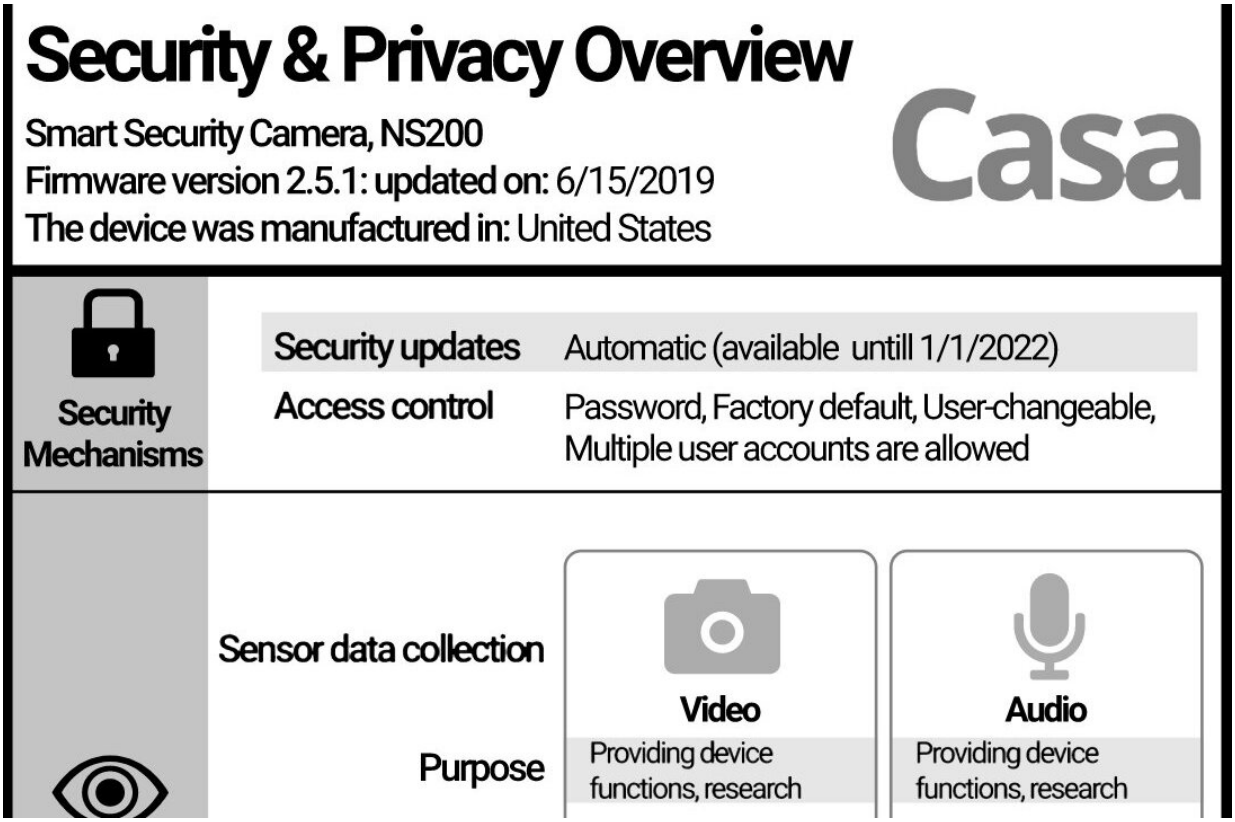
CyLab's IoT security and privacy label effectively conveys risk, study finds

May 28 2021, by Daniel Tkacik



A team of CyLab researchers have developed a security & privacy "nutrition label" that will allow users to readily learn about privacy and security features of their IoT devices and compare these features across devices, just as consumers compare calories and cholesterol in different food products. Credit: Carnegie Mellon University CyLab

Shoppers can check food packaging to learn how much fat is in their favorite ice cream, but can they check with whom their smart speaker shares their data, and why? Not yet, but it's in the works.

Last year, a team of researchers unveiled a prototype security and privacy "nutrition label" aimed to increase consumer awareness of the risks involved in purchasing and using Internet-connected devices. The label displayed various attributes—such as purpose of data collection, and with whom data is shared—were chosen based on input from security and privacy experts, so a question remained: how do actual consumers perceive risk when reading these attributes, and how does that affect their purchasing behavior?

That question was answered at this week's IEEE Symposium on Security and Privacy. The team behind the privacy and security label presented results from a new large-scale study bridging the gap between experts' knowledge and consumers' understanding.

"In general, we found that people accurately perceived the risk associated with the vast majority of attributes that we tested for, and their perceptions influenced their willingness to purchase devices," says Pardis Emami-Naeini, the study's lead author who performed the work as a CyLab Ph.D. student and is now a postdoctoral researcher at the University of Washington. "Our findings pave the path to an improved IoT privacy and security label, which can ultimately lead to a safer and more secure IoT ecosystem."

In the study, 1,371 participants were presented with a randomly assigned scenario about the purchase of a smart device. They were asked to imagine purchasing a smart device (e.g. a smart speaker or a smart light bulb) for themselves, for a friend, or for a family member. On the package of the device, a label explained the privacy and security practices of the device, and participants were asked how the information

on the label would change their risk perception and their willingness to purchase, as well as their reasoning.

The researchers found that the recipient of the device—the participants themselves, their friend, or their family member—did not impact their risk perception, but they were less willing to purchase devices for their friends and family than for themselves. While most of the security and privacy attributes shown on the label yielded accurate risk perceptions, there were some misconceptions.

For example, a large number of participants who were presented with the attribute Average Time to Patch, which had values of either one month, which is less risky, and six months, which is more risky, perceived both to be high risk and lowered their willingness to purchase. Some participants stated that a device that needs to be patched must not be secure, otherwise it wouldn't need to be patched.

"Our findings suggest that manufacturers need to provide consumers with justifications as to why patching may be necessary, why it takes them a specific amount of time to patch a vulnerability, and why it might not be practical to patch vulnerabilities faster," says Emami-Naeini.

The purpose of data collection was another factor that did not change participants' risk perception nor willingness to purchase as the researchers expected. This turned out to be due to participants' lack of trust in manufacturers.

"The companies who collect data are incredibly untrustworthy," one study participant wrote. "They do not have consumers' best interests in mind when they are utilizing the data they collect."

While the researchers provide some insights into the impact a label might have on consumers' willingness to purchase devices in this study,

they are planning future work to assess the label in more realistic settings to understand its impact on consumers' purchasing behaviors alongside other factors, including product price, brand, and ratings.

More information: Which Privacy and Security Attributes Most Impact Consumers' Risk Perception and Willingness to Purchase IoT Devices?Opens in new window

Provided by Carnegie Mellon University