PHYS ORG

Cyber kid stuns experts showing toys can be 'weapons'

May 16 2017, by Jo Biddle

Reuben Paul addresses the World Forum cyber security conference in The Hague

An 11-year-old "cyber ninja" stunned an audience of security experts Tuesday by hacking into their Bluetooth devices to manipulate a teddy bear and show how interconnected smart toys "can be weaponised".

American wunderkind Reuben Paul, may be still only in 6th grade at his school in Austin, Texas, but he and his teddy bear Bob wowed hundreds at a timely cyber security conference in The Netherlands.

"From airplanes to automobiles, from smart phones to smart homes, anything or any toy can be part of the" Internet of Things (IOT)," he said, a small figure pacing the huge stage at the World Forum in The Hague.

"From terminators to teddy bears, anything or any toy can be weaponised."

To demonstrate, he deployed his cuddly bear, which connects to the iCloud via WiFi and Bluetooth smart technology to receive and transmit messages.

Plugging into his laptop a rogue device known as a "raspberry pi"—a small credit card size computer —Reuben scanned the hall for available Bluetooth devices, and to everyone's amazement including his own suddenly downloaded dozens of numbers including some of top officials.

Then using a computer language programme, called Python, he hacked into his bear via one of the numbers to turn on one of its lights and record a message from the audience.

"Most internet-connected things have a blue-tooth functionality ... I basically showed how I could connect to it, and send commands to it, by recording audio and playing the light," he told AFP later.

"IOT home appliances, things that can be used in our everyday lives, our cars, lights refrigerators, everything like this that is connected can be used and weaponised to spy on us or harm us."

They can be used to steal private information such as passwords, as remote surveillance to spy on kids, or employ a GPS to find out where a person is.

More chillingly, a toy could say "meet me at this location and I will pick you up," Reuben said.

'Timebombs'

His father, information technology expert Mano Paul, told how aged about six Reuben had revealed his early IT skills correcting him during a business call.

Using a simple explanation from dad on how one smart phone game worked, Reuben then figured out it was the same kind of algorithm behind the popular video game Angry Birds.

"He has always surprised us. Every moment when we teach him something he's usually the one who ends up teaching us," Mano Paul told AFP.

But Paul said he been "shocked" by the vulnerabilities discovered in kids toys, after Reuben first hacked a toy car, before moving onto more complicated things.

"It means that my kids are playing with timebombs, that over time somebody who is bad or malicious can exploit."

Now the family has helped Reuben, who is also the youngest American to have become a Shaolin Kung Fu black belt, to set up his CyberShaolin non-profit organisation.

Its aim is "to inform kids and adults about the dangers of cyber insecurity," Reuben said, adding he also wants to press home the message that manufacturers, security researchers and the government have to work together.

Reuben also has ambitious plans for the future, aiming to study cyber security at either CalTech or MIT universities and then use his skills for good.

Failing that maybe he could become an Olympian in gymnastics—another sport he excels in.

Citation: Cyber kid stuns experts showing toys can be 'weapons' (2017, May 16) retrieved 1 May 2024 from https://phys.org/news/2017-05-cyber-kid-stuns-experts-toys.html