Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Introduction to connected vehicles

Content complexity
SIMPLE

For more cyber security advice

For more information on how to improve your cyber security, see our other guides at cyber.gov.au

Table of contents

Common features 4

Cyber security risks 5

CVs collect personal data 5

How to reduce risk 6

Connected services 7

How to reduce risk 8

Electric vehicle charging stations 8

How to reduce risk 8

Key points when buying and owning a CV 9

More information 9

Introduction to connected vehicles

A connected vehicle (CV) provides enhanced convenience, functionality and safety.

CV refers to any vehicle that is connected to the internet, such as through an inbuilt SIM card or a paired smartphone. Internet connectivity allows the vehicle to communicate with other devices and external infrastructure. CVs are not limited to electric vehicles (EVs) – vehicles with internal combustion engines are also considered CVs if they connect to the internet. Most new electric and conventional combustion engine vehicles sold in Australia include Internet of Things (IoT) devices and network-interfaced features as part of their design.

Trend of CVs in Australia

By 2021, there were an estimated 1.2 million CVs in Australia. By 2031, CVs will likely make up 93% of all new vehicles.[1] This means that there is a good chance the next vehicle you buy or rent will be a CV.

This guide provides cyber security information you should consider before buying and using CVs.

Common features

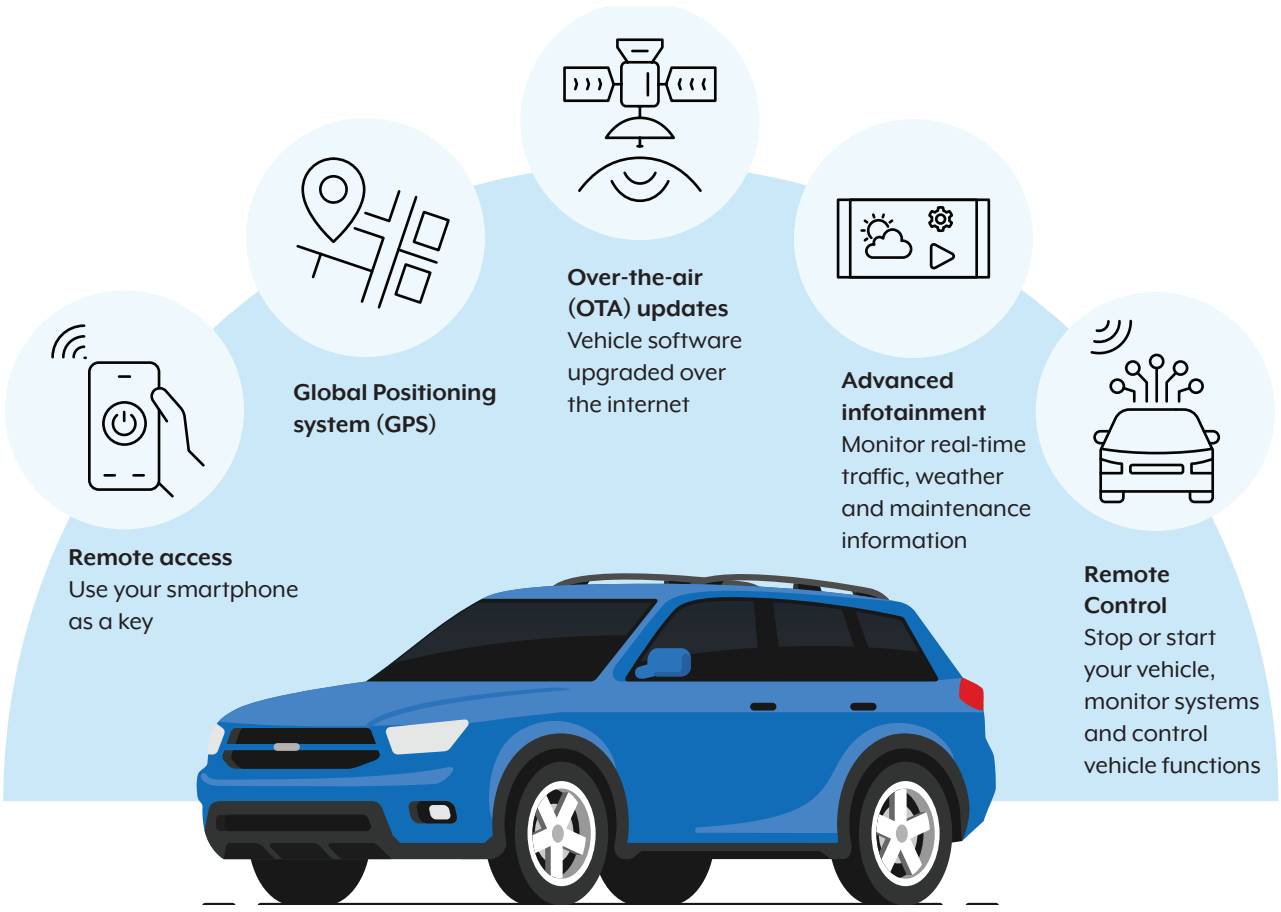


Figure 1. Common features of connected vehicles

1 Austroads, 'Future Vehicles Forecasts Update 2031 – AP-R654-21', 2021.

Cyber security risks

CVs carry cyber security risks that vary depending on their level of connectivity. These risks include personal privacy breaches and remote hacking.

CVs collect personal data

CVs have advanced telematics systems. Telematics systems collect and transmit a variety of data to manufacturers and third-party service providers in real time. How much data is collected can have serious implications for the privacy of users given it can be potentially sensitive data.

Examples of data that can be collected and transmitted include:

- external and internal image or video captures
- internal audio, including voice commands
- smartphone use, such as call logs, SMS logs, contacts and calendar events
- infotainment system use
- real-time Global Navigation Satellite System (GNSS) locations, including navigation entries
- driving behaviour metrics:
  - brake application
  - cornering speed
  - rate of acceleration
  - speed
  - stop sign violations
- driver focus metrics:
  - blinking intervals
  - driver eye tracking
  - face orientation
- vehicle performance and environment metrics:
  - cabin air quality
  - climate control use
  - driver and passenger weight
  - emissions
  - external and internal temperature
  - fuel efficiency
  - fuel level and battery life
  - odometer reading
  - tyre pressures
  - window use

Infotainment systems store messages and call logs

A CV's infotainment system can also collect data from any device that is connected to the vehicle. This data can include the entire content of SMS messages and social media use, music preferences and more. It can also include transcripts of text messages, call logs and, possibly, recorded phone calls. This data is extracted from every device connected to the vehicle and can be stored permanently by the vehicle. The data can be recovered using specialist tools, in some cases without having physical access to the vehicle. Over time, if the automotive industry doesn't focus on improving cyber security, the ability for cybercriminals to illegally extract this data will likely become widespread.

Data gets extracted, analysed and shared

The data a CV collects can be stored by the manufacturer overseas, where Australian data protection laws will not apply. This data is attractive to cybercriminals, as demonstrated by several large and high-profile data breaches of manufacturers in recent years.

If manufacturers share data with third parties, these parties may also become targets of cybercriminals if they don't have best-practice cyber security protections in place.

How to reduce your risk

Carefully review the privacy and data collection policies of the manufacturer before deciding to buy a CV. Consider the data laws of the country in which the manufacturer will store the data. The data may be more accessible there to cybercriminals, or may be subject to laws that provide foreign intelligence services access to your data.

- Consider the potential benefits and risks of enabling 'smart driver' reports in your vehicle's features or services menu.
- Turn off the 'share vehicle data' option in your vehicle's features or services menu where possible.
- Consider the potential implications of connecting your smart devices to the infotainment system (especially in rental vehicles), either by Bluetooth or USB.
- Restore your vehicle to factory settings before selling or disposing of it.
- Restore vehicle to factory settings before use when purchasing a used vehicle.
- Research the manufacturer's approach to cyber security when purchasing a vehicle.

Case study: Unauthorised recording

In January 2023, reports emerged about a potential vulnerability affecting CVs manufactured by a popular company. Unauthorised people could spy on and record CV owners' conversations without their knowledge, even when the vehicles were turned off.

When this vulnerability was publicly reported, the manufacturer fixed the issue.

As shown in figure 2, an unauthorised person could make a call to the inbuilt SIM number. The CV user didn't know there was an incoming call and their conversation could be recorded without their consent. There was also no option for the CV user to end the call, even by turning the vehicle off.

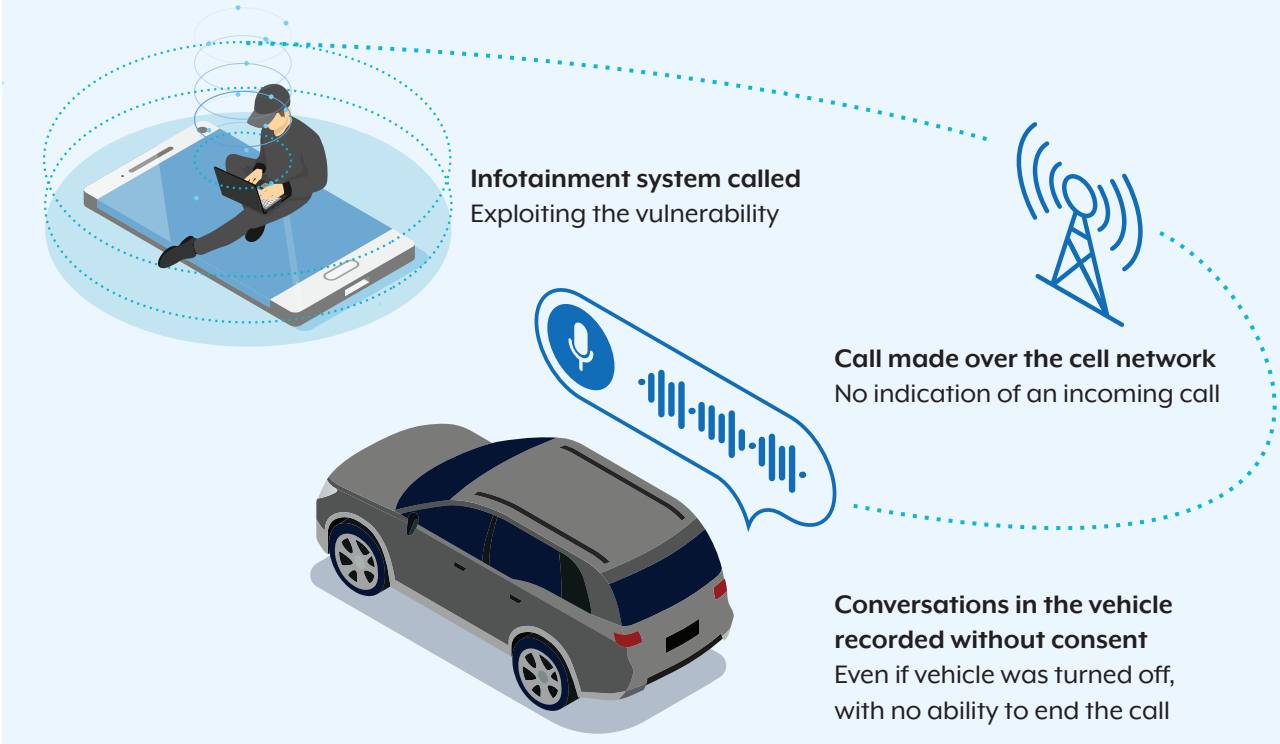


Figure 2. Case study unauthorised recording

Connected services

Internet connectivity in vehicles allows remote access to certain vehicle functions. An increasing number of manufacturers now offer connected services through mobile apps. These apps can allow a user to remotely:

- lock or unlock a vehicle
- start or stop the engine
- change climate control settings
- access the vehicle's external or internal cameras, and internal microphones
- view vehicle telemetry.

These apps often connect and communicate with cloud networks managed by the manufacturer, dealership or application service providers. This means that data is stored in the vehicle but also uploaded to the cloud on a regular or real-time basis.

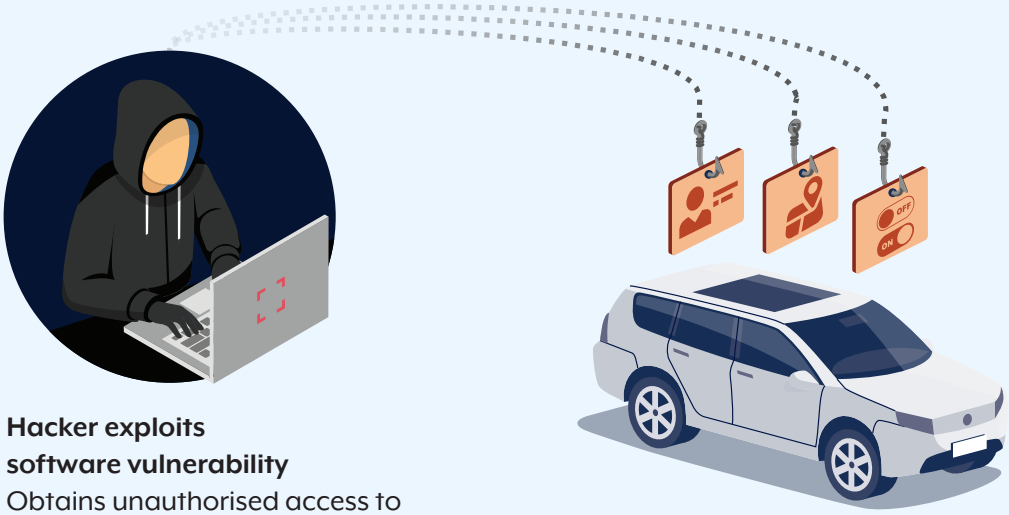
Interconnected apps in CVs work together to give consumers additional features. However, they create more ways for cybercriminals to gain access to your vehicle, steal information or control its functions remotely without your permission.

In the world of cyber security, this exposure is referred to as the 'attack surface'. The more connected a device is, the wider the attack surface, which increases the chance that a vulnerability can be exploited.

Case study: Remote access and control

In recent years, hundreds of software vulnerabilities were reported across connected services in modern vehicles. Often, vulnerabilities in management systems can allow potential cybercriminals to remotely access and control aspects of a CV. To do this, sometimes all they need is the Vehicle Identification Number (VIN), which is usually located behind the windscreen. When notified of these flaws, manufacturers took steps to fix them.

With minimal data needed to hack a CV, the cybercriminal has the ability to steal the user's personal information, remotely start or stop the engine, and find the location of the vehicle.



Hacker exploits software vulnerability
Obtains unauthorised access to vehicle management systems and targets a user with minimal data, such as the VIN

Hacker remotely accesses critical vehicle systems
Steals user's personal information, turns car on or off, and finds the location of the vehicle

How to reduce risk

- Consider the potential benefits and risks of using connected services through mobile apps.
- Carefully consider and periodically review the users which have been granted access to your vehicle's connected services through mobile apps.
- Unlink your vehicle from any connected services accounts before selling or disposing of the CV.
- Keep your mobile apps, your mobile phone's operating system and vehicle software up to date.
- Enable multi-factor authentication (MFA) for any connected services account.

Electric vehicle charging stations

The potential attack surface is bigger for an electric vehicle (EV). This is because almost all public EV charging stations are internet connected. Public charging stations handle sensitive data such as names, email addresses and payment details. As such, charging stations and services can be an attractive target for cybercriminals.

Most home vehicle chargers are also connected to the internet and are considered to be IoT devices. A compromise of your charger could lead to theft of potentially sensitive data from other devices also connected to your home network.

How to reduce risk

- Ensure you use a long, complex and unique password for any EV charging service account.
- Enable MFA for any charging service account.
- Store payment and card details for any charging service securely.
- Ensure that any home charger is installed in a physically secure location.
- Change the default username and password of your home vehicle charger using a long, complex and unique password.
- Set up a separate Wi-Fi network on your router for your home vehicle charger and other IoT devices. This may be known on your Wi-Fi router as a 'guest' network and will isolate the charger from sensitive data that may be stored on your other home devices.
- Turn off any unwanted or unnecessary features that your home vehicle charger may include.
- Keep all software up to date on your EV, vehicle charger and any associated mobile apps.
- Choose a reputable manufacturer and installer when purchasing a home vehicle charger.

To find out more about securing home vehicle chargers, search 'Internet of Things' on cyber.gov.au.

Key points when buying and owning a CV

Keep your CV and any linked mobile apps up to date

Install updates as soon as they are available. Keep mobile applications associated with your vehicle up to date. To find out more, search 'update your devices' on cyber.gov.au.

Consider the manufacturer's approach to cyber security when purchasing a new vehicle

Research the manufacturer's approach to cyber security and any past or current vulnerabilities affecting different makes and models. Review the manufacturer's privacy and data collection policies and consider the data laws in the country where the data will be stored.

Consider the risks of enabling any connected service or using a connected services mobile app

Consider whether their benefits outweigh the potential risks. If you decide to use these apps, carefully consider and regularly review which users have had access to your vehicle. If you do use connected services through mobile apps, make sure to enable MFA for your account and use a long, complex and unique password.

Restore your CV to factory settings when selling or disposing of it or when purchasing a used vehicle

Before selling or disposing of your vehicle, be sure to restore it to factory settings to limit the loss of any personal information. Be aware that a factory reset will not delete any data that has been sent to the cloud during the vehicle's life.

Remove your vehicle from any connected services accounts before sale or disposal. Likewise, when purchasing a used vehicle, be sure to reset it to factory settings and ensure the previous owner does not have access to any linked services before you start using the vehicle.

More information

- Find out how to protect yourself online at cyber.gov.au
- To find out more about how to securely buy and use Internet of Things devices, search 'Internet of Things' on cyber.gov.au.

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre