



Marc Weber Tobias Contributor

I am an investigative attorney and physical security specialist.

Opinions expressed by Forbes Contributors are their own.

TECH 9/24/2015 @ 9:00AM |

Another Reason Not To Steal Cars: Key Fobs Now Store A Ton Of Data



(Photo: CHRIS YOUNG/AFP/Getty Images)

During the past twenty years the locks and security systems for cars have undergone an incredible transformation from simple mechanical keys to sophisticated keyless entry systems that have often been difficult to compromise. Expensive high-end vehicles such as Mercedes, Audi, BMW, and Volvo have invested millions of dollars to make sure that thieves could not steal their cars by compromising the locking systems, because auto theft is an incredibly lucrative business. Few consumers think about the security of their key fobs, wireless access, and smartphone applications that communicate with your vehicle and a host of related internet-connected options that are now available. Even fewer consumers are aware of the information that is stored in their electronic keys, some of which is quite detailed.

I just spent a day at [the most sophisticated private forensic laboratory in Europe](#), located in Mayen, a small city in Southern Germany. Manfred Goth is a certified police forensic expert who runs the lab. They work for many of the large insurance companies in Europe, conducting forensic examinations on crimes that involve the analysis of locks, safes, cars, and buildings in civil and criminal cases of murder, arson,

burglary, auto theft and other potential crimes. Last year alone, the lab saved one insurance company about twenty million Euro on claims, including vehicle theft, that were fraudulent. They also consult with police agencies on the covert entry and bypass of security systems and are part of the *Lockmasters Group* that is based in Bergheim, Germany. Lockmasters specializes in the development and training of all forms of covert entry tools for government agencies and has expertise in all locking systems and how they are compromised.

Even though I work with lock manufacturers in testing the security of their hardware, I rarely pay attention to cars. My vehicle has keyless entry, but I never considered seriously the security vulnerabilities inherent in these systems, or any possible privacy issues because my professional focus is on high security locks. Even more to the point, it never occurred to me that vehicle data could be stored in my key fob which might be used by insurance companies and the police for investigations and prosecutions. That all changed when I visited the Goth laboratory and Lockmaster's office.

Manfred was working on a car theft case involving a BMW which, I was told, stores more information on their keys than any other car company. I was shown a decoder that is produced by *Abrites*, a company in Sofia, Bulgaria. This group of highly-skilled software engineers specialize in developing electronic decoding and bypass systems for most of the vehicles in the world that employ key fobs and keyless entry. They make tools for locksmiths and some highly restricted versions for government agencies. The immobilizer systems, keys, locks, and central computers in the modern car can all be hacked to enter vehicles, plant bugs or tracking devices, clone keys, decode keys, read out critical data, or steal the car. Not only are government agencies and locksmiths using these systems, so are car thieves.

Manfred Goth plugged the BMW key fob into the Abrites decoder and almost instantly, it read out a significant amount of data, including the Vehicle Identification Number, mileage, fuel level, and last time driven. Newer keys are also storing GPS data.

So how is this all relevant? It turns out that many insurance claims are filed for stolen cars, and a lot of those are false. In Europe, the insurance carriers require the owner to produce their car keys for examination upon making a report. Virtually no one understands that the data contained in their keys can be used against them

in a criminal prosecution for attempted insurance fraud, or a denial of claim. Case in point: the owner files a police report that his car was stolen three days ago. He turned over his keys to prove that they were not left in the vehicle or given to the thieves. What the driver did not know was that the memory in the key logs the last time the car was driven and the ending mileage. In this particular case, the information on the keys showed that the car had been driven the day before, which meant it had to be a false claim.

I went to Lockmaster headquarters in Begheim, Germany for a further demonstration of key decoding and how to intercept critical information between key fob and car to steal the vehicle. [Watch my interview](#) with Enrico Wendt, the Operations Manager of the company, as he shows how to decode a BMW key fob. In my next article, you can watch *Sascha Wendt*, Technical Manager, as he shows how easy it is to drive away in a new Audi.

While the primary purpose for storing data on keys is ostensibly for maintenance functions, there is no question that law enforcement and insurers are providing input to the auto manufactures and that more and more information will be stored in key fobs, just like on smartphones.

Keys for vehicles are only part of the security issues that are constantly under attack by covert entry specialists, law enforcement agencies, criminals, and hackers. I was shown how expensive cars can be stolen by high-tech thieves with a portable device that is also made in Bulgaria. And if that was not enough, I was briefed on how a key fob for one of the most secure high-end vehicles manufactured in Germany can be easily replicated through the infrared port in the ignition and plugged into a laptop, compliments of hackers in Poland. Car manufacturers are now paying attention to defects in the designs of their wireless entry systems and a very clever solution by a Swiss inventor who I interviewed in Zurich. Stay tuned.

RECOMMENDED BY FORBES

[10 Steps To Take When You Win A Lottery Jackpot](#)

[Meet The African-American Billionaire Businessman Who's Richer Than Michael...](#)