

ToorCamp Journal, Day 3: Finally, the Implantation Station

August 12, 2012 at 11:14 am by [Amal Graafstra](#) [0 Comments](#)

Share this:



The author implanting an RFID tag in a fellow ToorCamper.

[Editor's Note: Amal Graafstra was one of hundreds of people who attended [ToorCamp](#), a summer camp for geeks concluding today on the Washington coast. The author of the book [RFID Toys](#) and a "double RFID implantee," Graafstra won a ticket to the event through a GeekWire contest. He has been sending dispatches to give the rest of us a sense for life there, concluding with this post today. Previously: [Arrival](#), [Day 1](#) and [Day 2](#).]

For me, the final day of ToorCamp was by far the best, starting with my [RFID Implantation Station](#), where a lot of excitement on forums and around camp ultimately boiled down to only a few sign-ups. After setting up, I sat around for about a half-hour with nobody showing up ... but then a passer-by stopped, asked a few questions, and decided to go for it.

That started the ball rolling and several other bystanders got in line. At the table next to me, people were learning how to build [Geiger counters](#), WiFi pigeons were roosting, and rogue robots were lurking that didn't honor [Asimov's 3 laws](#). In total, 8 people received implants, crowds of spectators watched, and everyone was still smiling about it at the end of the day.

After wrapping up the Implantation Station, I nosedived into hack classes. Seattle hacker Parity taught us how to hack a PIN code out of just about any HTC Android phone, and how to apply the approach to other makes and models. Then Kos showed how you could use a [special USB OTG cable](#) to connect your Android phone (pre-loaded

with tools and scripts) to another Android phone and [pwn](#) it in under a minute, gaining access to photos, texts, emails, and even your Google account token.

After learning how to totally destroy anyone with an Android phone, I dropped in on the last 15 minutes of an 8 hour .NET software hacking class put on by Jon McCoy of [Digital Body Guard](#) ... and what I saw in 15 minutes made me stop and re-evaluate my life. Jon has created tools that allow anyone to easily crack open compiled .NET coded EXE files and essentially re-write it however they see fit, then write out the altered EXE. That means I could easily add features to compiled software, or change functionality, or even fix security holes that the software manufacturer either refuses to fix or simply hasn't gotten around to fixing yet. There are several software applications I use on a daily basis that I wish had some feature or just did something a slightly different way, and now I have the tools that not only make these things possible, it makes these changes trivial.

I'm headed home now, filled with a sense of disbelief that it's over, a giddy excitement as I scheme ways to apply what I've learned, and the definite intention to be first ticket holder on the list for next year's ToorCamp event.



Geiger counter kits at ToorCamp.



WiFi 'Pigeons'



A Kinect-powered robot at ToorCamp.

Follow Amal Graafstra on Twitter [@amal](#) and [find out more on his site](#). For more on ToorCamp, listen to [our recent GeekWire podcast interview with David Hulton](#), one of the organizers of the event.