Home automation rules are more risky and less risky than we thought

August 24 2020, by Daniel Tkacik

Credit: Pixabay/CC0 Public Domain

According to home automation company IFTTT (an initialism of If This, Then That) around 11 million people use over 1 billion home automation rules, commonly referred to as "applets," each month in their homes. But a 2017 study found that nearly half of the IFTTT applets may pose a security or privacy threat to users.

It turns out, many of those applets were risky in theory but not that dangerous in reality. But there are other types of threats that users should be aware of.

Those are the findings of a recent study led by a team of researchers from Carnegie Mellon University's CyLab. The findings were presented at the Symposium On Usable Privacy and Security (SOUPS), held virtually earlier this month.

While a previous study found that a large portion of IFTTT applets may expose users' private information to the public—a secrecy violation—or grant a less-trusted entity control over their information or their devices—an integrity violation—this latest study found that many of those risks don't play out in the real world.

"There's still a chance for risk in many ways, but realistically, users are safe for the most part," says CyLab postdoctoral researcher Camille Cobb, who led the study.

In the study, the team collected and analyzed 732 applets installed by 28 study participants, and asked participants a series of survey questions to gain a better understanding of their applets and how they use them. The team used a tool that scraped specific pieces of information about the participants' applets, including the user-specified applet title.

Their analysis found many instances where an applet could in theory cause a secrecy or integrity violation, but in the specific way that the applet was being used, it was not actually likely to cause any harm.

For example, many participants used applets that shared information about an action in their homes—such as a window opening, or motion detected on their front porch—to a cloud storage service like Google Sheets. Since Google Sheets can theoretically be shared publicly, the

original risk analysis concluded this applet may exhibit a possible privacy violation.

"In every case in which we asked, every user said they weren't sharing the Google Sheet with anyone else," says Cobb. "That's one example where we thought there might be risks, and there certainly could be, but in most realistic scenarios there probably isn't."

However, the researchers did find some real-life examples of what they refer to as "incidental user threats," something previous studies had not identified. In short, they found many applets that had a high chance of collecting information about people besides the users who set them—information that could potentially be stolen or misused.

"There was one rule that was titled something along the lines of, 'If anyone sends me an SMS, save the contents of that SMS to a Google Sheet,'" Cobb says. "People sending me text messages probably don't anticipate that whatever they send me will be saved in that form. Maybe they're not comfortable with that."

If the contents of the thought-to-be private text message conversation exist in two places, Cobb says, this increases the risk of accidentally being shared with a larger audience.

Given these results, the researchers propose guidelines for creating a better tool in the future to help identify risky applets. And while the study may overall sound like great news to most IFTTT users, Cobb warns they should still take the risky applets seriously.

"Just because we found fewer applets may be risky than we previously thought, that doesn't mean we shouldn't still devote efforts toward making the ones that are risky less so," says Cobb.

More information: camillec.com/SOUPS_2020_IFTTT.pdf