Abraham Perez
2/11/2024

Article Review #1: Cybersecurity's relation to social science (974)

Introduction:

In this article review, I will be covering the journal "Bugs in our Pockets: the risks of client-side scanning" in which it goes over how client-side scanning (CSS) is a risk that needs to be considered. I will be going into how this journal relates to the principles of social sciences and covering the essentials needed in a research paper. This would include; research questions/hypotheses, the methods used, data/analysis, and the overall contribution this research had to society. There will also be parts discussing how it relates to class and how it relates to the marginalized groups that are associated with this topic. Hopefully, this will be informal to the reader/audience.

Principles:

Several principles of social science can relate to this article. For instance, there is the principle of relativism, in which the risk of our privacy being looked into would cause cybersecurity firms to further strengthen their procedures for securing a client's privacy. There is also the principle of ethical neutrality, in which the journal focuses on whether CSS is an effective tool that can protect the user or the complete opposite. The principle of determinism is also taken into consideration, with how "Can adversaries influence the algorithms to avoid detection? Can adversaries use the detection capabilities to their advantage (e.g. to target opponents)?" (Ableson et. al., 2024, lines 31-33). The journal mainly focuses on the ethicality of CSS and what influences/motives are used with it.

Research question/hypotheses:

This journal hypothesizes that CSS, instead of being a tool to protect a client's device from being scanned and their privacy being hijacked, creates security and privacy risks for everyone. There is also the question of whose interests are being served and whether or not it is possible to enforce purpose limitation and privacy. Another question also relates to how a surveillance system for CSS uses safeguards for user privacy and prevents unauthorized parties from obtaining data through these means. There are many other questions within this journal, but the main focus is how can the security of CSS be strengthened and to what degree of surveillance is deemed lawful and unlawful. With these questions in mind, there should be some discussion as to what types of research methods are used.

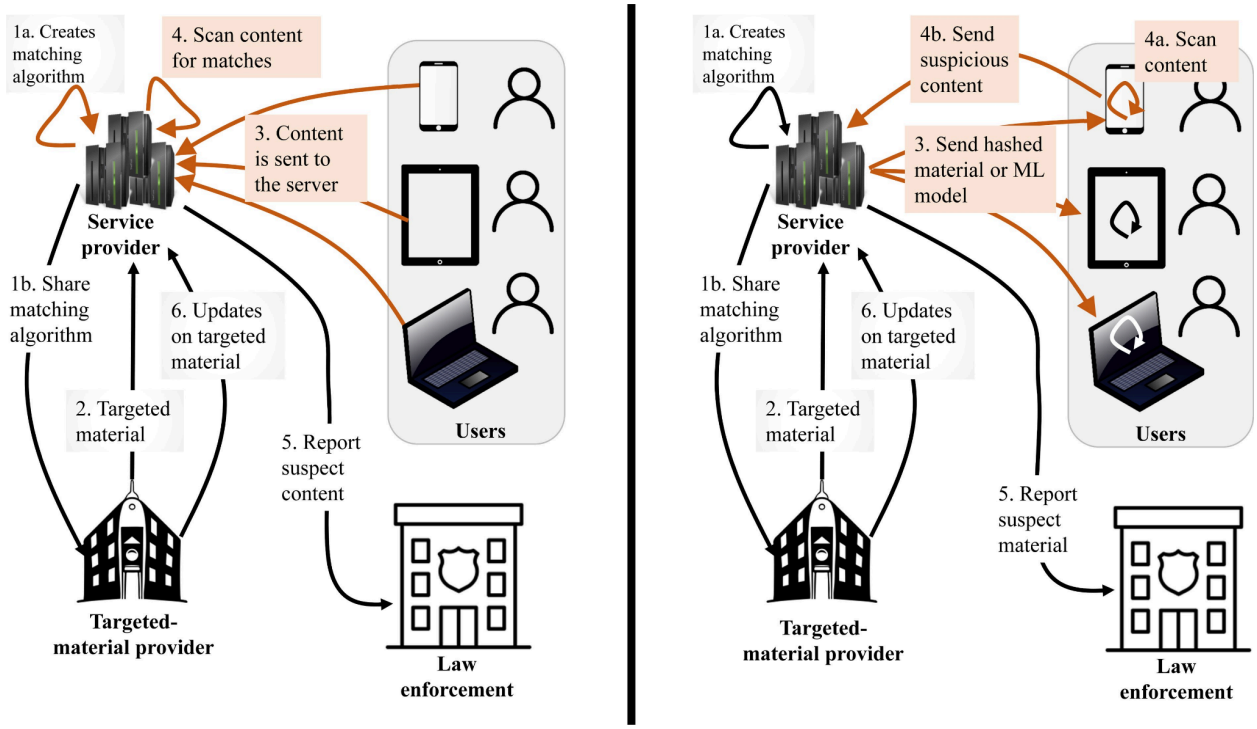
Research methods:

Multiple research methods were used in this journal. One would be archival research, an example of this is how the researchers used recent work by the US National Academies of Science, Engineering, and Medicine, which provided a framework to assess technical or policy options for getting unencrypted content. There was the 2019 Carnegie Endowment for International Peace study on encryption policy, which presents a set of principles to guide solutions as well. They also built on Paul Rosenzweig's early analysis of the policy issues raised by CSS, along with some of the technical issues. Overall the methods used were a full-on technical analysis of CSS and to cover the topic more generally-wise.

Data & Analysis:

Some of the data that was gathered in this journal covers how CSS is used and what it gathers.

Below is a diagram of CSS being used, in which the server that has CSS analyzes the content being sent through the server and detects any suspicious content.



There is also the analysis of how compared to its server-side predecessors, CSS increases the attack surface, which leads to new technological failure points and more powerful insiders who may be compromised, manipulated, or hacked. This complexity increases with the sophistication of surveillance systems.

Relation to class:

As stated in previous sections, this journal can relate to our class with various principles of social science. The ethicality of CSS is a number one priority due to how much data is being stolen by said CSS user. But there is also the major consideration of human factors. The risk of human error plays a prime role in the CSS topic, with how one's privacy can easily be compromised if the proper safety measures aren't taken. Evidently, this journal can be seen in the middle of being related to our class but also being its own thing and not relating at all.

Relation to marginalized groups:

The journal discusses how CSS can compromise society's privacy, it begs the question of who is being affected. The majority of those who are being affected are normal people who happen to cross the range needed for CSS to scan their devices and steal any private information. But there is also the concern of how CSS can be used in political decisions. Examples may include obtaining private information about political rivals, and other countries, or even manipulating information/"bad mouthing" about the LGBTQ+ community. The range seems to be endless with client-side scanning, which can raise the challenge of how security can diminish these problems.

Overall contributions:

The journal's contribution to society may seem miniscule, but it can be thought-provoking. With it being published only recently, i.e. last month, it gives awareness of how a person's privacy can easily be compromised just by passing by someone. It also shows how CSS can even bypass legal warrants of seizure, which may make one reconsider the overall quality of law enforcement. It seems that this journal is a kind of "wake-up call" that shows how easy it is for your information to be stolen. Whether or not this will help spark more research to be done, depends on how much of a risk it is.

Conclusion:

This journal covers how client-side scanning can be a detriment to society and what information has/can be taken by it. It went over the various data and analyses that help provide its stance on the topic, albeit it should be more objective than subjective. The relation of it to our class is just enough to be of interest but still can be its own thing. There was also the debate about how this journal can contribute to society and the marginalized groups it focuses on. The

main takeaway of this article review is that client-side scanning is an interesting topic to be discussed and makes the reader question whether they have the proper safety measures to protect themselves from it.

Works Cited

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Callas, J., Diffie, W., Landau, S., Neumann, P. G., Rivest, R. L., Schiller, J. I., Schneier, B., Teague, V., & Troncoso, C. (2024). Bugs in our pockets: The risks of client-side scanning. *Journal of Cybersecurity*, *10*(1). https://doi.org/10.1093/cybsec/tyad020