CSEP564 : Computer Security : Reading 9

Karuna Sagar Krishna

December 5, 2024

Paper Title

The Moral Character of Cryptographic Work

Paper Authors

Phillip Rogaway

Problem

The author is deeply concerned about mass surveillance and its impact on the society. The author considers the root cause of the problem is the role played by cryptographers and culture of cryptographers community. Specifically, cryptographers limit their work to cool math problems and puzzles but refrain from considering the social impact and how their work is used to influence power dynamics.

Approach

The author describes the social responsibility of scientific and engineering communities by drawing an analogy to nuclear program from 1900s. The author references Russel-Einstein manifesto which galvanized the peace and disarmament movement and hopes that this paper has a similar effect, specifically on the field of cryptography leading to anti-surveillance movement. Though researchers and engineers try to avoid taking part in politics, the authors shows that they always engage politically in either implicit or overt modes and hence they should adopt and practice ethics of responsibility in their work. The author points that there is a general decline in such ethics and blames it on unbridled technological optimism that undermines ethics and social responsibility and urges that we adopt a balanced, contextual mindset.

The author points out the irony about the political nature of cryptography - outsiders perspective shows clearly that the cryptography is highly political as it influence power, while insider perspective shows that cryptography work is divorced from politics and purely academics. Many notable cryptographers entered the field trying to address concerns with sociopolitical dimension. However, the field has fragmented and mostly marginalized socially impactful problems such as secure messaging. This has resulted in 3 classes of cryptographic work - crypto-for-security (commercial purpose), crypto-for-privacy (sociopolitical purpose) and crypto-for-crypto (academic purpose); while crypto-for-security has done well, crypto-for-privacy has suffered and most of the research falls under crypto-for-crypto.

The paper shows that mass surveillance is framed and justified by different institutions for their benefits. Law enforcement frames mass surveillance as a necessary tool to fight the bad guys, so by promoting privacy and encryption we enable bad guys win. Cyberpunks has

an opposing view and frame mass surveillance as cyberwar that thwarts and reverses social progress taking away freedom.

The author offers few suggestions on how we can improve contribution under crypto-for-privacy category. The author urges researchers to chose problems responsibility, specifically around secure messaging protocols, designing protocols that preserve privacy under pervasive monitoring and studying attack vectors enabling mass surveillance. The author cautions researchers on institutions funding their research since these institutions nudge research direction towards their benefits. Finally, the author suggests cryptographers be open-mind to diverse models, cultivate systems view of how crypto is used in practice.

Conclusions

The author mainly urges the scientific, engineering and specifically cryptographic community to develop and practice social responsibility to humanity by paying attention to individual and institutional values. Though the author and paper seem to paint a pessimistic view, the cryptography field has seen progress in communication tools like Whatsapp and research papers post Snowden. In particular, the author urges cultural change to focus on crypto-for-privacy.

New Ideas

The author shows that scientists and engineers participate in politics whether they like it or not. Though this is a tough pill, it is a good idea to embrace, introspect and understand who benefits from our work.

The authors idea of urging researchers to have a systems view is a great idea to develop a holistic solution. Further building cryptographic commons help take these solutions to the masses.

Improvements

The authors point of view are extreme, not balanced and seems like mostly personal. It would be great to have a balanced view potentially by coauthoring this with others.

Though the authors points out issues with mass surveillance, he does not add any quantitative data to support his claim and the list the impact it has had on the society and its citizens. At the moment, the paper seems to be running a risk of fear-mongering.

New Directions

As Russel-Einstein manifesto had multiple authors bringing in various perspectives, we need a balanced and diverse perspective on this topic of surveillance and social responsibility in cryptographic field.

Clearly there are bad actors in society and the cryptographic community should come up with a solution that help law enforcement track these bad actors while preserving privacy by default of all citizens. This might be hard and conflicting in nature but that is what needs to be solved.