

## Vehicle remote keyless entry systems and engine immobilisers: do not believe the insurer that this technology is perfect

Stephen Mason, <http://www.stephenmason.eu/>

*Barrister*

The author thanks the anonymous technical reviewer of this article for their valuable help and Professor Ross Anderson for his comments.

### ABSTRACT

**In the 1990s, governments put pressure on motor vehicle manufacturers to provide better security for vehicles. Thieves could steal cars and lorries with relative ease. The manufacturers responded by introducing electronic systems to make it more difficult for vehicles to be stolen without the key. However, as with most forms of technology, the software can be bypassed. In recent years, thieves have manipulated weaknesses in the technology, so that vehicles can be stolen without the key.**

© 2012 Stephen Mason.

**Keywords:** Vehicle remote keyless entry systems; engine immobilisers; digital evidence; theft of motor vehicles

This article was first published in *Computer Law and Security Review*, Volume 28, Issue 2 (April 2012), 195 – 200

In the 1970s, vehicle manufacturers began to use electronics to control fuel injection systems, and by the 1980s computers were being used for the purpose of diagnosing faults, such as the failure of indicator bulbs, and remote keyless systems (this is an electronic system using either radio frequency or infra-red to lock and unlock vehicle doors) were also beginning to be introduced, allowing the driver of a vehicle to lock and unlock the doors of a vehicle by pressing a button on the key. Such systems are widely used now, and their introduction was initially responsible for a reduction in the number of vehicles stolen.<sup>1</sup> Nevertheless, thieves,

---

<sup>1</sup> Richard Scott, the transport correspondent for the BBC, is recorded as stating that ‘unless criminals can get their hands on the keys, new cars are all but impossible to steal’, in ‘Car industry declares victory in war on thieves’, *BBC News*, 16 June 2011, available at <http://www.bbc.co.uk/news/uk-13787442>; the following assertion is taken from the Aviva Risk Management Solutions web site entitled ‘Knowledge Store, Motor Vehicle Security [Hardfacts]’: ‘Immobilisers prevent the engine from starting without the original key or transponder by isolating at least two of the operating circuits’ [https://help.aviva.co.uk/risksolutions/motor-risk/vehicle/REF\\_HF11001](https://help.aviva.co.uk/risksolutions/motor-risk/vehicle/REF_HF11001); the evidence does not support these assertions, although the following article illustrates that vehicle security devices undoubtedly reduced the numbers of thefts until thieves worked out how to by-pass the systems put in place by manufacturers: Graham Farrell, Andromachi Tseloni and Nick Tilley, ‘The effectiveness of vehicle security devices and their role in the crime drop’, *Criminology and Criminal Justice*, February 2011,

mainly organized gangs, have begun to master the technology, to the extent that remote keyless entry systems are not immune from being bypassed, thus enabling the thief to unlock the doors of a vehicle without any outward appearance of a forced entry,<sup>2</sup> even if a deadlock system is fitted to the vehicle.

## 1. How remote keyless entry systems work

The software in the chip that communicates with the software in the computer in the vehicle operates over a radio frequency transmitter. The range at which the device operates will vary between manufacturers, although the ability of the signal to reach the vehicle also varies because the corner pillars and other physical objects may act to reduce the range. The transmitter sends encrypted digital data to the receiver in the vehicle. If the data exchange between the keyless controller and the vehicle computer is compatible, then the vehicle doors will lock or unlock. This technology is similar to that used to open garage doors since the 1950s. In its simplest form, the signal to the door was not encrypted (it had a fixed code), which meant that the owner of an electronic operating system could open all the garage doors fitted with the same control device (often a small number of codes used in a series, possibly 100).

There are also ‘passive keyless entry systems’, where the doors unlock only when the computer in the vehicle detects the signals from the passive keyless device held by the driver: this method does not require any action by the user – it requires the driver to either touch a capacitive sensor (usually fitted in the outside door handle) or by pushing a button fitted in the handle – often limited to a two meter range from the door. Some systems lock the doors as the driver walks away from the vehicle, but most require the driver to press a button on the outside door handle. Another system is the ‘keyless go system’, which dispenses with the physical blade of the key<sup>3</sup> and the need for an ignition lock, although the majority still have a steering lock, although this is often electronically controlled. Other vehicles such as the Toyota Prius and BMW X5 use an electronically controlled transmission lock. This is important, because all vehicles sold in the EU are required by legislation to be fitted with a steering lock or transmission.<sup>4</sup> When the driver, using a keyless device, enters the vehicle, the

---

11: 21-35. This article includes a number of references to a wide variety of relevant research in the field.

<sup>2</sup> For an example of this problem, John Holl, ‘High-tech thieves use laptops to steal cars’, *ForbesAutos.com*, 26 June 2006, available at <http://www.msnbc.msn.com/id/13507939/ns/business-autos/t/high-tech-thieves-use-laptops-steal-cars/>; John Leyden, ‘Thieves jam key-fob lock signals in mystery car thefts’, *The Register*, 21 September 2010, available at [http://www.theregister.co.uk/2010/09/21/car\\_jammer\\_vehicle\\_theft\\_scam/](http://www.theregister.co.uk/2010/09/21/car_jammer_vehicle_theft_scam/); and Duncan Graham-Rowe, ‘Criminals find the key to car immobilisers’, *New Scientist*, 6 December 2011, Issue 2789, available at <http://www.newscientist.com/article/mg20827894.500-criminals-find-the-key-to-car-immobilisers.html>.

<sup>3</sup> The key blade is sometimes retained for emergency starting, and all keyless systems use a key blade as an emergency method of unlocking the doors.

<sup>4</sup> Council Directive 74/61/EEC of 17 December 1973 on the approximation of the laws of the Member States relating to devices to prevent the unauthorized use of motor vehicles, OJ L38, 11.2.1974, p. 22–28; Commission Directive 95/56/EC, Euratom of 8 November 1995 adapting to technical progress Council Directive 74/61/EEC relating to devices to prevent the unauthorized use of motor vehicles, OJ L286, 29.11.1995, p. 1–44.

engine can be started with the press of the engine start button, or the twist of a start knob. The electronic control unit will communicate with the device to enable the engine to be started. New systems are under development, and no doubt will be brought into use in due course. All of these systems include a form of electronic immobilizer, which is an electronic control system designed to prevent the engine from starting unless the correct messages, usually digital signatures, have successfully been passed between the device in the possession of the driver and the electronic control unit.

## **2. Case example**

In Issue 72 (September/October 2008) of the ‘ombudsman news’ published by the Financial Ombudsman Service (FOS), there were two reports about remote keyless entry systems. The findings in relation to complaint number 72/1 are of interest in understanding the nature of digital evidence, and how to challenge the assertions made by ‘experts’.

In this instance, the owner’s car was discovered close to their home. It was badly damaged. The insurer refused the claim on the basis that its loss adjusters indicated that the car could only have been operated by the use of “an ‘intelligent’ (programmed) key”.<sup>5</sup> The key had not been left in the car and neither of the two keys were lost or stolen. The insurer cited a report from ‘motor vehicle security experts’ (whoever they were) in support of its assertion that the car could only have been taken by someone who had the key. In turn, the owner produced evidence from the original dealer to illustrate that the security could be by-passed, and that the car could be operated without the use of the programmed key. The insurer implied that the owner or a member of the family had taken the car and caused the accident.

The Financial Ombudsman Service rejected the complaint on the basis that the technical evidence supplied by the original dealer was of a very general nature, and it did not make any specific reference to the make and model of the car, unlike the technical evidence produced by the insurer, which referred specifically to the exact make and model in question.

### **2.1. How remote keyless entry systems can be subverted**

There is an increasing amount of technical literature on how keyless entry systems can be undermined successfully.<sup>6</sup> The main methods by which the software of a keyless entry system can be successfully subverted include:<sup>7</sup>

1. A relay attack, which is a technique that is only relevant to ‘keyless’ systems, where the thief uses hardware and software to extend the frequency range of the radio frequency transmitter, and to intercept the data being transmitted between the key fob<sup>8</sup> and the vehicle. Generally, the thief must be within 60 metres of the key and the

---

<sup>5</sup> It is not known what ‘intelligent’ means in this context, because software is a set of instructions written by human beings.

<sup>6</sup> An early text is Kerstin Lemke, Christof Paar and Marko Wolf, editors, *Embedded Security in Cars* (Springer-Verlag, Berlin, 2006).

<sup>7</sup> Kerstin Lemke, Ahmad-Reza Sadeghi and Christian Stübke, ‘Anti-theft Protection: Electronic Immobilizers’, pp 54 – 66 and Kai Schramm, Kerstin Lemke and Christof Paar, ‘Embedded Cryptography: Side Channel Attacks’, pp 187 – 204 in Kerstin Lemke, Christof Paar and Marko Wolf, editors, *Embedded Security in Cars* (Springer-Verlag, Berlin, 2006).

<sup>8</sup> The OED electronic version provides a number of definitions of ‘fob’, one of which is ‘1.1 A small pocket formerly made in the waistband of the breeches and used for carrying a watch,

vehicle. The messages are relayed from the key fob to the computer in the vehicle to make it appear that the key is physically closer to the vehicle than is the case. The software in the key is instructed to send a signal to the vehicle's computer. The computer in the vehicle receives a digital signature that indicates the key is within range and activates the unlocking sequence. The vehicle can be driven away, and when the engine is running, the thieves can program a new key to the vehicle, depending on the make and model of car. This type of attack can work without the physical presence of the key or raising the suspicion of the owner.<sup>9</sup>

2. By monitoring the transmission of the code from the key fob. In this instance, the owner presses the button on the key fob to instruct the vehicle to lock the doors, but the thief monitors the transmission, and in doing so, captures and records the code, and simultaneously stops it. This prevents the vehicle from being locked. At this moment, the thief possesses the temporary hopping or rolling code. This is encrypted data, which is designed to change every time the button is pressed (hence the term hopping or rolling code<sup>10</sup>), is sent to the vehicle.<sup>11</sup> When the owner presses the button

---

money, or other valuables'. It is assumed that the word 'fob' was introduced by the motor vehicle industry to describe the key fob, that is a key that fits into the pocket. The use of the word 'key fob' is widely used.

<sup>9</sup> Aurélien Francillon, Boris Danev and Srdjan Capkun, 'Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars' available at <http://eprint.iacr.org/2010/332.pdf>.

<sup>10</sup> See Michael Bender, *The Fast, The Fraudulent, & The Fatal: The Dangerous and Dark side of Illegal Street Racing, Drifting and Modified Cars*, (Authorhouse, 2009) for a description of the remote keyless entry system at pp 79 – 93; Kerstin Lemke, Ahmad-Reza Sadeghi and Christian Stübke, 'Anti-theft Protection: Electronic Immobilizers' in Kerstin Lemke, Christof Paar and Marko Wolf, editors, *Embedded Security in Cars* (Springer-Verlag, Berlin, 2006), pp 52 – 54; note that a vehicle's immobiliser system can be affected by the radio waves emanating from buildings, thus requiring vehicles to be towed away, as occurs in Bern: Gunther B. Pamberg, letter to the editor, *Financial Times*, April 9/April 10, 2001, p 10, 'Electronic car key fobs fail on Southampton street', BBC News (Hampshire and the Isle of Wight), 12 October 2011, available on-line at <http://www.bbc.co.uk/news/uk-england-hampshire-15278838>.

<sup>11</sup> For attacks on a well-known and widely used software system for garage doors and vehicles, see Sebastiaan Indestege, Nathan Keller, Orr Dunkelman, Eli Biham and Bart Preneel, 'A Practical Attack on KeeLoq', in Nigel Smart, editor, *Advances in Cryptology – EUROCRYPT 2008, Lecture Notes in Computer Science*, Volume 4965, (Springer-Verlag, 2008) pp 1 – 18; Thomas Eisenbarth, Timo Kasper, Amir Moradi, Christof Paar, Mahmoud Salmasizadeh and Mohammad T. Manzuri Shalmani, 'On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoq Code Hopping Scheme', in David Wagner, editor, *Advances in Cryptology – CRYPTO 2008 Proceedings of the 28th Annual International Cryptology Conference, Lecture Notes in Computer Science*, Volume 5157, (Springer-Verlag, 2008), pp 203 – 220; Martin Novotný and Timo Kasper, 'Cryptanalysis of Keeloq with COPACOBANA', in ECRYPT II (SHARCS '09), 9 – 10 September 2009, Lusanne, Switzerland, pp159 – 164; Markus Kasper, Timo Kasper, Amir Moradi and Christof Paar, 'Breaking KeeLoq in a Flash: On Extracting Keys at Lightning Speed' in Bart Preneel, editor, *Proceedings of the 2nd International Conference on Cryptology in Africa: Progress in Cryptology* (Springer-Verlag, 2009), pp 403 – 420; Amir Moradi and Timo Kasper, 'A New Remote Keyless Entry System Resistant to Power Analysis Attacks', in *Seventh International Conference on Information, Communications and Signal Processing – ICICS 2009*, (IEEE, 2009), available at [http://www.emsec.rub.de/chair/\\_staff/amir-moradi/](http://www.emsec.rub.de/chair/_staff/amir-moradi/); Thomas Eisenbarth, Timo Kasper, Amir Moradi, Christof Paar, Mahmoud Salmasizadeh and Mohammad T. Manzuri Shalmani, 'Physical Cryptanalysis of KeeLoq Code Hopping Applications',

on the key fob a second time, the thief obtains and records the signal whilst simultaneously blocking it, and sends the first signal to lock the car. The owner will then leave, assuming the doors are locked, and the thief can transmit the recorded second signal to unlock the doors.

3. An sms attack. Two security consultants, Don Bailey and Matthew Solnik demonstrated at the Black Hat conference in Las Vegas in 2011 that they could send commands from a laptop computer to unlock the doors of a Subaru Outback, and then start the car by sending messages over the Global System for Mobile Communications (GSM) telephone network in the form of sms messages. It took two hours to set up a private GSM network before they obtained the number of the system inside the vehicle. They were then able to masquerade as an authorized server.<sup>12</sup>
4. Other methods include reverse engineering of the key programming procedure, breaking the cryptographic key, simulating the cryptographic key,<sup>13</sup> and obtaining inside information about a system by working in a dealership or garage, vehicle manufacturer or tier one component supplier,<sup>14</sup> or having an insider make duplicate keys, illustrating the lack of concern for security by the manufacturer.

### 3. Failure to understand<sup>15</sup> the nature of the digital evidence

---

available at <http://eprint.iacr.org/2008/058.pdf>; Christof Paar, Thomas Eisenbarth, Markus Kasper, Timo Kasper and Amir Moradi, 'KeeLoq and Side-Channel Analysis—Evolution of an Attack', in Luca Breveglieri, Israel Koren, David Naccache, Elisabeth Oswald and Jean-Pierre Seifert, editors, *Workshop on Fault Diagnosis and Tolerance in Cryptography, Proceedings of the Sixth International Workshop, FDTC 2009* (IEEE Computer Society, 2009), pp 65 – 69; Idan Sheerit and Avishai Wool, 'Cryptanalysis of KeeLoq code-hopping using a Single FPGA' (2011), available at <http://eprint.iacr.org/2011/>.

<sup>12</sup> John D. Sutter, 'How to unlock a car with a text message' 3 August 2011, CNN, <http://edition.cnn.com/2011/TECH/mobile/08/03/black.hat.war.texting/>; 'Digital car jacking – Researchers show how to unlock, start a car remotely', Homeland Security News Wire, 5 August 2011 <http://homelandsecuritynewswire.net/researchers-show-how-unlock-start-car-remotely/>; 'Texting, grand theft auto style; alarms pose risk', Associated Press, 19 August 2011; their presentation is available at 'War Texting: Identifying and Interacting with Devices on the Telephone Network', [http://www.isecpartners.com/storage/docs/presentations/iSEC\\_BH2011\\_War\\_Texting.pdf](http://www.isecpartners.com/storage/docs/presentations/iSEC_BH2011_War_Texting.pdf).

<sup>13</sup> These methods are discussed and illustrated in Stephen C. Bono, Matthew Green, Adam Stubblefield, Ari Juels, Aviel D. Rubin and Michael Szydlo, 'Security analysis of a cryptographically-enabled RFID device', *Proceeding SSYM'05 Proceedings of the 14th conference on USENIX Security Symposium*, Volume 14, pp 1 – 15; for an introduction to some of the issues relating to vehicle security, see Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham and Stefan Savage, 'Experimental Security Analysis of a Modern Automobile', 2010 IEEE Symposium on Security and Privacy, pp 447 – 462.

<sup>14</sup> Jarno van de Moosdijk and Dick Visser, 'Car security: remote keyless "entry and go"', revision 232 (June 2009) refer to this in their paper.

<sup>15</sup> Smugglers of illegal drugs identify people crossing frequently between Mexico and the United States, acquire the vehicle identification number of the motor car from the dashboard, then obtain a duplicate key for the car from a corrupt locksmith with access to the relevant vehicle database (Ford vehicles were the vehicles mainly chosen); they then place the drugs into the boot of the vehicle, and

As with some ATM and internet banking cases adjudicated by the Financial Ombudsman Service, the decision in the case outlined above was based on an erroneous understanding of the various methods that can be used to obtain access to a motor car without the key, and a failure to understand the nature of the ‘expert’ evidence submitted by both parties.

There are the flaws in the decision making process by employees of the Financial Ombudsman Service, and they are pronounced: decisions are made based on evidence submitted on paper only (although apparently there is an increasing use of interviews over the telephone); print-outs of digital evidence submitted by organizations such as banks is usually believed without challenge,<sup>16</sup> and evidence submitted by an individual, such as a statement from an independent witness, tends to be ignored in favour of the evidence submitted by the bank or insurer. In essence, the assessment of evidence fails to balance the need to ensure the party that must prove its case (the bank or insurer) does so with sufficient conviction. When the complainant raises doubts about the assertions of the bank or insurer, providing such doubt is based on evidence of reasonable substance, then the FOS should either reach a determination in favour of the complainant, or conduct further research to establish why the evidence of the bank or insurer is better or more reliable than the evidence put forward by the complainant.

It might be that the Financial Ombudsman Service has objections to such a view, on the basis that it is for the parties to submit the evidence upon which they rely, and therefore it is for them to take care over the quality of the evidence that they submit; that there is not enough time to conduct such an enquiry, and even if there was, it would be far too expensive. These objections have merit, given the nature of the exercises carried out by the FOS. However, computer technology is now so complex, it is not possible for a lay person to sit in judgment between an individual and an insurer (as in the case outlined above), and reach a fair decision in the absence of more informed evidence. In respect of the evidence rejected in the case noted above, it is arguable that the FOS made a significant error, because the description of the evidence put forward by the complainant was highly relevant to the issue of remote keyless entry systems in general, highlighting, as it did, that the security could be by-passed, and the complainant should have had the opportunity of challenging the evidence put forward by the insurer.<sup>17</sup>

#### **4. The future of using software in motor vehicles**

---

the driver unwittingly drives the car across the border with the drugs: Jason Beaubien, ‘At Border, Teacher Becomes Unwitting Drug Smuggler’, 21 July 2011, NPR at <http://www.npr.org/2011/07/21/138548294/at-border-teacher-becomes-unwitting-drug-smuggler>; for more detail, see an FBI criminal complaint filed on 1 July 2011 in the U.S. District Court Western District of Texas in the case of United States of America v Jesus Chavez at <http://txn.fd.org/Blind%20mules,%20FBI%20affidavit,%20July%202011.pdf>.

<sup>16</sup> That is, despite the failure to provide a proper evidential foundation and the fact that digital evidence is far from perfect, for which see Stephen Mason, general editor, *Electronic Evidence*, (2nd edn, LexisNexis Butterworths, 2010), Chapter 5.

<sup>17</sup> For an instructive discussion about the merits of the evidence surrounding a similar case in the USA, albeit in the context of legal proceedings, see *McCoy v Progressive West Insurance Company*, No. B199978, 2009 DJDAR 2849 (Cal. Ct. App. Feb. 26, 2009) an appeal from a judgment of the Superior Court of Los Angeles County, available at <http://law.justia.com/cases/california/court-of-appeal/2009/b199978/>.

Motor vehicles already contain software systems, although they are not as complex as many manufacturers infer.<sup>18</sup> How these systems are linked will be a significant part of problems in the future, and because of the way the software has gradually been introduced into vehicles, the method used to link the different systems has made the control of software more complex, and therefore prone to more errors and the introduction of ‘backdoors’ by software engineers.<sup>19</sup> Although the more expensive motor cars have far more computing power than cheaper vehicles, nevertheless many vehicles now include electronic systems to control various systems, some of which include night vision, monitoring for driver alertness, accident recorders, interior lighting, voice and data communications, active noise suppression inside the car, active environment controls (heating, air conditioning), entertainment systems, navigation systems, security systems, active suspension, anti-lock braking, parking systems, seat position control, transmission control, electronic valve timing, electronic throttle control and so on.<sup>20</sup> Examples of what have occurred include:

1. Omar Ramos-Lopez, 20, a former employee of Texas Auto Centre in Austin, Texas is accused of hacking into the company computer system to disable the on-line account that enabled the company to deactivate the starter motor and activate the horns and GPS of many of the vehicles they had sold. Apparently over 80 customers complained that they missed work, could not get to school or complained of towing expenses and vehicle repairs.<sup>21</sup>
2. Dutch police obtained data about the speed of motor vehicles in aggregate form from TomTom satellite navigation systems and used it to set speed traps.<sup>22</sup>
3. A penetration tester tapping into the live feed coming from two separate cameras mounted on a police motor vehicle, simultaneously being able to control the hard drive of the DVR, and, by using default passwords in the FTP server of the DVR, presented with the ability to upload, download, and delete files that stored several

---

<sup>18</sup> This is changing, especially with high end motor vehicles. For instance, the McLaren MP4-12C is almost entirely controlled by software, which has caused serious problems. Ron Dennis has admitted that ‘virtually every single problem has its root cause in software’, and if customers wanted to take delivery of a vehicle immediately, they would have to do so without satellite navigation or with a working in-car telephone: ‘Teething problems for McLaren – with knobs on’, *The Times*, Saturday 12 November 2011, 63.

<sup>19</sup> Manfred Broy, ‘Challenges in Automotive Software Engineering’, *Proceedings of the 28th international conference on software engineering*, (ACM, 2006), pp 33 – 42.

<sup>20</sup> For just one early example of the research and development of software for motor vehicles, an entire issue (IE 30 Issue 2, May 1983) of *IEEE Transactions on Industrial Electronics* was given over to articles relating to the use of software in vehicles. For more recent articles, see H. Gharavi, K. V. Prasad and P. A. Ioannou, ‘Special Issue on Advanced Automobile Technologies’, *Proceedings of the IEEE*, February 2007, Volume 95, Issue 2, pp 325 – 327; M. Broy, I.H. Kruger, A. Pretschner, C. Salzmann, ‘Engineering Automotive Software’, *Proceedings of the IEEE*, February 2007, Volume 95, Issue 2, pp 356 – 373.

<sup>21</sup> Kevin Poulsen, ‘Hacker Disables More Than 100 Cars Remotely’ *Wired*, 17 March 2010.

<sup>22</sup> Charles Arthur, ‘TomTom satnav data used to set police speed traps’ *The Guardian*, 28 April 2011.

months' worth of video feeds, thus having the ability to tamper with or destroy evidence.<sup>23</sup>

As a result, it is highly probable that there will be more examples of the unintended acceleration reported across the Toyota, Scion, and Lexus models that occurred in the United States of America in 2010 and 2011.<sup>24</sup> As an aside, the use of software in motor vehicles and their use of wif fi and Bluetooth will increasingly mean they are susceptible to being affected by more powerful communication systems. Apparently, vehicles parked in front of the Swiss Parliament in Bern regularly need towing away because the car park is located between the Swiss National Bank, Credit Suisse and the Swiss Federal Parliamentary Services.<sup>25</sup>

There are two significant problems that act to ensure that customers will continue to have their motor cars stolen in the EU where there will be no evidence to demonstrate a forced entry. They are, first, the expiry (31 May 2010) of the Motor Vehicle Block Exemption Regulations,<sup>26</sup> and second, the policy of the motor industry to keep software developments secret. This is colloquially known as 'security by obscurity' based on Kerckhoffs principle, where the method of coding and transmitting information secretly ought to be secure, even if everyone knows how it works.

#### **4.1. Expiry of the Motor Vehicle Block Exemption Regulations**

When the Motor Vehicle Block Exemption Regulations expired, new regulations were put into force.<sup>27</sup> The new rules are intended to increase competition in the market for repair and maintenance to vehicles by improving access to the technical information needed for repairs, making it easier to use alternative spare parts, and to prevent manufacturers' from insisting that the cars they manufacture are serviced only in authorised garages when under warranty. As beneficial as this may seem on the surface, it will cause serious security problems in the

---

<sup>23</sup> Dan Goodin, 'Hacker pwns police cruiser and lives to tell tale The dark side of 'situational awareness'', *The Register*, 3 May 2011; Kevin Finisterre, *Owning a cop car*, at <http://www.digitalmunition.com/OwningCopCar.pdf>; Stuart McClure, André Weimerskirch, Ph.D., Marko Wolf, Ph.D., Professor Christof Paar, Winfried Stephan and Stefan Goss, Ph.D., *Caution: Malware Ahead An analysis of emerging risks in automotive system security* (McAfee/Wind River, 2011) at <http://www.mcafee.com/us/resources/reports/tp-caution-malware-ahead.pdf>.

<sup>24</sup> Michael Barr, 'Firmware forensic: best practices in embedded software source code discovery', *Digital Evidence and Electronic Signature Law Review*, 8 (2011), 148 – 151 for a discussion of the tests that should be carried out and those tests that were not carried out by the National Highway Traffic Safety Administration and the team from NASA's Engineering and Safety Center, thus undermining the conclusions in their joint report.

<sup>25</sup> Gunther B. Pamberg, 'Tyler's appliances are caught in a Bermuda triangle' letter to the editor, *Financial Times*, April 9/April 10, 2011, 10.

<sup>26</sup> Commission Regulation (EC) No 1400/2002 of 31 July 2002 on the application of Article 81(3) of the Treaty to categories of vertical agreements and concerted practices in the motor vehicle sector, OJ L 203, 1.8.2002, p. 30–41.

<sup>27</sup> Commission Regulation (EU) No 461/2010 of 27 May 2010 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to categories of vertical agreements and concerted practices in the motor vehicle sector (Text with EEA relevance), OJ L129, 28.5.2010, p. 52–57; Commission notice — Supplementary guidelines on vertical restraints in agreements for the sale and repair of motor vehicles and for the distribution of spare parts for motor vehicles (Text with EEA relevance), OJ C 138, 28.5.2010, p. 16–27.

future, because it will be more difficult for a manufacturer to protect the digital security of the motor cars produced effectively. It will undoubtedly be the case that some independent garages will employ staff (wittingly or unwittingly) that have only one intent in mind: that is to steal sufficient amounts of proprietary information relating to the security system of a vehicle to enable thieves to steal cars more effectively. A number of law enforcement agencies also take the view that many organised criminal groups operate legitimate businesses as a means to either carry out their illegal activities or to launder money.

#### 4.2. Security by obscurity

As most of the dominant software businesses began to learn in the early years of producing personal computers, keeping software secret served two purposes: first, to make mistakes whilst selling the software as a working product (and then to rectify the mistakes by selling up-dates), and second, in an indirect way, to challenge hackers intent on finding out the weaknesses in the software, because it was secret. Whilst it can be said of the software industry that there is a certain amount of openness in relation to the development of software at the time of writing (although it is not, by all means, the same across the industry), this is not the case in respect of motor manufacturers. There are two problems that need to be overcome. First, the New Vehicle Security Assessment that is used to assess the vehicle's ability to resist theft by testing the immobiliser, locks and vehicle identification issued by the Motor Insurance Repair Research Centre<sup>28</sup> (also known as 'Thatcham') is confidential. Second, the motor manufacturers have generally adopted the same view: that proprietary software should not be subject of scrutiny.<sup>29</sup> This attitude is summed up in the paper by Jarno van de Moosdijk and Dick Visser, at 7.4:

*'We tried to find out what the reason was for the chipset manufacturers refusal to give security information on their products, by asking them this question:*

In case you cannot answer some of our questions, we would like to have a short reaction on the Kerckhoff principle:

*"A Cryptosystem should be secure even if everything about the system, except the key, is public knowledge."*

One Hella<sup>30</sup> gave an actual answer:

*"If everything, except the key, is known, a car would become unsecure very soon due to the fast growing computing power of IT technology compared to automotive technology and their life cycle."*

---

<sup>28</sup> The Motor Insurance Repair Research Centre, which is not a government organization, was originally established by the Association of British Insurers to assess the theft risk and the damage repair cost for the UK insurance industry. Although their employees attend many committees, they do not have any official influence on the police or the Home Office. Their main priorities will always be, undoubtedly correctly, with the insurance industry.

<sup>29</sup> Marcus Heitman, 'Security Risks and Business Opportunities in In-Car Entertainment' in Kerstin Lemke, Christof Paar and Marko Wolf, editors, *Embedded Security in Cars*, pp 242 – 244.

<sup>30</sup> Hella are a tier 1 electronics supplier but do not produce transponder chips, they make keyless systems using other makes of transponder. A transponder is a passive device that is made up from the words 'transmitter' and 'receiver'. It is a device fitted in the vehicle key head or the keyless integrated circuit board that communicates to the immobiliser system (which is an electronic system that prevents the engine from starting) via an antenna, and is powered by a magnetic field and a capacitor.

A circular and unsatisfactory response, if ever there was one. With this attitude, owners of vehicles can expect to find their cars stolen in the future without any sign of entry. Unless motor manufacturers improve the quality and design of software in vehicles, the future for owners of motor vehicles is far from satisfactory. Researchers have already demonstrated that they have the ability to control a vehicle's computer systems, partly because the systems increasingly use wi fi and Bluetooth as a means of communicating between processing units, thus increasing the opportunities for thieves to break into cars without physically entering them.<sup>31</sup> When a vehicle is stolen, the owner will then face the problem of proving they were not to blame for the theft of their vehicle. This will be exceedingly difficult.<sup>32</sup>

**Stephen Mason** ([stephenmason@stephenmason.eu](mailto:stephenmason@stephenmason.eu)) is a barrister.

He is the author of *Electronic Signatures in Law* (3rd edition, Cambridge University Press, 2012), *When Bank Systems Fail Debit cards, credit cards, ATMs, mobile and online banking: your rights and what to do when things go wrong* (2nd edn, PP Publishing, 2014), *Email, social media and the internet at work: A concise guide to compliance with the law* (7th edn, PP Publishing, 2014), and was one of the first lawyers to write an e-book, *The millennium bug: a guide to the legal issues for business* (4th edn, May 1999).

He is the general editor of *Electronic Evidence* (3rd edition, LexisNexis Butterworths, 2012) and *International Electronic Evidence* (British Institute of International and Comparative Law, 2008).

He is also the founder, general editor and publisher of the international journal *Digital Evidence and Electronic Signature Law Review*, which has become an international focal point for researchers in the area.

---

<sup>31</sup> When a thief obtain access to the diagnostic port on the dashboard of a motor vehicle, it is possible to take over the electronics and reprogram it to do arbitrary things. Reported in, amongst other journals, Erica Naone, 'Taking Control of Cars from Afar', *Technology Review*, 14 March 2011 and Larry Greenemeier, 'Hack My Ride: Cyber Attack Risk on Car Computers', *Scientific American*, 31 May 2011. The reference for the report is: Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, Tadayoshi Kohno, 'Comprehensive Experimental Analyses of Automotive Attack Surfaces', National Academy of Sciences Committee on Electronic Vehicle Controls and Unintended Acceleration, 3 – 4 March 2011, although it is secret and not available to the public. For a further report by a similar group of authors that is not focused on remote keyless entry system issues, but includes the description of a demonstration in which a remote keyless entry system is bypassed via a compromised electronic control unit, see Stephen Checkoway, Damon McCoy, Danny Anderson, Brian Kantor, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno, 'Comprehensive Experimental Analysis of Automototive Attack Surfaces', *Proceedings of the USENIX Security Symposium*, San Francisco, CA, August 2011, available at <http://www.autosec.org/publications.html>.

<sup>32</sup> For a snapshot of the extent of the problem, a blog entitled 'Car Crime UK' <http://carcrimeuk.blogspot.com/> set out details of UK lost or stolen vehicles between 1 January 2011 and 5 February 2011 (the figures are from a 36 day sample from statistics that were generated from the Police National Computer using key words. Additional offences may have occurred and are not identified within the report). In one month, 2,916 (33%) vehicles were stolen from the home address or in the vicinity where the owner claimed to have the keys, and 2,824 (32%) vehicles were stolen away from the home where the owner claimed to have the keys: that is, in relation to 64 per cent of all thefts, the vehicle was stolen without the keys.