Cybersecurity and the Social Sciences (CYSE 201S) School of Cybersecurity Old Dominion University Instructor: Diwakar Yalpi Student: Charles Martin March 24, 2024

Article Review #2 - Bugs in our pockets: the risks of client-side scanning

Link: https://academic.oup.com/cybersecurity/article/10/1/tyad020/7590463?searchresult=1

Introduction:

With the increase in digital technology in all manners of life, cryptography is needed to protect our digital footprint. However, when such protection interferes with law enforcement and national security agencies without the need for backdoors and weak encryption. (Harold Abelson, 2024)Client-side scanning (CSS) is a potential candidate for providing the protection needed for data and the ability for law enforcement to achieve their goals. Unfortunately, this type of scanning has risks that indirectly affect the marginalized.

Methods & Data Analysis:

The research method and data collection are archival and analysis on CSS, focusing on what CSS does in terms of data. "We have built our study on the work of many others...US National Academies of Science, Engineering, and Medicine, which provides a framework for evaluating policy or technical approaches to access the unencrypted content...the 2019 Carnegie Endowment for International Peace study on encryption policy...Paul Rosenzweig's early analysis of the policy issues raised by CSS, along with some of the technical issue" (Harold Abelson, 2024). The article gets its information from archives or other documents that study this scientific endeavor.

Marginalized Groups:

One of the most marginalized groups that are affected by CSS is the LGBTQ+ community, which, depending on the purpose of the scanning, could target the data of such a group as targeting them. "All three already have laws enabling them to mandate tech companies to repurpose or retarget existing scanning techniques...the legal constraints against government action become weaker and the range of targeted content becomes larger, typically including LGBTQ+ content, political activists, and domestic rivals of authoritarian regimes." (Harold Abelson, 2024) In actuality, any group can be targeted in any political aspect. This type of scanning provides a means of political manipulation and repression of any group that may be adverse. (Harold Abelson, 2024) Children, including women, are not safe when it comes to CSS. As the article states, in terms of local adversaries, women who are trying to leave an abusive relationship are hindered by the adversary that can install stalker ware on their phone or any other "smart" product to control their victim. (Harold Abelson, 2024) The same goes for children and their abuse. Any form of it that happens to them is usually personal more than not. (Harold Abelson, 2024) CSS is unable to prevent situations like this that occur to these marginalized groups of people, which is a huge issue.

Social Science Principles:

Relativism is one of the most pronounced principles throughout this article. It ties every aspect of society, including the social, criminal justice, and technological systems related to cybersecurity. CSS involves law enforcement, an ineffectual option that affects society regarding its legality and the issue of its use as a weapon in the political system. The technological system is used obviously because of what CSS is used for.

Conclusion/Contributions:

In conclusion, CSS has some serious issues with the risk involved with its implementation, which allows law enforcement and national security agencies to track and enforce laws/policies. The way that Client-side scanning can fail and be manipulated shows the risk involved with its use. The paper successfully explains that for the justice system to benefit from cybersecurity, it needs to find a better means that does not hurt the marginalized and helps protect them better.

References

Harold Abelson, R. A. (2024). Bugs in our pockets: the risks of client-side scanning. *Journal of Cybersecurity*, 1-18.