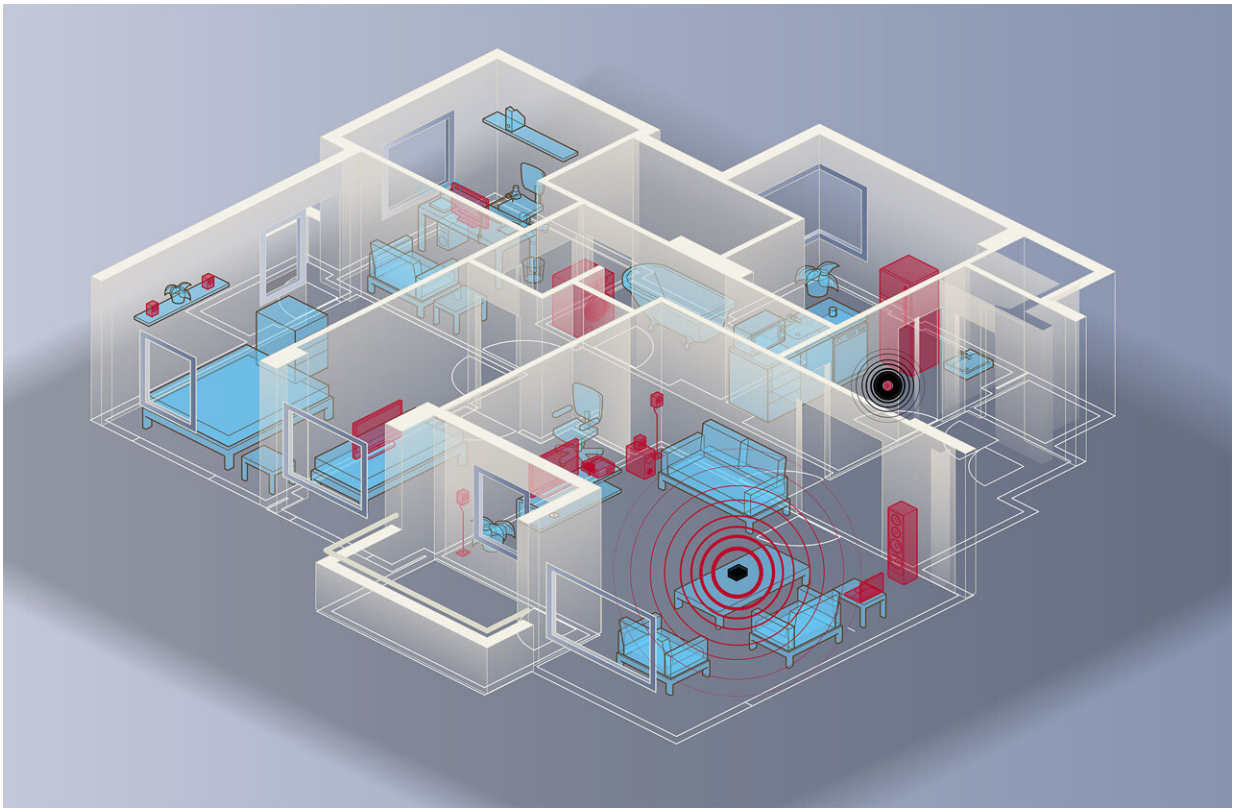
Smart home hubs leave users vulnerable to hackers

November 16 2022, by Leigh Beeson



UGA researchers developed a system called ChatterHub that can successfully disclose the cyber activity of a variety of smart hubs almost 90% of the time, making users vulnerable to hackers. Credit: Lindsay Robinson

Machine learning programs mean even encrypted information can give cybercriminals insight into your daily habits.

Smart technology claims to make our lives easier. You can turn on your lights, lock your front door remotely and even adjust your thermostat with the click of a button.

But new research from the University of Georgia suggests that convenience potentially comes at a cost—your personal security.

The study focused on smart home hubs, the centralized device that enables you to control all your smart devices in one easy spot. These hubs rely on technology that connects them—but not your individual smart devices—to the internet.

That's important because the hubs theoretically make using the smart devices safer. In the past, cybercriminals have hacked into internet-connected baby monitors or smart cameras in people's homes, enabling them to monitor their target's comings and goings.

Hackers can't get into a device if it's not Wi-Fi enabled.

But the UGA researchers developed a system called ChatterHub that can successfully disclose the cyber activity of a variety of smart hubs almost 90% of the time.

"The good thing is all traffic to and from a smart home hub is encrypted," said Kyu Lee, lead author of the study and an associate professor in the Franklin College of Arts and Sciences. Lee is also the associate director of UGA's Institute of Cybersecurity and Privacy. "The bad thing is that we were able to use machine learning technology to figure out what much of the activity is without even having to decrypt the information."

ChatterHub doesn't have to be physically close to the system it's hacking. And the hacker doesn't need any prior knowledge of the types of smart

devices or the maker of the hub to break into the system remotely.

Encrypted information can still be useful to criminals

Smart hubs send packets of information to and from individual devices. That's what enables you to flick on some music through an app or to check your Ring camera when you're out and get a delivery.

Those information packets are encrypted, meaning an outsider can't know exactly what's said in them.

"For example, when a smart home lock is locked, it sends a packet to the hub, and the smart home hub passes that onto the server," Lee said. "We cannot see the actual information that the lock has locked, but using the patterns, the size of the packet and the timing of the packet, we can figure that information out with very high accuracy."

Even though the information is encrypted, attackers can still make use of it.

They can figure out daily patterns of homeowners and determine whether someone is home at a given time, leaving the homeowner vulnerable to a break-in.

Perhaps more concerningly, they can inject their own random packet into the information going to and from the hub.

"If we inject some garbage packet in the patterns we figured out from the machine learning programs, that packet will be delivered to the smart lock and potentially make it malfunction," Lee said. "So that can actually prevent the homeowner from locking their door."

If the criminals are smart, you probably won't even know your door isn't

locked since the app will say it's correctly locked, just like usual. So while you may think your house is secure, the hackers know it's not.

Cybercriminals can use a similar tactic to drain the batteries in smart devices by bombarding the hub with useless packets, the researchers said. But this strategy runs the risk of the smart home hub alerting the homeowner to a low battery.

Changing passwords can keep smart devices, routers safe

So what can users do to protect themselves? Unfortunately, not much.

The real solutions need to come from Samsung, Amazon and other smart home hub giants, Lee said.

The manufacturers could use techniques known as packet padding, which entails making the packets sent back and forth from the hub all the same length. That would make it impractical for hackers to determine which packets do what, preventing them from, say, determining which ones are connected to your door lock, for example.

Another option for the tech companies is implementing random sequence injection, where the hubs send out irregular and meaningless packets to the network. That makes it harder to detect which packets contain useful information.

In the study, the researchers showed that using these techniques together successfully hides the unique network patterns generated by smart devices, making it difficult—if not impossible—for hackers to crack those codes.

Until the companies implement such strategies, though, you can take some easy steps to make your network more secure, Lee said.

Make sure the firewall in your router is turned on. Keeping hackers out of your router is key. Once they're in, cybercriminals can monitor all the network packets in your home and can easily figure out your smart device habits.

You'll also want to change the passwords on your individual smart toys.

Keeping your devices safe is as easy as picking different difficult-to-hack passwords for each one. But many people use an iteration of ABC123 or other easy to remember ones, leaving them vulnerable to cyberattacks.

"We say in the cybersecurity world that humans [are] the weakest link," Lee said.

Published in *Pervasive and Mobile Computing*, the study was co-authored by UGA's Omid Setayeshfar, Karthika Subramani, Xingzi Yuan, Raunak Dey and In Kee Kim, and Dezhi Hong from the University of California, San Diego.

More information: Omid Setayeshfar et al, Privacy invasion via smart-home hub in personal area networks, *Pervasive and Mobile Computing* (2022). DOI: 10.1016/j.pmcj.2022.101675

Provided by University of Georgia

Citation: Smart home hubs leave users vulnerable to hackers (2022, November 16) retrieved 27 April 2024 from https://techxplore.com/news/2022-11-smart-home-hubs-users-vulnerable.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.