300,000 American Homes Open To Hacks Of 'Unfixable' SimpliSafe Alarm

Thomas Fox-Brewster,
Forbes Staff

I cover crime, privacy and security in digital and physical forms.

“There is something terribly wrong with the alarm industry.” Thus reads marketing material on the site of SimpliSafe, a Boston-based “smart” alarm provider with more than 300,000 customers in the US. It’s been on a mission to improve home security since it formed in 2006 by using cellular technology to warn customers via their smartphone if someone has broken in, whilst allowing them to control alarms from afar.

SimpliSafe, which received a $57 million investment from Sequoia in 2014, is not wrong about the industry. But like a growing number of alarm companies claiming their Internet-connected system provides better security than traditional services, SimpliSafe is actually leaving houses open to burglars with rudimentary hacking skills, researchers have told FORBES.

Anyone who can locate a SimpliSafe owner can use basic hardware and software, bought for between $50 and $250, to harvest customer PINs and turn alarms off at a distance of up to 200 yards away, said Dr Andrew Zonenberg, senior security consultant at IOActive. SimpliSafe has also installed a one-time programmable chip in its alarm, meaning there’s no chance of an over-the-air update. It means there’s no patch coming, leaving all owners without a remedy other than to stop using the equipment, Zonenberg said.

Such weaknesses, and more severe ones, have been found across the home and business alarm industry. In a separate FORBES story released today, your reporter found it was easy to hack into an alarm system in San Francisco, all via a browser and armed with easily-guessable passwords. The access, which was attained with permission from the owner, allowed your reporter to unlock doors, turn off alarms and access the CCTV controls of the affected building from more than 5,000 miles away in London, though he didn’t go that far.

The SimpliSafe flaw

With the well-reviewed SimpliSafe alarm system, attacks need to be carried out in the vicinity of a device, as explained in a technical blog from IOActive shown to FORBES ahead of publication. The hack, as demonstrated in a video by Zonenberg, starts by intercepting the signals that turn alarms on and off. Those signals pass between the portable keypad and the base station within the house.

Zonenberg used a separate SimpliSafe system, disconnecting the main processors and hooking up his own microcontroller to the device radios. His code, written in the C language, would listen to incoming 433 MHz radio traffic and pick out a SimpliSafe “PIN entered” data packet. An LED would light up every time a PIN had been recorded. All he had to do then was press a button to replay the PIN signal and the alarm could be disarmed.

An attacker would have to pay at least $250 for their own SimpliSafe system to carry out this attack. But Zonenburg and IOActive head of research Cesar Cerrudo told FORBES an attack of this calibre could be carried out using a software defined radio and related hardware that could be bought for under $50. Just a few hours’ work would be required.

SimpliSafe’s system promises better security, but researchers believe it opens up avenues for theives.

The attacks are not dissimilar to those demonstrated in 2014 against devices from bigger beasts than SimpliSafe. ADT ADT +%, this week bought for $7 billion, and Vivint were also caught out using unencrypted signals between the sensors and devices used to manage alarms.

SimpliSafe spokesperson Melina Engel told FORBES that it was planning on releasing hardware with over-the-air firmware updates and that customers would be given a discount on those once they were available. She also pointed out that customers are notified every time someone disarms an alarm, so customers should notice when something was amiss even if not checking logs, whilst PINs could be changed from the SimpliSafe smartphone app.

“The security of our systems is our top priority. We’re working to resolve this concern, which also affects other major home security providers. It’s theoretically possible but highly unlikely, and we’re not aware of it being exploited.

“Our system provides customers notifications of their disarm events, so they could catch the criminal in the act. Also customers can change their passcodes anytime locally or remotely via our webapp; so if this ever did happen, any passcode data collected

useless in a matter of minutes.

“Unlike with many alarm systems, SimpliSafe customers are protected from many of the more common, low-tech, and easy methods to bypass home security systems, such as cutting the phone line or power to the home.”

It’s unclear just how far away a hacker would have to be to hoover up PIN codes. The SimpliSafe keypad works up to 100 feet, but Zonenberg believes the attack could work up to 100 yards away, even taking into account the disturbances of obstacles and humidity in the transmission of radio waves.

Smart alarm ‘fraud’

Despite the irony of SimpliSafe’s marketing, it’s right: the alarm industry is doing plenty wrong. Alongside the problems identified in Bay Alarm’s products, FORBES is also reporting on unfixed vulnerabilities in Samsung’s SmartThings home security devices and Comcast CMCSA +0.61%’s Xfinity service, which was determined vulnerable in January by Boston-based security consultancy Rapid7.

Cerrudo believes the collective failures of the alarm industry amount to a “fraud”. “They are promoting something to secure your home but they’re making your home more vulnerable. That should have repercussions, regulation or something. That’s kind of fraud,” Cerrudo said.

“The impression that I’ve got is that the home security product industry isn’t really actually putting any effort into security, whether it’s because they don’t realise the problem, or they don’t care, is not something I’m going to be able to tell you. It’s not just the SimpliSafe system that’s insecure,” Zonenberg added.

“These people are advertising security products that provide little to no actual security.”

Troubles with disclosure

What also became apparent to IOActive and your reporter during our respective research was that disclosing these vulnerabilities to the companies responsible for them was not simple.

SimpliSafe did not have a direct security contact; IOActive decided to reach out to SimpliSafe via LinkedIn LNKD -0.33% messages, the contact form on SimpliSafe’s website and the email listed on its website domain records. SimpliSafe’s spokesperson Engel said the company only saw the emails after FORBES reached out. Bay Alarm was difficult to contact too, with no security or press contacts, which had to be found from an external site by guessing email addresses. And according to the researcher who discovered the Samsung flaws, the firm promised patches that it didn’t deliver.

The myriad weaknesses across smart home devices is only exacerbated by the difficulties associated with warning the companies responsible. And yet it’s the end users who ultimately carry the risk.