RISK ASSESSMENT / SECURITY & HACKTIVISM

Hopelessly broken wireless burglar alarm lets intruders go undetected

A lack of encryption opens SimpliSafe system up to game-over "replay" attacks.

by **Dan Goodin** - Feb 18, 2016 5:35pm PST

102

Enlarge

SimpliSafe.com

A security system used in more than 200,000 homes has an unfixable flaw that allows tech-savvy burglars to disarm the alarm from as far away as a few hundred feet.

The wireless home security system from SimpliSafe is marketed as costing less than competing ones and being easier to install, since it doesn't use wires for one component to communicate with another. But according to Andrew Zonenberg, a researcher with security firm IOActive, the system's keypad uses the same personal identification number with no encryption each time it sends a message to the main base station. That opens the system to what's known as a replay attack, in which an attacker records the authentication code sent by the valid keypad and then recycles it when sending rogue commands transmitted over the same radio frequency.

"Unfortunately, there is no easy workaround for the issue since the keypad happily sends unencrypted PINs out to anyone listening," Zonenberg wrote in a blog post published Wednesday. "Normally, the vendor would fix the vulnerability in a new firmware version by adding cryptography to the protocol. However, this is not an option for the affected SimpliSafe products because the microcontrollers in currently shipped hardware are one-time programmable. This means that field upgrades of existing systems are not possible; all existing keypads and base stations will need to be replaced."

The hack required about $250 (£175) worth of commodity hardware to build a microcontroller and a few hundreds lines of code to make it communicate with the SimpliSafe base station. With that one-time investment out of the way, an intruder would then hide the device within a few hundred feet of the SimpliSafe base station and wait for the owner to activate or deactivate the alarm. The attacker could later replay the captured PIN along with a deactivation command to prevent the alarm from sounding during a home break in.

Zonenberg said he made attempts through multiple channels to alert SimpliSafe officials to his findings and never received a response. According to the company's LinkedIn page, the system is used in more

LATEST FEATURE STORY

FEATURE STORY (2 PAGES)

Review: Sony's Xperia Z5 Compact is the best small Android phone you can buy

If you hate big phones and don't mind last year's hardware, this one's for you.

WATCH ARS VIDEO

CES 2016: Ars walks the length and breadth of CES so you don't have to

Ars Technica Automotive Editor Jonathan M. Gitlin walked the length and breadth of the Consumer Technology Association conference (CES) in Las Vegas, Nevada.

STAY IN THE KNOW WITH

LATEST NEWS

TREASURE, HO!

PSA: The most underrated twin-stick co-op shooter of 2011 is currently free

NextDoor boots reporter for reporting on police press conference

While any wireless system is susceptible to this type of attack from a sufficiently savvy and motivated intruder, our systems can be backed up with with a land line or an internet connection for no additional cost. Also, this type of attack represents such a small percentage of total break-ins that the FBI does not even keep a count. This is because the majority of break-ins are a quick forced entry and not the sophisticated type of attack that requires diligent planning as well as highly illegal and cost-prohibitive equipment. Assuming an intruder has the requisite technology, he would need to know the frequency ranges he needs to jam, and also know the layout of your home beforehand, as he would have to avoid motion detectors even in the unlikely event that he bypassed a door sensor.

SimpliSafe isn't the only burglar alarm system to be recently called out as flawed. Last month, researchers from security firm Rapid7 reported that Comcast's home security system could be disarmed when intruders used commodity radio-jamming equipment to interfere with its internal communications.

Post updated on Feb 19 9:34 to add comment from SimpliSafe.

PROMOTED COMMENTS

supax | Wise, Aged Ars Veteran jump to post

I got simpli-safe for my mom's house because I didn't want to pay for a wired system with a cell backup. I suppose for the money it is better than nothing but I can't believe a security system would have less protection than your average garage door opener.

I'm really tired of everyone taking the easy way out. I deal with contractors all of the time constantly trying to cut every little corner possible. I suppose that's all we can expect from people these days.

164 posts | registered Jul 11, 2002

READER COMMENTS 102

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

laugh limits with interrogation-fueled *Spyfall*

WE NEEDED A STUDY FOR THIS

Homeopathy successfully turns water into a placebo

Tiny, blurry pictures find the limits of computer image recognition

Disney's *Gravity Falls* is weird Americana meets Lovecraft for kids