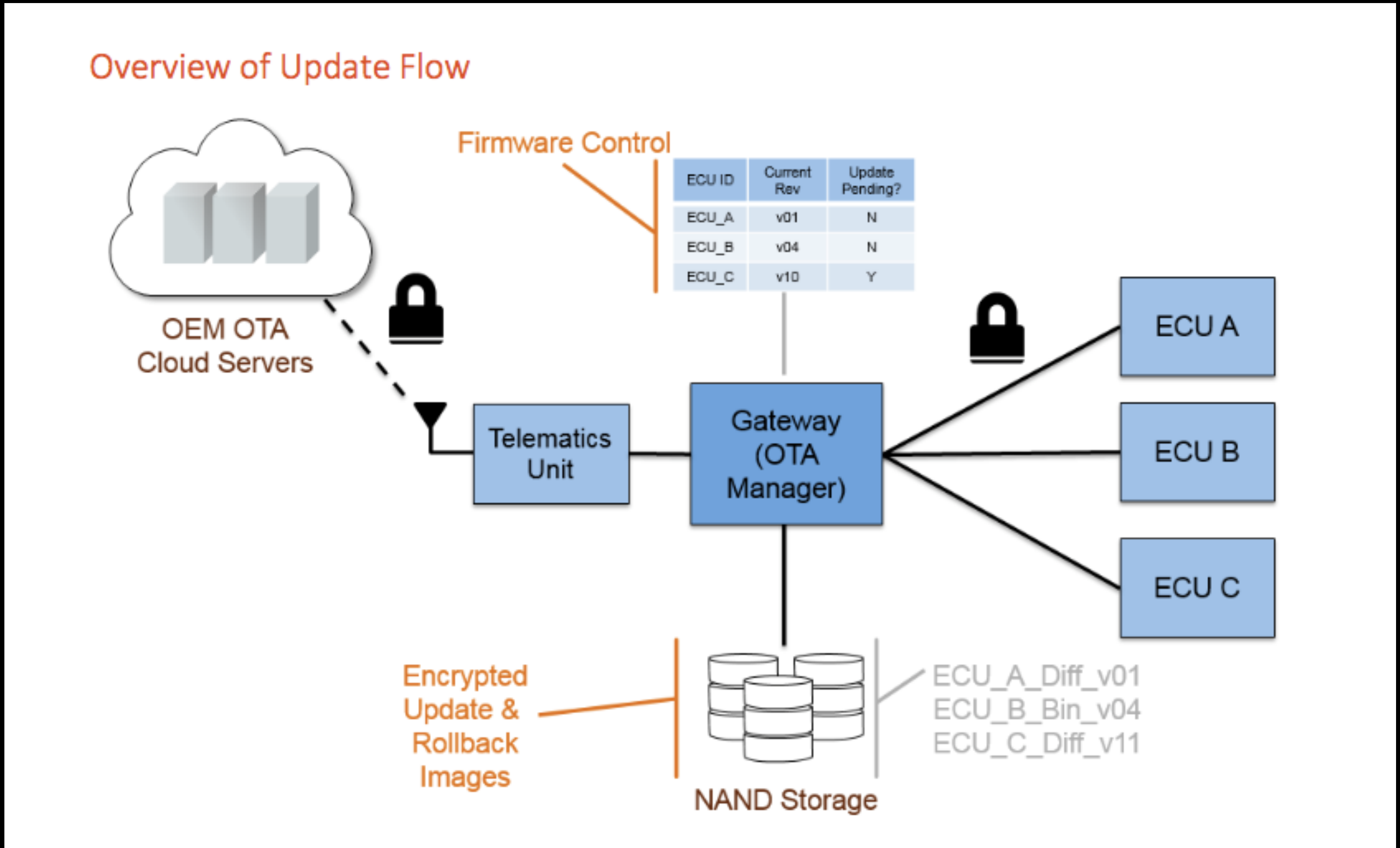
Communication Security

Anonymization



Communication Security

Secure Over-The-Air Patch



https://www.iot-now.com/2017/02/27/59018-securing-automotive-air-updates/

Communication Security

When You Design Vehicle Communication System

Do NOT Trust Anyone On The Communication Link , Only Rely On What You Have Absolute Control Over to Implement Your Security.

Because:

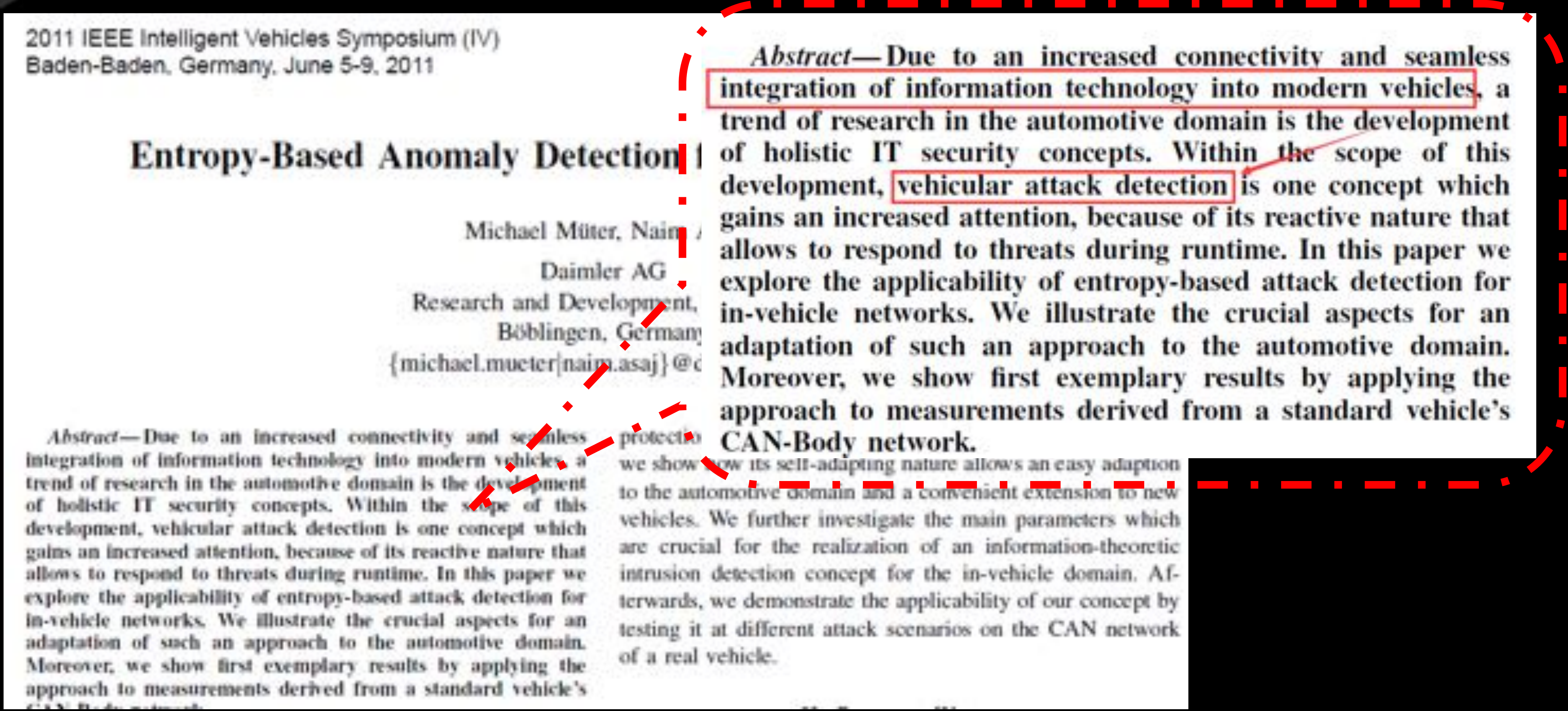
- 2G Had Been Broken
- 3G,4G Already Have Minor Bugs and Will Eventually be Broken
- 5G Will be Broken
- Wifi, Bluetooth ?
- ”What man makes, man breaks”

Cloud Security

The Future：Some Suggestions

- Intro of Modern Cars
- Attack Surface of Modern Cars
- The Past：Some Vulnerabilities
- The Present： Some Remediations
- The Future：Some Suggestions

Implementation of Anti-Hacking Features



2011 IEEE Intelligent Vehicles Symposium (IV)
Baden-Baden, Germany, June 5-9, 2011

Entropy-Based Anomaly Detection

Michael Müter, Naim

Daimler AG
Research and Development,
Böblingen, Germany
{michael.mueter|naim.asaj}@

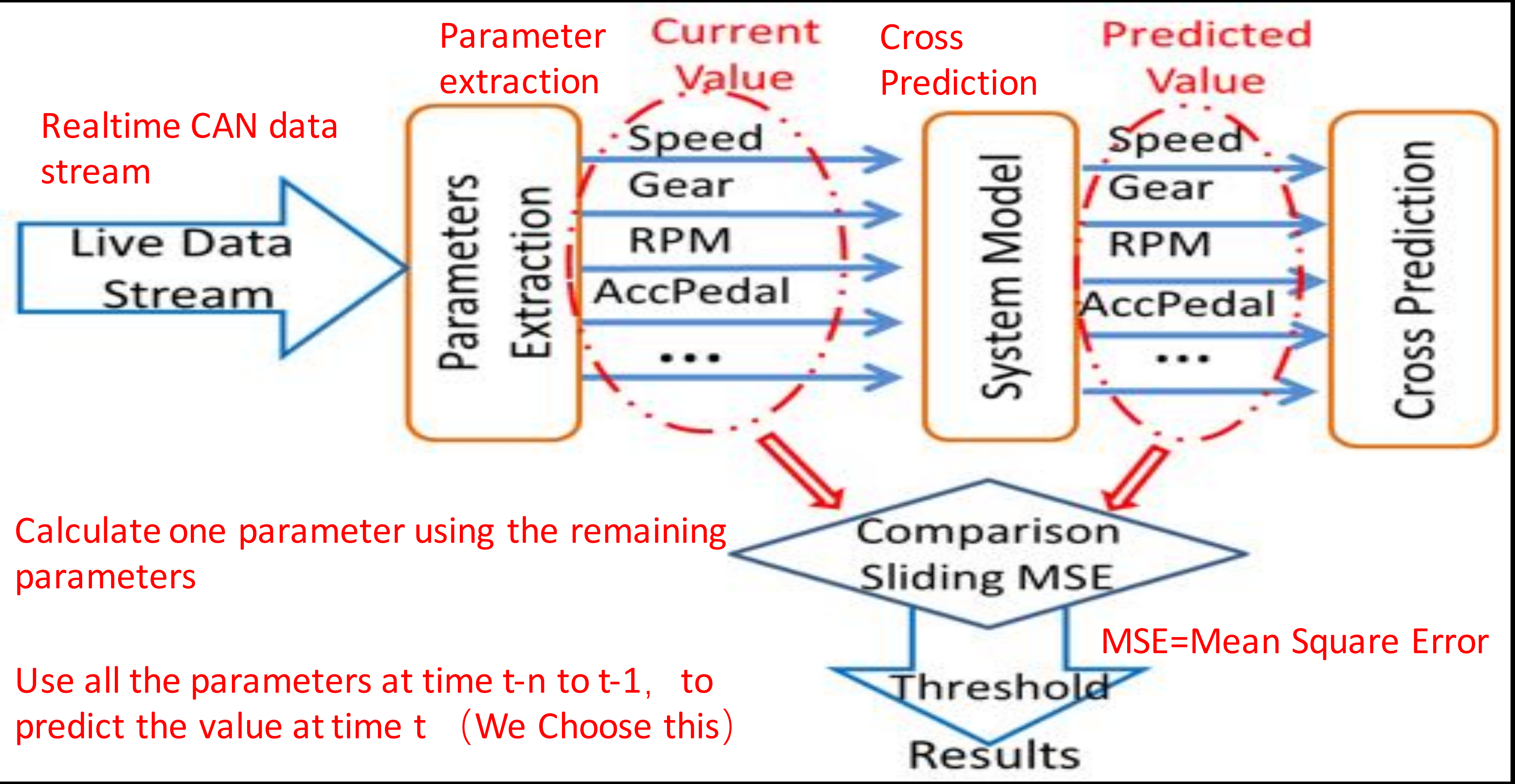
Abstract—Due to an increased connectivity and seamless integration of information technology into modern vehicles, a trend of research in the automotive domain is the development of holistic IT security concepts. Within the scope of this development, vehicular attack detection is one concept which gains an increased attention, because of its reactive nature that allows to respond to threats during runtime. In this paper we explore the applicability of entropy-based attack detection for in-vehicle networks. We illustrate the crucial aspects for an adaptation of such an approach to the automotive domain. Moreover, we show first exemplary results by applying the approach to measurements derived from a standard vehicle's CAN-Body network.

protectio... we show how its self-adapting nature allows an easy adaption to the automotive domain and a convenient extension to new vehicles. We further investigate the main parameters which are crucial for the realization of an information-theoretic intrusion detection concept for the in-vehicle domain. Afterwards, we demonstrate the applicability of our concept by testing it at different attack scenarios on the CAN network of a real vehicle.

Abstract—Due to an increased connectivity and seamless integration of information technology into modern vehicles, a trend of research in the automotive domain is the development of holistic IT security concepts. Within the scope of this development, vehicular attack detection is one concept which gains an increased attention, because of its reactive nature that allows to respond to threats during runtime. In this paper we explore the applicability of entropy-based attack detection for in-vehicle networks. We illustrate the crucial aspects for an adaptation of such an approach to the automotive domain. Moreover, we show first exemplary results by applying the approach to measurements derived from a standard vehicle's CAN-Body network.

Implementation of Anti-Hacking Features

Anomaly detection system



Research & Implementation of Anti-Hacking Features

Cooperation on Drafting&Following Standards

SAE INTERNA

HOME AEROSPACE AUTOMOTIVE COMMERCIAL VEHICLE TOPICS SHOP

LEARN
Articles
Events
Publicati
Standar
Students
Training
Webcast

- Researching and evaluating design processes and standards
  - Evaluating potential to adapt existing functional safety approaches
- Investigating Protective/Preventive solutions
  - Message authentication for communications Interfaces (V2V project initiating)
  - Gateways, firewalls (project initiating)
- Researching Intrusion Detection Solutions
  - Vehicle bus monitoring for anomalous behavior; (project initiating)
- Assessing Treatment Solutions
  - Feedback loop for continuous improvements (Monitor Automotive ISAC).
- Crosscutting Research:
  - Vulnerability Testing (Publish reports in 2016)
  - Software – including over the air updates
  - Evaluate Heavy Vehicle Cybersecurity

NHTSA
NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION

Cooperation with Security Companies

Open To Security Community

Q&A

Just Shoot ;)

The Endless

TECHIE BANG

Where hypes are challenged

Thanks