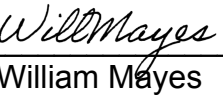
Sociotechnical Synthesis

STS 4600-022

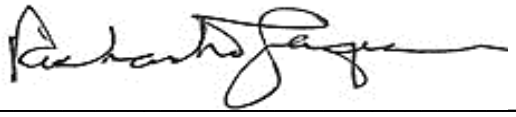
Spring 2022

William Mayes

Computer Science

Signature  Date 08 May 2022

William Mayes

Approved  Date 08 May 2022

Richard D. Jacques, Ph.D. STS Advisor, Department of Engineering & Society

Sociotechnical Synthesis

General Research Problem

How can online data privacy and integrity be protected?

Internet users generally value privacy, but companies value users' data, collecting it to target advertising (Martin & Murphy, 2016). Many internet users report concerns about privacy while "huge availability of data attracts abusive usage" (Schomakers et al., 2020). Cybercriminals also value and strive to obtain online user data (Mapmile & Mangoale, 2019). Identity theft is an extreme invasion of personal privacy. Because both legal and illegal data collection can constitute invasions of digital privacy, both regulatory and criminal enforcement responses are necessary.

Protecting data privacy requires both technical and social solutions. When data is given willingly, proper protections must be in place to prevent unauthorized access to that data. When companies are overzealous with data collection, careless with data protections, or otherwise unconcerned with user data privacy, advocacy groups push for policy within both the private and public sphere to enforce data privacy boundaries. These protections and policies and how they are used will inevitably impact the future of the internet.

Testing BLUESPAWN

How can the efficacy of BLUESPAWN, an open-source anti-malware tool, be measured and ensured?

I worked on this project in the CS department under Yonghwi Kwon. The goals were to add testing to BLUESPAWN to measure and record current performance and ensure proper performance in the future.

BLUESPAWN is an open-source, active defense tool for Windows computers (Smith & Krist, 2020). The project's goal is to provide a tool for cybersecurity professionals to respond to advanced cyber threats. Endpoint Detection & Response (EDR) platforms are the state-of-the-art antivirus tools but come with the downside that they function largely as black boxes. BLUESPAWN provides insight into detections by identifying malware behaviors as defined by the MITRE (2019) ATT&CK Framework (McDowell, 2021). BLUESPAWN is gaining attention from the cybersecurity community, having received over 900 stars on Github, but is not yet ready for at scale use. BLUESPAWN can be found at https://github.com/ION28/BLUESPAWN (Smith et al, 2020).

For any software to be usable at large scale, developers must extensively evaluate it. BLUESPAWN has yet to include such tests. By designing and developing a full suite of tests for BLUESPAWN, I aided the project in becoming dependable at scale.

I focused my efforts on system testing, also known as integration testing. I designed a suite of tests adhering to the MITRE ATT&CK framework techniques that BLUESPAWN currently targets in its hunts. Each hunt performs malicious appearing activity on the system, runs BLUESPAWN, and checks that BLUESPAWN both noted a detection for the activity and took proper remediation steps. Every hunt also then cleans up after itself to restore the operating system to a functioning state. The tests I designed focus on detecting bugs in threats BLUESPAWN should catch rather than evaluating the breadth of BLUESPAWN's detection capabilities. Several bugs were caught in the designing of these tests, highlighting the necessity of adding testing to the project.

Organizing for Privacy: How data privacy advocates advance their agenda

How do digital privacy advocacy groups advance their agendas?

While online user data is collected and monetized on a vast scale (Martin & Murphy, 2016), privacy advocates seek to limit the practice.

The Electronic Frontier Foundation (EFF, 2021) works to hold companies accountable for consumer privacy In September 2021, it organized a protest Apple software that it contends "will endanger the privacy … of its customers." By then, privacy advocates had already compelled Apple to delay releasing the software. Apple cited concerns from "customers, advocacy groups, researchers, and others." (Apple, 2021) Privacy International (2020) uses ad targeting campaigns to expose "how difficult it is to understand how our data's used." Californians for Consumer Privacy (2020, November 4) ran a political campaign to pass California Prop 24 to "give Californians the strongest online privacy rights in the world." This law mandates that businesses obtain additional consumer permissions for collection of sensitive personal information. This law was passed in November 2020 despite opposition from No on Prop 24 (2020) and other groups.

Through case studies on the above advocacy groups, I propose a framework for categorizing campaigns by privacy advocacy groups. I categorize campaign goals as educational, private lobbying, or public campaigning. I show how these categories are similar and different as well as how they interact. This categorization can be used to further study how these groups organize to achieve their goals.

Conclusion

Both projects will help to advance the cause of data protection and privacy in the future of the internet. Adding integration tests to BLUESPAWN brings the project one step closer to being a production ready tool able to be deployed on enterprise computers. Advancing the study and understanding of how fights for privacy policy occur is essential to understanding the future of the internet.

I was unable to accomplish all my initial goals regarding adding testing to BLUESPAWN. Future work on this will include adding unit tests to BLUESPAWN and performing fuzzing to check for hangs and crashes. Once BLUESPAWN has testing to ensure accurate performance of all its components, future research can measure its efficacy against real world malware. Future study on privacy advocacy groups can expand on my research to further delve into the methods used by these groups and how those methods change as their goals change.

References

Apple. (2021, Sep. 3). Expanded Protections for Children. Apple.com.

Bernstein, S., & Hoffmann, M. (2018). The politics of decarbonization and the catalytic impact of subnational climate experiments. *Policy Sciences, 51(2), 189–211*. Web of Science.

Californians for Consumer Privacy. (2020, November 4). *California voters approve Prop 24*. Yes on Prop 24. https://www.caprivacy.org/california-voters-decisively-approve-prop-24/.

Californians for Consumer Privacy. (2020, November 1). (*Consumer and privacy advocates join California leaders in support of Prop 24*. Yes on Prop 24. https://www.caprivacy.org/consumer-and-privacy-advocates-support-of-prop-24/.

EFF. (2021, Sep. 9). Electronic Frontier Foundation. EFF Activists To Lead Protest Demanding https://www.eff.org/press/releases/eff-activists-lead-protest-demanding-apple-cancel-iphone-scanning-program-and-keep.

Apple Cancel iPhone Scanning Program and Keep Its Privacy Promises To Customers.

Introna, LD. & Gibbons, A. (2009). Networks and Resistance: Investigating online advocacy networks as a modality for resisting state surveillance. *Surveillance & Society. 6(3), 233-258*. Web of Science.

Mapimele, F., & Mangoale, B. (2019). The Cybercrime Combating Platform. *International Conference on Cyber Warfare and Security 2019*, 237–242.

Martin, K. D., & Murphy, P. E. (2016). The role of data privacy in marketing. *Journal of the Academy of Marketing Science, 45(2), 135–155*. Web of Science.

McDowell, J. (2021, May 17). *BLUESPAWN Design and Architecture*.

MITRE Corporation. 2019. Matrix - Enterprise | MITRE ATT&CK®. MITRE ATT&CK. *https://attack.mitre.org/matrices/enterprise/windows/*

No On Prop 24. (2020, September). *Los Angeles Area Chamber of Commerce Opposes Prop 24: Joins Consumer, Privacy and Small Businesss Advocates*. No On 24 CA. https://noon24ca.org/wp-content/uploads/2020/09/No-on-24-Release.LA-Chamber.pdf.

Privacy International. (2020, Sep. 24). Advertisers on Facebook: who the heck are you and how did you get my data? *https://privacyinternational.org/campaigns/advertisers-facebook-who-heck-are-you-and-how-did-you-get-my-data*

Schomakers, E.-M., Lidynia, C., & Ziefle, M. (2020). All of me? Users' preferences for privacy-preserving data markets and the importance of anonymity. *Electronic Markets, 30(3), 649–665*. Web of Science.

Smith, J., Krist, C. (2020, May 8). *BLUESPAWN: An Open-Source, Active Defense & Endpoint Detection and Response (EDR) Software for Windows-based Systems*.

Smith, J., Krist, C., Mayes, W., & McDowell, J. 2020. BLUESPAWN. *https://github.com/ION28/BLUESPAWN*