Poster: Balancing Disclosure and Utility of Personal Information

Aarathi Prasad
Institute for Security, Technology and Society
Dartmouth College

Xiaohui Liang
Institute for Security, Technology and Society
Dartmouth College

David Kotz
Institute for Security, Technology and Society
Dartmouth College

ABSTRACT

The ubiquity of smartphones and mobile and wearable devices allow people to collect information about their health, wellness and lifestyle and share with others. If it is not clear what they need to share to receive benefits, *subjects* (people whose information is collected) might share too much, thus disclosing unnecessary private information. On the other hand, concerned about disclosing personal information, subjects might share less than what the recipient needs and lose the opportunity to enjoy the benefits. This balance of disclosure and utility is important when the subject wants to receive some benefits, but is concerned about disclosing private information.

We address this problem of balancing disclosure and utility of personal information collected by mobile technologies. We believe subjects can decide how best to share their information if they are aware of the benefits and risks of sharing. We developed ShareBuddy, a privacy-aware architecture that allows recipients to request information and specify the benefits the subjects will receive for sharing each piece of requested information; the architecture displays these benefits and warns subjects about the risks of sharing. We describe the ShareBuddy architecture in this poster.

Categories and Subject Descriptors

K.4 [**COMPUTERS AND SOCIETY**]: Privacy

Keywords

sharing controls, mobile devices, personal information

1. INTRODUCTION

Mobile technologies allow people to collect their personal information at any time to achieve some personal goals. Currently the most popular mobile technologies are health and wellness devices and applications which *subjects*, i.e., people whose information is collected, use to monitor their health information and improve their lifestyle. Some share their health and wellness information with family, friends and peers for emotional support, clinical advisors for diagnosis and health advice, employers and insurance companies for monetary benefits and researchers for contributing to the greater good. The people and groups that subjects share information with are collectively referred to as *recipients* and the benefits the subject wants to receive by sharing her information with the recipients, i.e., the value perceived by the subject in sharing is referred to as *utility*. Typically in such scenarios, the subject uses a sensor (e.g., a medical device or an activity tracker) to collect her information. The sensor forwards the subject's data to a networked device (her smartphone or laptop) which then uploads the data to her personal account on the cloud and shared with the recipients.

For the subject to receive the benefits they desire, i.e., to maximize the utility, the information disclosed must be useful to the recipients so they can help the subject achieve her goal. Unfortunately many subjects limit the information they share out of privacy concerns that stem from the fact that they are not aware of how their information will be used by the recipients; this leads to under-sharing of their information, i.e., limiting disclosure and utility of the information. On the other hand, most subjects are incapable of deducing what sensitive inferences could be made from their data. Also, to receive benefits, subjects might share more than necessary because it is unclear to them what information the recipients really need. The latter two cases might lead to over-sharing, i.e., increased disclosure of information but with almost no increase in utility. If the sharing does not reflect their privacy preferences, subjects might become frustrated and ultimately limit or stop using the device. Mobile technologies should strive for a balance, allowing subjects to limit disclosure of information but obtain meaningful utility, so that subjects can enjoy the benefits provided by the technologies without worrying about the disclosure of their sensitive information.

In this poster, we present ShareBuddy, a privacy-aware architecture that helps subjects achieve this balance; the architecture is shown in Figure 1. ShareBuddy allows subjects to review requests from recipients on their mobile phone; these requests describe what information they need to share and why. ShareBuddy also provides flexible sharing controls that warn subjects about sharing information that could be used to make sensitive inferences about them. We conducted a lab study with 21 participants using a prototype of ShareBuddy to explore the effect of displaying benefits and risks of requested information on subjects' sharing behavior.

MobiSys'14, June 16–19, 2014, Bretton Woods, New Hampshire, USA.
ACM 978-1-4503-2793-0/14/06.
http://dx.doi.org/10.1145/2594368.2601448.

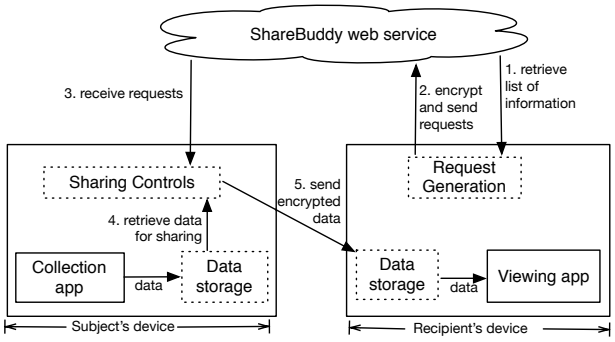

Figure 1: Shapes in dotted lines are part of the ShareBuddy architecture. This diagram shows the workflow for recipients to request and view data and for subjects to share data.

2. SHAREBUDDY

ShareBuddy is a privacy-aware architecture that helps subjects balance disclosure and utility of their information. ShareBuddy has three components:

ShareBuddy on the subject's phone stores data collected by the applications on the subject's phone (referred to as *collection* apps) and helps subjects decide what data to share and with whom,

ShareBuddy web service allows developers to register collection apps, recipients to request for data collected by these applications, requests and data to be sent between recipients and subjects, and

ShareBuddy on the recipient's device receives the data sent by the subject and allows the recipient to view the data on their mobile and/or web application (referred to as *viewing* app).

Before registering collection apps with ShareBuddy, the developers must add hooks to their collection app so that the ShareBuddy component on the subject's phone can access the information collected by it.

Both subjects and recipients need to register with ShareBuddy before using the service. ShareBuddy allows recipients to choose from the list of information collected by all registered collection apps. For every type of information they request, recipients must clearly state why they need it and what benefits the subject will receive for sharing the information. The recipient must also specify their level of need for the information, i.e., is the information *necessary*, *nice-to-have* or *unnecessary*. Once they create the request, the recipients enter the phone number of the subject whose information they are requesting for. Subjects who are not registered with ShareBuddy receive a request to install the component on their phone and to register with the ShareBuddy service. If the subject is already registered, the request generator on the recipient's device encrypts the request with the subject's public key (her phone number) and forwards the message to the subject's phone, along with a session key that the subject can use to send the data later.

The subject views the request on her device and decides how to share the information requested by the recipient. ShareBuddy provides an opt-out approach; the information deemed as necessary by the recipient will be selected for sharing by default. These sharing defaults allow subjects to receive benefits without changing any settings, while also limiting their information disclosure. If subjects are not willing to share *necessary* information, they can opt out of sharing completely because they know that they will not receive any benefits. The request will also help subjects realize that they will not receive any benefits by sharing just the *nice-to-have* information without certain *necessary* information or by sharing any *unnecessary* information. *Nice-to-have* information is usually context associated with the *necessary* information that might be useful to recipients to better understand the *necessary* information; context could be used to make sensitive inferences about the subject when combined with associated target information. ShareBuddy uses visual clues to warn subjects about the risks of sharing if they choose any combination of information types that could be used to make sensitive inferences about them. The information sharing starts as soon as the subjects submit their sharing choices. Subjects can review and change the sharing settings at any time on their device.

The ShareBuddy component on the subject's device encrypts the information with the key provided by the recipient and forwards the message to the ShareBuddy component on the recipient's device. When the recipient wants to view the information, the viewing app retrieves the information from the data storage on the recipient's device; the viewing app developer can write their own visualization functions or use the visualization APIs that are submitted to the ShareBuddy server by the collection app developers.

The goal of ShareBuddy is to help subjects understand the benefits and risks of sharing, so that they can limit disclosure of their information but obtain meaningful utility. By design, it also guarantees confidentiality (only intended subjects can view the requests and intended recipients can view the data).

3. USER STUDY

We developed a prototype of the ShareBuddy architecture for wellness applications. We conducted a lab study with 21 participants to explore the effect of displaying benefits and risks of requested information on the subjects' sharing behavior. The study methods were approved by the Dartmouth Institutional Review Board. The study helped us confirm our hypothesis that knowing about benefits and risks of sharing helps subjects better balance the disclosure and utility of their information. We expect ShareBuddy to be useful to subjects in making sharing decisions that match their privacy preferences and so we plan to deploy the ShareBuddy system in real-world wellness and addiction programs.

4. ACKNOWLEDGMENTS

We wish to thank Denise Anthony, Celeste Campos-Castillo, Shrirang Mare and Andres Molina-Markham for their guidance and the anonymous reviewers for their comments. This research results from a research program at the Institute for Security, Technology and Society at Dartmouth College, supported by the National Science Foundation under award numbers CNS-1143548 and CNS-1329686.