RISK ASSESSMENT / SECURITY & HACKTIVISM

Meet RollJam, the $30 device that jimmies car and garage doors

Widely used keyless entry systems can be hacked in seconds with wallet-sized device.

by **Dan Goodin** - Aug 6, 2015 10:20am PDT

79

Samy Kamkar

Over the past decade, keyless entry systems have largely displaced traditional physical keys as the means for locking and unlocking cars and garages around the world. Just push a button and the electronic devices transmit a secret code that activates or deactivates the lock, saving people the hassle of manually controlling it.

Now, serial hacker Samy Kamkar has devised RollJam, a $30 device that steals the secret codes so attackers can use them to gain unauthorized access to a car or garage. It works against a variety of market-leading chips, including the KeeLoq access control system from Microchip Technology Inc. and the High Security Rolling Code generator made by National Semiconductor. RollJam is capable of opening electronic locks on cars from Chrysler, Daewoo, Fiat, GM, Honda, Toyota, Volvo, Volkswagen Group, Clifford, Shurlok, and Jaguar. It also works against a variety of garage-door openers, including the rolling code garage door opener made by King Cobra.

Rolling codes are similar to the pseudo-random numbers used by the RSA SecurID and similar two-factor authentication devices—with one important difference that will be explained later in this post. An algorithm inside the electronic key and the lock allow the two devices to remain synchronized so the lock can determine when it has received a legitimate rolling code sent by the authorized key. A legitimate rolling code is valid until it's received by the lock. The next time the electronic key is pressed, it will issue a different code. In the event that the key issues a rolling code that isn't received by the lock—say, when the two devices aren't within radio range of each other—the lock is able to accept a newer rolling code and invalidate any earlier rolling codes that weren't received.

Jam, steal, replay

RollJam uses a clever hack to exploit this system whenever it's within range of a key and lock. The device contains two radios. The first jams the airwaves to prevent the lock from receiving the rolling code sent by the electronic key. Since the car or garage door doesn't unlock, a user almost certainly will press the lock or unlock button again. Once RollJam has collected the latter rolling code, it uses the second radio to broadcast the earlier rolling code to the lock. RollJam then stores the latter rolling code. Because the code was never received by the lock, it remains valid. By replaying it later—say, after the car owner has locked the car and walked away—RollJam is able to unlock the car or garage. Kamkar said he has tested the device on several makes of cars and all were susceptible.

The reason many electronic locks are vulnerable to RollJam is that the rolling codes are invalidated only after it or a subsequent rolling code is received. Devices like the RSA SecurID, by contrast, cause validation codes to expire after a specific amount of time.

"Rolling codes should be valid only for limited period of time," Kamkar told Ars. "Code should be associated with a period of time."

At the moment, RollJam is about the size of a wallet, but with additional work it could be the size of a car key. Kamkar will be demonstrating the device this weekend at the Defcon hacker convention in Las Vegas. There are plenty of scenarios where RollJam may not succeed, but it still underscores a weakness in many keyless entry systems in use today that in certain settings could be exploited with minimal effort by a hacker with moderate skill. Kamkar said Microchip Technology Inc. has introduced a newer KeeLoq model that invalidates rolling codes after a specific period of time, but it's unclear how widely used it is.

READER COMMENTS 79

Dan Goodin / Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.
@dangoodin001 on Twitter

← OLDER STORY NEWER STORY →

YOU MAY ALSO LIKE


Windows 10's privacy policy is the new normal


How *Heroes of the Storm*'s objectives, less toxic games refreshed the MOBA

GAME OVER?
In just 2 years, Zynga's daily average users have fallen by half


Video: Movies that predicted the future—and some that didn't