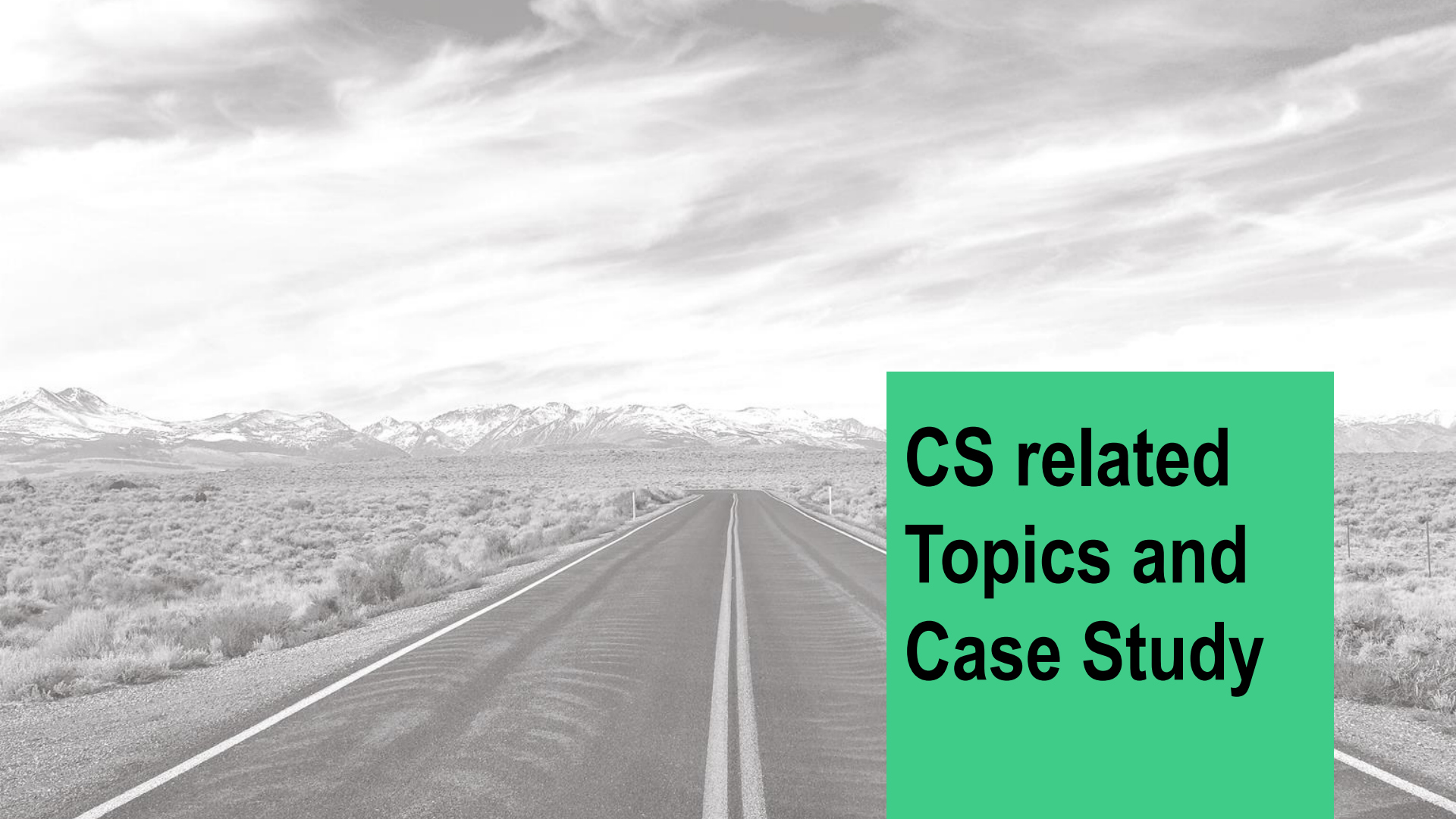


CS related Topics and Case Study

CS related Topics and Case Study

Introduction to CIA

Confidentiality: This property ensures that only trusted and accredited personnel are provided privileges or special access to adapt or modify the data contents. Two-factor authentications and rolling passwords are often used to ensure security.

Integrity: This property ensures that the legitimacy and accuracy of the data are maintained, thereby making it available to the authorized personnel to view this data at assigned periods of time. Such data when viewed is always in its pure state without any unauthorized modifications.

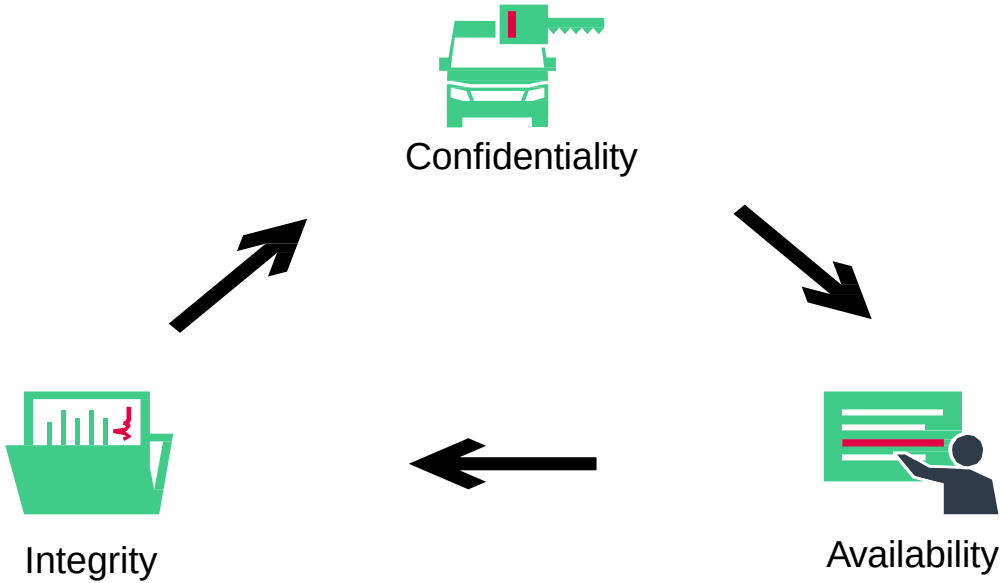
Availability: This property provides the above-mentioned authorized personnel the possibility to access the data at any point when requested.

It is important to understand that organizations generally have a different set of employees or personnel with a defined set of authorizations to cater to the CIA when it comes to data management.

CS related Topics and Case Study

Confidentiality, Integrity and Availability – A Triad Model

The CIA Triad Model is the most prominent representation of information security within organizations and acts as a guide to establish data security.



CS related Topics and Case Study

DEKRA DIGITAL

Threat Scenario Identification

- For each damage scenario, corresponding threat scenarios are identified
- Threat scenarios can include:
  - Targeted asset
  - Compromised security property
  - Action to achieve damage scenario
- For methods like brainstorming, use case elicitation, etc. STRIDE could be used

CS related Topics and Case Study

DEKRA DIGITAL

Threat Scenario Identification : Relationship between CIA and STRIDE

- STRIDE is a mnemonic for six possible threats Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege.
- STRIDE was in the 90's by engineers from Microsoft – Loren Kohnfelder and Praerit Garg as a part of threat modelling process. The threats are categorized based on the goals and purposes of the attacks
- Relates threats with security attributes (security properties)
- The extended CIA model includes Authenticity, authorization and non-repudiation. The relationship between STRIDE and extended CIA are illustrated in the table to the right.

Threat	Security property
Spoofing	Authenticity
Tampering	Integrity
Repudiation	Non-repudiability
Information disclosure	Confidentiality
Denial of service	Availability
Elevation of privilege	Authorization

CS related Topics and Case Study

DEKRA DIGITAL

Threat Scenario Identification: Spoofing

- Spoofing is an attack method where an attacker or a malicious code imitates an authentic entity
- Spoofing attacks compromise the authenticity of property
- Authenticity is a special case of integrity property
- Some of the well-known spoofing attacks are man-in-middle attacks, GPS spoofing, Pharming attacks, evil twin attacks, etc.

Example:

Camera-based ADAS systems are tricked by projecting false road signs as phantom images

CS related Topics and Case Study

DEKRA DIGITAL

Threat Scenario Identification: Tampering

- When the integrity of a data is compromised, it leads to tampering
- Tampering is an act of illegally modifying an asset, data, or a hardware component
- Physical tampering of components could also lead to cyber attacks
- Security fuses, chips made of tempered glass, encapsulation are some physical security controls
- Anti tamper controls in software include write protection, checksums, obfuscation, etc.

Example:

Reengineering the components (such as sensors) can be considered tampering

CS related Topics and Case Study

DEKRA DIGITAL

Threat Scenario Identification: Repudiation

- Repudiation attacks may happen if the actions performed are not logged
- Repudiation is an attack where a person denies an action that he/she performed
- Authentication is a by-product of non-repudiation
- Non-repudiation is more a legal concept than technical
- Event logs, digital signatures, etc. are some methods used against repudiation attacks

Example:

A bad driver after causing an accident claims to have applied brakes while he didn't and blames the braking system.

CS related Topics and Case Study

Threat Scenario Identification : Information Disclosure

- Information disclosure attacks happens when the confidentiality of a data is breached
- Information disclosure is when sensitive information such as personally identifiable information, confidential data, intellectual property, etc. are obtained unlawfully without proper access or authorization by an attacker
- Encryption, access control, physical security controls, etc. are employed to protect the confidentiality of the data

Example:

An attacker gaining access to the navigation system and finding out the frequently visited places, location of interest of the vehicle user is an information disclosure attack

CS related Topics and Case Study

DEKRA DIGITAL

Threat Scenario Identification : Denial of Service

- A Denial-of-Service attack is an attack against the operationality of a system/functionality, making it unavailable
- It targets the Availability of CIA, and Operational of SFOP
- The attacker often tries to consume the resources of the system by flooding, having an impact on the performance until the system/service is not available anymore
- Flooding detection, resource allocation, filtering are mitigations that can be used to prevent DoS attacks
- Encryption, access control, physical security controls, etc. Are employed to protect the confidentiality of the data

Example:

An attacker floods the OBD port with thousands of Diagnostic requests, making the targeted ECU unavailable if no security measures are taken.

CS related Topics and Case Study

DEKRA DIGITAL

Threat Scenario Identification : Elevation of Privilege

- This attack is carried out once an attacker has access to the system
- Elevation of privilege attack is performed by an attacker to gain access to the resources/functionalities that are protected from the user
- Encrypting software components, strict access controls, the principle of least privilege, etc. Are some strategies used to tackle the elevation of privilege

Example:

A vehicle user who doesn't have the permissions to use some functionalities in a car, gets it illegally is considered an elevation of privilege attack

CS related Topics and Case Study

DEKRA DIGITAL

Defense in depth: State of the art security controls

Hardware Security Modules (HSM)

- Manage cryptography keys, perform encryption and decryption ...
- Hardened hardware module resistant to attacks
- Secure boot

Network architecture

- Isolate subnetworks physically or with VLANs
- Prevents communication between non-related areas of the vehicle

CS related Topics and Case Study

DEKRA DIGITAL

Defense in depth: State of the art security controls

Authenticity checks

- Communication protocols to verify the authenticity of upcoming messages (CAN, IPsec, ...)
- Matching configuration to avoid intrusion (DoIP, ...)

Intrusion detection

- Logging and analyzing logs in order to identify abnormal behavior
- Specifications defined in AUTOSAR for the vehicle
- Can also be performed on back-end level

Firewalls

- Modern vehicles are equipped with gateways that can also enable complex network communications and filter abnormal signals.

CS related Topics and Case Study

DEKRA DIGITAL

Defense in depth: State of the art security controls

Annex 5 of R155

- R155 regulation document gives a lot of hints on what could be the measures to apply in order to mitigate the threats.

in Table C2.

Table C2

Mitigations to the threats which are related to "Unintended human actions"

Table A1 reference	*Threats relating to "Unintended human actions"*	*Ref*	*Mitigation*
15.1	Innocent victim (e.g. owner, operator or maintenance engineer) is tricked into taking an action to unintentionally load malware or enable an attack	M18	Measures shall be implemented for defining and controlling user roles and access privileges, based on the principle of least access privilege
15.2	Defined security procedures are not followed	M19	Organizations shall ensure security procedures are defined and followed including logging of actions and access related to the management of the security functions

CS related Topics and Case Study

DEKRA DIGITAL

Cybersecurity Controls

Cybersecurity controls are the measures that are implemented to modify the risk thereby reducing the residual risk.

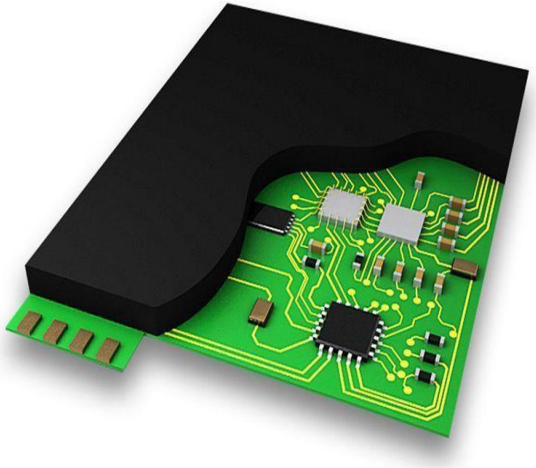
- Based on the type, security controls can be categorized as
  - Physical controls such as locks, protective casing, etc.
  - Technical controls such as authentication systems, encryption, etc.
  - Administrative controls such as organizational rules, processes, etc.
- The security controls perform
  - Preventive functions to stop attacks. E.g., Firewall
  - Detective functions to detect attacks. E.g., Intrusion detection systems
  - Corrective functions to repair damage to attacks and return the system to its previous state. E.g., Polling functions, Vehicle safe state modes, etc.
- STRIDE is commonly used to identify cybersecurity threats.
  Hence, security controls can be assigned to mitigate these threats

CS related Topics and Case Study

DEKRA DIGITAL

Physical Cybersecurity Controls

- Physical controls ensure cybersecurity by restricting access to the component, some of the common physical cybersecurity controls in vehicles are
  - Encapsulation of ECUs
  - Tamper proofing chips (e.g.)
  - Secure casing for components
  - Tamper resistant sensors



Source: https://www.sbhpp.com/products-applications/automotive.html

CS related Topics and Case Study

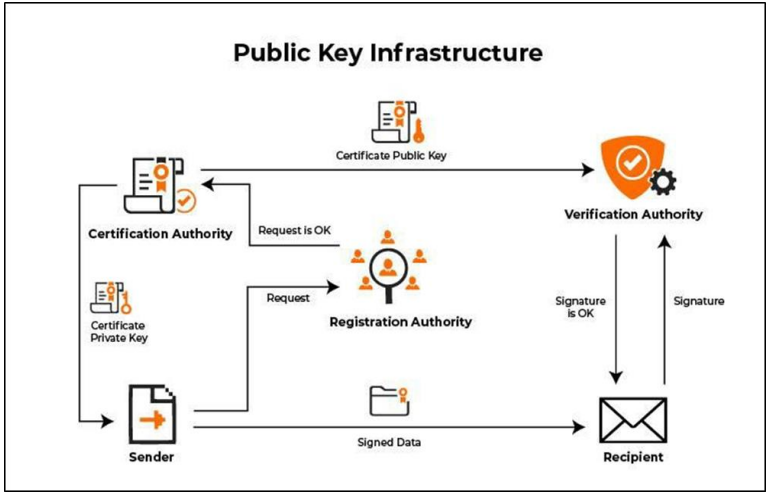
DEKRA DIGITAL

Technical Security Controls

Technical security controls can be hardware or software modules and can be implemented in the item.

Some of the technical security controls employed in vehicles are

- Vehicle firewall
- Intrusion detection systems
- Encryption and PKI
- Data Logging modules
  (e.g., Log accident data)
- Honey pots in in-vehicle networks
- Vehicle antivirus



Source: https://www.appviewx.com/education-center/pki/

CS related Topics and Case Study

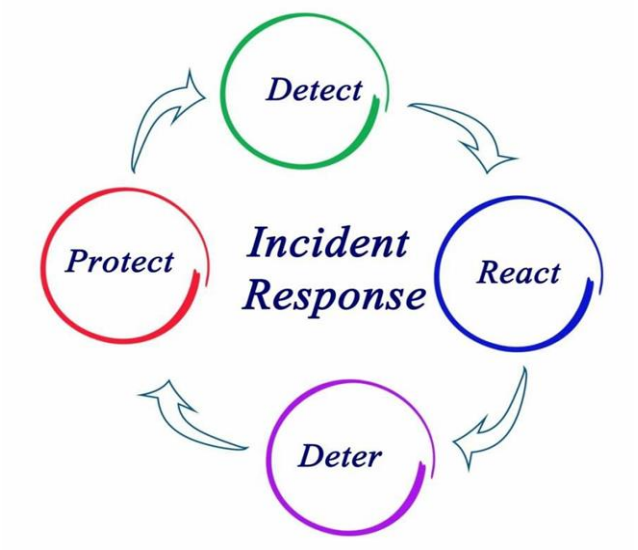
DEKRA DIGITAL

Administrative Security Controls

Administrative security controls refer to policies, processes, and guidelines followed within the OEM or the supplier‘s organization that enhance the security of the vehicle or a vehicle component.

Some of the administrative security controls that are employed in vehicles are

- Following secure design and development processes
- Using coding standards (e.g., MISRA C)
- Setting up incident response activities and processes
- Setting up continuous monitoring activities



Source: https://blog.24by7security.com/test- cybersecurity-incident-response-plan

CS related Topics and Case Study

DEKRA DIGITAL

Threat Modeling

What is threat modeling?

Threat modeling is a structured approach of identifying and prioritizing potential threats to an item/component/system and determining the value that potential mitigations would have in reducing or neutralizing those threats

Why threat modelling is important?

Computers and ECUs play a major role in today's road vehicles. This creates the possibility of a wide range of attacks. This forces the component manufacturers and OEM to develop secure by design products. Identifying the possible threats and risks play a major role in secure development.

The infamous Cherokee Jeep hack is one example that signifies the importance of threat modeling and security by design approach.

CS related Topics and Case Study

DEKRA DIGITAL

Threat Modeling

- Data flow graphs, threat model diagrams are used to perform threat modeling
  - Threat modeling can be used as an initial step for TARA
  - The data flows, assets are identified
  - The threats corresponding to loss of security properties of the data are identified (STRIDE can be applied)
  - The attack methods and attack paths for each threat are identified
  - The risks for each threat are identified
- Microsoft threat modeling tool is used in the secure development lifecycle.
- Threat modeling is used to determine security objectives and security requirements of a system

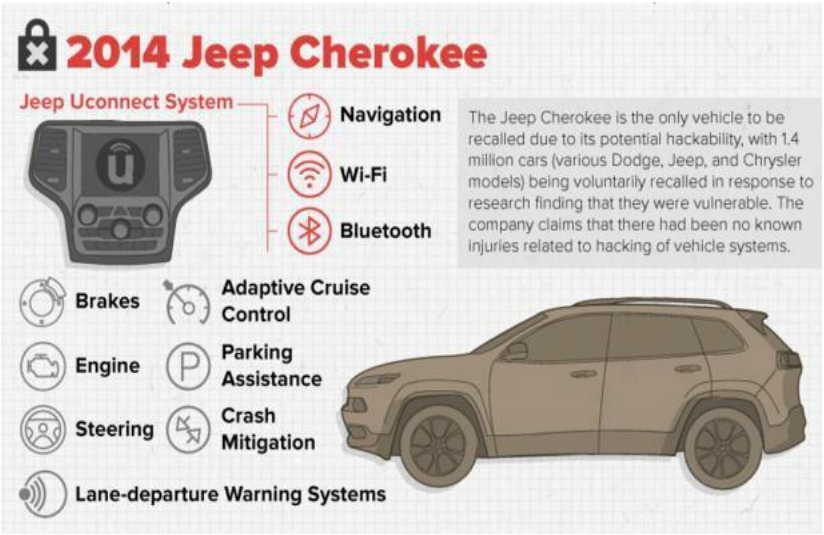
Threat modeling, attack analysis, identifying threats will be discussed in detail during TARA training

CS related Topics and Case Study

Cherokee Jeep Hack: Case Study

Researchers Charlie Miller and Chris Valasek presented their findings at black hat USA 2015. They have managed to carry out the following attack by exploiting Uconnect infotainment system:

- Gain access via Wi-Fi using brute force method
- Take control of the Head unit's system
- Track the car with the GPS and navigational systems
- Access CAN bus and read CAN messages
- Using special components, a firmware upgrade is performed allowing complete control of the vehicle products



Source: https://illmatics.com/Remote%20Car%20Hacking.pdf

CS related Topics and Case Study

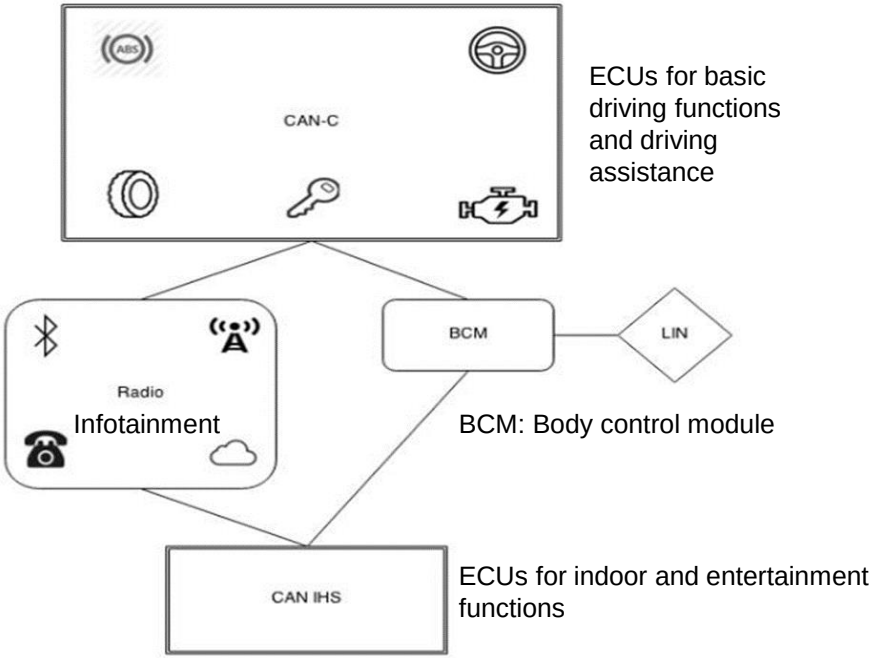
Cherokee Jeep Hack: Case Study

Network architecture

- Head Unit is connected to both CAN buses
- Compromising radio could provide access to ECUs on both CAN-IHS and CAN-C networks
- No CAN bus architectural restrictions (such as isolation of steering)

Cyber-Physical Features

- Adaptive cruise control
- Forward collision warning
- Lane departure warning
- Park assist system



Jeep Cherokee Communication Diagram

CS related Topics and Case Study

DEKRA DIGITAL

Cherokee Jeep Hack: Case Study

Attack vectors

- Every component, data, or technology that interacts with the outside world is a potential entry point for an attacker)

Entry Point	Compromised system	BUS
RKE	RFHM	CAN C
TPMS	RFHM	CAN C
Bluetooth	Radio	CAN C, CAN IHS
FM/AM, GPS	Radio	CAN C, CAN IHS
Cellular	Radio	CAN C, CAN IHS
Internet / Apps	Radio	CAN C, CAN IHS

RKE: Remote Keyless Entry
TPMS: Tire Pressure Monitoring System
RFHM: Radio Frequency Hub Module

CS related Topics and Case Study

DEKRA DIGITAL

Cherokee Jeep Hack: Case Study

Affected models:

- 2013-2015 MY Dodge Viper specialty vehicles
- 2013-2015 Ram 1500, 2500, and 3500 pickups
- 2013-2015 Ram 3500, 4500, 5500 Chassis Cabs
- 2014-2015 Jeep Grand Cherokee and Cherokee SUVs
- 2014-2015 Dodge Durango SUVs
- 2015 MY Chrysler 200, Chrysler 300, and Dodge Charger sedans
- 2015 Dodge Challenger sports coupes

CS related Topics and Case Study

DEKRA DIGITAL

Cherokee Jeep Hack: Case Study

Aftermath:

Jeep owners urged to update their cars after hackers take remote control

Security bug allows remote attack of Uconnect system, letting hackers apply the brakes, kill the engine and take control of steering over the internet

NEWS

Jeep hack raises questions about responsibility for security

The hack of a Jeep raises the question whether users or car manufacturers should be responsible for protecting against cyber attackers

JULY 22, 2015

Fiat Chrysler says it has a software fix to prevent hacking

Fiat Chrysler recalls 1.4 million cars after Jeep hack

24 July 2015

Hackers That Exposed Jeep Cherokee Security Flaws Wreak More Havoc

They find new ways to hack a Cherokee even after the security patch

DEKRA

DEKRA DIGITAL

Thank you for your attention