Household robots do not protect users' security and privacy, researchers say

October 8 2009

People are increasingly using household robots for chores, communication, entertainment and companionship. But safety and privacy risks of information-gathering objects that move around our homes are not yet adequately addressed, according to a new University of Washington study.

It's not a question of evil robots, but of robots that can be misused.

"A lot of attention has been paid to robots becoming more intelligent and turning evil," said co-author Tadayoshi Kohno, a UW assistant professor of computer science and engineering. "But there is a much greater and more near-term risk, and that's bad people who can use robots to do bad things."

He and colleagues discovered security weaknesses in three robots currently on the market. They presented the findings last week at the International Conference on Ubiquitous Computing in Orlando, Fla. Co-authors are UW graduate students Tamara Denning, Cynthia Matuszek and Karl Koscher and UW affiliate faculty member Joshua Smith.

During the past year the team ran tests to evaluate the security of three consumer-level robots: the WowWee Rovio, a wireless, buglike rolling robot marketed to adults as a home surveillance tool that can be controlled over the Internet and includes a video camera, microphone and speaker; the Erector Spykee, a toy wireless Web-controlled "spy" robot that has a video camera, microphone and speaker; and the

WowWee RoboSapien V2, a more dexterous toy robot controlled over short distances using an infrared remote control.

The concerns the researchers uncovered with the wireless robots include the fact that:

- The robots' presence is easily detected by distinctive messages sent over the home's wireless network.
- The robots' audio and video streams can be intercepted on the home's wireless network or in some cases captured over the Internet.
- Only some robots give an audible or other alert when a user logs on, letting people nearby know that someone new is accessing the data.
- Only some robots periodically generate a noise or other signal when stationary, reminding people nearby that the robot is collecting data.

The authors also identified scenarios in which a robot might physically harm its owner or the home environment. While the risks today are relatively small, researchers say they believe the risks will become more serious as robots become more widespread.

"These are technologies that are being used in the home," noted Denning, a UW doctoral student in computer science and engineering. "The attacks here are very simple. But the consequences can be quite serious."

"In the future people may have multiple robots in the home that are

much more capable and sophisticated," Denning added. "Security and privacy risks with future household robots will likely be more severe, which is why we need to start addressing robot security and privacy today."

The robots the researchers studied were purchased in or before October 2008. The researchers said they believe other robots now on the market offer a similar level of security.

Owners of household robots can do some simple things to significantly increase their security, researchers said, such as turning on encryption for a home wireless network, and disabling Internet access to the robot's controls.

Education is key, says co-author Matuszek, a UW doctoral student in computer science and engineering.

"Before they go and buy something people will typically go online and do some research," she said. "People know to look for small parts in children's toys, or look for lead paint. For products that combine more advanced technology and wireless capabilities, people should look at whether it protects privacy and security."

Researchers said they hope privacy will someday be on buyers' minds when they look at products, and that in the future electronic privacy and security could be included as a category in Consumer Reports and other product reviews.

More information: More information on the project is at www.cs.washington.edu/research/security/robots/ .

Source: University of Washington (news : web)