Nation-based mapping

Relation between Nations and Locations

To reveal the differences in ICV security across countries of manufacture, we analyzed the distribution of vulnerabilities across different modules in ICVs from various nations, as shown in Table. 1. ICVs manufactured in China account for the vast majority of all recorded vulnerabilities (88.6%). This is largely due to the lack of unified and mature standards for ICV production, with many regulations still in trial stages, leading to heterogeneous network architectures and protection mechanisms across manufacturers. In contrast, vulnerabilities in American vehicles are predominantly concentrated in in-vehicle components (such as ECUs and IVIs), accounting for as much as 89.3%, with almost no cloud platform vulnerabilities.
German ICVs exhibit a more balanced distribution, with 59.4% of vulnerabilities involving cloud platforms and APPs, and 40.6% tied to in-vehicle systems—indicating simultaneous emphasis on internal and external system protection.

Table 1: Mapping location results of the ICV nation-based taxonomy.

Location \ Nation	China	German	America	Japan	Korea	France	Sum
Cloud platform	221	14		7	1	2	245
IVI	191	7	10				208
APP	55	5	3	1	2		66
ECU	41		5				46
Network	29		1	1			31
T-Box	21	1	6				28
Radio	7	5	3				15
Charging pile	10						10
Sum	575	32	28	9	3	2	649

Relation between Nations and Types

As shown in Table. 2, from a vulnerability type perspective, authorization issues dominate across all nations but are especially prominent in Chinese ICVs (36.87\%), suggesting persistent challenges in access control and identity verification. Chinese vehicles also show high instances of information leakage (104) and injection vulnerabilities (73), indicating gaps in secure data handling and input sanitization. German vehicles present a more distributed type profile, though authorization flaws remain primary. In contrast, American vehicles, despite having fewer total vulnerabilities, show a low proportion of information leakage (7.1\%), highlighting concerns with data exposure and insufficient boundary protections. These patterns reflect differing priorities and levels of cybersecurity maturity among ICV-producing nations.

Table 2: Mapping type results of the ICV nation-based taxonomy.

Type \ Nation	China	German	America	Japan	Korea	France	Sum
Authorization	212	12	5	5		2	236
Information leakage	104	4	2	2			112
Injection	73	3	2		1		79
OS	52	1	2				55
DoS	35	3	6	1	2		47
File operation	35	1	1	1			38
Interception	30	4	2				36
Web-specific	23	3					26
Memory	11	1	8				20
Sum	575	32	28	9	3	2	649

APP class-based mapping

The app in the competition is the default app provided by the car manufacturer, developed often in Java, and serves informational and entertainment functions, such as a car owner forum and remote door unlocking.

We classify the 66 app vulnerabilities we have collected into two categories: the first category includes vulnerabilities within the app itself, such as car mileage information leakage and arbitrary account password login, called “ APP-internal”; the second category involves vulnerabilities that affect vehicle safety, such as the ability to control the vehicle's unlocking, called "APP-to-vehicle". As shown in Table. 3, it can be observed that while the car manufacturer has implemented some protection for communication between the app and the car, they have overlooked the app's security, leading to vulnerabilities such as owner information leakage and arbitrary account logins.

Therefore, car manufacturers should not only focus on the app's security during communication with the car but also pay attention to the app's full lifecycle security, from the development phase to the usage phase, in order to avoid common basic errors during the development stage, such as information leakage (27), unauthorized accessing (19), and unvalidated inputs (Command injection (6), SQL injection (1)).

Table 3: Mapping results of the APP class taxonomy.

Type	APP-internal	APP-to-vehicle	Sum
Information leakage	25	2	27
Unauthorized accessing	19		19

Type	APP-internal	APP-to-vehicle	Sum
DoS	7		7
Command injection	5	1	6
Weak password	2		2
Replay	1	1	2
SQL injection	1		1
Man-in-the-middle	1		1
Identity spoofing	1		1
Sum	62	4	66