VicOne

USE CASE

Protecting a Telematics Control Unit From Remote Attacks

Analyzing a contactless attack on a telematics control unit

In 2017, Tencent Keen Security Lab conducted a comprehensive research with various BMW car systems, which included performing physical and remote attacks on the in-vehicle infotainment (IVI) system and telematics control unit (TCU). After 13 months of in-depth experiments, the researchers discovered 14 exploitable vulnerabilities and published a summary report describing their findings.

In this use case, we take a closer look at the experiment that exploited the TCU via a cellular network and map the activity to the VicOne Automotive Attack Matrix and the threat categories listed in UN Regulation No. 155 (UN R155).

UN R155 threat category mapping

The attack techniques used in the research can be mapped to the threat categories defined in UN R155, as illustrated in the following diagram. Manufacturers can use this information to conduct further investigations and make necessary mitigation plans.

4.3.1	**4.3.2**	4.3.3	4.3.4	**4.3.5**	**4.3.6**	**4.3.7**
Back-end servers	Communicat-ion channels	Update procedures	Unintended human actions facilitating a cyber attack	External connectivity and connections	Vehicle data/ code	Potential vulnerabilities

How it's done

1. Establish connection with the victim vehicle through a cellular network.

The researchers built a false cellular base station with stronger signal strength so that the TCU in the victim vehicle had a higher chance of connecting to it.

Once the TCU connected to the false cellular base station, the researchers suppressed the TSP signals with a signal suppressor to ensure that the victim vehicle was serviced by their false cellular base station.

UN R155

- 4.3.2 Communication channels
- 4.3.5 External connectivity and connections

Automotive Attack Matrix

- Manipulate Environment
- Rogue Cellular Base Station
- Manipulate Device Communication

2. Exploit zero-day vulnerabilities in the TCU.

By sending crafted telematic messages, the researchers exploited the TCU vulnerabilities (CVE-2018-9311 and CVE-2018-9318) to trigger remote diagnostic services.

UN R155

- 4.3.2 Communication channels
- 4.3.7 Potential vulnerabilities

Automotive Attack Matrix

- Initial Access
- Exploit via Radio Interface

3. Obtain root privileges to the TCU.

The researchers found a memory corruption vulnerability in the TCU firmware, allowing them to bypass signature protection and gain root access to the TCU via remote code execution (RCE).

UN R155

- 4.3.2 Communication channels
- 4.3.5 External connectivity and connections
- 4.3.6 Vehicle data/code

Automotive Attack Matrix

- Defense Evasion
- Subvert Trust Control

4. Take control of the vehicle remotely.

After compromising the TCU, the researchers can send crafted Controller Area Network (CAN bus) messages to affect control of other electronic control units (ECUs) in the vehicle.

UN R155

- 4.3.2 Communication channels
- 4.3.5 External connectivity and connections
- 4.3.6 Vehicle data/code

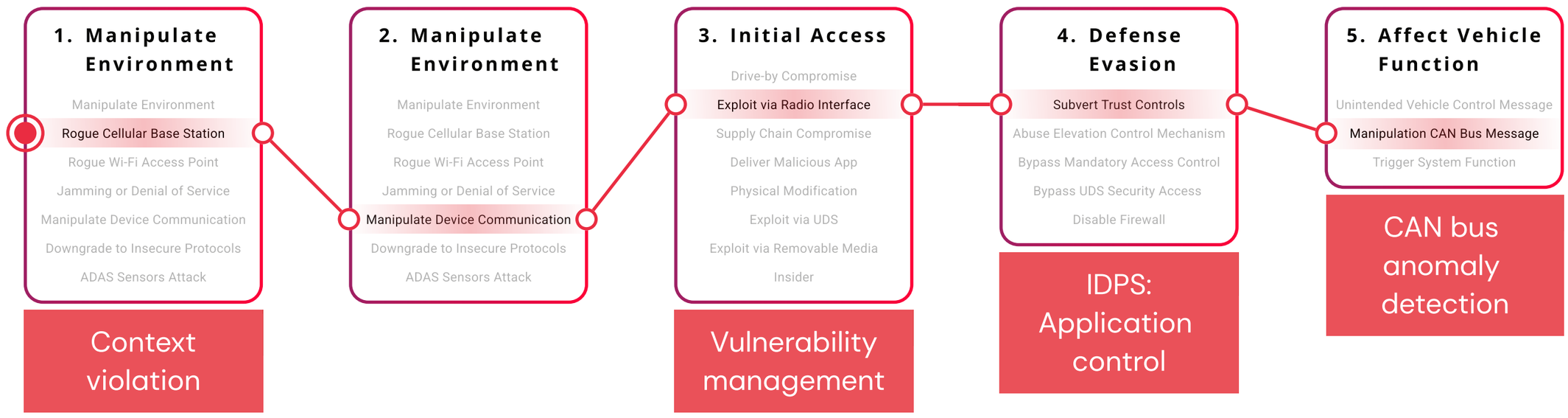
Automotive Attack Matrix

- Affect Vehicle Function
- Manipulation CAN Bus Message

How can VicOne help?

By utilizing the Automotive Attack Matrix, we understand the goal and reason of using a particular technique in each hacking stage. In this section, we discuss how VicOne can help manufacturers prevent this attack and secure their systems throughout a vehicle's life cycle.

Based on what we learned from this research, the following are some ways that VicOne can help boost automotive security:



- **Identify anomalous vehicle events to protect vehicle function.**

  By comparing and analyzing vehicle telematics and profile, xNexus can identify anomalous vehicle events, such as disconnection from the telematics server due to connection to a false cellular base station and injection of malicious CAN bus messages.

- **Discover vulnerabilities and mitigate risks at an early stage.**

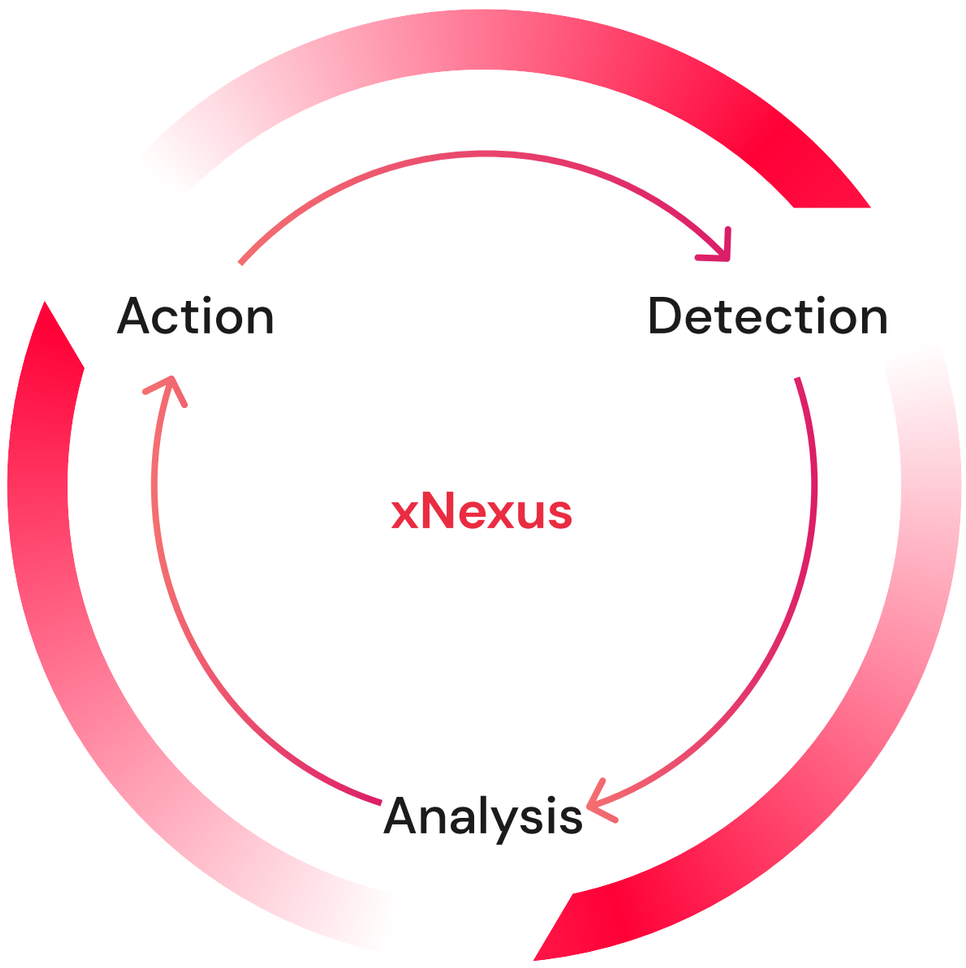
  xZETA can identify software vulnerabilities in ECUs, allowing manufacturers to mitigate risks before production.

- **Prevent privilege escalation with application control.**

  xCarbon provides application control to restrict the applications that can run in vehicles. This helps prevent privilege escalation attacks or unauthorized application execution.

About VicOne Automotive Security

Our Automotive Security team offers comprehensive protection against cyberattacks targeting connected vehicles through xNexus, a cloud-based vehicle security operation center (VSOC). By leveraging extended detection and response (XDR) capabilities, automotive threat intelligence, OEM data, and xCarbon in-vehicle sensors, xNexus ensures compliance with UN Regulation No. 155 (UN R155), maps threats to the ATT&CK Matrix, highlights threats applicable to automotive cyberattacks, and keeps up with the latest automotive cybersecurity incidents.



Detection

Receives data or security notifications from various sources

Analysis

Conducts broad-spectrum correlation analysis of threats

Action

Visualizes analysis results in a unified view to assist in further investigations or mitigation

For more information:

Website:

https://www.vicone.com/

Contact:

https://www.vicone.com/contact-us