Tesla’s Model 3 will be the prime target at upcoming hacker contest



The Pwn2Own contest is one of the biggest events in competitive security research, a place where up-and-coming hackers can show off their skills and earn money by finding new vulnerabilities in widely used programs. But this year, there will be a new target on the list — a brand-new Tesla Model 3.

Tesla is partnering with the event’s organizers to include the Model 3 as the sole target in the automotive category, challenging hackers to find new ways to compromise the car’s security. The car is also a prize, to be awarded to a single winner in the automotive category.

It’s the first time a car has been put to the test at Pwn2Own, and a measure of Tesla’s commitment to digital security. “Our work with the security research community is invaluable to us,” said Tesla’s vehicle software chief David Lau. “We look forward to learning about and rewarding great work in Pwn2Own so that we can continue to improve our products and our approach.”

Since 2014, Tesla has operated a bug bounty program that encourages researchers to report vulnerabilities in exchange for payment, a practice that has since been adopted by General Motors and Fiat Chrysler. Tesla has also been a popular target for hackers: in 2015, researchers were able to take control of a Model S’s instrument cluster and information display, although no automotive functions were affected.

Pwn2Own has traditionally focused on software, and recent years have produced a string of eye-opening browser hacks. In

2015, a researcher earned $225,000 for three browser vulnerabilities affecting Chrome, Internet Explorer, and Safari.

https://www.theverge.com/2019/1/14/18182539/teslas-model-3-pwn2own-cansec-west-bug-bounty-hacked