The Changing Face of Car Theft: A Motivation to Improve Car Security

1. Introduction

Since car theft in Europe peaked in the early 1990s, manufacturers have increasingly fitted electronic immobilisers and other security features in response to the introduction of legislation, insurers' demands for improved security, and the need to maintain their brand image.

Whilst the initial motivation for improved security came from Europe, many car manufacturers have subsequently introduced some of the same security measures in other markets, often with the same positive effect on theft rates in these regions. The result of such global harmonisation is a wide range of cars fitted with similar security systems and a larger car parc for criminals to study in order to find weaknesses which can then be exploited in a majority of markets.

In recent years, criminals have caught up with electronic immobiliser technology and have developed a range of equipment to facilitate car theft. These devices are typically designed to exploit weaknesses in the embedded software of the in-car systems. In parallel, third party companies have developed a plethora of devices, ostensibly for the vehicle locksmith market, which can include functions such as unlocking the car via CAN bus, deactivating the alarm and permitting programming of new keys even when there are no existing keys present.

Figure 1. Typical New Key Programming Process (Aftermarket Tool)

Source: SBD

With the spread of organised crime in all markets, the numbers of cars stolen using electronic theft methods has increased. We define 'electronic' in this sense as where a contemporary car (i.e. protected by an electronic immobiliser system) is driven away without the thief having physical access to an original key.

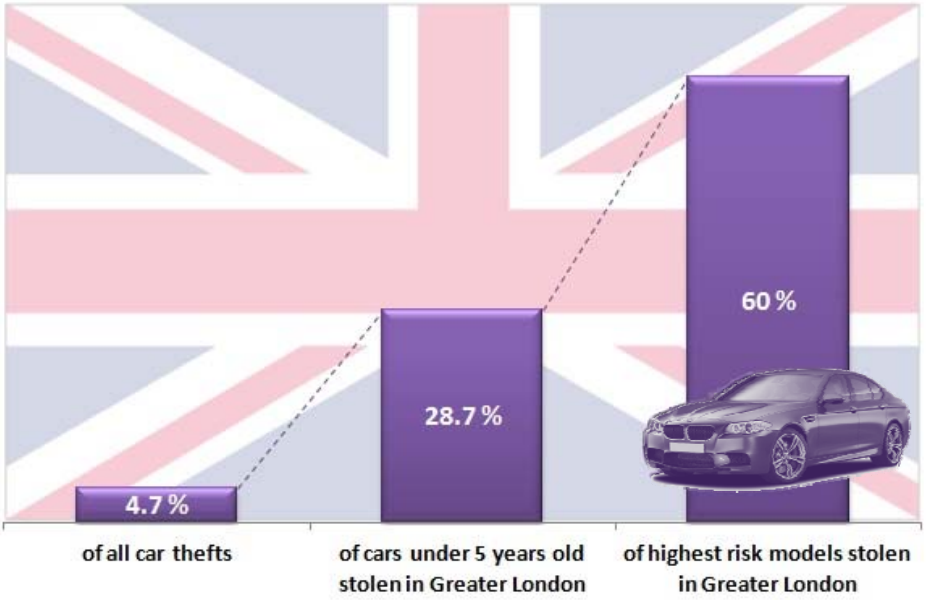
2. The Extent of Electronic Theft Methods

Electronic theft methods are being used by ***Organised Crime Groups*** (OCGs) to steal cars for profit in many different markets. There can be no definitive statistics for this type of theft because, where successful, the cars are not recovered and so the method used cannot be determined with certainty.

From SBD's research, the current penetration of electronic theft methods varies considerably from one country to another at between 0.5 % and 16 % of all car thefts. In the majority of the countries studied, this type of theft is becoming increasingly common.

In England, SBD estimates that electronic theft accounts for around 4.7 % of all car thefts. This statistic might not grab the attention, but bear in mind that many of these cars are older models not targeted by OCGs. It is more instructive to look instead at the statistics for newer cars, where electronic theft accounts for a significant 28.7 % of cars under five years old taken from the London area in the last year. This figure rises to 60 % or more for the most targeted models.

Figure 2. Extent of Electronic Theft for Cars in England

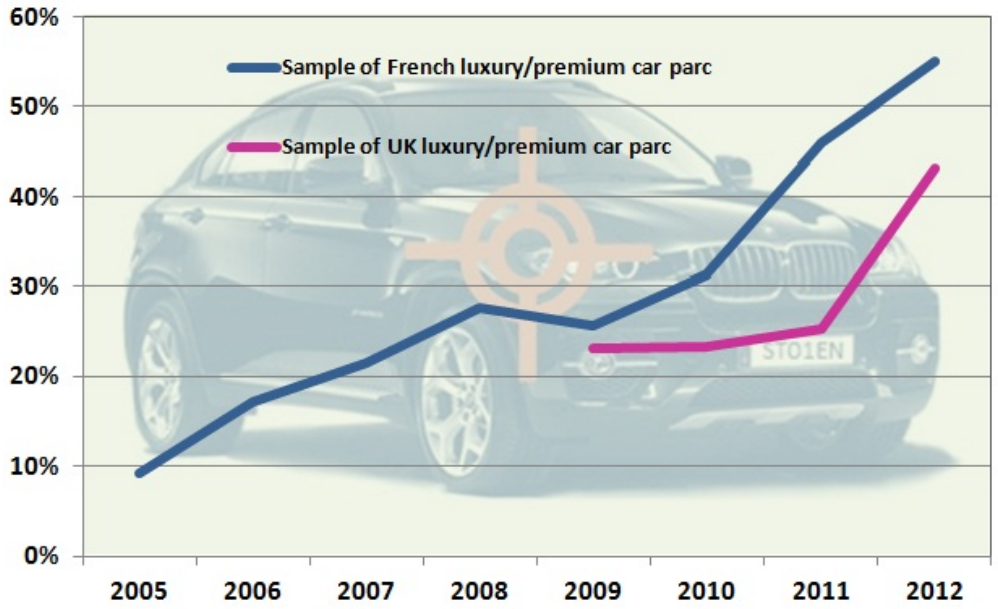


Source: SBD

Electronic theft methods have already reached a high level of penetration in Russia, accounting for an estimated 40 % of all car thefts in Moscow and St Petersburg. High-risk cars are targeted to an even greater extent; SBD estimates that up to 70 % of higher-risk models are stolen with electronic theft methods.

Indicative statistics such as 'key theft' data can provide insight into the uptake of electronic theft when correlated with local vehicle crime intelligence. An increase in the proportion of newer cars stolen 'without the key' provides some evidence to suggest that OCGs may be using electronic theft in preference to established methods such as obtaining the original key, typically through house burglary.

Figure 3. Increasing Trend of Car Thefts 'Without the Key'



Source: SBD

Where effective theft tools exist for attractive cars in markets with strong demand or export potential, OCGs can take advantage to the degree that 'without key' theft methods can account for 75 to 80 % of all thefts of targeted models.

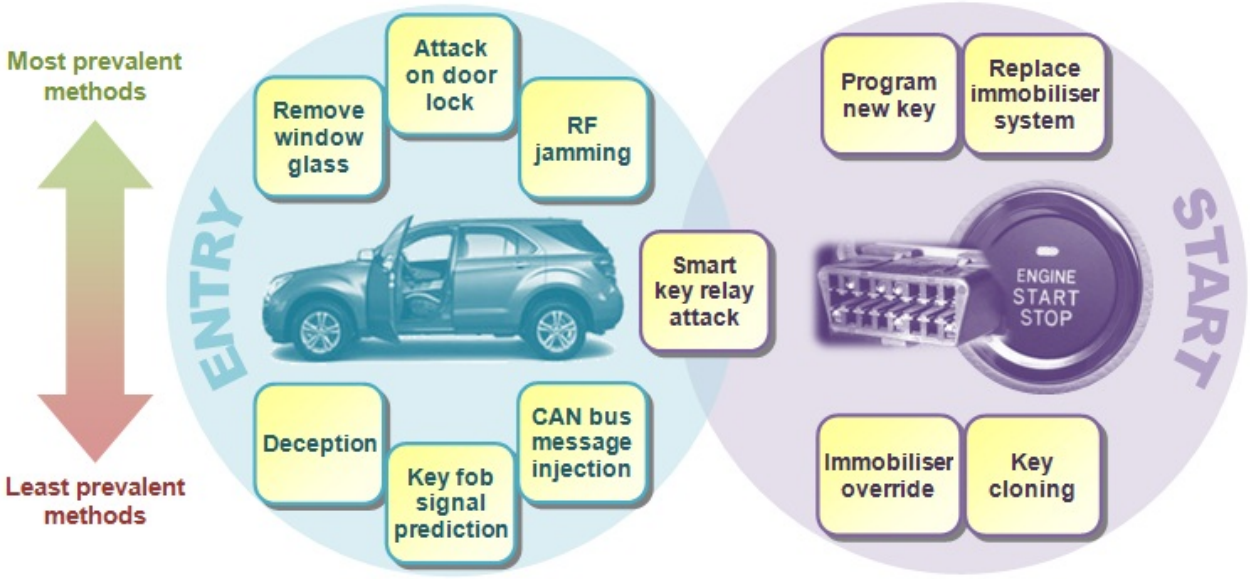
Indeed, data from the ***Metropolitan Police*** shows that, in the last year, around 80 % of all two to five year old models from a particular German manufacturer which were stolen in the Greater London area were taken without the key. Many hundreds of cars were taken in this way and this trend was even featured on prime-time TV in the UK.

3. Typical Methods used by Thieves

Theft patterns have changed significantly since the first immobiliser systems were launched and cars became more secure. Thieves have been forced to find new ways to operate and are using a range of methods such as stealing the key, carjacking, fraud and, more significantly, the development of electronic methods of overcoming car security systems.

Evidence suggests that OCGs using electronic theft methods plan meticulously and do not tend to use entry methods that are inefficient, such as requiring them to be near the car when the owner exits. Door lock manipulations or removal of the window glass are generally the most common methods to gain access to the car.

Figure 4. Entry and Start Methods used by Thieves



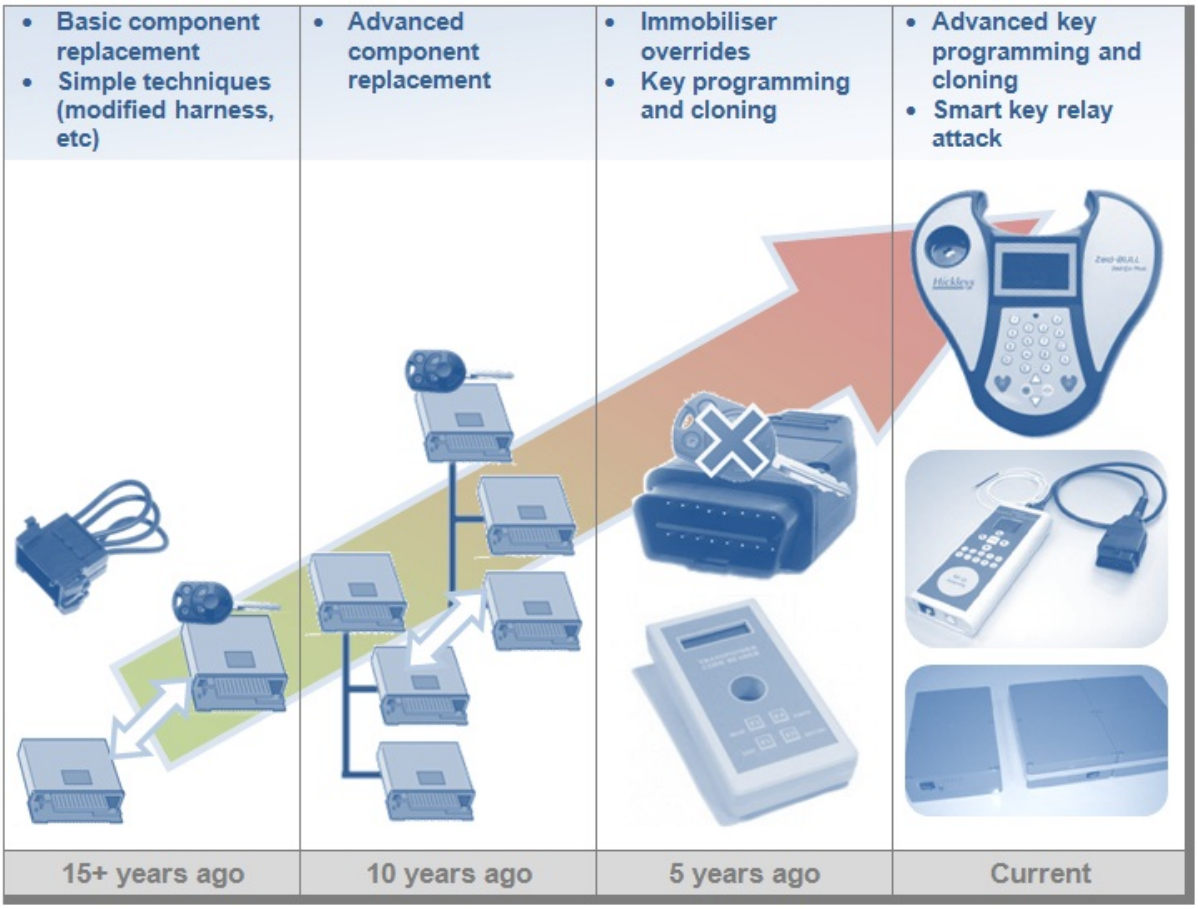
Source: SBD

A multitude of tools are available, covering almost all car models, to help thieves overcome the immobiliser once inside. Whilst home-made tools have been recovered, a majority now appear to be sourced from the internet. Their effectiveness has been confirmed by both Police and insurance investigators, as well as SBD's internal testing. Devices recovered include key programming and cloning tools as well as immobiliser 'override' units.

Historically, a popular method to defeat the immobiliser was to replace the relevant control units in the car, but such ***hardware*** attacks have been largely replaced by ***software*** attacks where a thief simply connects a key programmer or override tool to the car's OBD port. Within a couple of minutes (or just seconds for some tools) the thief is able to drive away.

Whilst the equipment may be sophisticated, no particular skill is required of the user except to have the correct tool for the target car and to be able to locate the OBD port.

Figure 5. Electronic Theft Method Timeline



Source: SBD

4. Conclusions

Whilst the overall level of car theft in many developed countries has reduced in the past decade, the level of profit-motivated theft by OCGs has increased. Vehicle theft is a lucrative activity for criminal groups and it is estimated to generate revenues in excess of $20 billion in the USA and Europe alone.

Facilitated by the vast amount of information on the internet, leaks from within vehicle manufacturers or their increasingly global supplier base, the activities of reverse-engineering specialists and continued use of outdated, proprietary cryptography, many tools have been developed which are capable of overcoming the embedded security. These tools are effective and are widely sold online.

The penetration of electronic theft methods, as a proportion of all car thefts, is rising in most of the markets studied. This is especially true in mainland Europe, where cars can be exported quickly after theft and there are a relatively high number of newer cars to target.

Vehicle manufacturers should take note that thieves are already stealing a significant number of cars using electronic theft methods. Even where a risk analysis shows that a vehicle manufacturer is not targeted with such methods at the current time, market demand can change quickly and all brands are therefore encouraged to evaluate the tools available for their vehicles to understand the security weaknesses they exploit.

If countermeasures are deemed necessary or prudent, a proper understanding of how the theft tools were developed may be vital for any solution to be effective over an extended period.

Another action point concerns all industry stakeholders; there is an almost complete lack of relevant statistics. Without access to basic statistics, it is very difficult for vehicle manufacturers to perform accurate risk assessments. However, in practical terms it is difficult for the Police to increase their knowledge and tackle organised car crime because many specialist vehicle crime units have been disbanded as politicians have paid attention solely to top-level theft statistics.

5. Caution for the Future

Increasingly, cars are being fitted with telematics systems to provide the connectivity demanded by a new generation of buyers. With vehicle connectivity likely to become ubiquitous in the years to come, future theft methods may move from ***physical*** attacks, where the criminal overcomes the security from within the car, to ***remote*** attacks performed by sophisticated hacking techniques, requiring only that the thief is able to locate the car in order to steal it.

Researchers from the Universities of San Diego and Washington in the US recently released a paper outlining their successes in performing several ‘proof of principle’ attacks on a vehicle telematics system. With these attacks, they demonstrated the capability to remotely locate the car using GPS (the vehicle could even broadcast its position to their computer), and send commands to remotely unlock the car doors, deactivate the alarm, deactivate the gearshift lock and start the engine.

The automotive industry may soon need to understand the motivations and methods of a new type of attacker; the cyber-criminal. Many OCGs already count such individuals among their number and, if they can provide the technical capability to enable remote car thefts, the existing OCG structure will undoubtedly be able to monetise it.

About the Author:

Paul Burnley – Senior Consultant, Electronic Theft Methods

Paul graduated from the University of Surrey with a Masters degree in Electrical and Electronic Engineering. He has worked with a number of leading suppliers designing advanced automotive electronic products. His strong technical background makes him an expert in analysing in-car systems. Within SBD's Secure Car division, Paul leads on electronic theft methods, including the development of relay attack equipment, analysis of electronic locksmith tools and cutting-edge research into emerging theft trends and future attack methods. He has spoken at several international conferences on both vehicle security and telematics subjects.

About SBD:

SBD is an independent technical consultancy specialising in the design and development of Vehicle Security, Telematics and ITS systems. From technical trend reports to conducting end user surveys, SBD has over 15 years of experience of providing strategic advice, insight and expertise to the automotive and associated industries globally.

At SBD, we help vehicle manufacturers and their suppliers bridge that gap between system design and actual market needs. Our diverse team of experts understand global market and technical requirements and how to plan cost-effective systems for the future that customer's value and are willing to pay for.