Sam Yarcho

SE-4930 – Secure Software

Article Summary 1

12/14/11

The Invisible Computers

IEEE Security and Privacy: November/December 2011 (vol. 9 no. 6) pp. 3

The beginning of this article, Marc Donner states that almost everything we use today has computers in it. A very interesting example, something that I didn't know, was that cars have so many computers in them that they require internal network. Even car keys have computers in them. Medical devices are making a huge leap in technology with the use of computers in their components. Now people are getting implantable defibrillators and peacemakers that contain computers in them to control their API. The doctors that design these components did so for the sole reason for saving lives, are shocked when they are asked about security on these components. What would happen if someone hacked into someone's defibrillator and made it stop? Or how about Radcliffe's demonstration: "Radcliffe, a diabetic who is connected to an insulin pump and glucose monitor at all times, demonstrated how a malicious third party could transmit wireless commands to remotely disable his insulin pump." (Gillis) Just like with the computers in the cars, "…Researchers with iSec Partners recently demonstrated how it's possible to force some cars to unlock their doors and start their engines by sending special text messages to a car's anti-theft system." (Gillis) These are real security problems that are being implemented into systems every day that are not being handled and could cause devastating effects.

Marc continues on and points out that the technology evolution has shifted from mechanical engineers to software engineers ever since the iPhone came out. It used to be all about adding smaller buttons and more features and more surfaces, but with the emergence of the iPhone, it was shown that everything could be done with one button, and from then on mobile phones would be "primarily a piece of software." Computer systems are getting more and more complex. No longer can one recognize the computer body plan of a screen, keyboard, and pointing device. Computers are now appearing everywhere and are becoming "increasingly sophisticated in behavior." Along with the increasingly sophisticated behavior, computers are becoming more and more connected, which leads to many security and privacy issues. These privacy issues are still being understood. Marc gives an example of how it is now possible to track stolen cameras using web services that scan published photographs and index them by

metadata included in .jpeg or .tiff files. This is great for users trying to find their phone, but the privacy risks are not understood yet.

Marc talks about the automobile computer cluster again, saying how the addition and connection of computers in automobiles has lead to groundbreaking safety, performance, and functionality enhancements, but also introduces many safety concerns, many of which are not yet known or fully understood. Marc concludes with stating that security and privacy practitioners and researchers have become too comfortable working in the standard scope of computers and have not kept up with the rapidly changing computing world. He says that more effort should be put into the new challenges that are coming with the fast-paced evolution of technology.

I learned a lot from Marc's article and found it very interesting. I never knew cars or medical devices were being hacked into, it puts a new perspective on the word "hacking" to me. As a student focusing on software security, it also opens my eyes to working in a field that prevents these kinds of security breaches from happening. I would want nothing more than to be able to prevent patients from getting their defibrillator hacked by some malicious, no good third party and having them die because of it. With the coming of these new technologies comes great responsibility, and we need to start training more people in the art of security so we don't forget about it and keep developing new, unprotected systems.

If I could ask Marc a question, I would ask him if he has worked on some of these security issues personally and how he went about solving them. I would ask him if he thinks the world is going to start focusing more on security, and how he thinks that will affect the future of computers. With more people knowing about security and privacy control, more people will also know what it takes to get past the security. How does he want to make security more prominent but also keep safety knowledge away from malicious users? It could be a double edged sword.

Bibliography

Donner, Marc. "The Invisible Computers." *IEEE Security and Privacy* Nov.-Dec. 2011: 3. Web. 14 Dec. 2011.

Gillis, Tom. "With the Internet, Your Car Could Be Hacked - Business - Forbes.com - Msnbc.com." *Msnbc.com*. 23 Oct. 2011. Web. 15 Dec. 2011. <http://www.msnbc.msn.com/id/44990721>.