Hackers May Be Able to Control Your TV or Car

(Articles reprinted by permission of River Run Computers, Inc.)

Forget Smartphones, It's Smart TVs We Should Be Worried About

Technology has afforded us with a level of convenience and entertainment that was unimaginable just 10 years ago. But despite all of the positive attributes that gadgets like smartphones and Google Glass, there's an underlying issue that has become downright frightening over the past several months largely due to revelations concerning the NSA and the FBI's spying abilities: personal privacy.

Once the idea of conspiracy theorists and the paranoid, it's now come to pass that if a connected device has a camera and/or a microphone, it can be used as a spy tool. Smartphones are usually the first to be associated with spying simply because they are on you at all times. That's true, but they are usually kept in a pocket, a purse or on a desk where the camera would be of little to no use to a hacker.

But what about a smart TV?

According to at least three security researchers at the Black Hat conference in Las Vegas, a smart TV is the most dangerous item in your house. Why? Well as iSEC Partners Aaron Grattafiori and Josh Yavor outlined during a recent conference session, a smart TV is really just a smartphone with a big screen.

Along those lines, it can be compromised by anyone in the world with enough knowledge to do so. To demonstrate their idea, the duo managed to hack into a Samsung Smart TV using the Skype app but truth be told, any smart TV app used to communicate over the web can be a portal for hackers.

Once inside the television, virtually anything is fair game. A hacker can record video using the set's camera, steal your username and password and even force the web browser to visit virus-infested websites.

As such, a smart TV is a much more dangerous weapon for spying than a smartphone because it's always watching you because, well, you are watching it. Televisions are the centerpiece for many living rooms and even bedrooms. Do you really want someone seeing everything that goes on in your bedroom behind closed doors? If you have a smart TV in your room, that's exactly what could be happening!

SeungJin Lee, another security researcher speaking at the conference, said surveillance isn't about himself or even you. If your PC is hacked, it's mostly your problem; but if a smart TV is compromised, the entire family – your wife / girlfriend and kids – are also victims without ever knowing it.

Of course, spying isn't the only mischievous deed a malicious hacker could perform. With the right skill set, a hacker could even play tricks on you. For example, you

© 2013 by River Run Computers, Inc.

could be watching a newscast and a hacker could display a fake graphic or headline that could potentially cause a lot of trouble or inflict great fear.

I, for one, will be sticking with my dated LCD TV for the foreseeable future.

Hackers Demonstrate Toyota Prius Hijacking On Video

The two hackers who in July 2013 announced plans to reveal details concerning how to hack a Toyota Prius and Ford Escape have gotten together with Andy Greenberg from Forbes to demonstrate the technique and just how much trouble they can cause once they have hijacked a vehicle's computers.

In the video they produced, Chris Valasek and Charlie Miller get into the backseat of a Prius with a dismantled dashboard and ask Greenberg to start driving. The two hackers are giddy in the backseat as they cycle through a series of attacks that trigger various functions of the car

The hackers were able to cause a variety of events to occur that ranged from mildly annoying to potentially dangerous. Seemingly with the push of a button from the back seat, the Prius's horn sounded and the seat belts snapped tight against the chests of the passengers.

Most of the attacks operate by tricking the car into thinking that an incident is occurring. For instance, the seatbelts can be suddenly made taut using the vehicle's pre-collision system by 'forging' that the car is about to be in a crash.

The 'tricks' with more nefarious potential include the ability to jerk the steering wheel to one side by triggering the automatic parking assistance, and completely disabling the brakes.

Valasek says that there are upwards of 35 electronic control units (ECUs) in the Prius, and nearly every one of them serves their own function. By compromising these systems individually, an attacker can manipulate the car in unusual ways. Fortunately, for now, it seems that the attacker needs to be inside the car to operate the hacks.

For more information contact:

T.E. Brennan Company
330 South Executive Drive, Suite 301
Brookfield, WI 53005-4275
Phone: (262) 754-1162
(888) 271 2232
www.tebrennan.com
consult@tebrennan.com

OR

River Run Computers Inc.
2320 W. Camden Road
Glendale, WI 53209
Phone: (414) 228-7474
www.river-run.com
marketing@river-run.com

© 2013 by River Run Computers, Inc.