Mithril: A Rule Learning Framework for Privacy and Security Management

Abstract: There are ongoing Security and Privacy concerns around mobile platforms that are increasingly being used by citizens. For example a newly discovered security flaw in WhatsApp that allows another application to upload a user's entire database of chats to a third-party server, without their consent. Or, the Brightest Flashlight application that logged precise location and a unique user identifier. There are no comprehensive mechanisms for handling privacy management on the smartphones today, which can protect their users from such breaches. There are systems like *XPrivacy* and *Xposed* that are interesting but demand substantial policy engineering efforts on the part of the user. We propose an alternative solution of building a framework that will allow us to learn the privacy rules for a particular user on their phones employing a simple user feedback mechanism. The rule learning framework consists of a "learning mode" where it observes and learns from user behavior and a "working mode" where it implements the learnt polices to protect user privacy. The privacy policies are defined using the Semantic Web Rule Language. The antecedents of the rules are context information pieces that are derived from a context management middleware. The main contributions of our system are: first, the system will learn new policies and will modify current policies to control the data flow between the various data providers on the user's phone, including sensors and services and the requester of such data. Second, we plan to implement a context management middleware which generates the user's context, in a cost efficient manner. We have a three-fold solution, as designed in our previous work - COntext MANager miDDleware (COMANDD), for energy cost management that includes reordering of the antecedents of the rules according to their energy costs, choosing the least costly sensors and choosing when to actually query sensors. The complete implementation of this system is underway. We are working on a prototype system for Android devices to carry out our rule-learning work.

Topic alternatives available:

1) **A Rule Learning Framework for Privacy and Security Management on Mobile Devices**
2) **Protecting Mobile Users by Learning their Privacy and Security Habits**
3) **Protecting Mobile Users' Privacy and Security by Analyzing their Habits**
4) **Learning Privacy and Security Preferences in Mobile Environments**
5) **Teach me how to protect your privacy!**