Mobile Apps vs. Web Browsers: A User Perception Study with Android Apps and Google Chrome

Harel Berger
Georgetown University
hb711@georgetown.edu

Abstract

This study examines user perceptions of mobile applications (apps) versus web browsers for accessing online services, with an emphasis on security, privacy, and usability aspects. Through a combination of an experiment and a survey with Android smartphone users, the research seeks to identify the key concerns and preferences that influence their choice between mobile apps and web browsers. The findings will offer valuable insights for developers to improve the security, privacy and usability of both platforms by addressing user concerns and misconceptions.

1 Introduction

In today's digital landscape, numerous online services are accessible via smartphones through mobile apps, web browsers, or both. Although there are mutual threats across platforms, such as attacks on anti viruses [1, 2, 11, 13] each platform offers distinct advantages and disadvantages on various aspects, including security, privacy and usability [10]. Mobile apps can be a platform of broad malicious activities, as their content includes different types of files [5]. No explicit download of additional files is needed to get hacked besides the app itself. However, mobile operating systems and apps may use advanced security features like biometrics authentication [14]. Web browsers, relying on cookies for session management, can be susceptible to web attacks [4, 6, 7, 9]. However, significant attack on the host machine cannot be acheived soley through webservers without additional downloaded files.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2024.
August 11–13, 2024, Philadelphia, PA, United States.

Privacy concerns also differ. Mobile apps request access to sensitive data and actions, controlled by user permissions, while web browsers pose risks through tracking and data collection [8].

Regarding usability, mobile apps integrate better with device features like cameras, GPS, and notifications, and they can work offline, while it is rare to find certain types of websites that would be usable also in offline mode [12]. Web browsers, however, do not require installation and updates, offering simpler use.

This study examines user perceptions of mobile apps versus web browsers, focusing on security, privacy and usability, with Android apps and Google Chrome as case studies. The findings will help developers enhance security, privacy and usability. By comparing these platforms, the study will reveal user misconceptions about the features of these platforms. The findings will show contexts where one platform is preferred, aiding service providers in meeting user needs and creating more user-friendly services.

2 Research Questions

RQ1: What security concerns influence users' choice between mobile apps and web browsers for online services?
RQ2: How do users' privacy concerns differ between mobile apps and web browsers?
RQ3: What usability features do users prefer in mobile apps versus web browsers?
RQ4: How do users' concerns and preferences differ across various online service categories (e.g., banking, e-shopping, news, social media) between mobile apps and web browsers?

3 Methodology

This study will utilize two research methods: an experiment and a survey.

Participants: Approximately 100 students who use Android smartphones will participate in the experiment.

Experiment: The experiment will involve participants performing specific tasks using both mobile apps and web browsers, employing the think-aloud protocol to capture real-time thoughts and reactions. Scenarios will be designed to mimic realistic usage of online services. For example, participants will be asked to complete several tasks using their accounts, to be as authentic as possible: (1) Perform a banking transaction (e.g., transferring money) using a banking app and the web version of the bank's service; (2) Purchase an item from an online store using both the mobile app and the web browser; (3) Access a news website and read an article using both the mobile app and the web browser.

During these tasks, participants will verbalize their thoughts, describing their actions, any security warnings or alerts encountered, and steps taken to secure their actions (e.g., use of biometrics, password entry). Their actions and difficulties will be recorded for further analysis.

Survey: Following the experiment, participants will complete a survey to capture their perceptions and concerns regarding the use of mobile apps versus web browsers. Some questions will require participants to respond using a Likert scale, ranging from 1 to 10.

Example Survey Questions:

1. How concerned are you about malware when downloading mobile apps?
2. How effective do you find browser security warnings (e.g., untrusted website warnings)?
3. How comfortable are you with the permissions requested by mobile apps (e.g., access to contacts, location)?
4. Do you feel more in control of your privacy settings in mobile apps or web browsers?
5. Which platform do you find easier to navigate: mobile apps or web browsers?
6. How important is offline access for you when using an online service?
7. Does the available storage on your device influence your decision to download a new app?

Additionally, demographic information such as age and language proficiency will be collected from participants.

Data Analysis: The data from the experiment will be analyzed to identify patterns and issues related to security, privacy, and usability. The analysis will be categorized based on services, such as e-shopping, news, direct messages, etc.

Qualitative data from the think-aloud protocol experiment and the open-ended survey questions will be thematically analyzed to uncover deeper insights. This data will reveal user concerns and experiences, such as reactions to security warnings and privacy permissions, together with participants' explanations for their preferences. Recurring themes, like app permissions or web browser navigation, will be identified.

Quantitative data will be statistically analyzed to highlight significant user preferences and concerns. Comparisons will be made between concerns about malware in mobile apps versus web browsers, and preferences for offline access and ease of navigation.

Common themes, like the need for better security features in mobile apps or simpler web browsers, will be identified.

Examples of analyzed data include security warning frequencies, user comments on security measures like biometrics, statistical comparisons of malicious activity concerns, analysis of permissions granted or denied, concerns about data tracking, and usability observations like task completion times and navigation ease.

4 Ethics

Participants' consent will be obtained prior to participation. All personal data will be anonymized to ensure privacy and confidentiality. Prior to the commencement of the study, approval will be obtained from the Institutional Review Board. By combining experimental tasks with the think-aloud protocol and survey responses, this methodology aims to provide a comprehensive understanding of user preferences and concerns regarding mobile apps and web browsers.

5 Expected Outcome

This study aims to provide insights into users' preferences and concerns regarding mobile apps and web browsers for accessing online services.

We expect to identify security concerns, such as worries about malware in mobile apps and web attacks on web browsers. Privacy concerns are anticipated to center around permissions in mobile apps versus control over privacy settings in web browsers, such as "incognito" mode. For example, people may prefer e-shopping through web browsers rather than mobile apps, because apps save payment methods by default, thus creating a threat of information theft in case the device is lost or stolen.

Usability preferences will likely highlight the functionality and offline access of mobile apps against the ease of navigation and lack of installation for web browsers. For example, people may prefer accessing services through a browser, to prevent overloading their storage, compared to mobile apps that consume storage [3].

6 Anticipated Contribution

The findings will inform developers on how to enhance security, privacy and usability of mobile apps and websites based on user concerns and preferences.

Additionally, the study will contribute to academic literature on user behavior, security, and privacy in both mobile and web contexts, providing valuable data for future research in usable security and privacy. This includes the potential to extend the research to other domains, such as comparing user perceptions of iOS apps versus the Safari browser.

References

[1] Harel Berger, Amit Dvir, Enrico Mariconti, and Chen Hajaj. Breaking the structure of mamadroid. *Expert Systems with Applications*, 228:120429, 2023.

[2] Harel Berger, Chen Hajaj, Enrico Mariconti, and Amit Dvir. Crystal ball: From innovative attacks to attack effectiveness classifier. *IEEE Access*, 10:1317–1333, 2021.

[3] Ashish Bijlani, Umakishore Ramachandran, and Roy Campbell. Where did my 256 gb go? a measurement analysis of storage consumption on smart mobile devices. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, 5(2):1–28, 2021.

[4] Fiona Carroll. Human-browser interaction: Investigating whether the current browser application's design actually make sense for its users? *International Journal of Human–Computer Interaction*, pages 1–12, 2023.

[5] Shaoyong Du, Pengxiong Zhu, Jingyu Hua, Zhiyun Qian, Zhao Zhang, Xiaoyu Chen, and Sheng Zhong. An empirical analysis of hazardous uses of android shared storage. *IEEE Transactions on Dependable and Secure Computing*, 18(1):340–355, 2018.

[6] Shashank Gupta and Brij Bhooshan Gupta. Cross-site scripting (xss) attacks and defense mechanisms: classification and state-of-the-art. *International Journal of System Assurance Engineering and Management*, 8:512–530, 2017.

[7] Vicki Ha, Kori Inkpen, Farah Al Shaar, and Lina Hdeib. An examination of user perception and misconception of internet cookies. In *CHI '06 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '06, page 833–838, New York, NY, USA, 2006. Association for Computing Machinery.

[8] Jonathan Muehlstein, Yehonatan Zion, Maor Bahumi, Itay Kirshenboim, Ran Dubin, Amit Dvir, and Ofir Pele. Analyzing https encrypted traffic to identify user's operating system, browser and application. In *2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, pages 1–6, 2017.

[9] Filipo Sharevski, Mattia Mossano, Maxime Veit, Gunther Schiefer, and Melanie Volkamer. Exploring phishing threats through qr codes in naturalistic settings. In *Symposium on Usable Security and Privacy (USEC) 2024*, 2024.

[10] Dolière Francis Somé. EmPoWeb: Empowering Web Applications with Browser Extensions. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 227–245, 2019.

[11] Fu Song, Yusi Lei, Sen Chen, Lingling Fan, and Yang Liu. Advanced evasion attacks and mitigations on practical ml-based phishing website classifiers. *International Journal of Intelligent Systems*, 36(9):5210–5240, 2021.

[12] Antero Taivalsaari, Tommi Mikkonen, Dan Ingalls, and Krzysztof Palacz. Web browser as an application platform. In *2008 34th Euromicro Conference Software Engineering and Advanced Applications*, pages 293–302, 2008.

[13] Li Xu, Zhenxin Zhan, Shouhuai Xu, and Keying Ye. An evasion and counter-evasion study in malicious websites detection. In *2014 IEEE Conference on Communications and Network Security*, pages 265–273. IEEE, 2014.

[14] Xinman Zhang, Tingting He, and Xuebin Xu. Android-based smartphone authentication system using biometric techniques: A review. In *2019 4th International Conference on Control, Robotics and Cybernetics (CRC)*, pages 104–108. IEEE, 2019.