Internet of Things poses new security risks

January 11 2014, by Sophie Estienne

The Kolibree toothbrush, the world's first Internet-connected toothbrush, is displayed at the "CES: Unveiled," media preview for International CES, at the Mandalay Bay Convention Center in Las Vegas on January 5, 2014

The hackers who got into your computer or smartphone are now taking aim at the Internet of Things.

The connected toothbrush, sports gear with embedded sensors and smart refrigerators are just a few of the objects showcasing innovations at the

Consumer Electronics Show.

They are all impressive but "they're all breachable" said Kevin Haley, director of Symantec Security Response, while attending the huge high-tech trade show.

"If the object is connected to the Internet, you will find it, and if it has an OS (operating system) you can hack it," he told AFP at the Las Vegas expo.

Haley said the pace of innovation could outstrip the security protecting the devices.

"As we start to bring all this new stuff in our houses, we're going have to take some responsibility," he said.

The devices displayed the CES show included an array of gear from a connected basketball to baby clothing which monitors an infant's breathing and positioning.

And security researchers have shown the possibility, at least in theory, of hacking into automobile electronics or medical devices like pacemakers.

Catalin Cosoi, chief security strategist at the firm Bitdefender, said the threat remains mostly theoretical for now.

"I don't think the bad guys have understood the benefits for them of making use of such things yet," he said.

But Cosoi said some new hack in inevitable which could cause people to take notice.

The display embedded in the front of a LG smart refrigerator on the final day of the 2014 International CES, January 10, 2014 in Las Vegas, Nevada

"We're definitely going to see something happening this year... we might see the first collateral victim, a person being physically harmed," he added.

The introduction of Internet-enabled door locks at CES poses the obvious question of whether the devices can be compromised by hackers.

Alex Colcernian, director of product development at Unikey, which powers Kwikset remote-control locks, said the technology includes "military grade encryption" to stay secure.

Leo Herlin of French-based Medissimo, which introduced a smart pill box, said the system is "extremely secure" to prevent unwanted intrusions.

One factor that mitigates the risk is that with billions of objects likely to be connected, the value to hackers could be limited in most cases: would a hacker penetrate a refrigerator to steal someone's grocery list?

"You've got to be smart consumers when you're using a smart device," said Randy Overton, national product trainer for South Korean giant LG, which showed off its smart appliances that can communicate by text message with the owner.

To allay potential concerns, computer chip giant Intel announced at CES that it would offer its McAfee security service for connected devices free of charge,.

Intel chief executive Brian Krzanich told a CES keynote that offering this level of security would "allow this ecosystem to flourish."

Equipment maker Cisco estimates that 50 billion objects worldwide will be connected by 2020.

Photograph obtained January 7, 2014 courtesy of Heapsylon shows a woman working out wearing the Sensoria Fitness bra, made by Heapsylon

"It is impossible to put security software on every object," said Cisco's David Orain.

The answer is to look and address "abnormal activity" linked to the connected devices, said Orain, noting that this is part of what Cisco offers clients.

One of the areas where security concerns are paramount are in industrial applications.

Andreas Haegele of the France-based digital security firm Gemalto said electronic tracking has been done for decades for things like shipping containers and petroleum platforms, and that the security of these objects is now in focus.

US cybersecurity officials have also stepped up warnings for hacking into so-called critical infrastructure like pipelines and power grids.

Symantec's Haley said that last month's publicized hacking into a nanny cam drew headlines but that no real damage was done.

But the same technique could be used for industrial espionage.

"If I can break into the security cameras of my competitor's factory, I can see exactly how the factory works," Haley said.

Citation: Internet of Things poses new security risks (2014, January 11) retrieved 26 April 2024 from https://phys.org/news/2014-01-internet-poses.html