参考译文

Today's cars have loads of computer smarts built in. Like the chips that allow you, with the push of a button to unlock your car. And as new cars move down the assembly line, automakers program those functions into the car.

现在的汽车中有大量的电脑智能系统。例如，一按按钮，车门就开了。随着新车从移出装配线，汽车制作商已经在汽车内设置了这些功能。

"They produce one car and they program a cryptographic secret in it, in order to secure it against thieves." Timo Kasper, a cryptographer and engineer at the security and IT consulting company Kasper & Oswald. "Then comes the next car on the production line and they put the same secrets into the second car. And then comes the third car on the production line and they again put the same secrets into this car. And they repeat this process for millions of cars in the world. And now millions of cars in the world share the same cryptographic secret. Of course, this secret is not so well protected anymore, because it's in every of these million cars, and in every remote control. And this is of course a typical example of how to not do it."

为了避免偷窃行为，汽车制造商每生产一辆汽车，就会在车内安装一个密码系统。Timo Kasper是安全咨询公司Kasper & Oswald的一名译解密码者，同时也是一名工程师。“在生产下一辆车的时候，他们在另外一辆车上，装上了同样的密码系统，然后是第三辆车，他们又装上了同样的密码系统。对于世界上数百辆车，他们都重复着同样的过程。现在，世界上数百万辆车拥有同样的密码。当然，现在人们没有保守好这个密码系统，因为，在数百万辆车中，在每个遥控装置中都存在这样的密码系统。这成为了一个应该避免的典型的例子。

And yet, he says that's exactly how the Volkswagen Group did do it, for many cars manufactured in the last 20 years. Kasper and his colleagues decoded that shared cryptographic secret by studying the design and operation of chips from VW Group cars and remotes. After hacking the hardware, they were easily able to eavesdrop on and decrypt unlocking signals, clone the remote control and unlock cars. They presented the details August 12th at the USENIX Security Symposium, in Austin, Texas.

Timo Kasper表示大众汽车就在对过去20年生产的汽车进行上述操作。Kasper和同事们通过研究大众汽车和其遥控装置的芯片，解码了共享的密码系统。在入侵硬件之后，他们很容易能够窃听和解密释放信号,克隆遥控器解锁汽车。8月12日，在德克萨斯州Austin的USENIX安全研讨会上，他们公布了具体的信息。

Kasper says VW is aware of the problem—and they're not alone. "This is not a VW bug but this is a red line, as we Germans say, through all the automotive industry." In fact, in the same study, they showed that another encryption system used by many other brands, including Ford, Chevy, Nissan and Mitsubishi, has a weak cryptographic algorithm—which, again, allowed the team to break into more than a dozen cars.

Kasper表示大众已经意识到了这个问题——同是，并不只是大众。“这不是大众的漏洞，就如我们德国人描述的那样这是一个危险警戒，是汽车行业的一个危险警戒。实际上，在同样的研究中，他们呈现了，其他品牌，如福特、雪弗兰、尼桑、三菱等使用的另外一种加密系统。这种系统使用的加密算法也有纰漏，这导致团队再一次成功解锁了数十辆汽车。

Bottom line? It's easier to hack into cars than many drivers might have imagined. So if you want to avoid eavesdropping, the researchers recommend simply ditching remote controls and cryptography, and just go back to the good old metal key.

结果呢?与许多驾驶者想象相比，入侵解锁汽车似乎更加简单。如果你想避免被窃听的话，研究人员建议，很简单，那就是不使用遥控和加密装置，而重新使用传统的金属钥匙。

听力原文

Today's cars have loads of computer smarts built in. Like the chips that allow you, with the push of a button to unlock your car. And as new cars move down the assembly line, automakers program those functions into the car.

"They produce one car and they program a cryptographic secret in it, in order to secure it against thieves." Timo Kasper, a cryptographer and engineer at the security and IT consulting company Kasper & Oswald. "Then comes the next car on the production line and they put the same secrets into the second car. And then comes the third car on the production line and they again put the same secrets into this car. And they repeat this process for millions of cars in the world. And now millions of cars in the world share the same cryptographic secret. Of course, this secret is not so well protected anymore, because it's in every of these million cars, and in every remote control. And this is of course a typical example of how to not do it."

And yet, he says that's exactly how the Volkswagen Group did do it, for many cars manufactured in the last 20 years. Kasper and his colleagues decoded that shared cryptographic secret by studying the design and operation of chips from VW Group cars and remotes. After hacking the hardware, they were easily able to eavesdrop on and decrypt unlocking signals, clone the remote control and unlock cars. They presented the details August 12th at the USENIX Security Symposium, in Austin, Texas.

Kasper says VW is aware of the problem—and they're not alone. "This is not a VW bug but this is a red line, as we Germans say, through all the automotive industry." In fact, in the same study, they showed that another encryption system used by many other brands, including Ford, Chevy, Nissan and Mitsubishi, has a weak cryptographic algorithm—which, again, allowed the team to break into more than a dozen cars.

Bottom line? It's easier to hack into cars than many drivers might have imagined. So if you want to avoid eavesdropping, the researchers recommend simply ditching remote controls and cryptography, and just go back to the good old metal key.