Student finds privacy flaws in connected security and doorbell cameras

May 27 2020

Ring, Nest, SimpliSafe and eight other manufacturers of internet-connected doorbell and security cameras have been alerted to "systemic design flaws" discovered by Florida Tech computer science student Blake Janes that allows a shared account that appears to have been removed to actually remain in place with continued access to the video

feed.

Janes discovered the mechanism for removing user accounts does not work as intended on many camera systems because it does not remove active user accounts. This could allow potential "malicious actors" to exploit the flaw to retain access to the camera system indefinitely, covertly recording audio and video in a substantial invasion of privacy or instances of electronic stalking.

The findings were presented in the paper, "Never Ending Story: Authentication and Access Control Design Flaws in Shared IoT Devices," by Janes and two Florida Tech faculty members from the university's top institute for cybersecurity research, L3Harris Institute for Assured Information, Terrence O'Connor, program chair of cybersecurity, and Heather Crawford, assistant professor in computer engineering and sciences.

Janes' work informed vendors about the vulnerabilities and offered several strategies to remediate the underlying problem. In recognizing the importance of the work, Google awarded him a $3,133 "bug bounty" for identifying a flaw in the Nest series of devices. Other vendors, including Samsung, have been communicating with Janes about recommended solutions to fix the vulnerability.

The flaw is concerning in cases where, for example, two partners are sharing a residence and then divorce. Each has smartphone apps that access the same camera. Person A removes Person B's access to the camera, but that is never relayed to Person B's device. So Person B still has access even though it has been revoked on the camera and Person A's smartphone and the account password has been changed.

The Florida Tech team found that this happens largely because the decisions about whether to grant access are done in the cloud and not

locally on either the camera or the smartphones involved. This approach is preferred by manufacturers because it allows for the cameras to transmit data in a way that every camera does not need to connect to every smartphone directly.

Additionally, manufacturers designed their systems so users would not have to repeatedly respond to access requests, which could become annoying and lead them to turn off that security check, were it in place, or abandon the camera altogether.

And the security is further complicated by the fact that the potential malicious actor does not need advanced hacking tools to achieve this invasion, as the attack is achievable from the existing companion applications of the devices.

"Our analysis identified a systemic failure in device authentication and access control schemes for shared Internet of Things ecosystems," the paper concluded. "Our study suggests there is a long road ahead for vendors to implement the security and privacyof IoT produced content."

The devices where flaws were found are: Blink Camera, Canary Camera, D-Link Camera, Geeni Mini Camera, Doorbell and Pan/Tilt Camera, Merkury Camera, Momentum Axel Camera, Nest Camera Current and Doorbell Current, NightOwl Doorbell, Ring Pro Doorbell Current and Standard Doorbell Current, SimpliSafe Camera and Doorbell, and TP-Link Kasa Camera.

Though fixes will originate with the manufacturers, if you have one of the aforementioned cameras, it is important to update to the current firmware. Additionally, customers concerned about their privacy after removing additional users should always change their passwords and power cycle their cameras.

Provided by Florida Institute of Technology