TechXplore

Testers look into security of car alarms

March 9 2019, by Nancy Cohen

Credit: CC0 Public Domain

A: "You mean your keyless-entry car was stolen in spite of your alarm?" B: "No, my car was stolen because of my alarm." Does this make any sense? It would if you read about a UK security firm's findings when they went looking into third-party car alarms.

In brief, security holes were found in third-party alarms showing up in brand-familiar cars. Yes, they were talking about those alarms that offer to keep cars from being hijacked. They have the option for a person to start up the car from a smartphone app. Are you thinking what we are thinking? Smartphone app? With an insecure alarm app, the researchers were able (1) to activate car alarms, (2) unlock car doors and (3) start the engine.

The security researchers exploited the brands that could leave the door open (a suitable quip) to wrest control. They saw a number of weaknesses in two alarm products tested. These included the findings that the car could be geo-located in real time, car type could be identified, could start the engine remotely and in some cases the engine could be killed.

The research was carried out for the BBC's Click technology program by UK-based Pen Test Partners, in the business of uncovering software flaws via penetration testing and security services. They shelled out $5,000 to buy and fit the smart alarms for cars.

A video on BBC News showed two hackers waiting to make their move on a chosen—then trapped—car. The victim in the black car had no idea (as re-enacted) of what was about to happen. The car panic alarm went off, causing the driver to stop. And then, in a small car behind the victim's car, the attackers got out and took control of the door locks.

"Get out of the car. Give me your keys."

The team contacted the vendors involved and gave them 7 days to take down or fix the vulnerable APIs. Fortunately, the firms did respond to the exposure and they have upgraded security to remove the flaws.

A UK representative at one of the firms responded in about 48 hours and had their other office take action quickly. The fix was overnight; the other company had a fix too.

Pen Test Partners assessed the vendors' reactions, saying that "the response of both vendors was actually pretty good. They acknowledged, responded, took immediate action and verified it. A lesson for all IoT vendors there!"

"As more things are network controllable, security gets more and more important," said *Hackaday.* As for BBC reader responses, it seems as if there is a car-owning segment who are not impressed with technology's steps forward. Not only are they unimpressed but are regretting the increase in dependence on technology affecting automobile functions.

One comment was that "there is no 'Intelligence' in any software .. it's nothing but statistics/probability. In other words it's a matter of time before the wrong choice is made."

Another comment said he wished he could buy a car "without all the automation. I don't want the computer turning wipers on for me, or changing the angle of my headlights when I turn, or beeping at me when I change lane. Dangerous distractions. I'm driving; I should be in control of the car."

Still another: "If its [sic] connected to the internet, its hackable, whether its a car or a nuclear power station. I worked for a company involved in safety critical transport infrastructure, and we had a strict rule that operational equipment was never connected to the internet, whether by VPN or other security technique."

Other comments indicate opinions that the focus should not be on the fragile nature of software but on the need for thorough testing and debugging before a product can be released.

One comment looked at the way in this instance the companies responded promptly. Security flaws are a fact of digital life, so just deal with it. The key focal points are "Vulnerability disclosure and effective remediation" which are a "crucial measure of trust." The comment added that more should be made of responding within 7 days than the aspect of "be afraid!"

More information: www.pentestpartners.com/securi … ploiting-car-alarms/
www.bbc.com/news/technology-47485731

Citation: Testers look into security of car alarms (2019, March 9) retrieved 27 April 2024 from https://techxplore.com/news/2019-03-testers-car-alarms.html