Proposal: Supply Chain as a Factor for App Selection

Primal Wijesekera
International Computer Science Institute (ICSI) & UC Berkeley

***Abstract*—Consumers make an array of security and privacy decisions about the software they use, without understanding how third-party code runs on those software could affect their privacy and security. In the specific use case of mobile apps, platforms are providing app permissions that are likely to be used during app execution, including by third-party components; it is unlikely that most end users understand that the consequences of their decisions to grant access to sensitive personal information rely heavily on the third-party components present. Hence, it is only fitting that we understand how we can nudge consumers using Software Bill of Materials (SBoM) to educate them on potential security and privacy risk stemming not only from the app they are going to install but also from the app's dependencies. With the increased use of third party code in mobile apps, it is high time, as a community, we understand how to increase the transparency and break the false notion that the consumer is going to run only the code developed by the advertised developer.**

***Index Terms*—Mobile Privacy, Supply Chain Transparency**

1. Introduction

The question is, how can platforms present the bill of materials (SDKs bundled in the system) [1] in a way that will catch the attention of the consumers and help the consumer to make an informed decision without overwhelming the consumer?

In the current day and age, consumers are already making various privacy and security decisions, from figuring out which app to install to set up new passwords. We should not add more questions and choices to the vast user burden unless necessary. However, with the current research, it is evident that even developers are unsure about what SDKs are collecting and sharing with third parties. As a result, users should be aware of whose code they are running apart from the app developer, and we believe third party components should be part of the equation users should consider when installing the apps. The theory of rational choice models posits that individuals aim to maximize their utility given their preferences and other constraints they may be subject to, for instance, the available budget [3]. Since privacy and security decisions also give rise to complex tradeoffs, such as the costs and benefits associated with disclosing or protecting sensitive information. We believe leaving this information out from users would rise to what economists would describe as a condition of incomplete and asymmetric information [2]. Security and privacy are rarely end-users primary tasks, and users have limited mental resources to evaluate all possible options and consequences of their actions—a phenomenon Herb Simon referred to as "bounded rationality" [5]. Literature has looked into how to effectively communicate potential privacy risks of mobile apps [4]. The following lists the research questions we plan to address:

- Given the option to examine third-party components of a mobile app, do consumers care to consider third-party components during the installation?
- How does the risk posed by third-party components affect the user's choice?
- What are the best indicators to communicate the risk posed by third parties?
  - The third party component name
  - Third party developer
  - Country of Origin
  - Intended Functionality of the third party
  - Open source vs Proprietary
  - Mean time taken to fix a vulnerability
  - Number of unresolved vulnerabilities
  - List of resources accessed and recipients of those resources
  - Prior allegations of misbehavior by each SDK
  - Security of any dependent library (to understand multi hop dependency and security implications)
- What role should be played by the platforms given the challenges in attribution?

We plan to conduct an online survey (Amazon MTurk, Prolific) with a mock Play store landing page (an app installation page) with different conditions for the same app. The control would be the installation page without third-party information, which resembles the current choice, and each of the other different conditions would be as above name, developer, country of origin, etc. By doing an online follow-up questionnaire, we can examine the rationale behind their actions to understand the impact of the increased transparency of the third-party components and their perception of the privacy risks posed by third-party components in the mobile app space.

We believe such knowledge will be critical in understanding how platforms can increase transparency and allow consumers to make informed decisions and the different factors that consumers value before making choices.

References

[1] Software Bill of Materials. https://www.ntia.gov/SBOM. [Online; accessed: 02-September-2022].

[2] G. A. Akerlof. The market for "lemons": Quality uncertainty and the market mechanism. In *Uncertainty in economics*, pages 235–251. Elsevier, 1978.

[3] G. S. Becker. *The economic approach to human behavior*, volume 803. University of Chicago press, 1976.

[4] M. Harbach, M. Hettig, S. Weber, and M. Smith. Using personal examples to improve risk communication for security &; privacy decisions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '14, page 2647–2656, New York, NY, USA, 2014. Association for Computing Machinery.

[5] H. Simon. A behavioral model of rational choice. *Models of man, social and rational: Mathematical essays on rational human behavior in a social setting*, pages 241–260, 1957.