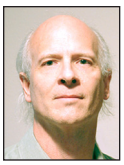
Interview with Periwinkle Doerfler

RIK FARROW

Periwinkle Doerfler is a PhD candidate at New York University's Tandon School of Engineering within the Center for Cybersecurity, advised by Professor Damon McCoy. Her research focuses on the intersection of intimate partner violence and technology. She looks at this issue with regard to abusers and how they come to use technology to perpetuate violence, as well as with regard to survivors and how technology can help or hinder escape from abusive situations. Her past work has also examined cryptocurrency as it relates to human trafficking, doxing communities, and authentication schemes.
periwinkleid@gmail.com



Rik is the editor of *;login:*.
rik@usenix.org

I met Peri Doerfler at Enigma 2019 during lunch and wanted to talk to her right away. Peri would be giving the closing talk the next day about interpersonal threats, a very different way of looking at security than any I had considered. In my life, the threats were attacks on my mail or web servers, or disclosure of financial information while I was attending USENIX conferences. Peri was taking on what sounded completely different, but also very relevant to the types of technology people are regularly using today.

I also have a very personal interest in Peri's research topic. All of the women I'd become close to during my life had told me stories of sexual abuse. I don't mean just verbal abuse, but actual assaults or rape. I was and still am astonished and appalled. The current statistics, relying on reported attacks, are one in three women and one in six men in the US have been sexually assaulted [1].

Rik Farrow: To start out with, how did you get interested in the interpersonal threat area? Reading online, I noticed that you interned at Google and worked on authentication issues.

Peri Doerfler: I've actually had a pretty varied set of research experiences that led me to this. The first project I got involved in when I started my PhD involved looking at Bitcoin and human trafficking, and as you noted, I interned at Google and worked on authentication. I had a second internship at Google working on Android permissions.

In doing some work on spyware and domestic violence, I found that there is a whole set of threats that people, but particularly women, are facing from the people they know. I have not continued to be heavily involved with the work that group at Cornell Tech (in NYC) is doing related to domestic violence, but they are doing great work, as are a few other groups, including one at Google. I think where I went from caring about the specific work to more of this vigilante attitude, if you will, is in attending conferences and hearing a lot of the community dismiss these concerns. I'm always frustrated to hear the security and privacy community talk about users as though they are stupid.

Further, I find that when you address what are, to be frank, more female concerns (not at all because men don't face the same technological concerns, but because men tend to have less fear of physical violence), they are even more summarily dismissed. I have often heard people express how "sad it is that that happens to some people" when discussing domestic violence, without realizing that it is such a common problem (transcending socioeconomic barriers, I must add) that it very likely affects someone they know well. So for me, I think that the best way to help the users who are not aware of the risks they may be taking by sharing their iPhone PIN (or similar) is to raise awareness in society at large, but also to try to get the community that controls this technology and its default settings to think about these risks as seriously as they think about risks from hackers and phishers.

RF: Speaking of which, how do you go about researching such sensitive areas? Do you rely on mining public comments? Are you gaining a reputation in this area so that people seek you out?

PD: When studying domestic violence specifically, a lot of good work is already done in collaboration with various governmental and nongovernmental agencies working with survivors. Most of the research on survivors is done from interviews at shelters. In my personal work in that space, I've focused more on studying the abusers and trying to understand how they're acquiring the awareness and know-how to become abusive with smartphones. That work relies on public information in reviews of apps, on Reddit and 4chan, and on the websites and advertising of the software makers.

In studying interpersonal privacy more generally, I think it will be a combination of the two methods. There's honestly not a lot of data out there now about things like password sharing even generally, and especially not specifically in relationships. I'm definitely hoping to gather some in future work.

RF: Let's stick with spyware for the moment. In March 2019, Eva Galperin of the EFF said she was going to speak about "eradicating spyware" at a Kaspersky conference [2]. The story itself is decent, and it relates to your work.

After the conference, Kaspersky Lab announced adding a feature to their Android AV product that pops up warnings, "Privacy Alerts," when it appears spyware is in use, allowing the user to block the theft of information [3]. I would think that helping the person delete the spyware app would be a better idea.

PD: Yes, the *Wired* story [2] does reference some of my work. I think Eva's coming from exactly the same place on this as I am, which is wanting to help in every way possible and being frustrated when others aren't as receptive as they could be. I liked this quote from the article:

> "...often because security researchers don't count spy tools that require full access to a device as 'real' hacking, despite domestic abusers in controlling relationships having exactly that sort of physical access to a partner's phone.

I think she makes another really good point about threat modeling, and that for the average smartphone user, the major threats the security industry tends to focus on don't really hold up:

> The Kaspersky users who worry about domestic abuser spying are rarely the same ones concerned with Russian intelligence. "It's really about modeling your threat. Most victims of domestic violence don't work for the NSA or the US government."

With regards to whether Kaspersky's move is enough, my response is a resounding no. The fact of the matter is that for it to help someone, they have to have Kaspersky antivirus on their phone before the spyware is installed, then whoever installs the spyware has to not know that it's there or not know how to tamper with the antivirus. Further, it appears from the *Wired* article that this feature is going to operate off of a blacklist. A lot of these apps have many, many versions with different hashes, and a blacklist is likely to miss them.

It's also not clear whether this blacklist will include dual-use apps coming from the Play Store. Assuming this chain of events, the victim gets this privacy notification, but the notification isn't as specific as it could be. It's better than the previous "not a virus" warning, but it doesn't articulate the delicacy of the situation, that someone *put this stuff on your phone*, as opposed to it being some awful adware bundled with something else. It doesn't clarify that the information being leaked could be your GPS data, text messages, and recent calls.

And it certainly doesn't do the most important thing in this context, which would be to help the victim understand that if they delete the offending application, the abuser may become aware of that and escalate to physical violence. That's the big problem I could see happening: in the case it does catch something, people are going to remove it without realizing what it was, and then potentially face violence as a repercussion or lose any evidence they may have had.

I will note, however, that Kaspersky has also reached out to me to ask for thoughts/guidance on how to improve this feature, and they have a whole team of people making a genuine effort to address this. That's incredibly reassuring to see, but it's frustrating that the scope of the protection will be limited to their customers. Hopefully, it puts pressure on other industry players to do the same.

RF: In your Enigma talk, you tell the story of someone being embarrassed after allowing someone access to the iPad to play some music. While phones typically autolock, lots of other devices, like iPads and laptops, don't. To be honest, I think of my home as my castle, but it's really not. I have guests sometimes, or workers, in the house. But in your area of interest, it's not the guests that are the problem, correct?

PD: In my research, guests and workers are part of the threat model, though they are less likely to be the source of a threat than a parent, coworker, or intimate partner. I'm generally interested in studying the ways that people perceive their digital privacy and security in relation to the people they know "IRL." Shared devices and accounts are increasingly ubiquitous, so I'm interested in questions ranging from "Do people moderate their viewing habits when sharing their parents' Netflix account?" to "To what extent do people share their devices with their partners, and what are their expectations of their partners' access to their device?"

RF: What are your plans for future work?

PD: One of the next studies I want to do is with respect to online dating, and asking a few questions inspired by true and very creepy anecdotes. First, if you're in a fairly self-contained community, like a college campus, how easily can you find someone on a dating app if you've only seen them, say, in class? What risks does this pose? Second, if you encounter someone on a dating app, how easy is it to find them elsewhere online or IRL? How does this change across apps, geographic density? Beyond studying dating apps, I'm hoping to do a deeper dive on device sharing and credential sharing in romantic relationships.

I'm also still working on some research related to doxing and harassment, as well as trying to understand pieces of the incel/pickup-artist space, and what the connection is between that and domestic violence.

References

[1] National Sexual Violence Resource Center statistics: https://www.nsvrc.org/node/4737.

[2] A. Greenberg, "Hacker Eva Galperin Has a Plan to Eradicate Stalkerware," *Wired*, April 2, 2019: https://www.wired.com/story/eva-galperin-stalkerware-kaspersky-antivirus/.

[3] S. Lyngaas, "Kaspersky Lab Looks to Combat 'Stalkerware' with New Android Feature," Cyberscoop, April 3, 2019: https://www.cyberscoop.com/kaspersky-lab-looks-combat-stalkerware-new-android-feature/.