Panel: PETs Post-Snowden

Implications of the NSA and GCHQ Surveillance Programs revelations for the PETs community.

with George Danezis, Nadia Heninger, Susan Landau, Wendy Seltzer, Marek Tuszynski, and Seda Gürses (moderator)

Despite the entertainment value of program names like “egotistical giraffe”, “onion breath” and “moth monster”, the revelations about the NSA and GCHQ surveillance programs are more than troubling. Specifically, BullRun (attacks on crypto) and the egotistical series, which focus on attacking Tor, pose challenges to the PETs community and the solutions they work on. This panel focuses on some of these challenges, discuss their implications for PETs researchers and practitioners, and explore ways forward. In the following, you will find a list of the questions that the panel participants have raised in preparation of the panel.

Delegation of responsibilities to Engineers?

The “PETS community”, if one can refer to it as such, is part of a growing class of engineers and scientists who have great influence in how our (technical) infrastructures, and hence our societies, are organized. What are the roles of PETS community members as researchers or practitioners after the Snowden revelations (and, not as politicians, mass educators, public intellectuals, policy advisors, etc.)? This is the bigger question that motivates our panel.

Is government surveillance ever legitimate and what limitations are acceptable?

The American Civil Liberties Union (ACLU) by principle rejects laws supporting government wiretapping. Note that however such laws, with only narrow exceptions, refer to wiretapping of U.S. "persons," US people or corporations. In fact, in the constitution of most sovereign states (not all!), privacy clauses offer citizens, but not foreigners, protection from surveillance programs. If surveillance programs are seen as legitimate, from a technical perspective, how reasonable are protections that are only limited for citizens? How about the problem of intelligence agencies exchanging information about each others’ citizens? Further, some argue that it is mass (bulk) surveillance that is an issue and targeted surveillance is legitimate for purposes of national security. But, what does it mean to find targeted surveillance legitimate? Who do these distinctions benefit and who do they leave out? What do these distinctions even mean when most of the infrastructure belongs to the private sector? Where do members of the PETs community stand with respect to surveillance, how to stop or limit it, and why?

Is loss of privacy the main problem?

Following the revelations about the NSA and GCHQ surveillance programs, public figures which included prominent cryptographers, security engineers, civil society and companies listed in the PRISM program started working on ways to change technology or legislation to reinstate privacy or at least limit the surveillance programs. Is privacy however the only issue of concern? Do the surveillance programs effect everyone in the same way? For example, George Danezis writes in his blog post "The Dawn of Cyber-Colonialism" that maintaining the ability of western signals intelligence agencies to perform foreign pervasive surveillance, requires total control over other nations’ technology, not just the content of their communication. This, he argues, is the context of the rise of design backdoors, hardware trojans, and tailored access operations. Are privacy solutions also

apt to address these other problems or should we be thinking of different threat models and strategies? What are the new challenges for those who may most need PETs, journalists, activists, minorities etc.?

How do we restore trust in our technical infrastructures?

The revelations about the surveillance programs led to a distrust in technologies, standards bodies, companies and government institutions. What needs to be done to reinstate trust in our technical infrastructures? When developing PETs, we often speak of minimizing trust. Are there different concepts of trust in place? How can we distinguish these? If trust is important, do we need to also worry about establishing trust in our community or the output of our community? If so, should we publicly position ourselves with respect to the surveillance programs, e.g., with respect to the attacks on Tor, crypto standards, and the weakening of security in general? And, as news trickle in that governments try to prevent companies from applying secure or privacy preserving designs that may be seen as obstructing law enforcement agencies from conducting investigations, what are ways in which we can keep PETs robust? Are projects to publicly scrutinize technologies the appropriate way to address these privacy, security and trust issues?

How about the effects of the surveillance programs on scientific practice?

The crypto-wars of the 90s saw activists like Philip Zimmerman, communities like the cypherpunks, as well as corporations, battling succesfully to make encryption available for civilian use. One of the gains from the crypto-wars was publicly available, open and free crypto research and civilian crypto practice. However, NSA and military researchers continue to engage in "closed research" in a secret parallel universe. Further, given the rise of national cybersecurity programs, more and more PETs researchers are engaging in research financed by or to the benefit of intelligence agencies and military applications. What are some ethical, political and economic issues at stake here for members of this community? What are critical and productive ways to deal with these entanglements?

What are ways in which the PETS community can make a difference?

There are numerous ways for PETs researchers and practitioners to engage in the post-Snowden programs for positive change. What are some of these? We can engage in future standards making, this may be through official standards organizations, solutions a la DJ Bernstein, or by joining the ranks of large companies which can set de facto standards, e.g., Google's Certificate Transparency project. We can help set up and be part of quality reviews of open protocols and standards. We can develop even more resilient PETs, e.g., against active adversaries. We can make sure we understand the experiences of those most in need of PETs and improve PETs to meet their needs. We can engage in civil society initiatives like the "13 Principles" led by EFF and make sure they are aligned with technical realities. On the policy side, we can support the drafting of new privacy and security laws that are technically reasonable, or participate in legal challenges brought forth by civil society to the surveillance programs as technical experts. Finally, we can include education about surveillance, ethics, privacy, economics and politics (and colonialism/imperialism) in our educational curricula as well as research projects. Surely the list is longer. What are some arguments for or against these engagements? What are some associated insights, obstacles and pitfalls?

References

George Danezis, The Dawn of Cyber-Colonialism http://conspicuouschatter.wordpress.com/2014/06/21/the-dawn-of-cyber-colonialism/

EFF, Necessary and Proportionate: 13 Principles https://necessaryandproportionate.org/take-action/EFA

Ottawa Statement on Mass Surveillance in Canada https://openmedia.ca/statement

Open Letter from UK Security Researchers http://bristolcrypto.blogspot.nl/2013/09/open-letter-from-uk-security-researchers.html

An Open Letter from US Researchers in Cryptography and Information Security http://masssurveillance.info

Susan Landau, Surveillance or Security? The Risks Posed by New Wiretapping Technologies, MIT Press, 2011.

Nadia Heninger and J. Alex Halderman, Tales from the Crypto Community: The NSA Hurt Cybersecurity. Now it should Come Clean, Foreign Affairs, 2013. http://www.foreignaffairs.com/articles/140214/nadia-heninger-and-j-alex-halderman/tales-from-the-crypto-community