Meteor: Distributed Security for Platforms with Multiple App Markets

David Barrera, William Enck, P.C. van Oorschot
Problem: Market Models

Single app market

- Market used as a central point of app control, allowing **app vetting and efficient cleanup** (kill switches)

Multiple markets

- Satisfy political, social and economic demands by developers and users
- More difficult to keep secure
Problem: Multi-markets

- Markets rarely consider security as their primary focus
- Vetting does not scale well, and everybody has to do it
- No central namespace
(Toward a) Solution

Meteor
**Meteor**

1. Download app from a market
2. Meteor phone
3. Decision install/remove
4. Preconfigured Servers List
   - Info Source
   - Info Source
   - Kill Switch
Meteor

Info Source ➔ UAppID ➔ Meteor phone ➔ UAppID ➔ Info Source

{UAppID, ...} ➔ UAppID ➔ Meteor phone ➔ UAppID ➔ UAppID ➔ Kill Switch Authority

Info Source ➔ UAppID ➔ Meteor phone ➔ UAppID ➔ UAppID ➔ UAppID ➔ Info Source

Info Source ➔ UAppID ➔ Meteor phone ➔ UAppID ➔ UAppID ➔ UAppID ➔ Info Source

Info Source ➔ UAppID ➔ Meteor phone ➔ UAppID ➔ UAppID ➔ UAppID ➔ Info Source
Components

- Information Sources
- Kill Switch Authorities
- UAppID - \( H(\text{dev cert} \ || \ \text{pkg name}) \)
  \( H(0xBEEF \ || \ \text{com.google.maps}) \)
Information Sources

● Application Databases
  ○ Software analysis
  ○ Privacy analysis
  ○ Malware analysis

● Kill Switch Authorities
  ○ Retroactively notify devices of problems
Information Sources

- **Application Databases**
  - Software analysis *(Stowaway, ComDroid)*
  - Privacy analysis *(ScanDal, TaintDroid)*
  - Malware analysis *(DroidRanger, AV)*

- **Kill Switch Authorities**
  - Retroactively notify devices of problems
How should Meteorite handle queries with no results?

Display apps with the same package name

Display apps signed with the same key

Both

Uninstall app

Enter the manifest URL for the new service:

http://example.com/manifest.json

Get server from URL

Name: Example Meteor Server
Description: This information source offers descriptions of apps that have been installed by members of an anonymous security lab.

Has services: application database

New package: com.wikilibs.
fan_plants_zombies_strategy_2
UAAppID:ed13a07f1286...0bebe443b846
(Querying servers...)
Source Code

https://github.com/davidbb/Meteorite

https://www.ccs.l.carleton.ca/software/meteor

Thanks
Thank you for trying out Meteorite. This simple app uses a Broadcast Receiver to detect when new apps are installed. The app displays a toast with the newly installed app’s UAppID.

Questions? Comments? Please contact dbarrera@ccsl.carleton.ca