TABLE OF CONTENTS

RELATED SBD REPORTS

Digital Key Guide - 712

This guide tracks the latest offerings of digital key, which uses a smartphone to lock/unlock and start the car. from OEMs in the three major regions. Also tracked are the features and pricing models of each system as well as the technologies used to produce them.

CYB

Cyber Security

#554

E-Theft Threat Guide

A growing number of intelligent systems and technologies are being installed in vehicles today, with more planned for installation in the future. While those innovations seen in the HMI and infotainment systems are most commonly noticed and marketed by OEMs, they also extend to safety and security. These features are now present across multiple vehicle segments and include, most notably, keyless entry. A function that sees the user's smartphone or key fob used to unlock the vehicle.

The rate at which these technologies are being installed and becoming more common within the industry, however, also increases the risk of electronic vehicle theft (e-theft). This sees a variety of electronic tools and devices used by criminal groups around the world that take advantage of built-in systems in order to steal vehicles.

The E-Theft Threat Guide identifies the range of methods that play a role in the theft of vehicles today. Theft tools and devices are extensively profiled on a number of topics - including their source, cost, and the type of theft they enable. Likewise, the models that have reportedly been stolen using these methods and tools are similarly profiled. The impact of these tools on vehicle theft worldwide is evaluated by their functionality, compatibility, and availability.

COVERAGE

GLOBAL NA CHINA EUROPE

FREQUENCY

ANNUALLY QUARTERLY ONE-OFF

PUBLICATION FORMAT

PDF POWERPOINT EXCEL ONLINE

PAGES

35

Request price

Key questions answered

- What are the current electronic theft methods used to steal vehicles?
- Which models are affected by a specific theft tool?
- How does theft impact the desirability or insurability of a vehicle?
- How available are those tools to buyers?

This research supports

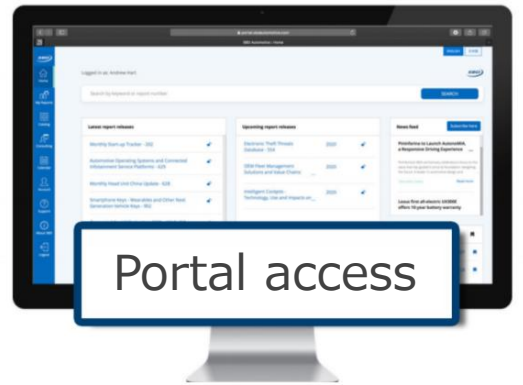
- PRODUCT PLANNERS
- ENGINEERING
- C-SUITE
- CYBER

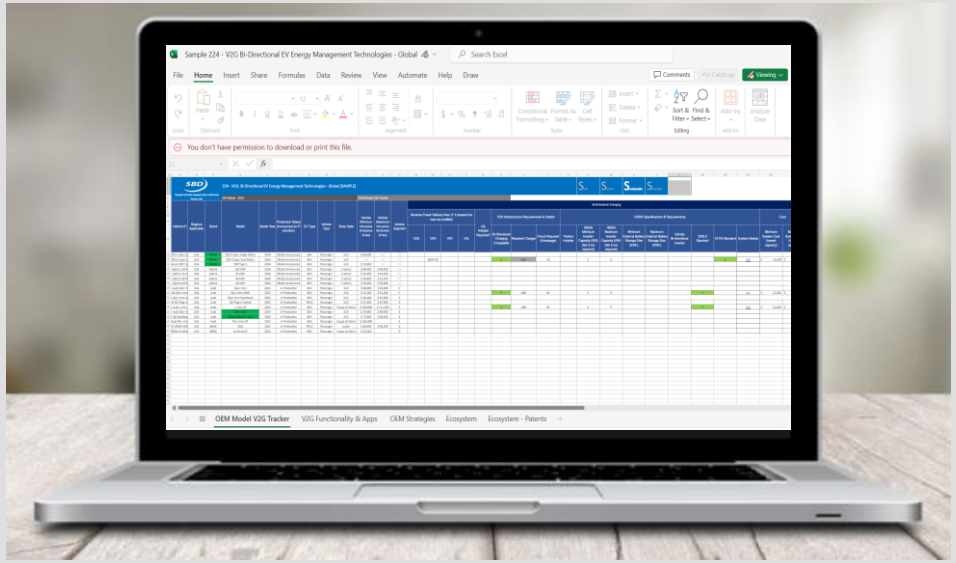
Do I have access?

100+ Reports published per year

50k+ Slides of insights, forecasts & data

4,000+ # of auto professionals who access our reports





View Excel Data Sheet Sample

E-Theft Threats Guide

For a comprehensive list of brand-level data on e-Theft tools, including cost, type, availability & compatibility

- >10,000 datapoints
- >290 tool details covered
- Models affected and website links

Click for Sample

Request price

554 – E-Theft Threat Guide

Contents

Electronic Theft Threat Guide

Total number of pages - 35

Introduction

Key questions answered in this report and chapter overviews

Contents Page
About SBD
Contact Us

Introduction

The **Electronic Theft Threat Guide** is designed to be a fully searchable reference tool and catalogue of the various devices available, designed to overcome standard fit security systems. The Excel Spreadsheet is a comprehensive list of current devices, what they are designed to do, what the seller claims they can do, and how much it costs. The spreadsheet lists the vehicle brands, models, and where possible, the model year that each tool claims to overcome or program.

The guide is designed to allow engineers, designers, investigators, and strategists to better understand the type and breadth of tools and devices currently available to overcome vehicle security systems. The tools listed can either bypass systems, program keys/ECUs, re-write commands or data, or re-flash vehicle firmware.

SBD Automotive designed the guide to highlight the tools and devices that operate on the latest or the most targeted brands and models. It focuses on tools and devices that are sold through known and 'trusted' tool developers, sellers and resellers. In this case, the term 'trusted' means tools that are sold by sellers that do not exaggerate a tool's capabilities or knowingly make false claims. All the chosen sites and sellers have been selected by SBD because of the known capabilities of the tools or through research carried out by SBD Automotive. The guide deliberately does not claim to include every tool or device available, as many of these are copies of tools already included or, cover model ranges or systems that are not current or considered relevant.

Note: SBD Automotive has **not tested** the majority of tools in this database to verify their effectiveness. SBD Automotive does have an ongoing theft tool test program and if you require further information on the tools being tested, please contact us by email: **info@sbdautomotive.com**

Section	Content
The Basics	Introduction to the history and the demand for this type of tool. How did different major global events and the introduction of specific legislation, drive demand for these types of tools? **Conclusion**: The requirement for a separate service and maintenance solution, along with a need for tools to bypass or legitimately circumvent vehicle security systems, has led to the emergence of an aftermarket tool landscape.
What's New?	What are the latest tools? Profiles are provided of the latest tools and bypass trends. There is also an overview of how the accompanying spreadsheet can be used to go deeper. **Conclusion**: The segment describes a blend of both traditional physical tools and modern electronic/software tools.
Outlook	SBD's view on the future trends of E-theft, including if new technologies and control features are being introduced into the automotive sector (such as UWB, biometrics, smartphone apps etc)) may be exploited. It will also look at some of the new features and options being included in the E-theft tool market, such as 'Pay as You Go' purchase options. **Conclusion:** This section discusses SBD's viewpoint of ways developer will choose to evade UWB(Ultra-Wideband).
Go Deeper	Can SBD help you with any unanswered questions?

Example slides from the report

Request price

Evolutionary factors of tool development

Mandatory immobilizers in Europe

Although immobilizers are good at preventing theft, the transponder keys used to control them made getting a replacement or additional keys very expensive. Since electronic engine immobilizer systems were made mandatory in the 1990s, locksmiths and independent service engineers were looking for new methods to allow them to continue to supply keys to their customers.

Tools for the independent market

By the early to mid-2000s, there were already several companies and individuals supplying lower-cost multi-brand tools, software, blank keys and coding information however, these mainly covered older models.

Cal. Senate Bill No. 1542 (2006)

CA SB 1542 (Legislation)
Legislation to allow a vehicle owner or family member (through a registered locksmith) to access information to permit the production of replacement key or similar device. This legislation was introduced in California but in essence was adopted across the US

(EU) Repair & Maintenance Regulation

(EU) Repair & Maintenance Regulation
"Access must include in particular the unrestricted use of the electronic control and diagnostic systems of a motor vehicle, the programming of these systems in accordance with the supplier's standard procedures, the repair and training instructions and the information required for the use of diagnostic and servicing tools and equipment"

The passing of this regulation was meant to prevent the OEMs from introducing anti-competitive practices and compelling customers to return to them for servicing and maintenance. However, it also prevented OEMs from restricting access to security components and information.

Right To Repair Act in the USA

Along with Repair and Maintenance regulations that compelled OEMs to give freelancers the same levels of access to tools, components and data as their dealership networks; it also stated that diagnostic tool suppliers should have equal access to coding and firmware information to allow them to develop service tools. Although the legislation was introduced with the best intentions, it inadvertently made it much easier for tool developers to access system data and components to allow them to reverse engineer solutions.
In 2022, New York became the 1st state to pass this law on electronic devices, followed by Massachusetts & Minnesota. California took upon the act in 2023, awaiting it to take effect in 2024.

Theft Tool Trends

The use of **Smart key systems** (passive entry and passive start systems) has most definitely changed the way cars are being stolen. Where vehicle ignition and start systems used to rely on a mechanical Steering Column Lock, the majority of newer models use electronically controlled steering or transmission locks, controlled from an electronic signal. For the thief, this means they only have to overcome the electronic command to, unlock the doors, de-activate the alarm, unset the steering lock and start the car.

The most well-known method to carry out this type of attack is to use a **Relay Tool**. This allows the thief to relay the key's signal over a larger distance, fooling the car into believing the key is within range and requesting an unlock and/or start request. These tools have been developed over the years to cover multiple brands, be more reliable and lower in cost (early versions cost in the region of 50k Euro but are now as low as 8k Euro). Interestingly, Keyless Repeater have introduced a new tool as part of their line up, that is limited to 3 uses. The purpose of this is so that purchasers can pay a lower price as a trial, if they like it, they can upgrade the tool over internet for an additional cost.

Many newer models are fitted with a so-called **'sleeping key'** countermeasure or the vehicle is fitted with **Ultra Wide Band** or Angle of Arrival **time of flight** technology. These technologies are good countermeasures to **Relay Attack,** and nobody, as far as SBD are aware, has successfully developed a tool to overcome them yet.

E – Theft Tools and their functionality

Relay Attack

Relay attacks consist in intercepting and potentially storing the signal the vehicle's smart key fob.

On a basic level, the attack is carried out by 2 thieves, one standing near the car and the other near the smart key fob.
Thief 1 transmits a signal to the car and then relays the authentication reply to thief 2. Thief 2 sends this signal to the key fob and then relays the reply to thief 1, who uses it to unlock and start the car.

Code Grabber

The code grabber is a device used to capture and store the coded signal transmitted by a key fob.

This signal is then simply replayed to unlock the vehicle or is used as a sample to predict the correct code (often by using the systems algorithm)

Key Programming

Key programming consists of connecting a dedicated device to the vehicles on-board diagnostic (OBD II) port or, via the system network (CAN, LIN etc.)

Specific software is then used to add or program a keyfob or transponder chip to the vehicles immobiliser system.

Transponder

Transponders are small RFID devices, sometimes encased in glass or carbon but, more recently, fitted to the keyfob PCB. Transponders are designed to store and transmit a coded signal after responding to a correct know challenge

These tools are designed to Read, Write and Program transponders so they can be used to deactivate vehicle security systems.

Security Control

Security control section covers other tools and devices designed to carry out a range or a specific action.
Features include:

- Immobilizer reset and/or bypass
- Unlocking central locking
- Disabling the alarm
- Read and write data to/from EPROM or IC
- Read, decode or bypass PIN code

Tool Overview

Tool Name

Diagnostics Software
Toyota / Lexus / Scion Key Programming
for Lexus 2022+ (TN016)

Vendor

Abrites

Compatible Brands

LEXUS

Description

- Works with AVDI
- Key programming
- Possible with all keys lost
- Compatible with specific Lexus models including 2023+ model year and newer

Features

UNLOCK

START

OBD
CAN
WIRELESS

Functionality

Key Programming

Price

€ 950

Example Compatible Models

Compatible Model	Model Year
Lexus LS	2018+
Lexus NX	2023
Lexus RX	2023
Lexus RZ	-
Lexus UX	2018+

Tool Image

Tool Overview

Tool Name

Global version all in one key programmer K518 Pro

Vendor

Lonsdor

Compatible Brands

CHEVROLET, HYUNDAI, KIA, TOYOTA, NISSAN, ALFA ROMEO, AUDI, SUBARU

There are many more compatible brands. Please check the attached Excel for more.

Description

- Key programming for remote and smart keys
- Perform functions such as reading and writing EEPROM chips, CPU main control chip operations, and reading EEPROM pin codes.
- Special functions include reading, writing and copying key transponders

Features

UNLOCK

START

OBD

CAN

WIRELESS

Functionality

Key Programming

Transponder

Price

€ 1,200

Example Compatible Models

Compatible Model	Model Year
Chevrolet Suburban	2021-2023
Hyundai Sonata	2023+
Kia EV6	2022+
Toyota Prius	2023
Toyota RAV4	2019-2023

Tool Image

Request the price

Request price

Contact SBD Automotive

Do you have any questions?

If you have any questions or feedback about this research report or SBD Automotive's consulting services, you can email us at info@sbdautomotive.com or discuss with your local account manager below.

info@sbdautomotive.com

Book a meeting

USA | UK | Germany | India | China | Japan

Garren Carr
North America
garrencarr@sbdautomotive.com
+1 734 619 7969

Luigi Bisbiglia
UK, South & West Europe
luigibisbiglia@sbdautomotive.com
+44 1908 305102

SBD China Sales Team
China
salesChina@sbdautomotive.com
+86 18516653761

Andrea Sroczynski
Germany, North & East Europe
andreasroczynski@sbdautomotive.com
+49 211 9753153-1

SBD Japan Sales Team
Japan, South Korea & Australia
postbox@sbdautomotive.com
+81 52 253 6201