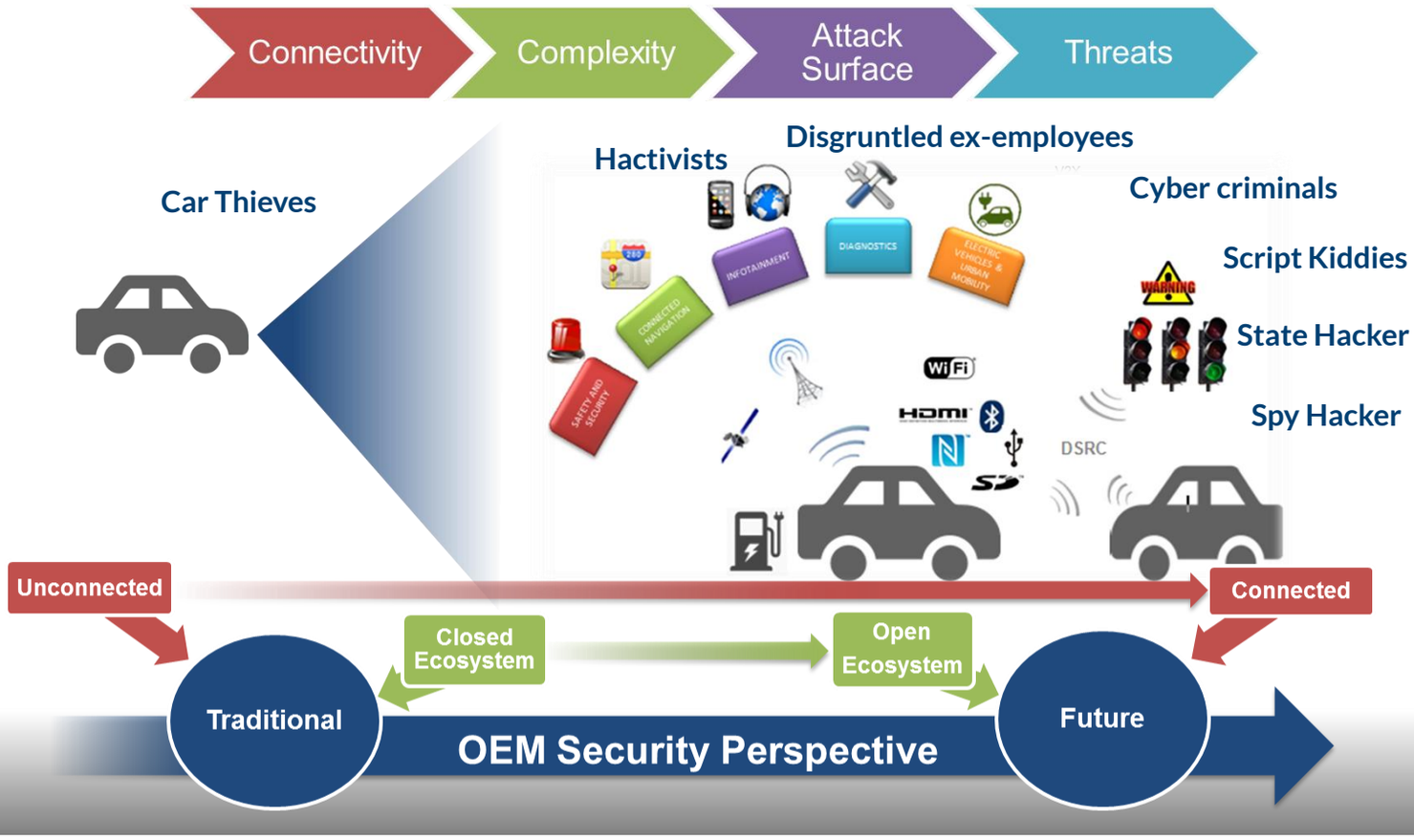
The Connected Car Ecosystem… What could be attacked and how.

In the rush to offer ever more connected services, are vehicle manufacturers losing sight of the need to ensure their systems are protected? »

Insight

A range of wired and wireless attack areas have emerged , increasing the number of security threats.



Bringing connectivity to the car has enabled vehicle manufacturers to offer an increasing range of services. This allows users to access information on the move and fulfil the promise of seamless connectivity.

The transformation of cars from mechanical systems to mobile computer networks has opened up an array of new attack points. This has invited the attention of hackers whose motivations could range from mere fun to more organised criminal activity.

Potential attacks include data extraction (personal or vehicle specific), theft of the vehicle, compromised safety via remote control and denial of service. As such attacks encompass all aspects of safety, security and privacy, vehicle manufacturers could face corporate liability lawsuits, damage to their brand reputation and financial loss.

This report is a vital guide to help all stakeholders in the connected car ecosystem. It explains the myriad of ways in which either the vehicle or the associated infrastructure could be compromised.

For each of the attack points identified, SBD's engineers have evaluated the potential impact of such an attack and the 'threat status' based on the current cyber crime environment, published research and likely future trends.

Whilst each attack point is an area of risk, the report highlights which are the 'key' attack points where attackers are expected to focus their future efforts.

Above all, the report demonstrates the need to take a holistic view on security from inside the car, through the mobile network, to the IT backend infrastructure.

Cyber attacks on cars are a reality. There are over 50 attack points in a connected car ecosystem. Do you understand ways in which a modern car could be compromised? What are the attack points? What are the attack methods? SBD's research identifies these threats and the methods being used to exploit the modern vehicle.

Secure Car: Securing the Connected Car –Attack Points and Methods

Ref: SEC/553

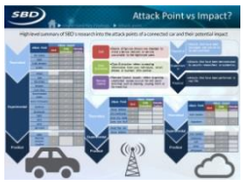
The benefits of connected car technologies are now an accepted and convenient feature in modern vehicles. SBD's latest research 'Securing the Connected Car', identifies the theoretical and real threats to these systems. As the complexity of vehicle systems is increasing so too are the range of risks and security threats.

This report has been created to support our customers in understanding ways in which a connected car could be at risk and the motivation behind the attacks. The scope includes inside the car, through the mobile network to the IT backend infrastructure.

Report contents;

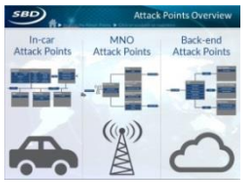
Trend Towards Connectivity

Changing Risks

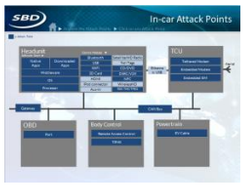


Attack Point vs Impact

Analysis of Key Attack Points



Key Attack Points



Over 50 attack points

Split into 3 clear areas

- In-Car Attack Points
- MNO Attack Points
- Back-End Attack Points

Understand the Key Findings

Glossary

Analyse the Attack Points

Find out More

Call us: +44 (0) 1908 305 101
Email us: info@sbd.co.uk

Secure Car: Securing the Connected Car –Attack Points and Methods

Ref: SEC/553

Call us: +44 (0) 1908 305 101 **Email us:** info@sbd.co.uk

About the Authors

Jithesh Joshy , Specialist – Secure Car Division

Jithesh graduated from Cochin University, India with a Bachelor's degree in Electronics and Communication Engineering. His extensive experience working for Tier-1 automotive suppliers allows him to perform in-depth analyses of in-car systems. Within SBD's Secure Car team, Jithesh specialises in reverse engineering electronic theft tools to understand the weaknesses they exploit, enabling vehicle manufacturers to develop effective countermeasures.

Mike Parris, Head of Secure Car Division

Mike graduated from the University of Birmingham with a degree in Electronic and Electrical Engineering. He is a Chartered Engineer and a Member of the Institution of Engineering and Technology. Mike has over 30 years of experience in a variety of technical, management and consulting roles in Europe, Asia and North America. At SBD he leads the Secure Car division.

Related Reports

Global Theft Guide

Ref: SEC/533

The guide analyses the situation of vehicle crime in 34 countries. Each country included in this research has a four page breakdown detailing all aspects of the domestic theft situation. This includes a top-level overview, a typical profile of car theft in that country, statistics and analysis, insight into security fitment and legislation, as well as SBD's verdict into the future of theft in that country.

Electronic Theft Threats Database **(SEC/554)**

The Electronic Theft Threats Database highlights some of the tools and devices that are being used by criminal groups across Europe. The database has been compiled using information and intelligence gathered by our specialists and reports from our partners across the world.

The database provides the user with an easy to manage list of the tools that are available globally, along with an indication of typical cost, functionality, and a summary of the vehicles that they claim to be compatible with.