Investigating the Value of Privacy within the Internet of Things

Alex Mayle
Computer Science,
Ohio University
am218112@ohio.edu

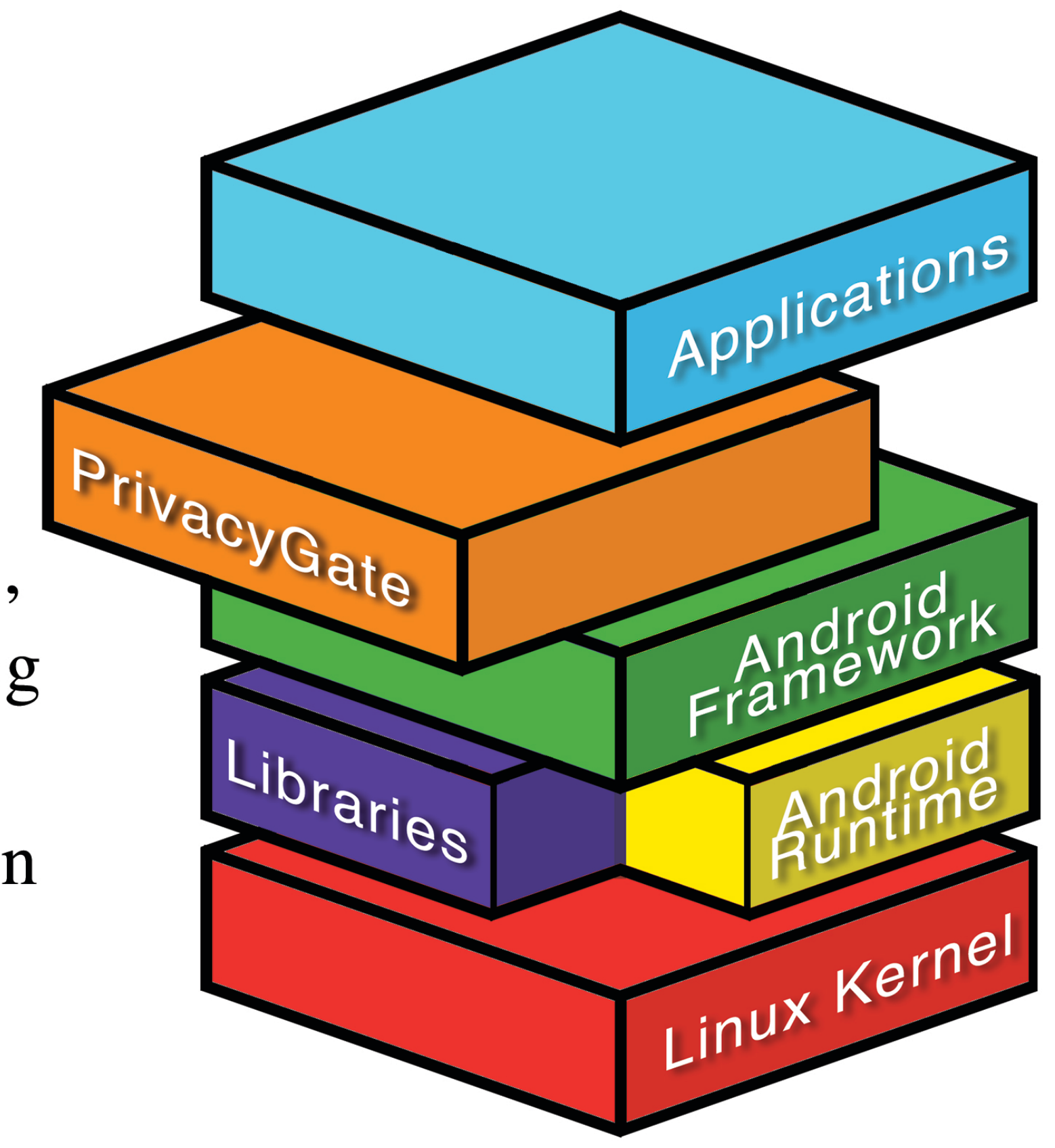
Sina Masnadi, Safa Bacanli
Computer Science,
University of Central Florida
{sina, bacanli}@knights.ucf.edu

Dr. Turgut, Dr. Wisniewski
University of Central Florida
turgut@cs.ucf.edu
pamela.wisniewski@ucf.edu

Abstract

Many companies within the IoT sector rely on user data to both deliver and monetize their services, creating a high demand for personal information. A user can be seen as making a series of transactions, each involving the exchange of personal data for a service. We argue that privacy can be described quantitatively, using the the game-theoretic concept of Value of Information (VoI), enabling us to assess whether each exchange is an advantageous one for the user. We introduce PrivacyGate, an extension to the Android operating system built for the purpose of studying privacy transactionally. An example study, and its initial results, are provided to illustrate its capabilities. Finally, we recommend further research questions and methods.

PrivacyGate gate is implemented between the Android framework, responsible for exposing system APIs, and the applications installed on the device.



Related Work

- The *Value of Information* was originally introduced in game theory, defined as the value for which an optimal player would buy a piece of information [1].
- A similar metric, the *Quality of Information*, has been applied to the decision of transmitting a chunk of data within sensor networks [2].
- Utilizing the Value of Information to study the exchange of services for privacy has been inspired by research in *pragmatic VoI* [3].

PrivacyGate

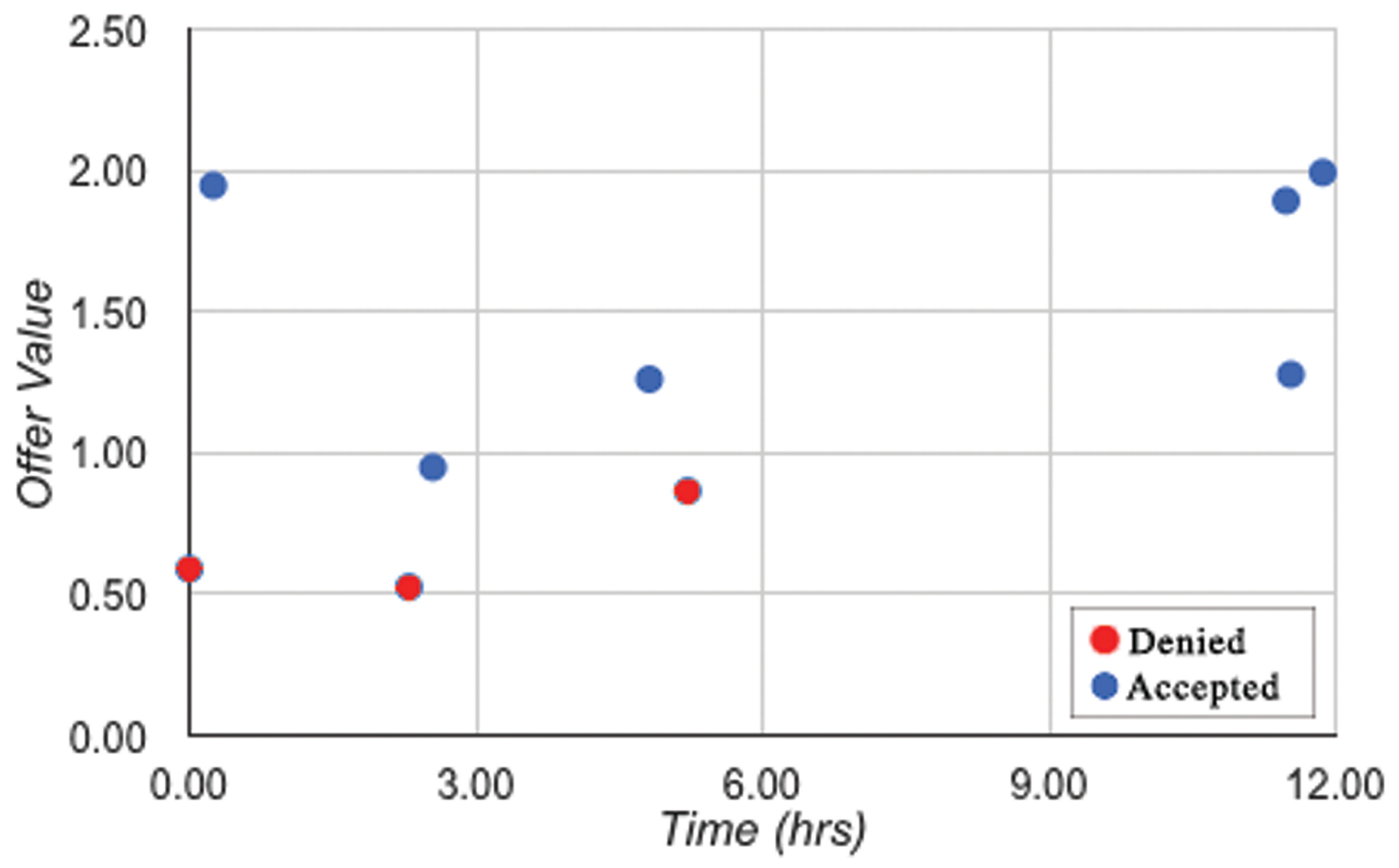
- Most mobile OSs initially prompt the user for consent when transmitting private data, but then apply this decision at later times. This forces the user to frequently adjust their settings if they wish to control privacy at a more granular level.
- In contrast, PrivacyGate prompts for the user's consent if one of the following conditions has been met.

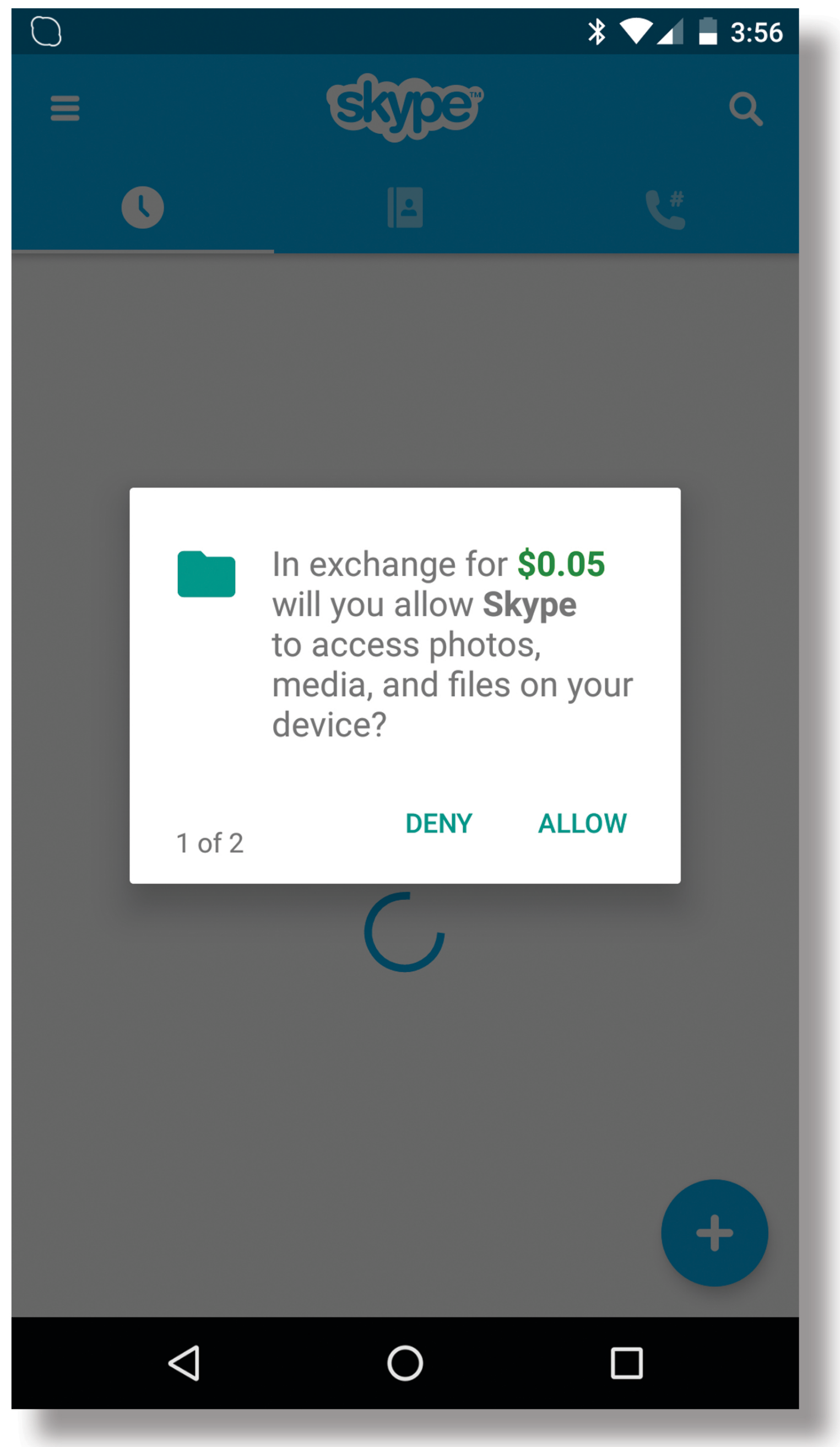
> - The app has not been used in X time
> - The user has not been prompted for consent in Y time
> - The app was force closed by the user
> - The device was restarted
>
> *where X and Y are non-negative values set by the user such that X < Y*

- Accordingly, "transactions" are defined by the values X and Y, and enable the study of users' behavior in such an environment
- Limitation: Only works on apps made for Android 6.0 and later, as older apps will crash if their access to private data is revoked

Initial Results

- Developed a user study atop PrivacyGate in which users are given monetary offers for their private data
- Offers are generated randomly at the time of each potential transaction
- Users' responses can quantify their Value of Privacy for different types of sensitive data



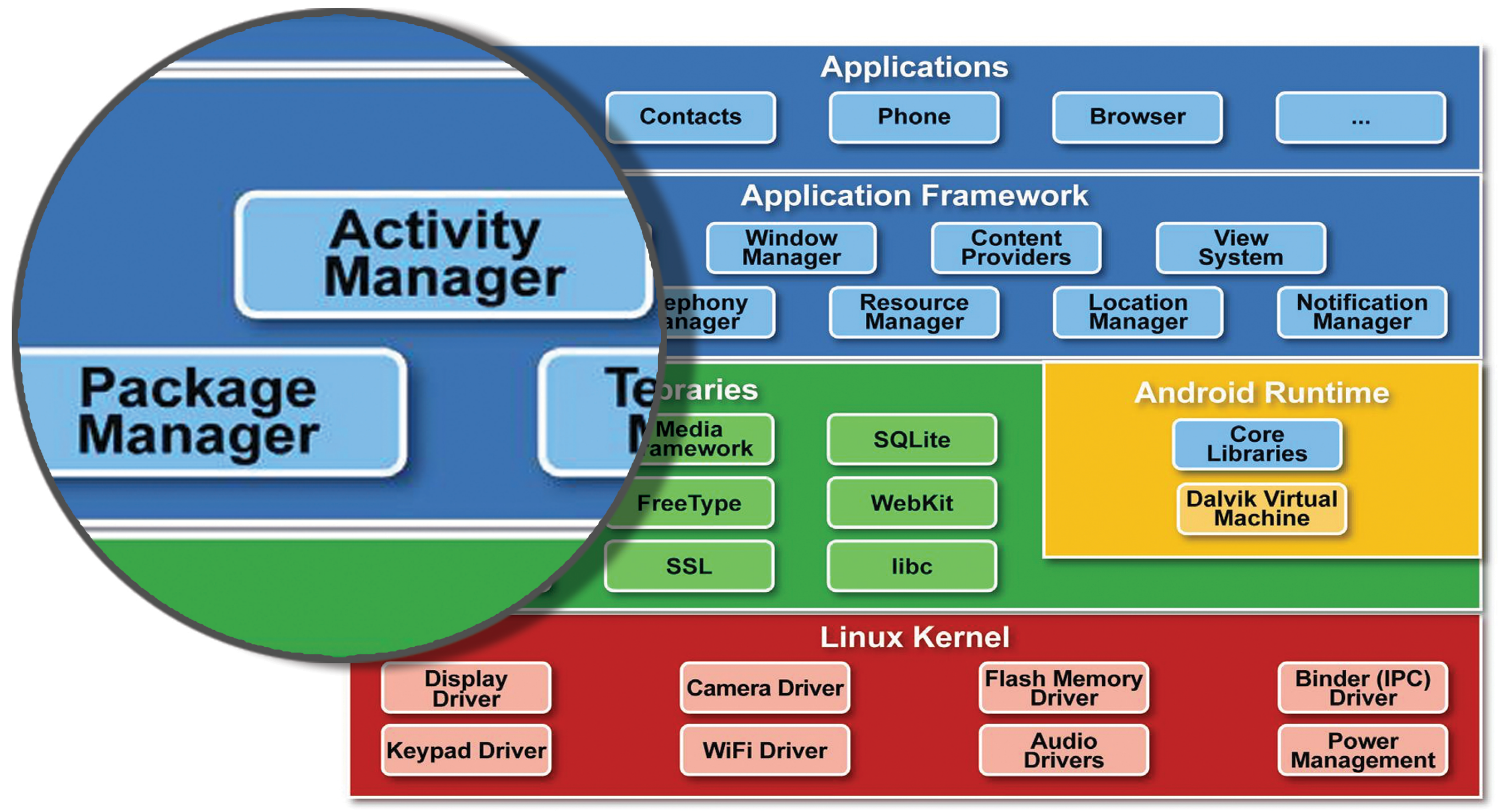


In exchange for **$0.05** will you allow **Skype** to access photos, media, and files on your device?

1 of 2

A user's decisions when offered various amounts of money for access to their device's files

Implementation



- PrivacyGate is implemented using the Android Framework's Activity & Package Manager components
- The Package Manager's API is extended, allowing hooks in the Activity Manager to revoke applications' access to private data upon certain conditions

Future Work

- Expand on the initial results by conducting a full scale user study, revealing the Value of Privacy for different forms of private data (locations, contacts, etc...).
- Quantifying the value users' attach to different services, perhaps through a pre-participation survey, will enable us to assess whether users are making advantageous transactions with their privacy.

References

[1] R. A. Howard, "Information value theory," Systems Science and Cyber- netics, IEEE Transactions on, vol. 2, no. 1, pp. 22–26, 1966.

[2] C. Bisdikian et al, "Building principles for a quality of information specification for sensor information," in IEEE Intl. Conf. on Information Fusion (FUSION), July 2009, pp. 1370–1377.

[3] D. Turgut and L. Bölöni. IVE: improving the value of information in energy-constrained intruder tracking sensor networks. In Proceedings of IEEE ICC'13, pp. 6360–6364, June 2013. Best Paper Award.

Acknowledgments

The support for this work was provided by the National Science Foundation REU program under Award No. 1560302. Any opinions, findings, and conclusions and recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation. The authors thank Dr. L. Boloni and Neda Bidoki for user study contributions.