Investigating the Value versus Cost of Privacy in the Internet of Things

Patrick Dorton
Dept. of Computer Science
University of Central Florida
pdorton89@knights.ucf.edu

Neda Hajiakhoond and Safa Bacanli
Dept. of Computer Science
University of Central Florida
{hajiakhoond,sbacanli }@cs.ucf.edu

Dr. Damla Turgut
Dept. of Computer Science
University of Central Florida
turgut@cs.ucf.edu

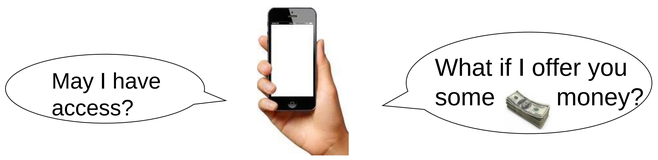
ABSTRACT

With the vast number of Internet of Things (IoT) devices in the market today, *privacy* is one of the biggest concerns facing people in their lives. There is a high demand on user information to be able to monetize it and offset the cost of the creation as well as improve the operation of many services. We are investigating how a user might be able to go about protecting themselves from sharing information without their consent, and how this method can be applied to IoT devices.

PRELIMINARIES

When IoT devices are everywhere, the privacy headaches just get worse. The success of IoT depends on the creation of a business model that both customers and providers perceive as beneficial [1, 3]. The customer privacy is one of the important factors in this realm which needs attention from the researchers and developers.

We initially developed *PrivacyGate* application in Android Operating System to study the user privacy as a series of transactions [2].



Value of Privacy (VoP) represents the perceived value that the user puts into keeping their information private.

VoS_{Shared} is the value of service when the user's information is **shared**

$VoS_{not\ Shared}$ is the value of service when the user's information is **not shared**

The following is an expansion on the method used to calculate the Value of Privacy (VoP). The method will have new transactions for ceasing the release of private information. The user must accept an offer to end the sharing process explicitly. This will allow for more inference behind the value of the service and the value of privacy and how they are related to one another at the time of the transaction.

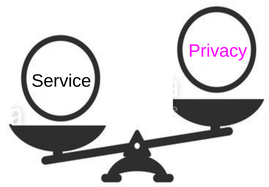
Currently PrivacyGate generates the monetary offers by bounding a random number between $0.10 and $2.00. The offers will now be dynamically generated accounting for the previously accepted offers. The previous accepted offers will be used as a new upper boundary. If an offer is rejected it will reduce the distance between the current offer and the last previously accepted offer tightening the boundary from the lower end to find the most accurate estimation for the user's threshold of acceptance.

TRANSACTION STATES

Secure

$$VoS_{Shared} < VoP \leq VoP + VoS_{Not\ Shared}$$

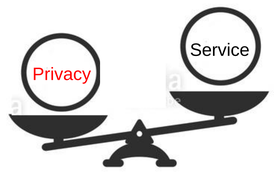
By not sharing their information the user shows that the value of the service in which they must share their information to be less than the value of their privacy.



Public

$$VoP \leq VoP + VoS_{Not\ Shared} \leq VoS_{Shared}$$

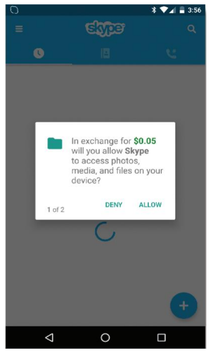
By sharing their information the user shows that the value of the service has more value to them than what it costs them to not have privacy.



Accepted protection offer

$$VoS_{Shared} < VoP \leq VoP + VoS_{Not\ Shared}$$

By accepting the offer for protection, the user shows that the value of their privacy is greater than their perceived value for the service provided.



The above states describe the new metrics that we can bound the value of privacy by. We believe that the value of privacy is always going to be bound by its relation to the perceived value of the services provided to the user.

If the user is unwilling to share their information it would mean that the value of their privacy alone could be higher than the need for the service, but also it could be a combination of the value of their privacy and the value of the service in which they are not required to share their information.

If the user is willing to share their information, the VoS_{shared} has changed to be higher than the user's need to stay private. This allows us to say definitively that the user's value of privacy combined with the $VoS_{not\ shared}$ is lower than VoS_{shared}.

When the users choose to stop sharing their information it could mean a few things semantically. One explanation would be that the need for the service in which they have to share their information has decreased beyond the threshold of their privacy. Therefore they chose to cease sharing their information as they no longer have the need for the service.

Another possibility is that the value of their privacy has risen above the need for such service. In this case the user is unwilling for some reason to continue sharing their information regardless of their need for a service.

FUTURE WORK

- The PrivacyGate framework can dynamically determine the offers that it will be given to the users to evaluate against their need for privacy.
- After a user study is conducted, the data will be analyzed to determine the differences in how users evaluate the different types of privacies that they have.

ACKNOWLEDGEMENT

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.

REFERENCES

1. D. Turgut and L. Boloni, "Value of information and cost of privacy in the internet of Things," Accepted to appear in IEEE Communications Magazine, 2017.
2. A. Mayle*, N. H. Bidoki*, S. Masnadi*, L. Boloni, and D. Turgut, "Investigating the Value of Privacy within the Internet of Things," Accepted to appear in IEEE GLOBECOM, Singapore, 2017.
3. D. Turgut and L. Boloni. "IVE: Improving the value of information in energy-constrained intruder tracking sensor networks," IEEE International Conference on Communications (ICC'13), pp. 6360–6364, June 2013. **Best Paper Award**

* denotes student author