A Report on Security and Privacy research in emerging computing paradigms

Abhinaya S B
sbabhinaya@gmail.com

CONTENTS

LIST OF FIGURES

A Report on Security and Privacy research in emerging computing paradigms

***Abstract*—As a new generation of smart gadgets finds its way into our homes, offices, and public spaces, the distinction between the zones of privacy gets blurred. With a great variance in the architecture of smart devices, identifying vulnerabilities in a diverse set of implementations is paramount. At the same time, the exponential rise in data collection necessitates technological and policy interventions to protect users' privacy. This paper summarizes the research efforts in tackling security and privacy issues for existing and emergent computing paradigms. We further describe categories of research, and comment on the gaps in literature that can be closed by future work.**

I. Introduction

As a new generation of smart gadgets finds its way into our homes, offices, and public spaces, the distinction between the zones of privacy gets blurred. With a great variance in the architecture of systems and an exponential rise in data collection, security and privacy (S&P) have become paramount. While the former requires the identification of vulnerabilities in diverse implementations, the latter entails technological and policy interventions that protect people's reasonable right to privacy.

Addressing security challenges in IoT entails the identification of loopholes in the flow of control like in mis-ordered execution of events in trigger-action platforms (1), side channels that may leak sensitive information (2), and user-error prone scenarios due to incorrect programming of IFTTT (if-this-then-that) applets (3). With the advancement of machine learning (ML), there are many instances of ML based attacks, like the creation of misinformation using real news (4), and tampering with images to negatively impact image searches (5).

Existing privacy policies containing tedious technical jargon are ineffective at disclosing essential information to users. In a country like India, where only 8% of the population have a graduate education (6), while over 53% use mobile phones (7), these information disclosure methods should be designed more intuitively to avoid unintentional breaches of privacy. The growing body of research in this sphere has led to the design of personal privacy assistants (8–10), privacy policy analysis tools (11–16), security nudge mechanisms (10, 13), and improved permission models in the web, mobile and IoT platforms (17–20). Surveys and interviews have been conducted to learn user perceptions of targeted ads (21, 22), browsers warnings (23, 24), password management (25–27), security in IoT (2, 28, 29), and the cultural and social factors influencing S&P practices (30–33). With the smart device market booming, proliferation of extended reality (XR), and a widespread deployment of video surveillance, further research is imperative to develop solutions that are inclusive of different types of users.

This paper summarizes the research efforts in tackling security and privacy issues for existing and emergent computing paradigms. The security research concerns the analysis of system-level vulnerabilities that arise in web, mobile and IoT platforms, and the new forms of risks posed due to adversarial machine learning. The privacy research can be categorized broadly into the privacy policy enforcement techniques, privacy preference analysis, and studies to inform user perceptions of privacy. In each section we further describe categories of research, and comment on the gaps in literature that can be closed by future work.

II. Security Research

This section describes security vulnerabilities in technologies at a level that is agnostic to users' security and privacy preferences.

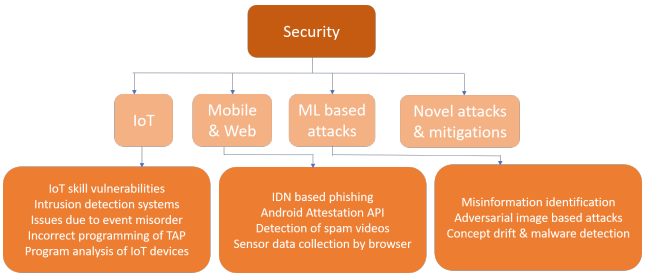

Fig. 1. An Overview of Security Research

A. IoT security

In (2), Celik et al. discuss program analysis techniques to uncover S&P issues in 5 popular IoT platforms. Hu et al. in (34) identify vulnerabilities in off-the-shelf devices like Google home and Alexa, and He et al. (29) describe possible adversaries in home IoT. Goksel et al. (1) discover that 29.8% of the IoT actuation commands are received in an incorrect order and they cause undesired system states. (3) and (35) discuss risks from a specific type of IoT devices – trigger action platforms. While (3) explores 8 cases where users may make mistakes while programming the rules, (35) uses the cryptographic scheme "garbled circuit" to ensure that a function cannot access any trigger data apart from what is

made available in the function definition. Cosson et al. (36) design an intrusion detection system that is platform agnostic, and Chandrasekaran et al. (37) prototype interventions that modify physical properties of the devices (like power) to enforce privacy.

B. Security in Mobile phones & the web

Das et al. and Ibrahim et al. uncover vulnerabilities due to improper use of mobile sensor data (38) and Android Attestation API (39) respectively. Hu et al. in (40) investigate mitigation mechanisms to detect IDN based browser phishing. In (41), Harsha et al. study the AES-GCM traffic to discover that password lengths can be directly inferred from encrypted web traffic, and prove the substantial advantage this information provides to the attacker. Bouma-Sims et al. (42) identify scam videos on YouTube by analysing like / dislike ratio, comment activity etc. with non-scam videos.

C. Machine Learning and Security

(5) and (43) discuss image-based adversarial attacks that leverage visual similarity with a significantly different perceptual hash, and manipulation of illuminating light respectively, while Grover described in (4) is an NLP based generator that can rewrite existing news into misinformation. Yang et al. in (44) investigate the detection and resolution of concept drift in machine learning models, a scenario when the real world samples are changing significantly without a corresponding change in training data.

D. Novel attacks and mitigations

Jubur et al. (45) describe a Human Indistinguishable Notification Attack that leverages 2FA mechanism to send multiple push notification that mask the genuine one needed for authentication. (46) outlines a speech privacy attack that uses aerial reverberations on the loudspeaker and vibration information from the accelerometer to identify the gender of the speaker, contents of speech, etc.

Shi et al. (47) develop a user authentication system for wearables by examining similarity between the unique voice characteristics captured by the accelerometers of the wearable device and the microphone of the voice assistant system. Shrestha et al. (48) design a non-stop authentication system using a wrist-worn personal wearable device that authenticates the user continually by correlating the keyboard and mouse activities with the user's hand movements captured via the wearable's sensors.

E. Remarks

Security research till date has considered system aspects and the human aspects of security in home IoT. While the sample space of users has largely been limited to tech-savvy consumers in the US, it would be interesting to consider users with lesser technical expertise, and from countries with a lesser adoption of these technologies. Further research in the domain of scam identification in social media, and automatic flagging of problematic links in websites would strengthen the reliability of online sources. As ML progresses in leaps and bounds, it is essential to identify ways to mitigate identity theft and copyright misuse through adversarial image-based ML. NLP research to preserve the integrity of genuine media outlets is also imperative.

III. Privacy Research

This section focuses on two types of research – the psychological studies conducted to comprehend aspects of a technology that may contribute to a security or privacy threat for different users, and the technical interventions that arose as a result of such prior studies.

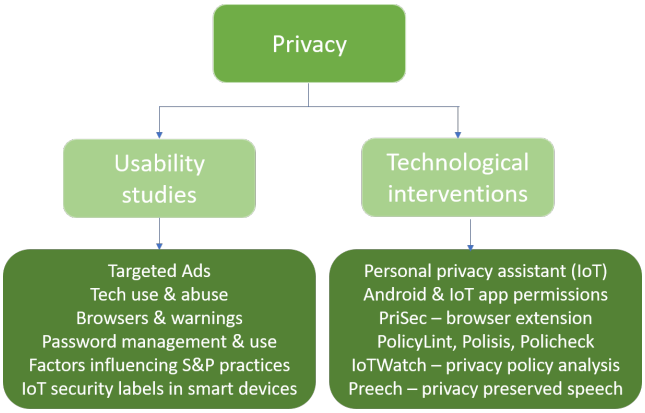

Fig. 2. An Overview of Privacy Research

A. Usability studies

Several researchers have conducted interviews and surveys (49) to identify the social factors that contribute to security practices and the consumption of security-related information. Das et al. in (31) observe the effect of social, forced and proactive triggers in people with varied levels of Security Behavioural Intention (SBI). (30) and (50) discuss the effect of real-world events like data breaches that influence future security practices of consumers. Murthy et al. (51), Vashistha et al. (52), and Watson et al. (33) explore how specific groups of people navigate technology usage and the risks associated. In the realm of IoT, Emami-Naeni et al. (53, 54), and Cobb et al. (55) study the importance of security labels in IoT devices, willingness to buy an IoT device based on disclosed security information, and the privacy concerns of incidental IoT users respectively. Zeng et al. in (21, 22) analyse problematic ads across different ad platforms, website types, and observe how users categorize them as clickbait, politicized ads etc. (56) and (23) discuss the warnings in different browsers and how they can be designed better to ensure they are heeded by the users. Yuxi et al. in (24) conduct a survey to understand the misconceptions of users about private browsing mode in leading web browsers like Chrome, Firefox, Safari etc. Another body of research by Cobb et al. (57) analyses online status

indicators and how they affect the use of apps that have them. (54) and (32) discuss technology usage practices of users in a romantic relationships, including abusive ones. Pearman et al. (25) and Song et al. (27) interview users regarding password management, the former in the context of workplace and the latter, for general usage. During the pandemic, there was a surge in privacy-related research around data collection and storage policies in contact tracing apps. (58, 59) collect public opinion on data collection strategies based on which entities will process, and with whom they will share the data.

B. Technological interventions

A new branch in privacy research uses machine learning to recommend privacy decisions. Zhang et al. study the privacy preferences of users about video analytics (9, 60) and cluster them into profiles based on similarities in their preferences. Barbosa et al. (61) derive privacy preferences in the context of a smart home. Das et al. use preference-based profiles clustering in the design of a personal privacy assistant for IoT (8),(10) to enforce automated opt-in/opt-out choices. Cobb et al. discuss the privacy implications of IFTTT applets in monitoring incidental users (62). Prisec (11), PolicyLint (12), Polisis (13), PoliCheck (15) and IoTWatch (14) are different techniques developed to analyse, inform, and enforce desired privacy settings in web and IoT. While Prisec enforces settings by emulating user clicks as a browser extension, Polisis and IoTWatch use NLP-based privacy policy analysis and provide security nudges to users. PoliCheck compares the data flow of the app to the policy statement using PolicyLint to find omitted, incorrect or ambiguous disclosures. Khandelwal et al. in (16) describe a sentence encoder capable of grouping similar privacy options via semantic matching. Ahmed et al. (63) describe a privacy-preserving speech transcription system that introduces noise to obfuscate the identification of the speaker's age, sex, emotional state etc. (17, 18, 20) discuss an improved design of app-level and global permission settings in Android phones, while (19) discusses overprivileged functionalities in SmartThings devices.

C. Remarks

With the proliferation of IoT, it is essential to identify potential ways of misusing this technology for undue surveillance in public spaces, or in temporary accommodations. It would be interesting to study the adoption of password management by average users, and identify novel methods of authentication. Usable security research in the use of non-traditional payment methods like UPI and digital wallets, would help in weeding out attack vectors that may have huge financial repercussions for their users. Privacy policy research efforts must continue till a point where users can readily consult a small amount of information to understand how their data is being used.

IV. Conclusion

This paper outlines the current research efforts to identify, tackle and prevent several security and privacy issues. New form factors of computers and the varying levels of technical expertise of their users necessitates the integration of Human-Computer Interaction, Data Science, and Machine Learning to analyze the myriad threat models. Further research in the use of common technologies in the web, mobile and IoT would benefit the average consumers in protecting themselves against the ever-expanding attack surface.

V. Bibliography

1. F. Goksel, M. O. Ozmen, M. Reeves, B. Shivakumar, Z. B. Celik, ArXiv210500645 Cs (2021) (available at http://arxiv.org/abs/2105.00645).

2. Z. B. Celik, E. Fernandes, E. Pauley, G. Tan, P. McDaniel, ArXiv180906962 Cs (2018) (available at http://arxiv.org/abs/1809.06962).

3. M. Palekar, E. Fernandes, F. Roesner, in 2019 IEEE Security and Privacy Workshops (SPW) (IEEE, San Francisco, CA, USA, 2019; https://ieeexplore.ieee.org/document/8844640/), pp. 138–143.

4. R. Zellers et al., ArXiv190512616 Cs (2020) (available at http://arxiv.org/abs/1905.12616).

5. Q. Hao, L. Luo, S. T. K. Jan, G. Wang, 16.

6. R.S, Only 8.15% of Indians are graduates, Census data show. The Hindu (2015), (available at https://www.thehindu.com/news/national/only-815-of-indians-are-graduates-census-data-show/article7496655.ece).

7.India: smartphone penetration rate 2040. Statista, (available at https://www.statista.com/statistics/1229799/india-smartphone-penetration-rate/).

8.A. Das, M. Degeling, D. Smullen, N. Sadeh, IEEE Pervasive Comput. 17, 35–46 (2018).

9. S. Zhang, Y. Feng, Anupam Das, 42.

10. B. Liu, Anupam Das, 43.

11. R. Khandelwal, T. Linden, H. Harkous, K. Fawaz, 18.

12. B. Andow et al., 19.

13. K. Fawaz, T. Linden, H. Harkous, in 2019 11th International Conference on Communication Systems & Networks (COMSNETS) (IEEE, Bengaluru, India, 2019; https://ieeexplore.ieee.org/document/8711280/), pp. 118–124.

14. L. Babun, Z. B. Celik, P. McDaniel, A. S. Uluagac, ArXiv191110461 Cs (2019) (available at http://arxiv.org/abs/1911.10461).

15. B. Andow et al., 18.

16. R. Khandelwal, A. Nayak, Y. Yao, K. Fawaz, in Proceedings of the Second Workshop on Privacy in NLP (Association for Computational Linguistics, Online, 2020; https://aclanthology.org/2020.privatenlp-1.4), pp. 28–38.

17. S. Chitkara, N. Gothoskar, S. Harish, J. I. Hong, Y. Agarwal, Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 1, 1–22 (2017).

18. J. I. Hong et al., 58.

19. A. Rahmati, E. Fernandes, K. Eykholt, A. Prakash, in 2018 IEEE Cybersecurity Development (SecDev) (IEEE, Cambridge, MA, 2018; https://ieeexplore.ieee.org/document/8543384/), pp. 29–36.

20. T. T. Nguyen, D. C. Nguyen, M. Schilling, G. Wang, M. Backes, in Proceedings of the 2021 ACM Asia Conference on Computer and Communications

Security (ACM, Virtual Event Hong Kong, 2021; https://dl.acm.org/doi/10.1145/3433210.3437511), pp. 578–592.
21. E. Zeng, T. Kohno, F. Roesner, 11.
22. E. Zeng, T. Kohno, F. Roesner, in Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (ACM, Yokohama Japan, 2021; https://dl.acm.org/doi/10.1145/3411764.3445459), pp. 1–24.
23. S. Egelman, L. F. Cranor, J. Hong, in Proceeding of the twenty-sixth annual CHI conference on Human factors in computing systems - CHI '08 (ACM Press, Florence, Italy, 2008; http://portal.acm.org/citation.cfm?doid=1357054.1357219), p. 1065. 24. Y. Wu et al., in Proceedings of the 2018 World Wide Web Conference on World Wide Web - WWW '18 (ACM Press, Lyon, France, 2018; http://dl.acm.org/citation.cfm?doid=3178876.3186088), pp. 217–226.
25. S. Pearman, S. A. Zhang, L. Bauer, N. Christin, L. F. Cranor, 21.
26. M. Shirvanian et al., in Proceedings of the 36th Annual ACM Symposium on Applied Computing (Association for Computing Machinery, New York, NY, USA, 2021; https://doi.org/10.1145/3412841.3442131), SAC '21, pp. 1683–1686.
27. Y. Song, C. Faklaris, Z. Cai, J. I. Hong, L. Dabbish, Proc. ACM Hum.-Comput. Interact. 3, 1–25 (2019).
28. E. Fernandes, A. Rahmati, K. Eykholt, A. Prakash, ArXiv170508522 Cs (2017) (available at http://arxiv.org/abs/1705.08522).
29. W. He et al., 17.
30. S. Das, J. Lo, L. Dabbish, J. I. Hong, in Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (ACM, Montreal QC Canada, 2018; https://dl.acm.org/doi/10.1145/3173574.3173575), pp. 1–12.
31. S. Das, L. A. Dabbish, J. I. Hong, 19.
32. J. Lin, J. I. Hong, L. Dabbish, Proc. ACM Hum.-Comput. Interact. 5, 1–27 (2021).
33. H. Watson, E. Moju-Igbene, A. Kumari, S. Das, in Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (ACM, Honolulu HI USA, 2020; https://dl.acm.org/doi/10.1145/3313831.3376605), pp. 1–12.
34. H. Hu, L. Yang, S. Lin, G. Wang, in 2020 IEEE Security and Privacy Workshops (SPW) (IEEE, San Francisco, CA, USA, 2020; https://ieeexplore.ieee.org/document/9283882/), pp. 76–81.
35. Y. Chen et al., ArXiv201205749 Cs (2021) (available at http://arxiv.org/abs/2012.05749).
36. A. Cosson et al., Sentinel: A Robust Intrusion Detection System for IoT Networks Using Kernel-Level System Information (2021).
37. V. Chandrasekaran, S. Banerjee, B. Mutlu, K. Fawaz, ArXiv181200263 Cs (2021) (available at http://arxiv.org/abs/1812.00263).
38. A. Das, G. Acar, N. Borisov, A. Pradeep, in Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (ACM, Toronto Canada, 2018; https://dl.acm.org/doi/10.1145/3243734.3243860), pp. 1515–1532.
39. M. Ibrahim, A. Imran, A. Bianchi, in Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services (ACM, Virtual Event Wisconsin, 2021; https://dl.acm.org/doi/10.1145/3458864.3466627), pp. 150–162.
40. H. Hu, S. T. K. Jan, Y. Wang, G. Wang, 18.
41. B. Harsha, R. Morton, J. Blocki, J. Springer, M. Dark, ArXiv200201513 Cs (2020) (available at http://arxiv.org/abs/2002.01513).
42. E. Bouma-Sims, B. Reaves, ArXiv210406515 Cs (2021) (available at http://arxiv.org/abs/2104.06515).
43. A. Sayles, A. Hooda, M. Gupta, R. Chatterjee, E. Fernandes, 10. 44. L. Yang et al., 18.
45. M. Jubur, P. Shrestha, N. Saxena, J. Prakash, in Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security (Association for Computing Machinery, New York, NY, USA, 2021; https://doi.org/10.1145/3433210.3453084), ASIA CCS '21, pp. 447–461.
46. S. A. Anand, C. Wang, J. Liu, N. Saxena, Y. Chen, in Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM, Abu Dhabi United Arab Emirates, 2021; https://dl.acm.org/doi/10.1145/3448300.3468499), pp. 288–299.
47. C. Shi, Y. Wang, Y. Chen, N. Saxena, C. Wang*, in Annual Computer Security Applications Conference (ACM, Austin USA, 2020; https://dl.acm.org/doi/10.1145/3427228.3427259), pp. 829–842.
48. P. Shrestha, N. Saxena, in Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM, Linz Austria, 2020; https://dl.acm.org/doi/10.1145/3395351.3399366), pp. 13–24.
49. C. Faklaris, L. Dabbish, J. I. Hong, 18.
50. S. Bhagavatula, L. Bauer, A. Kapadia, ArXiv201009843 Cs (2021) (available at http://arxiv.org/abs/2010.09843).
51. S. Murthy, K. S. Bhat, S. Das, N. Kumar, Proc. ACM Hum.-Comput. Interact. 5, 1–24 (2021).
52. A. Vashistha, R. Anderson, S. Mare, in Proceedings of the Conference on Computing & Sustainable Societies - COMPASS 19 (ACM Press, Accra, Ghana, 2019; http://dl.acm.org/citation.cfm?doid=3314344.3332499), pp. 1–12.
53. P. Emami-Naeini, Y. Agarwal, L. F. Cranor, H. Hibshi, ArXiv200204631 Cs (2020) (available at http://arxiv.org/abs/2002.04631).
54. P. Emami-Naeini, J. Dheenadhayalan, Y. Agarwal, L. F. Cranor, 18.
55. C. Cobb, S. Bhagavatula, K. A. Garrett, A. Hoffman, V. Rao, 22.
56. J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, L. F. Cranor, 34.
57. C. Cobb, L. Simko, T. Kohno, A. Hiniker, in Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (ACM, Honolulu HI USA, 2020; https://dl.acm.org/doi/10.1145/3313831.3376240), pp. 1–12.
58. T. Li et al., ArXiv200511957 Cs (2020) (available at

http://arxiv.org/abs/2005.11957).
59. L. Simko et al., ArXiv201201553 Cs (2020) (available at http://arxiv.org/abs/2012.01553).
60. S. Zhang et al., Proc. Priv. Enhancing Technol. 2021, 282–304 (2021).
61. N. M. Barbosa, J. S. Park, Y. Yao, Y. Wang, Proc. Priv. Enhancing Technol. 2019, 211–231 (2019).
62. C. Cobb, M. Surbatovich, A. Kawakami, M. Sharif, L. Bauer, 26.
63. S. Ahmed, A. R. Chowdhury, K. Fawaz, P. Ramanathan, 19.