Current and Future of automotive security

Oct. 26, 2017

Graduate School of Informatics
Nagoya University

Ryo Kurachi
kurachi@nces.i.nagoya-u.ac.jp

Thank you for introduction. I am very happy to have an opportunity to present our introduction to you.

Today I would like to be talking about current and future of automotive security.

Agenda

- Self Introduction
  - includes Nagoya, Nagoya University
- Current and Future of automotive security and our Activities
  - Automotive Platform consortium projects.
  - Automotive Cyber Security projects
- Concluding remarks

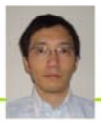
Let me first agenda of my presentation.

First, I am going to talk about self-introduction includes Nagoya and Nagoya University.

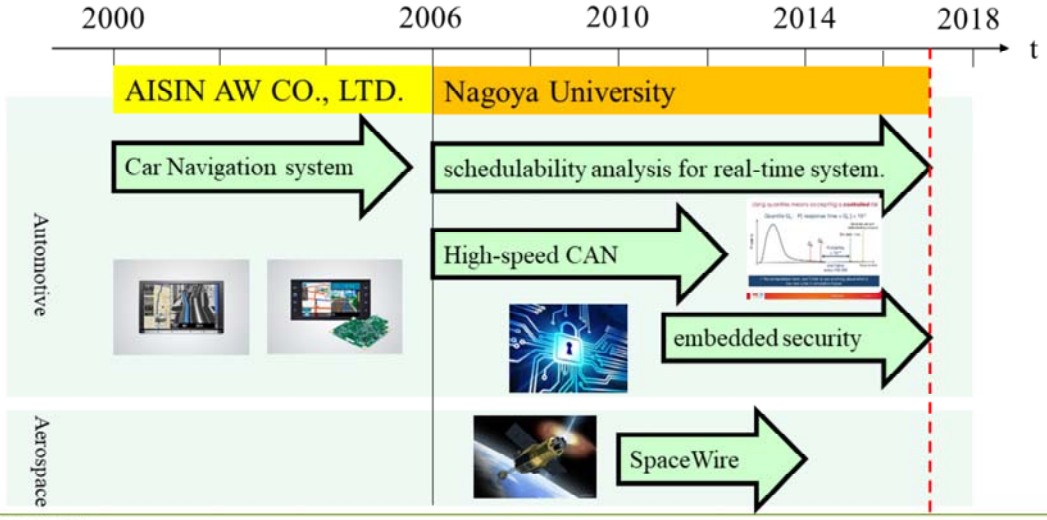
Then, I will talk about automotive security and our activities, in particular, I am going to explain our research topics in terms of AUTOSAR and security.

Finally, I will conclude my talk.

Introduction of Ryo Kurachi



- I am Ryo Kurachi received my Ph.D. degree in information science from Nagoya University in 2012. (Supervisor is Prof. Takada.)
- My research interests are real-time scheduling theory, cybersecurity and embedded security.



This slide is my introductions. I am an associate professor at Nagoya University. After graduate, I worked at AISIN AW Co., LTD to develop CAR navigation systems as software engineers for 6 years. After that, I left for Nagoya University. My research interests are real-time scheduling and cybersecurity.

Introduction of Nagoya and Nagoya Univ.

NAGOYA UNIVERSITY

- Nagoya
  - Center city of third largest metropolitan area in Japan
    - Tokyo (incl. Yokohama), Osaka, Nagoya, …
  - Located around the center of Japanese Main Island (between Tokyo and Osaka)
  - Manufacturing industry center of Japan
  - Automotive industries are concentrated, especially
    - The headquarters of Toyota Motor Corp. (located in Toyota City) is near to Nagoya.
- Nagoya University
  - National University located in Nagoya City
  - Within top 10 universities of Japan
  - 6 Nobel Prize Winners

4

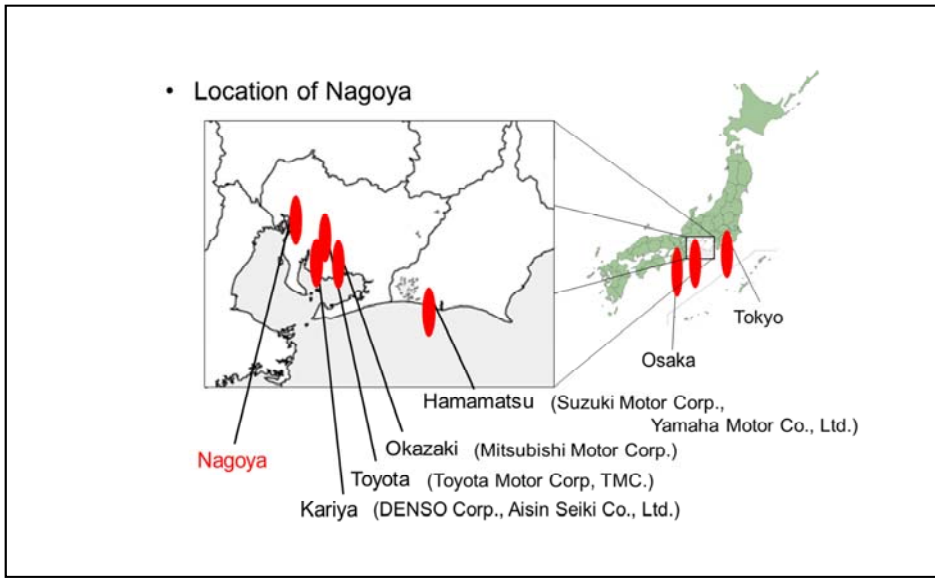
NCES 名古屋大学大学院情報科学研究科 組込みシステム研究センター

Nagoya is center city of third largest metropolitan area in Japan. And Nagoya Located around the center of Japanese main island between Tokyo and Oosaka.

And Nagoya also center of manufacturing industry in Japan, because automotive industry are concentrated around Nagoya.

Then, Nagoya university located in Nagoya city. And also the rank of university seems within 10 universities of Japan.

And Nagoya University has produced more Nobel Prize winners than any other universities in Japan (until today, six have been produced).



Toyota city has the headquarters of Toyota Motor Corp where is near to Nagoya.

Kariya city also has many auto parts suppliers such as DENSO and AISIN.

And Okazaki city has the headquarters of Mitsubishi motor corporation.

Hamamatsu city has the headquarters of SUZUKI and YAMAHA motor corporations.

As a result, a location of Nagoya is good to corroborate with several auto companies in Japan.

Nobel Prize Winners (Nagoya University)

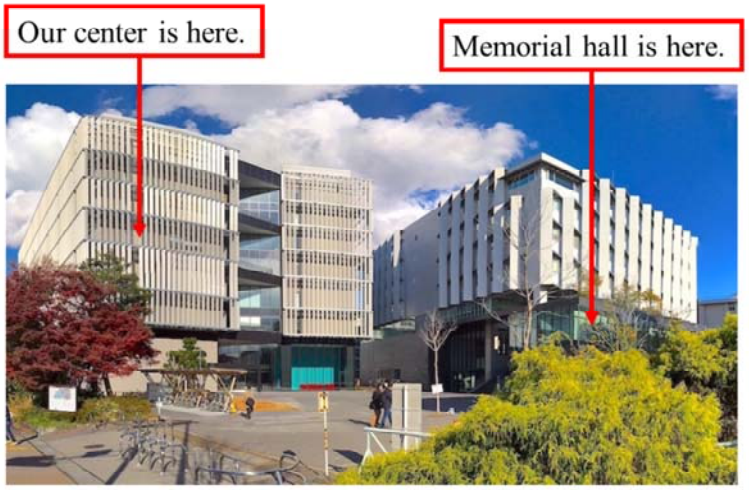
NAGOYA UNIVERSITY

- Nobel Prize Laureate in Chemistry, 2001
  - NU Professor: Dr. Ryoji Noyori
  - "for their work on chirally catalysed hydrogenation reactions"
- Nobel Prize Laureate in Chemistry, 2008
  - Alumnus & Former NU Associate Professor: Dr. Osamu Shimomura
  - "for the discovery and development of the green fluorescent protein, GFP"
- Nobel Prize Laureates in Physics, 2008
  - Alumnus & NU Professor: Dr. Makoto Kobayashi
  - Alumnus & NU Professor: Dr. Toshihide Maskawa
  - "for the discovery of the origin of the broken symmetry which predicts the existence of at least three families of quarks in nature"
- Nobel Prize Laureates in Physics, 2014
  - Former NU Professor: Dr. Isamu Akasaki
  - Alumnus & NU Professor: Dr. Hiroshi Amano
  - "for the invention of efficient blue light-emitting diodes which has enabled bright and energy-saving white light sources"

Nobel Prize memorial hall in Nagoya University

NAGOYA UNIVERSITY

- Nobel Prize memorial hall is a neighboring building of NIC.
- There are some exhibits of Nobel Prize winners in memorial hall.
- If you have time, please visit the hall.



Center for Embedded Computing Systems

NCES

- Introduction of NCES
  - NCES = Nagoya University, Center for Embedded Computing Systems
  - The director is professor Hiroaki Takada.

- Our Objectives
  - To establish a research and educational hub for embedded systems for satisfying strong industrial demands on technologies and human resources.
  - Analyzes industry issues and needs, reflected in the research at the university
- Past Major Research Projects of NCES
  - Integration of in-vehicle multimedia and control systems (TMC)
  - Analysis and design of real-time task scheduling for automotive integrated control systems (TMC)

  . . .

8

NCES 名古屋大学大学院情報科学研究科 組込みシステム研究センター

Next, I will talk about introduction of center for embedded computing systems. This center called NCES for short.

As can be seen, this picture is Prof Hiroaki Takada. He is a director of NCES.

Our objectives are to establish a research and educational hub for embedded systems for satisfying strong industrial demands on technologies and human resources. And We analyze industry issues and needs, reflected in the research at the university.

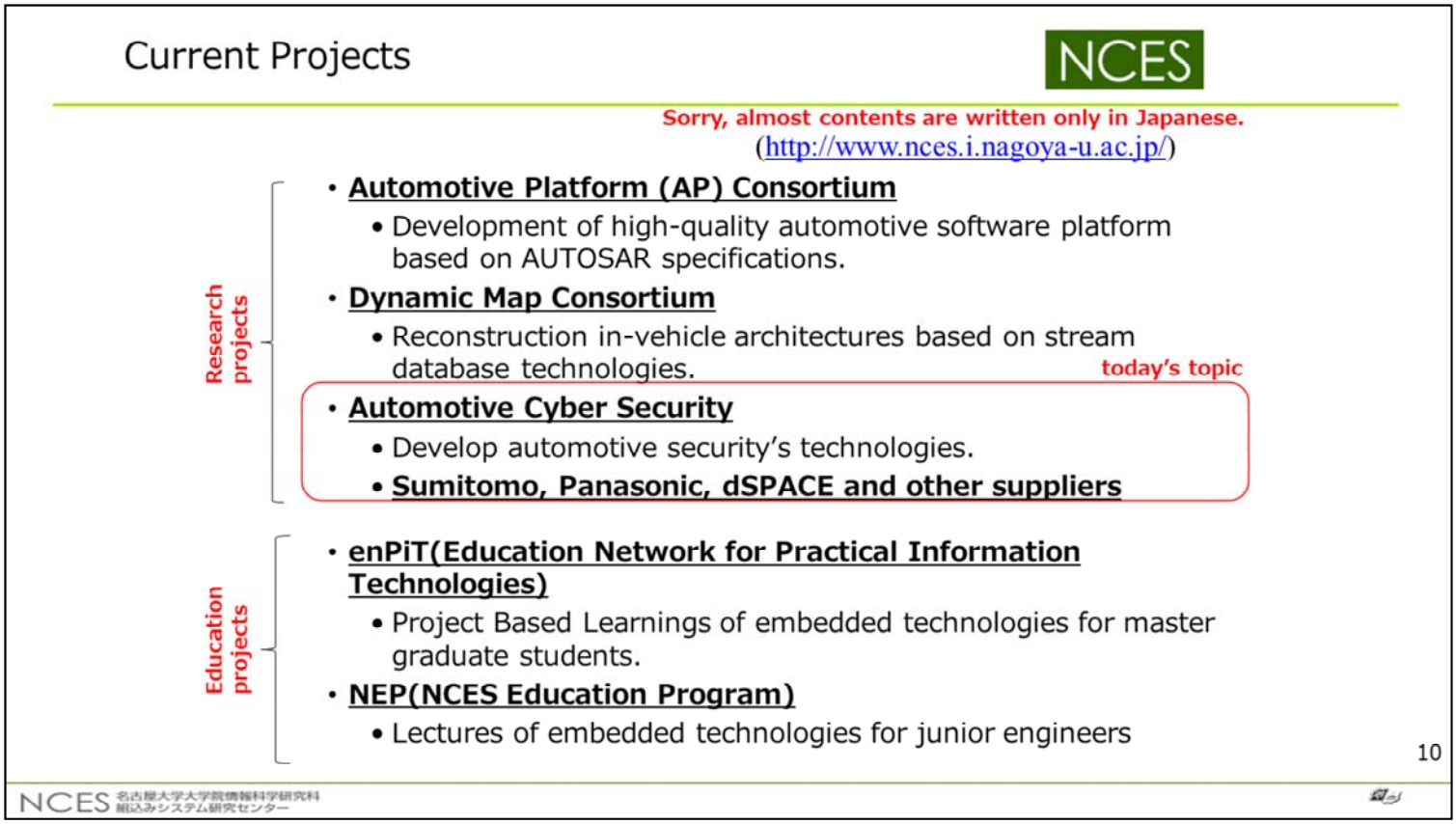
For example, in past major research projects, TMC and auto suppliers has launched a number of research projects to solve their problems.

Professor Hiroaki Takada

- Prof. Hiroaki Takada is an outstanding embedded software architect who has made major contributions to research in real-time OS and real-time scheduling area.
- Many RTOSs developed in his laboratory are distributed as open source software through the TOPPERS Project.
- He was the chair of the standardization of μITRON Specifications.
  - In the last decade, μITRON was de facto standard in japanese embedded devices includes in-vehicle systems
  - He introduced a real-time OS (μITRON) to TMC's vehicles in joint research with TMC about 25 years ago.
- He was a member of program committee for escar asia 2014.

Prof. Hiroaki Takada

TRON project had its 30th anniversary in 2014.



Here's a list of the current projects.

Our projects are divided into research projects and education projects.

Currently, we has 3 major research projects. In terms of automotive security, we do joint research with several suppliers. Sumitomo corroborates with us about 10 years to develop scheduling for in-vehicle networks and automotive security.

Panasonic also corroborates with us about 3 years to develop the automotive security evaluation method such as pen testing and fuzz testing.

dSPACE also corroborates with us to develop the security evaluation method integrating with HILs from 2 years ago.

Our honors in Japan

S-2 19th (Wed) 14:00-15:30 Conference Center 5F 502

Future of Connected Cars and Cyber Security

Hiroaki Takada Nagoya UniversityInstitute of Innovation for Future Society / Graduate School of Information ScienceProfessor

He talked about the future of cyber security in cars at ET 2014.
(http://www.jasa.or.jp/et/ET2014/english/conf/confpage-s.html)

ET Award Committee Special Award

Center for Embedded Computing Systems, Nagoya University

Our security solution (CaCAN) has won the ET award.
(http://www.jasa.or.jp/et/ET2014/english/event/et_award.html)

Security Countermeasures for In-vehicle Networks and Systems

Riyo Kurachi
Designated Assistant Professor,
Nagoya University

[Abstract]
In the last decade, security attacks in vehicles have been increasing and have been reported in several papers. Our research focuses on in-vehicle networks which is a critical system with real-time constrains. In particular, Controller Area Network (CAN) suffers from some common disadvantages such as limited baud rate and payloads. This seminar introduces the security countermeasures for in-vehicle networks and systems.

Almost 200 peoples attends my lectures in Automotive World 2015.

NISSAN has provided Q50 hybrid to TOPPERS booth at ET 2014.

11

NCES 名古屋大学大学院情報科学研究科 組込みシステム研究センター

Embedded technology is the largest exhibition of embedded systems area in Japan. In ET, Prof. Takada talked about the future of cyber security in cars. Then, our security solution won the award in ET 2014. This our security solution is also presented in escar EU 2014, which is called the centralized authentication in CAN.

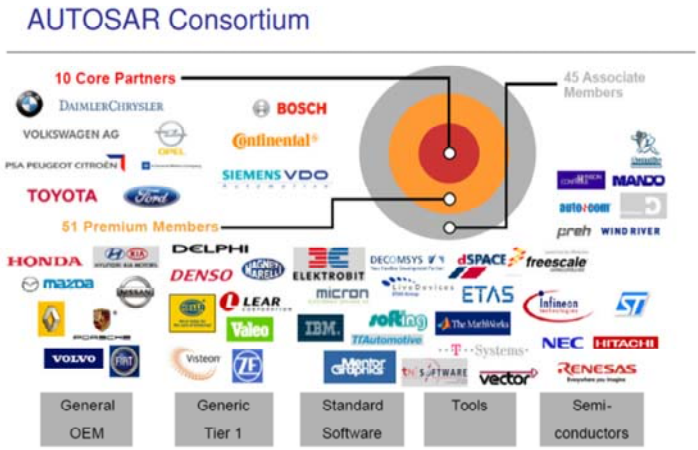
Main focus of today's lecture

- Trends for automotive security and security technologies
  - These days, security threats of automotive systems are often close-up, but I will be outlined research trends on countermeasures technologies.
- Concept of our proposal "Centralized authentication system"
  - Since many of the current countermeasures has proposed to be required modification of all nodes.
  - Our proposed centralized approach is reasonable solution to implement security features for in-vehicle systems.
- Our problem consciousness
  - EU/ USA leads standardization and studies several developments for automotive security.
  - How about in China?

Automotive Platform (AP) Consortium
- TOPPERS Project and TOPPERS/AP -

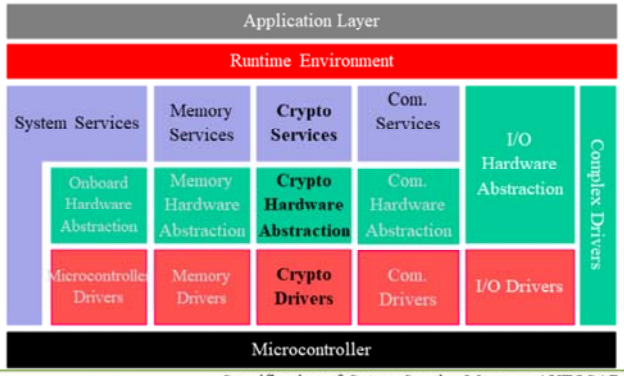
What's is AUTOSAR?

- AUTOSAR - AUTomotive Open Systems ARchitecture
- AUTOSAR is a consortium to develop the standard of automotive software platform. Especially, middleware and system-level standard, jointly developed by automobile manufacturers, electronics and software suppliers and tool vendors. (More than 100 members)



AUTOSAR architecture

- AUTOSAR aims standardization of components and interfaces.
- The software implementing the automotive functionality is encapsulated in software components.
- Software architecture including a complete basic or environmental software stack for ECUs –the so called AUTOSAR Basic Software –as an integration platform for hardware independent software applications.
- Current standard involves crypto services and the secure onboard communication technology (SecOC) to achieve security.



Specification of Crypto Service Manager AUTOSAR CP Release 4.3.0より

Introduction of Automotive Platform (AP) Consortium in NCES

- Problem of AUTOSAR
  - Runtime overhead (processing time and memory usage) is very large.
    - It is permissible for high-end-cars, but not for low-end cars.
  - Inefficient support for functional safety and security
    - Though functional safety and security requirements can be fulfilled with AUTOSAR, but not efficient.
- Objectives of the Project
  - To develop AUTOSAR based software platform with our improvement to achieve high quality and high reliablity
- Main Activities of the Project
  - Building a improved AUTOSAR Platform
  - Contributing the standardization and publishing open source of AUTOSAR platform from TOPPERS project

16

NCES 名古屋大学大学院情報科学研究科 組込みシステム研究センター

AUTOSAR has two major problems. One is a runtime overhead is very larger than traditional baremetal programing. Another one is the inefficient support for functional safety an security.

Therefore, our research focuses to develop AUTOSAR based software platform with our improvement to achieve high quality and high reliability.

And also, main activities of this project has following two topics. One is to build a improved AUTOSAR platform. And another one is contributing the standardization and publishing open source of AUTOSAR platform from TOPPERS project

What is TOPPERS Project?

TOPPERS = Toyohashi Open Platform for Embedded and Real-Time Systems

TOPPERS

- Objectives of TOPPERS project
  - To develop various open-source software for embedded systems including RTOS and to promote their use

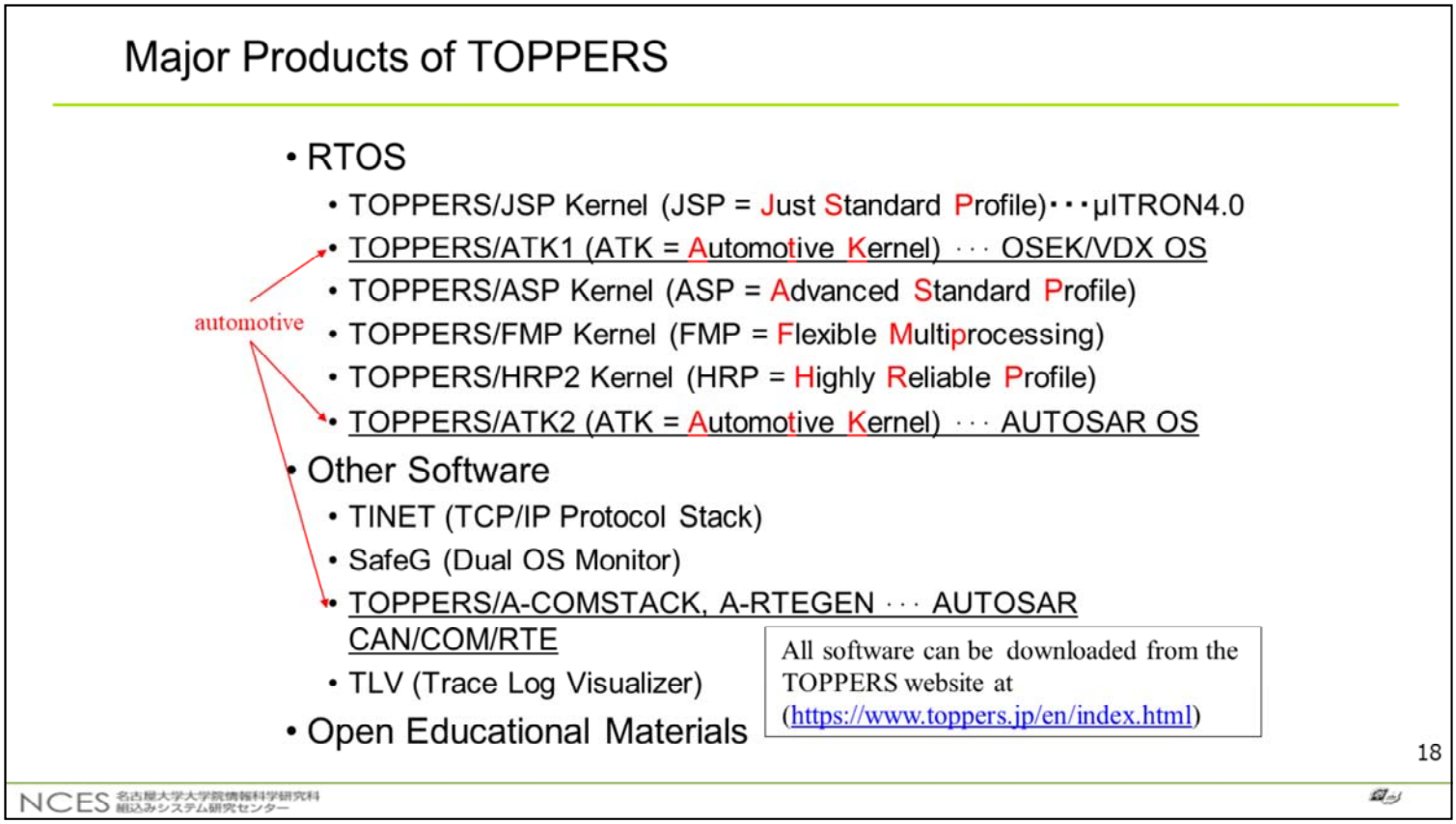
    Building a widely used open-source OS as Linux in the area of embedded systems!
- Main Activities of TOPPERS project
  - Building a definitive µITRON-conformant RTOS
  - Developing a next generation RTOS technology
  - Developing software development technology and tools for embedded systems
  - Fostering Embedded System Engineers

17

NCES 名古屋大学大学院情報科学研究科 組込みシステム研究センター

A part of our research results are opened to the public as open source software from TOPPERS projects. TOPPERS is launched by Prof. Hiroaki Takada.

And, objectives of TOPPERS projects is to develop various open source software for embedded systems including RTOS. Main activities of TOPPERS project is building a “definitive uITRON-conformant RTOS”. And also includes developing a next generation RTOS and embedded technologies.



This slides are summarized major products of TOPPERS.

TOPPERS JSP are based on uITRON 4.0 which is a last version of uITRON.

For automotive software, ATK1 which means that automotive kernel based on OSEK/VDX OS is released.

Next Automotive product are ATK2 which compliant with AUTOSAR OS. Of Couse, if you are interested in our product, all software can be downloaded from the TOPPERS website.

Major Products of TOPPERS

- Consumer Applications

PM-A970 (EPSON)

DO!KARAOKE
(PANASONIC)

SoftBank
945SH
(SHARP)
(TOPPERS FMP)

- Industrial and Other Applications

Skyline Hybrid (NISSAN)
(Q50 hybrid in EU)
(TOPPERS ATK1)

KIZASHI:2010
(SUZUKI Motor Corp.)
(TOPPERS ATK1)

H-IIB (JAXA)
(TOPPERS HRP)

19

NCES 名古屋大学大学院情報科学研究科 組込みシステム研究センター

This slide shows the major real-products of TOPPERS.

For example, TOPPERS JSP are applied to several consumer applications such as printer form EPSON and KARAOKE microphone from Panasonic. And also, a cell phone from sharp employed TOPPERS FMP which based on multi-core RTOS.

In automotive domain, TOPPERS ATK1 has been adopted to Skyline Hybrid from NISSAN and KIZASHI from SUZUKI Motor Corporations. In addition, TOPPERS HRP has been adopted to Japanese rocket and satellite control units because the (JAXA which means Japan Aerospace Exploration Agency) corroborate with us.

Major Products of TOPPERS

- TOPPERS to the Space*!*
  - The H-IIB rocket, in which the TOPPERS/HRP is used for guidance control computer, was successfully launched from Tanegashima Space Center in 21ST July, 2012.

Photo:
Hiroaki Takada

20

NCES 名古屋大学大学院情報科学研究科 組込みシステム研究センター

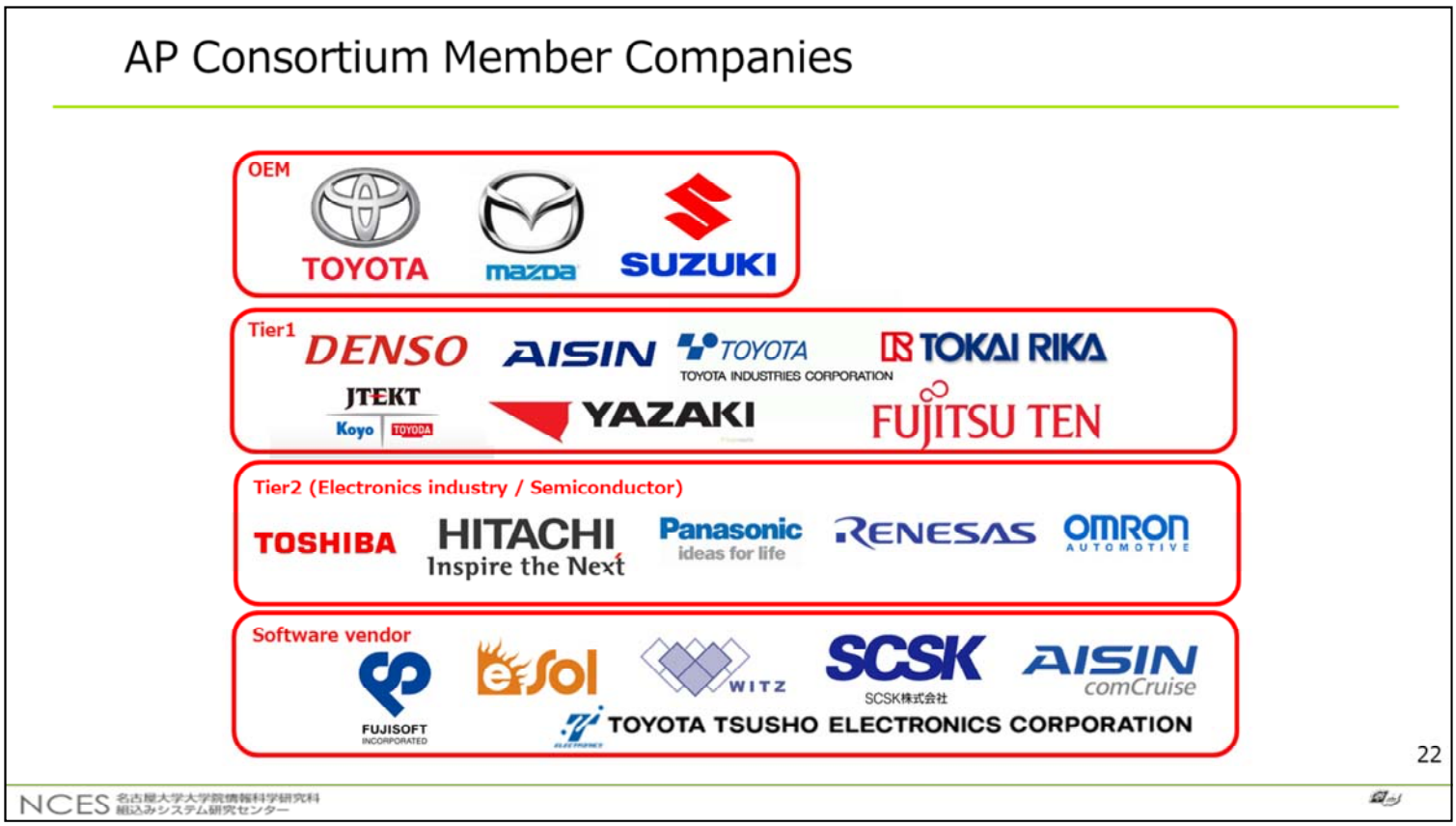
In 2012, TOPPERS HRP is used for guidance control computer, was successfully launched from Tanegashima. After that, JAXA employs TOPPERS HRP continuously. This is the picture that Prof Takada took in Tanegashima.

AP Consortium Member Companies

- AISIN COMCRUISE Co., Ltd.
- DENSO CORPORATION
- Eiwa System Management, Inc.
- eSOL Co., Ltd.
- FUJI SOFT INCORPORATED
- FUJITSU TEN LIMITED
- JTEKT CORPORATION
- Mazda Motor Corporation
- NEC Communication Systems, Ltd.
- OMRON Automotive Electronics Co., Ltd.
- OTSL Inc.
- Panasonic Advanced Technology Development Co., Ltd.
- Panasonic Corporation
- Renesas Electronics Corporation
- Ryoden Trading Co., Ltd.
- SCSK Corporation
- Sunny Giken Inc.
- SUZUKI MOTOR CORPORATION
- TOKAI RIKA CO., LTD.
- TOSHIBA CORPORATION
- TOYOTA INDUSTRIES CORPORATION
- TOYOTA TSUSHO ELECTRONICS CORPORATION
- WITZ Corporation
- YAZAKI Corporation
- Yamaha Motor Co., Ltd.

21

This slide shows that Automotive Platform Consortium Member companies. The number of our consortium member companies reached 25 companies as of the end of 2016.



I also categorized automotive consortium member companies.

As OEM, Toyota mortar corporation and MAZDA and SUZUKI motor corporation has joined our consortium. And also, as Tier 1 supplier, DENSO, AISIN, TOYOTA Industries Corporation, TOKAI RIKA YAZAKI and Fujitsu ten also joined our consortiums.

Current Products of TOPPERS/ATK2

- RTOS based on the AUTOSAR OS
  - SC1 … full set of SC1 (basic functions)
  - SC3 … a subset of SC3 (*memory protection*)
  - SC1+MC … SC1 with *multicore* support
  - SC3+MC … SC3 with *multicore* support
- TOPPERS/A-COMSTACK
  - Communication stack for CAN
  - subsets of AUTOSAR COM, CANIF, and CAN
- TOPPERS/A-RTEGEN
  - a subset of AUTOSAR RTE supporting TOPPERS/ATK2 and A-COMSTACK.

You can download them from the TOPPERS web site.

23

NCES 名古屋大学大学院情報科学研究科 組込みシステム研究センター

Here is the research results of AP consortium.

We built the several classes of AUTOSAR OS, such as SC1 and SC3.

SC1 employs the basic function of the AUTOSAR, and SC1 also compliant with OSEK/OS.

And, to achieve functional safety, we develop SC3 which includes memory protection profiles.

Then, to connect the CAN networks, we developed the communication stack and RTE generators.

If you are interested in, you can download them from TOPPERS web site.

Current Development of TOPPERS/ATK2

- Various documents of ATK2 and others required for ISO 26262 compliance
- Two timing protection mechanisms for ATK2
  - a subset of SC2 of AUTOSAR OS
  - original temporal partitioning scheme
- Multicore optimization of A-COMSTACK
- Watchdog manager, interface, and driver

- Currently, we avoid using the term “open source” for TOPPERS/AP
  - Because AUTOSAR requires those who commercially exploit software based on AUTOSAR to be AUTOSAR partner.

As a result, Nagoya University was involved with the start-up of new company.

24

I will talk about my current development status of toppers /atk2.

We develop the several functional safety features for satisfy the requirement of ISO 26262.

On the other hand, currently, we avoid using the term “open source”, because AUTOSAR requires those who commercially exploit software based on AUTOSAR to be AUTOSAR partner.

Thus, we were involved with the start-up of new company.

Introduction of APTJ

http://www.aptj.co.jp/?l=1

- In 2015, Automotive Platform Technology Japan (APTJ Co., Ltd.) was founded as a startup with support from Nagoya University and several Japanese auto suppliers.
- APTJ aims to develop an AUTOSAR based software platform in partnership with several auto suppliers.
- Prof. Hiroaki Takada became a chairperson and CTO of APTJ.
- APTJ has been accepted as a premium member of AUTOSAR, and joins the JasPar to contribute to standardization of AUTOSAR and security features.

JasPar: Japan Automotive Software Platform and Architecture (https://www.jaspar.jp/en)

25

NCES 名古屋大学大学院情報科学研究科 組込みシステム研究センター

In July 2017, we totally get 2 billion Japanese yen from several funds and suppliers.

My contributions

http://www.aptj.co.jp/?l=1

- I am participating in AUTOSAR standardization activities.
  - Working Groups in AUTOSAR, contributing their expertise to the consortium.
  - Especially, I become a member of working groups for security in AUTOSAR, named WP-X-SEC where we discuss the security features in AUTOSAR.
  - Currently, using our experiences, we support JASPAR to create and promote the future automobile design standards.

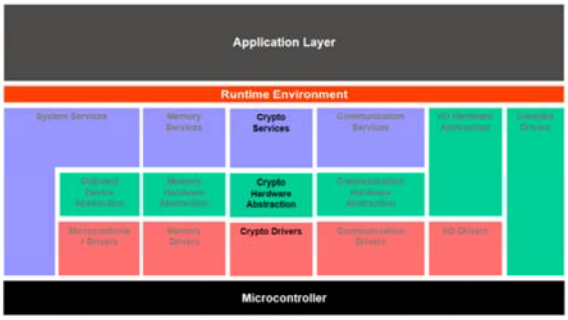


Figure. AUTOSAR crypto stack

Automotive Security Project
- Countermeasures, Evaluation methods –

Automotive electronic control systems

- Today's vehicle has:
  - many number of devices (sensors and actuators)
  - hard real-time constraints for control processing.
  - Therefore, complex distributed systems in embedded computing systems.
  - CAN is most widley used in-vehicle network protocol.

（例）VW Phaeton 2014:
- 11,136 electrical parts in total
- Communication:
  - 61 ECUs in total
  - external diagnosis for 31 ECUs via communication
  - 35 ECUs connected by 3 CAN-busses sharing
  - approximately 2500 signals in 250 CAN messages

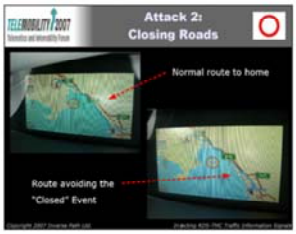
http://www.iestcfa.org/presentations/wfcs04/keynote_leohold.pdf

Today

Why do we need automotive security ?

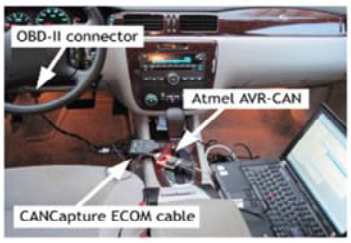
- Recent works has demonstrated potential security weaknesses in vehicles.

RDS-TMC (2007)



http://www.telemobilityforum.com/eng/images/stories/daniele%20bianco.pdf

Ford (2010)



http://www.autosec.org/pubs/cars-oakland2010.pdf

Prius (2013)

http://hackaday.com/2013/07/26/defcon-presenters-preview-hack-that-takes-prius-out-of-drivers-control/

- Especially, OEM need to adopt security measures to protect vehicles from the serious security attacks, such as message injection in a safety-relevant network or rewriting malicious software, target vulnerable safety-critical applications.

29

NCES 名古屋大学大学院情報科学研究科 組込みシステム研究センター

Let me mention briefly why we decided to conduct the present study.

In the last decade, security attacks in vehicles have been increasing and have been reported in several papers.

However, existing vehicles are not designed to meet current and future security challenges.

In addition, the CAN protocol does not provide security features such as an authenticating transmitter and encrypted message payloads.

As a result, an adversary can connect equipment to the CAN bus and easily gain access and inject counterfeit messages.

Why do we need automotive security ?

- Recent research has been focused on helping people enjoy the benefits of a computerized architecture while providing strong assurance of safety, security and privacy.
- Two papers exploring safety, security and privacy are worth noting here.
- The first is the “Experimental Security Analysis of a Modern Automobile” and the second is the “Comprehensive Experimental Analysis of Automotive Attack Surfaces “
  - Experimental Security Analysis of a Modern Automotive, IEEE Symposium on Security and Privacy, May 2010
  - Comprehensive Experimental Analysis of Automotive Attack Surfaces, USENIX Security Symposium, August 2011

Vulnerability Case 1 (1/2)

- Researchers used two identical 2009 model cars
- Wrote a packet sniffer/injection tool, introduced into the CAN by simply plugging a device in to the car's federally mandated universal OBD-II diagnostics port
- Used "fuzzing" to enumerate the commands that the car responds to
- Using the commands they discovered, performed live tests to see how much of the car they could control

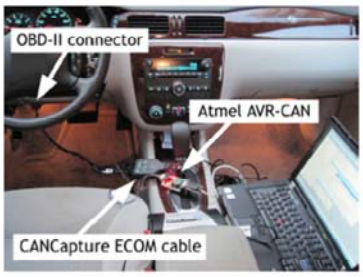


Figure 2. Example experimental setup. The laptop is running our custom CARSHARK CAN network analyzer and attack tool. The laptop is connected to the car's OBD-II port.

Figure 6. Displaying an arbitrary message and a false speedometer reading on the Driver Information Center. Note that the car is in Park.

31

NCES 名古屋大学大学院情報科学研組込みシステム研究センター

K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental Security Analysis of a Modern Automobile," in 2010 IEEE Symposium on Security and Privacy (SP), May 2010

Researchers do experimental Security Analysis in modern automobiles.

Vulnerability Case 1 (2/3)

- Researchers could not only fully control the car using their device, they could do it while the car was going 40 MPH
- Among the things they could control:
  - Disable brakes
  - Engage brakes
  - Disable wipers and continuously spray fluid
  - Permanently activate horn
  - Kill engine
  - Unlock all doors
- Also found that they could write programmatic commands, or "viruses", that would activate under certain conditions
- Disable all lights when driving over 40MPH
- Even though they had physical access to the CAN, they noted that the same commands could potentially be executed wirelessly

The problem of automotive security

- CAN is an insecure low-level protocol
- Every message is an unencrypted plain-text broadcast to every device on the CAN
- Possible messages and communication procedures are often documented and made available freely
- No component authentication
- Any device can send a command to any other devices.
  - Attacker could use tire pressure gauge to turn off brakes

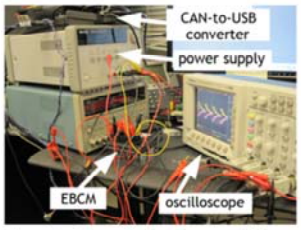


Figure 1. Example bench setup within our lab. The Electronic Brake Control Module (ECBM) is hooked up to a power supply, a CAN-to-USB converter, and an oscilloscope.

Figure 3. To test ECU behavior in a controlled environment, we immobilized the car on jack stands while mounting attacks.

Vulnerability Case 2

S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno, et al. Comprehensive experimental analyses of automotive attack surfaces. USENIX Security Symposium, 2011.

- In 2011, Researchers shows some remote attack potentials.
  - Radio
  - Telematics
  - Vehicle to Vehicle Communication
  - GPS
  - Remote Key Fob
  - Bluetooth

Figure 1: *Digital I/O channels appearing on a modern car.* Colors indicate rough grouping of ECUs by function.

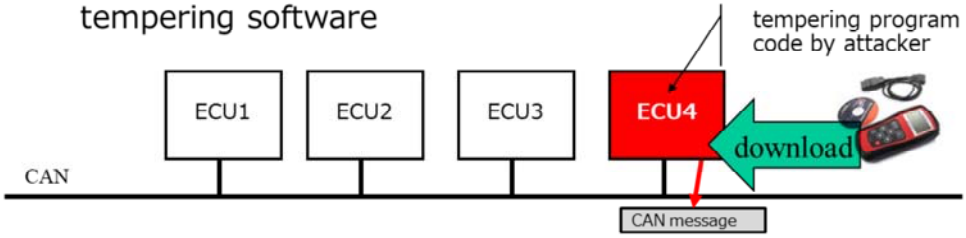
https://www.youtube.com/watch?v=bHfOziIwXic

Conclusion of Comprehensive Studies

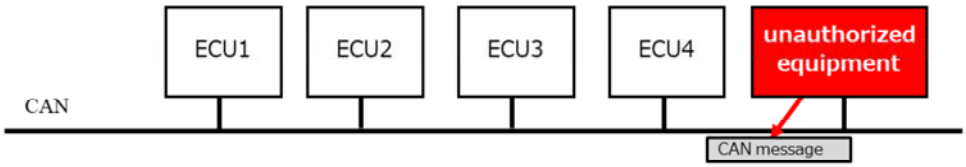
- Authors of the experimental studies note that automobile owners should not be overly concerned about attacks to automotive architectures.
- Rather, they focus squarely on addressing potential automotive security and privacy issues that future cars will have – with even more sophisticated computer control and broader wireless connectivity.
- Security and privacy protections will need to be addressed for voice, data and location.
- For example, experimental analysis of remote exploit controls has found that an attacker who has compromised a automobiles' telematics unit can record data from the in-cabin microphone (normally reserved for hands free calling) and exfiltrate data over the connected IRC channel.
- It is easy to capture the location of the automobile and track where a driver goes.

Attack scenario

- A malicious node can get access to the network and send counterfeit messages or replay attacks.
  - Scenario 1) A node becomes malicious because of tempering software



  - Scenario 2) Connecting unauthorized equipment



36

NCES 名古屋大学大学院情報科学研究科 組込みシステム研究センター

As you can see, we give two examples of our expected use case of spoofing attacks.

First scenario illustrates an example of counterfeit data transmission on a CAN by the manipulated ECU.

To protect this attack, we need to check the validity of the control software program in each ECU.

Second scenario illustrates an example of injecting counterfeit messages from unauthorized equipment.

To protect this action, the end-nodes need the authentication mechanism to prevent the unauthorized messages.

How to minimize attack potential ?

- Countermeasures:
  - **Confidentiality**: Cryptography
  - **Data integrity**: Message Authentication Codes (MACs)
  - **Authentication**: Authentication nodes and messages by identity
- Problem:
  - OEMs require the cost effective solutions.
    - Existing methods are good solutions but very expensive.
      - Especially, hardware costs will increase.
- **Our goal is to propose a first step to achieve a secure in-vehicle systems.**

37

NCES 名古屋大学大学院情報科学研究科 組込みシステム研究センター

From the other point of view, OEM require the cost effective solutions.

Therefore, our goal is to propose a first step to achieve a secure in-vehicle systems.

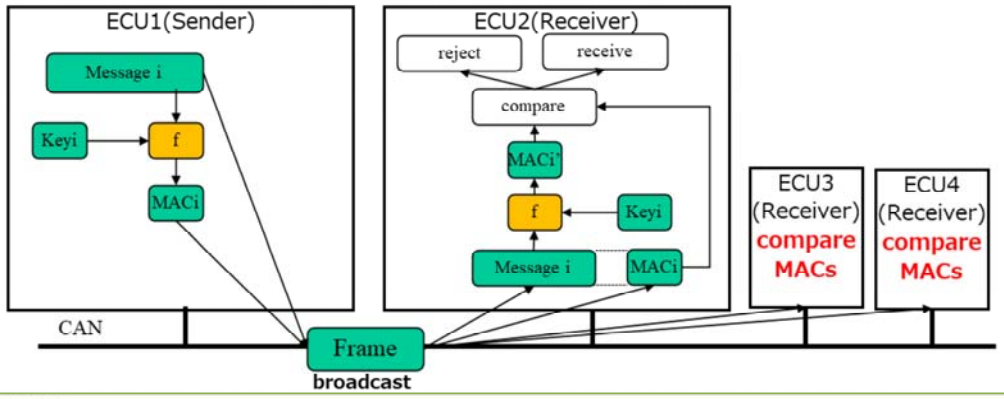
In our system, all legitimate nodes do not detect and reject unauthorized messages, because of easy migration from existing systems to our proposed systems.

By taking advantage of the broadcast bus, Our solution is that the monitor node can be responsible for these nodes by proxy.

We provide message authentication and integrity by including a Message authentication codes in a message but not encryption.

Existing approach (Distributed approach)

- Achieve data integrity by message authentication
  - Each pair of nodes has a shared secrete key
  - A sender computes Message Authentication Codes (MACs) and broadcast the message with the MACs
  - All receivers computes a MAC and compares it with the receiving MACs



Almost related works are employed distributed approaches.

Distributed approach achieves very high-security performance.

However, almost solution is difficult to apply to a traditional CAN.

Difficulties on CAN and existing system

- The communication overhead is too high.
  - Key exchange protocol needs huge number of messages because of broadcast authentication.
    - Number of messages for key exchanges
      = receiving nodes(m) × sending nodes(n)

- Existing ECUs needs hardware extensions.
  - Almost nodes needs to change CPU/hardware to calculate MACs because of having lower CPU.
  - Increasing cost !!! ⇒ Centralized approach is needed !!!

39

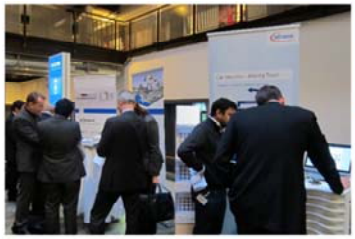
And, I think the related solutions is too expensive.

Automotive Security Project
- Countermeasures, Evaluation methods –

a) escar EU 2014

- Because escar is very influential conference, I recommend you to present more Japanese technologies and solutions.
- I feel so good opportunity for business networking.



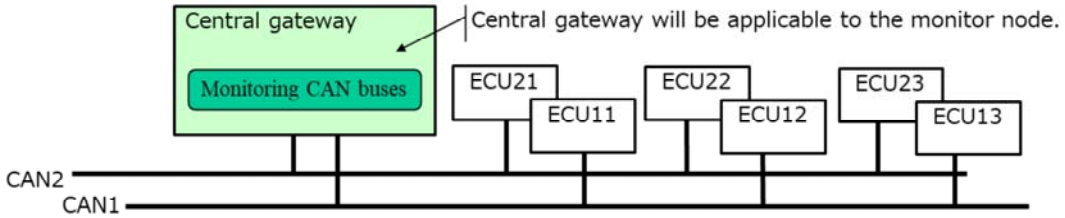


a) Our proposal – Centralized approach - CaCAN

※CaCAN = Centralized Authentication System in CAN

- Assumption:
  - The monitor node belongs to one of monitoring CAN bus.
  - The monitor node authenticates all other nodes which it belongs to monitoring CAN bus.
  - The monitor node authenticates all CAN messages with Message Authenticate Codes (MACs).

- Advantage:
  - Hardware extension is only monitor nodes. ⇒ Cost effective!
  - Easy install to existing in-vehicle systems.



42

NCES 名古屋大学大学院情報科学研究科 組込みシステム研究センター

We assume as follows. The monitor node belongs to one of monitoring CAN bus.

The monitor node authenticates all other nodes which it belongs to monitoring CAN bus.

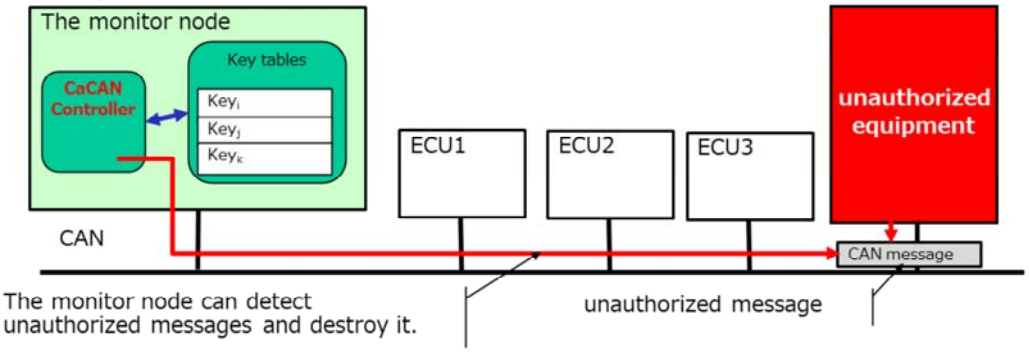
The monitor node authenticates all CAN messages with Message Authenticate Codes (MACs).

To achieve cost-effeciency, CaCAN achieves some advantages from existing method. One is a hardware extension is only monitoring nodes. And easy install to existing in-vehicle systems.

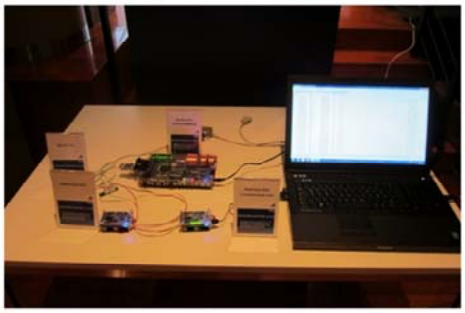
Then, we plan to implement the real central gateway of sumitomo.

a) Overview of our proposed system (Centralized approach)

- To authenticate ECUs, our protocol is designed to authenticate between a monitor node and other ECUs.
  - Number of authentication messages = 3 × Number of sending nodes with MACs
- The monitor node has the specialized CAN controller (named **CaCAN Controller**), but other existing nodes does not change implementation.
- The CaCAN controller can destroy unauthorized message by overwriting it by error frame.



b) escar EU 2015

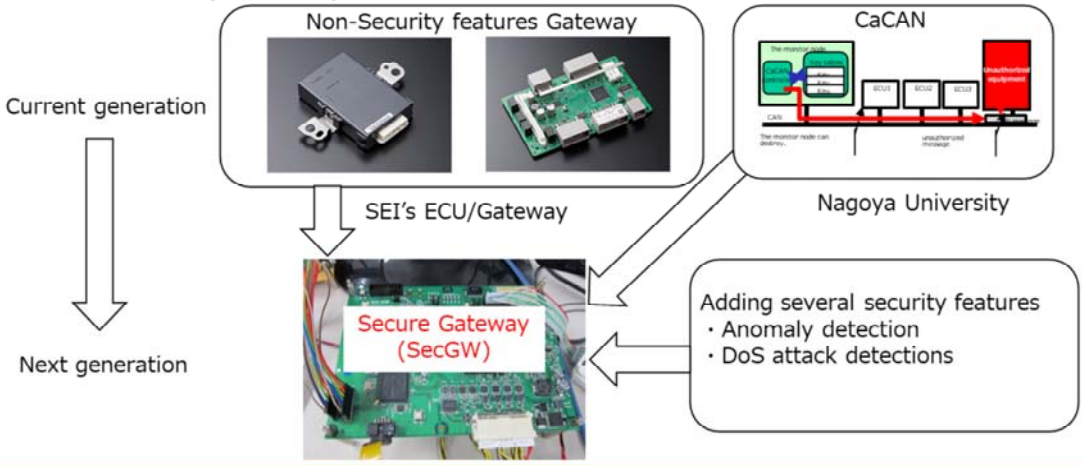


44

As can be seen, this slide shows the state of the escar EU 2015. At this conference, we presented the research topics and demonstrates the CaCAN system in tabletop.

b) Objectives: CaCAN implemented Gateway

- Sumitomo Electronics Industries, Ltd. (SEI) provides the ECU/Gateway to several Japanese OEMs. But not implemented security futures in current generations.
- SEI and Nagoya University developed the next-generation secure gateway (named SecGW) in which several security features (includes CaCAN) are implemented.

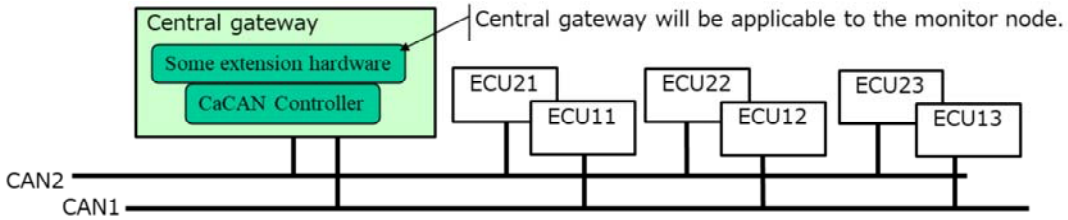


45

The details of secure gateway are discussed in later.

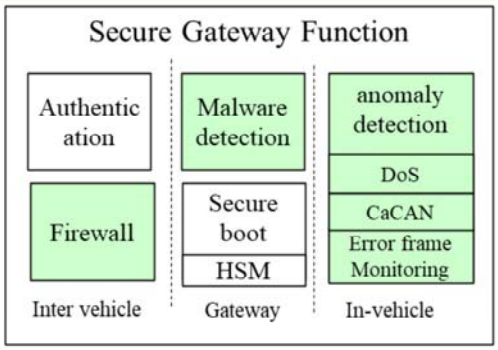
b) Concept of Security gateway

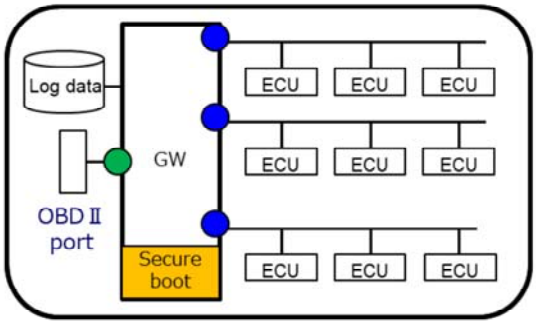
- Assumption:
  - Hardware extension is only central gateway.
  - The central gateway equips with the CaCAN Controller.
  - The central gateway monitors in-vehicle and inter-vehicle network.
    - But this paper only focuses in-vehicle networks.
- Advantages:
  - Based on the centralized approach, our secure gateway improves the security levels of in-vehicle networks.



I will tale about the assumption of secure gateway.

b) The secure gateway features





: monitoring & anomaly detection
: authentication, firewall

	Features	Add HW	Add SW
Firewall	HW-based filtering	Yes	No
Malware detection	HW-based filtering	Yes	No
Anomaly detection	CaCAN	Yes	No
〃	Error frame monitoring	Yes	No
〃	Dos detection	Yes	No

47

NCES 名古屋大学大学院情報科学研究科 組込みシステム研究センター

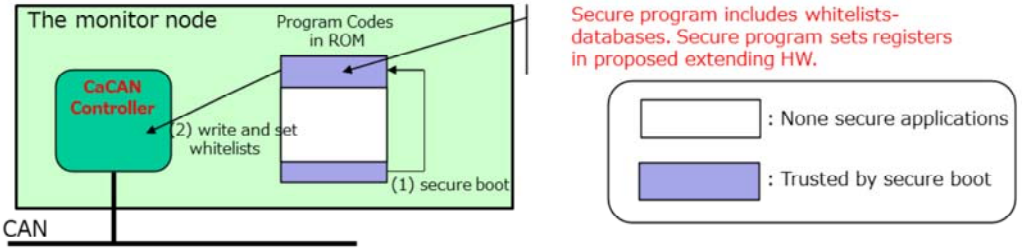
To illustrate the concept of our proposed secure gateway (SecGW), we provide in this figure a diagrammatic view of its components and the interactions between ECUs on the buses.

The main features of SecGW are a DoS attack detection, error-frame monitoring, and malware detection mechanisms.

All security features are implemented in a gateway to enable cost effectiveness. However, some features can be implemented on ECUs to improve the security levels. The details of security function will be explained in later:

b) Our Approach based on extending HW

- Problems of software-based approach
  - The updating of routing tables/Whitelists is non-secure.
  - Gateway performance must be high.
- Our Proposals:
  - **HW-based security protections with secure boot.**
  - With secure boot, trusted program must set all configurations registers includes whitelists, because most in-vehicle systems are "static" in the sense that all the messages they use are assigned in design phases.



48

NCES 名古屋大学大学院情報科学研究科 組込みシステム研究センター

In terms of security, existing software-based approach cannot achieve two aspects.

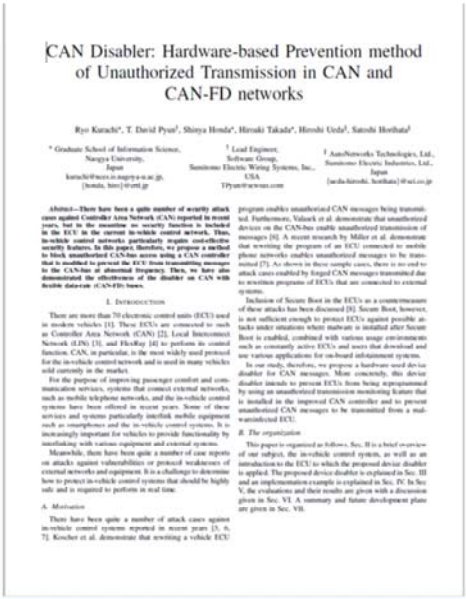
One is the secure updating of routing tables and whitelists. Thus, the security gateway can achieve secure updating by using a secure process.

The other is the reduction in gateway performance.

By executing protections in secure hardware (with minimum reliance software), we significantly reduce the possibility of malware subverting the protective mechanisms and thereby achieve a low-overhead technique.

c) escarUSA2016

- Research presentation of CAN Disabler.
- Demonstrated in Sumitomo presentation booth



CAN Disabler: Hardware-based Prevention method of Unauthorized Transmission in CAN and CAN-FD networks

Ryo Kurachi*, T. David Pyun†, Shinya Honda*, Hiroaki Takada*, Hiroshi Ueda‡, Satoshi Horihata‡

* Graduate School of Information Science, Nagoya University, Japan
kurachi@ertl.is.nagoya-u.ac.jp, {honda, hiro}@ertl.jp

† Lead Engineer, Software Group, Sumitomo Electric Wiring Systems, Inc., USA
TPyun@sewus.com

‡ AutoNetworks Technologies, Ltd., Sumitomo Electric Industries, Ltd., Japan
{ueda-hiroshi, horihata}@sei.co.jp

Abstract—There have been a quite number of security attack cases against Controller Area Network (CAN) reported in recent years, but in the meantime no security function is included in the ECU in the current in-vehicle control network. Thus, in-vehicle control networks particularly require cost-effective security features. In this paper, therefore, we propose a method to block unauthorized CAN-bus access using a CAN controller that is modified to prevent the ECU from transmitting messages to the CAN-bus at abnormal frequency. Then, we have also demonstrated the effectiveness of the disabler on CAN with flexible data-rate (CAN-FD) buses.

I. Introduction

There are more than 70 electronic control units (ECU) used in modern vehicles [1]. These ECUs are connected to each as Controller Area Network (CAN) [2], Local Interconnect Network (LIN) [3], and FlexRay [4] to perform its control function. CAN, in particular, is the most widely used protocol for the in-vehicle control network and is used in many vehicles sold currently in the market.

For the purpose of improving passenger comfort and communication services, systems that connect external networks, such as mobile telephone networks, and the in-vehicle control systems have been offered in recent years. Some of these services and systems particularly interlink mobile equipment such as smartphones and the in-vehicle control systems. It is increasingly important for vehicles to provide functionality by interlinking with various equipment and external systems.

Meanwhile, there have been quite a number of case reports on attacks against vulnerabilities or protocol weaknesses of external networks and equipment. It is a challenge to determine how to protect in-vehicle control systems that should be highly safe and is required to perform in real time.

A. Motivation

There have been quite a number of attack cases against in-vehicle control systems reported in recent years [5, 6, 7]. Koscher et al. demonstrate that rewriting a vehicle ECU program enables unauthorized CAN messages being transmitted. Furthermore, Valasek et al. demonstrate that unauthorized devices on the CAN-bus enable unauthorized transmission of messages [6]. A recent research by Miller et al. demonstrate that rewriting the program of an ECU connected to mobile phone networks enables unauthorized messages to be transmitted [7]. As shown in these sample cases, there is no end to attack cases enabled by forged CAN messages transmitted due to rewritten programs of ECUs that are connected to external systems.

Inclusion of Secure Boot in the ECUs as a countermeasure of these attacks has been discussed [8]. Secure Boot, however, is not sufficient enough to protect ECUs against possible attacks under situations where malware is installed after Secure Boot is enabled, combined with various usage environments such as constantly active ECUs and users that download and use various applications for on-board infotainment systems.

In our study, therefore, we propose a hardware-used device disabler for CAN messages. More concretely, this device disabler intends to prevent ECUs from being reprogrammed by using an unauthorized transmission monitoring feature that is installed in the improved CAN controller and to prevent unauthorized CAN messages to be transmitted from a malwareinfected ECU.

B. The organization

This paper is organized as follows. Sec. II is a brief overview of our subject, the in-vehicle control system, as well as an introduction to the ECU to which the proposed device disabler is applied. The proposed device disabler is explained in Sec. III and an implementation example is explained in Sec. IV. In Sec V, the evaluations and their results are given with a discussion given in Sec. VI. A summary and future development plans are given in Sec. VII.

In the interest of time, I would like to omit this item

d) Fuzz testing on CAN and CAN-FD protocols

- Objective of this Research:
  - As far as we know, although existing research mentions fuzzing tests of CAN, there is no mention of fuzzing tests of CAN-FD. Therefore, with this paper we have designed and evaluated a fuzzing test tool that supports CAN-FD.
- We can get the license of beSTORM from beyond security.

Implementation of the CAN-FD Protocol in the Fuzzing Tool beSTORM

50

NCES 名古屋大学大学院情報科学研究科 組込みシステム研究センター

Next topics is a fuzz testing for in-vehicle networks.

As far as we know, although existing research mentions fuzzing tests of CAN, there is no mention of fuzzing tests of CAN-FD. Therefore, with this paper we have designed and evaluated a fuzzing test tool that supports CAN-FD.

We implemented CAN and CAN-FD fuzzing tools by integrating bestorm.

As a results, We already presented this research topics at IEEE international conference.

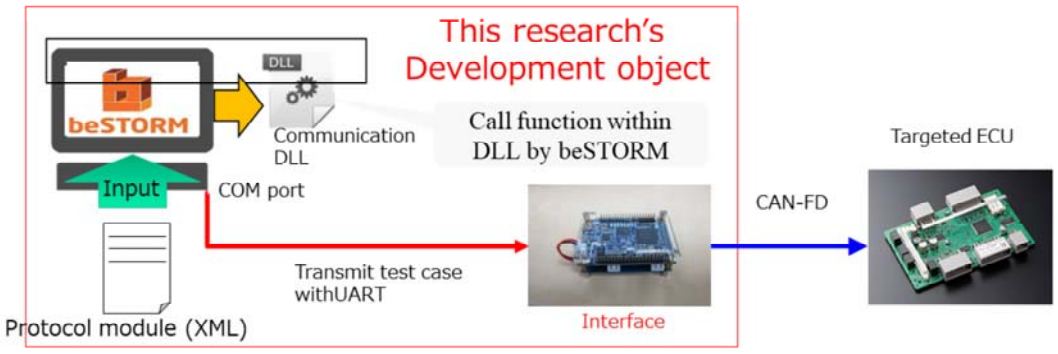
d) Fuzz testing on CAN and CAN-FD protocols

Components :

1. beSTORM ⇒ generation and execution of test cases
2. Interface ⇒ conversion of test data received from beSTORM into CAN-FD packet

Communication between beSTORM and Interface :

1. Transmit test cases generated by beSTORM with UART (red arrow)
2. DE0-NANO Received test cases transmits CAN-FD bus (blue arrow)



We have designed and implemented to integrate the existing fuzzing tool beSTORM with a CAN-FD interface.

As CAN-FD interface, we used FPGA board DE0-NANO.

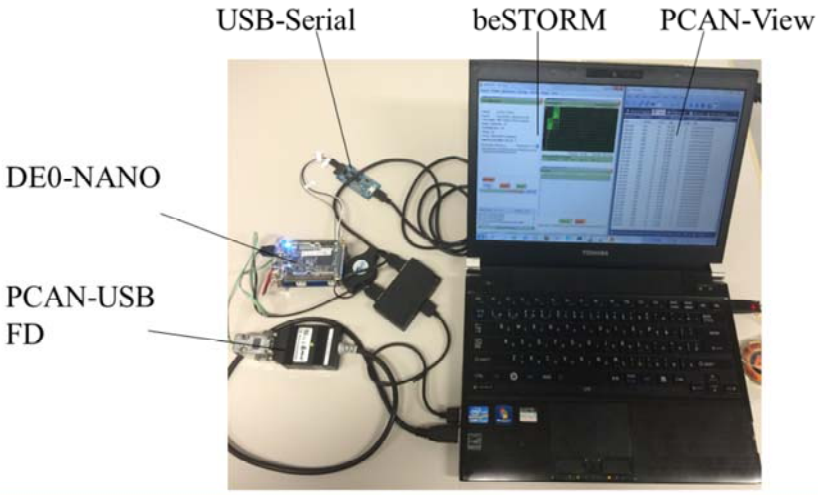
The beSTORM is necessary to define a protocol module. It is assumed that the protocol module will be described in the XML format.

The fuzzing data generated by beSTORM is transmitted from the COM port of the PC to DE0-NANO by the called function inside the DLL.

In our tool, this fuzzing data is received in the DE0-NANO from the UART port, converted to a CAN/CAN-FD frame, and transmitted to the ECU that is the evaluation target.

d) Fuzz testing on CAN and CAN-FD protocols

- Implementation environments



Concluding Remarks

Conclusion

- Currently, we collaborate with several auto suppliers to achieve secure automobiles.
- We also have successfully developed new security functionalities for in-vehicle systems.
  - For example, centralized approach, gateway and fuzz and pen testing.
- We hope that our work provides a good starting point to discuss approached for secure automobiles.
- Finally, we plan to investigate the following in future works.
  - 1) Machine learning for automotive security
  - 2) Appropriate security functionalities based on embedded techniques

54

NCES 名古屋大学大学院情報科学研究科 組込みシステム研究センター

Let me summarize my talk.

We have successfully developed new security functionalities for in-vehicle systems.

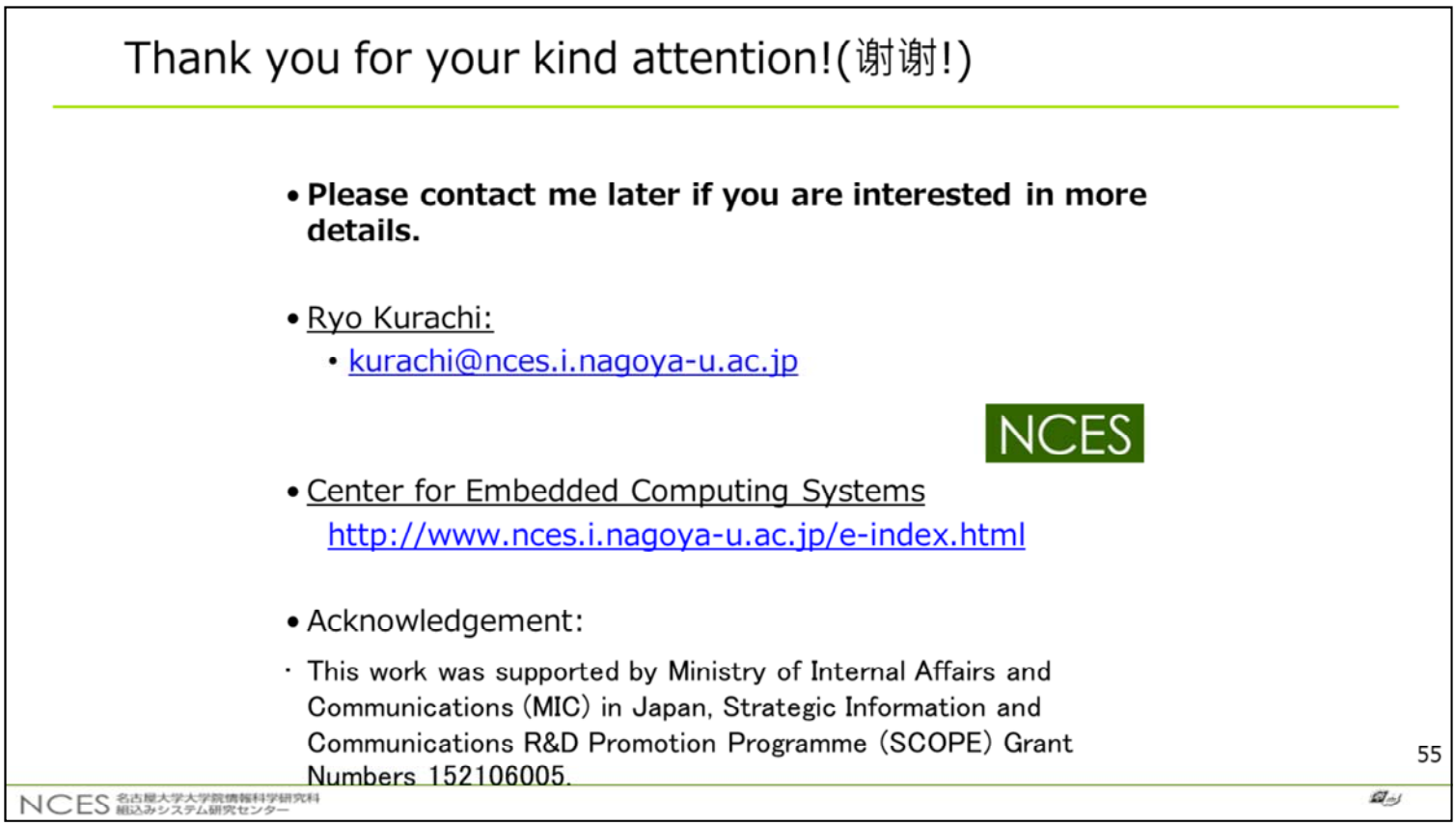
The implementation results confirms that our proposed solutions improves security performance compared to the performance of non-secure systems.

Finally, we plan to investigate the following in future works.

1) Machine learning for automotive security

2) Appropriate security functionalities based on embedded techniques

Thank you for your kind attention.



(A) I'm sorry, I couldn't hear you. Would you say that again.

(B) I don't quite understand your question. Could you please rephrase your question?

(C) I totally agree with you.

(D) That's very challenging question for me to answer.

I'm not sure I'm qualified enough to answer your question, but I'll try.

(E) That's a question I'm not sure I can answer right now.

The question you just asked me is hard to answer. It would require further research.

I'm sorry I can't answer that question since I'm still working on it myself.