Running cryptoparties with free software

Steve Revilak

March 21, 2015

(This was given as a five-minute "lightning talk" during Libre Planet 2015.)

Hello, my name is Steve Revilak, and I'm the quartermaster (aka "treasurer") of the Massachusetts Pirate Party. I mind the doubloons, and file periodic reports with the Massachusetts Office of Campaign and Political Finance.

The Mass Pirate party is a small political party in Massachusetts, but we're part of the global Pirate Party Movement. We care deeply about things like government transparency, and the areas where policy and technology intersect. We value the right to personal privacy, and we're deeply concerned about digital surveillance – both government and corporate.

About a year and a half ago, we decided to start holding cryptoparties on a regular basis. A cryptoparty is an event where people get together to learn about cryptography, communications security, and privacy enhancing technologies. When the Snowden leaks started coming out, we figured that some people would want to learn how to protect their privacy online, and we wanted to help them. So for the last year and a half, we've been doing around one cryptoparty per month, and in fact, I'm heading out to Worcester to do one tomorrow afternoon.

Overall, the response has been positive. Some of our cryptoparties have been big productions; for example, we did a day-long event at Northeastern Law School, in conjunction with the Massachusetts ACLU. Most have been smaller; a couple of hours with a small group of people who've had more specific needs or concerns.

We cover things like GnuPG, Enigmail, Tor, Jitsi, OTR, packet sniffing, KeePass, and meshnets.

Who comes to our cryptoparties? It's a variety of people. Lawyers seem to have a particular interest in communications security, especially when it comes to attorney/client communications. Activists are another group. There's also unions, college students, librarians. Finally, there are ordinary people who just want the freedom to talk freely, without the fear of being surveilled. In short, a lot of the groups we've worked with aren't what you would call technology geeks. Bright people, but not technology geeks.

I've heard people say "encryption tools are too difficult for the average person to use". I have mixed feelings about this. On one hand, easy to use is good. Easy to use means a low barrier to adoption; making it more likely for someone to pick up the tools and start using them. Usability isn't perfect, but I think it's really improved over the last few years.

On the other hand, security is not a product, but a process – and it will always be a process. I'm always worried about giving people the impression that "if you use X you're going to be secure". I really want them to understand what the tools do, and why they're important. I want them to understand risks, trade offs, and how to figure out what makes sense for their individual situation.

I've also found that most people "get it", if you take the time to teach them.

I've recently come to the conclusion that learning PGP is a lot like learning to ride a bicycle. It takes a little effort, and most people fall down a couple of times. But anyone can learn how to do it. And once you learn, it's a piece of cake.

What I'd like to do today is to express my gratitude for some of the free software crypto tools we have: GnuPG, Tor, OTR, Jitsi, and many others. Having free software makes it much easier for people who care about their privacy to take the next step, and actually do something about it.

If anyone has ideas about how to run cryptoparties, or the balance between teaching tools and teaching risk management, let me know – I'd love to talk with you.