

Value-Based Information Flow Tracking in Software Packages

Tech ID: 29155 / UC Case 2018-176-0

SUMMARY

A collaboration between UCLA and Rutgers have developed a novel information flow tracking technique to detect potential data leaks in mobile devices.

BACKGROUND

Mobile devices have a variety of sensors that enable a wide range of useful applications from step tracking to providing point of care medical services. As their integration into daily life and capabilities increase, it becomes important that information from these sensors do not get leaked to outside parties. Information flow tracking (IFT) can be used to detect these leaks by monitoring data flow from a sensor to see if it reaches an outlet such as a network socket, a file, or a message shared with another app. Different IFT techniques exist, but they suffer from several usability and precision issues that have hindered their adoption.

INNOVATION

A collaboration between the departments of electrical engineering and computer science at UCLA and Rutgers have developed a novel information flow tracking technique (IFT), called METRON, to detect potential data leaks from apps on mobile devices. The innovative way in which METRON detects data leaks allows it to maintain the same accuracy as state of the art IFT techniques while overcoming the problems that they currently face. METRON does not require any modification to the operating system or to the app of interest. It can be run on current Android platforms, whereas current techniques have yet to do so. Most importantly, METRON can report more detailed operation histories of potentially leaked data than the vague leakage reports of current IFT's, while using less memory and computational power.

APPLICATIONS

- ▶ Mobile and software security analysis
- ▶ Privacy protection on mobile devices
- ▶ Data flow analysis for bug detection

ADVANTAGES

- ▶ Better accuracy at detecting data leaks than current IFT's
- ▶ Provides more detailed leakage reports
- ▶ Uses less memory and computational power
- ▶ Simple to use: can be used without having to modify the operating system or the apps of interest
- ▶ Can be used on current Android and iOS platforms

PATENT STATUS

Country	Type	Number	Dated	Case
United States Of America	Issued Patent	11,347,887	05/31/2022	2018-176

CONTACT

UCLA Technology Development Group
 ncd@tdg.ucla.edu
 tel: 310.794.0558.



INVENTORS

- ▶ Srivastava, Mani B.

OTHER INFORMATION

KEYWORDS

Mobile, mobile devices, Android, iOS, Google, Apple, security, mobile apps, privacy protection, information flow technology, data leakage

CATEGORIZED AS

- ▶ **Computer**
 - ▶ Security
- ▶ **Security and Defense**
 - ▶ Cyber security
- ▶ **Sensors & Instrumentation**
 - ▶ Other

RELATED CASES

2018-176-0

UCLA Technology Development Group

10889 Wilshire Blvd., Suite 920, Los Angeles, CA 90095

tdg.ucla.edu

Tel: 310.794.0558 | Fax: 310.794.0638 | ncd@tdg.ucla.edu

© 2018 - 2022, The Regents of the University of California

[Terms of use](#)

[Privacy Notice](#)

