Controlling Disclosure in App Ecosystems

Gabriel Bender, Lucja Kot, Johannes Gehrke, Cornell University

Johannes Gehrke

A formal approach to disclosure control and tracking

Platforms such as Facebook, Android, iOS, Box are repositories for private user data

- Data is used by a variety of apps with different trust levels
- Data may be generated by some apps and used by others
- A challenging environment in which to track and control disclosure of private info

Key challenge

- Intermediate levels of disclosure
- Many apps legitimately need to access a proper subset of the data to function
- But need to give each app only what it really needs and only if the user is willing to disclose the info

Approach

Fine-grained disclosure control

- Formally define data disclosure including meaningful intermediate levels
- Disclose only what an app genuinely needs to do its work
- Allow fine-grained custom privacy policies

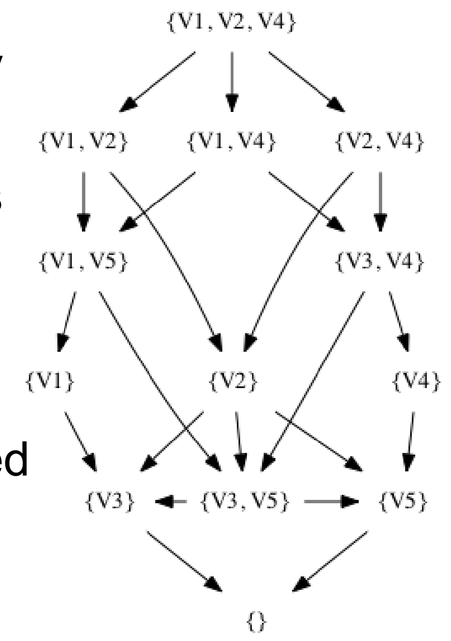
End-to-end information flow tracking

- Automatically identify and tag sensitive information as it leaves the database
- Track info in the system and ensure never flows to unacceptable recipients

Current Results

Formal view-based theory of disclosure

- Ground set of security views
- User or admin defines access policy on the views
- Apps ask queries
- Each query is assigned a label based on the information it requires
- Permitted or denied depending on policy



Ongoing Work

Develop full system for disclosure control in app stores and platforms

- Design a system architecture suitable for various platforms – unique issues in Web, mobile, social settings
- Design and build infrastructure for tracking information flow through the system
- Study and address the issue of data integrity (and not only confidentiality) in app ecosystems
- Study confidentiality and integrity in multi-platform mashups (the "Girls Around Me" problem)

Interested in meeting the PIs? Attach post-it note below!

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Secure and Trustworthy Cyberspace Inaugural Principal Investigator Meeting
Nov. 27 -29th 2012
National Harbor, MD

Cornell University