Connected devices in smart homes have control issues

3 April 2014, by Nancy Owano

(Phys.org) —Smart homes are growing smarter. But it all depends on how you define "smart." Smart, as in connected to the Internet, or smart as in a well-planned architecture of intelligent gadgets that can be managed optimally? The Internet of Things can signal a new era of Breaking-into Things. Mundane objects such as fridges could pose security threats as more daily-use objects gain connectivity and go online.

Last month, *V3* reported that Jan Neutze, Microsoft director of cyber security policy for Europe, the Middle East and Africa, spoke at CeBIT, saying cyber criminals will shift their hacks away from businesses and instead begin to look at everyday items. "What happens when somebody attacks your refrigerator? Who's going to patch your fridge? Is it the energy company that runs your smartgrid, is it the software company, is it the manufacturer of the device? We're going to have to look at new models of collaboration that have never existed before." he said.

According to a recent report in *Communications* of the ACM, the publication of the Association for Computing Machinery (ACM), it is not likely the systems can be able to resist being hacked, not without further security considerations.

Smart doorlocks may unlock. Smart webcams may result in pictures posted online. While interactive features of connected devices pose convenience, they may also offer opportunities for abuse. Pranksters may turn lights off and on, but that is not the worst case scenario. Thieves may disable automated doorlocks, or deranged characters can spy on child monitoring cameras.

The ACM publication reported on the paper "The Current State of Access Control for Smart Devices in Homes," by Jaeyeon Jung and Stuart Schechter at Microsoft Research and Blase Ur, a doctoral student at Carnegie Mellon University. The most important devices to secure first, said Jung, were those critical for the physical security of the home, such as door locks and home security cameras, followed by devices collecting sensitive information in the home, such as sleep monitors with Web cameras, according to Communications.

The authors discussed today's homes that are kitted out with smart home automation devices with access control features. "Although connected devices and smart homes are now marketed to average consumers, little is known about how access-control systems for these devices fare in the real world," they said. They examined three items in particular, an Internet-connected lighting system, bathroom scale, and electronic door lock..

They found that each device had its own "siloed access-control system"referring to how each of the three devices operated within its own silo. They also observed a lack of mechanisms for monitoring access, making it impossible for users to understand who has accessed their devices. Jung and collaborators have been working on a prototype of an auditing interface for connected devices configured as a Web interface, which can

also be accessed via smartphone.

More information: The Current State of Access Control for Smart Devices in Homes, (PDF) cups.cs.cmu.edu/soups/2013/HUPS/HUPS13-BlaseUR.pdf

APA citation: Connected devices in smart homes have control issues (2014, April 3) retrieved 9 August 2022 from https://techxplore.com/news/2014-04-devices-smart-homes-issues.html