

Introducing SBD ...

SBD is a knowledge specialist within the automotive sector globally.

Working closely with 90% of global vehicle manufacturers and the majority of their partners and industry bodies, SBD help their clients select the right technologies, suppliers and strategies when developing more connected, safe and secure vehicles.

SBD is a unique knowledge partner in the industry, not only in the breadth of its automotive experience but also its depth. Across the Connected, Safe and Secure Divisions SBD provide research and analysis, information services, design and evaluation and strategic support.

With the launch of SBD North America in 2014 the organization boasts a presence in Europe, the Far East and North America.

In October 2014, SBD and global information assurance firm NCC Group announced a unique and strategic partnership to tackle the growing risks from automotive cyber security...

SBD Securing the Connected Car

Total Liability of Cyber Attacks to the Auto Industry by 2020
according to SBD estimate

over **\$75 billion**

Where Are The Threats? Over 50 Attack Points in the Connected Car Ecosystem

In the Car: OBD (Fuel, Immobilizer), Headunit (Tethered Access, Downloaded APP, Multimedia, IOS, Processor), Body Control (Remote Access Control, TRMS), Powertrain (EV Gate), TCU (Tethered Modem, Embedded Modem, Embedded SIM), CAN Bus, Ethernet/USB.

Mobile Network: Voice (MSC, Home Location Register, Authentication Centre), M2M Platform, SIM Management Portal, Data (CGDN, SMSC), Radio Network (Base Station, Radio Access Control).

Back-End: Call Centres (CCDN), Content Providers (Content Providers, App Providers), Data Users (Set Party Data Users, O2 Data Users etc.), TSP (Dispatcher, App Store, Billing Engine, CRM/VSM, Driver Portal).

Why Worry?

- Growing Connectivity:** Over half of new vehicles globally will be connected by 2020. (Bar chart showing growth from 1.4% in 2010 to 53% in 2020).
- Growing Complexity:** The 2012 Ford Taurus has over 50 million lines of code. This level of complexity makes it virtually impossible to detect every weakness.
- Growing Attack Surface:** Only one of the many components shown here must be compromised in order to launch an attack on the connected car.
- Growing Range of Attackers:** Includes Hacktivists, Cyber Criminals, Disgruntled Employees, State & Corporate Hackers, and Script Kiddies.

What Can You Do? Securing The Connected Car (REF: SEC553-14)

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 spans from inside the car, through the mobile network to the IT back-end infrastructure.

www.sbd-na.com info@sbd-na.com +1 (734) 619 7969

The partnership combines the expertise of SBD in connected car architectures and automotive security with NCC Group’s expertise in cyber security testing. Together they have created the Automotive Secure Development Lifecycle (ASDL) to help vehicle manufacturers and their suppliers mitigate cyber security risks when developing connected cars.

This month we Spotlight On...

GPS Tracking Devices used by Criminals

There is increasing evidence that OCGs are using portable tracking devices to allow them to locate target vehicles that they first identify during daytime reconnaissance. In such cases, a particular model of the correct age, colour and specification may be seen by a gang member while driving around a certain location. They will covertly plant a GPS GSM tracking device on this car – perhaps using a magnetic attachment to install it underneath the car. Using an internet-connected PC they can then track the vehicle to see where it is kept overnight, before going to this location equipped to steal it.



This M.O. has been observed several times by the Dutch police recently and was one of the reconnaissance methods used by the OCG targeting BMW X5's. Another car targeted by thieves in the Netherlands is the Lexus RX450h.



Mike Parris is the Head of SBD's Secure Car Division with over 30 years of experience in a variety of technical, management and consulting roles in Europe, Asia and North America. He is a Justice of the Peace, a Chartered Engineer, a Fellow of the Institution of Mechanical Engineers and a Fellow of the Institution of Engineering and Technology.

Editor's Note: Thanks to IAATI ATPA Committee Chair Reg Phillips for sending this in.