Privacy Keeper

Goals

- Improve security of smartphones in terms of data confidentiality.
- Introduce a framework for monitoring and detecting outgoing communication that might expose sensitive data about the device's owner.
- Detect unnecessary/irrelevant personal data being sent to Web-applications.

Description

Smartphone users often store confidential information on their devices. Smartphones do not provide satisfactory protection for private content and do not have any mechanisms to prevent users from providing unnecessary personal data to websites.

Our solution for detection of data leakage will be based on a combination of:

- Manual knowledge-based detection – Pre-specified rules with user’s ongoing updates.
- Automatic Machine-Learning based detection – The system will detect leakage based on previous decisions and user inputs in order to minimize user interaction.
- Information automatically extracted and analyzed from the website.

The system is able to identify if a site is requesting or accessing illegitimate information. The system includes an off-line training module and an on-line analyzer. The training module is trained with sites that are analyzed by experts to approve their requests as legitimate. The analyzer is capable of distinguishing inappropriate data requests from appropriate ones. The user should be able to see the requested Web page together with security labels attached to form fields (if present) that indicate whether or not information requests are excessive or not.

Researchers

Prof. Bracha Shapira
bshapira@bgu.ac.il

Prof. Yuval Elovici
elovici@bgu.ac.il

Prof. Shlomi Dolev
dolev@cs.bgu.ac.il

Dr. Asaf Shabtai
shabtaia@bgu.ac.il