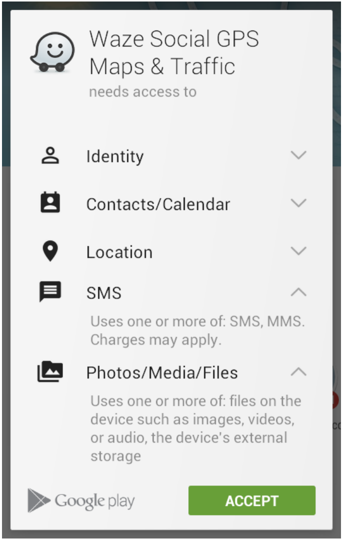
Coq Framework for security policies and proof of concept application

Anders Kaseorg, Jason Gross, and Peng Wang

December 10, 2014

6.858 — Fall 2014

The Problem



Waze Social GPS Maps & Traffic
needs access to

Identity

Contacts/Calendar

Location

SMS

Uses one or more of: SMS, MMS. Charges may apply.

Photos/Media/Files

Uses one or more of: files on the device such as images, videos, or audio, the device's external storage

- Fixed set of coarse permissions
- No information flow control

Our Idea

- Design expressive language allowing:
    - enforcement of fine-grained security policies
    - little to no runtime overhead

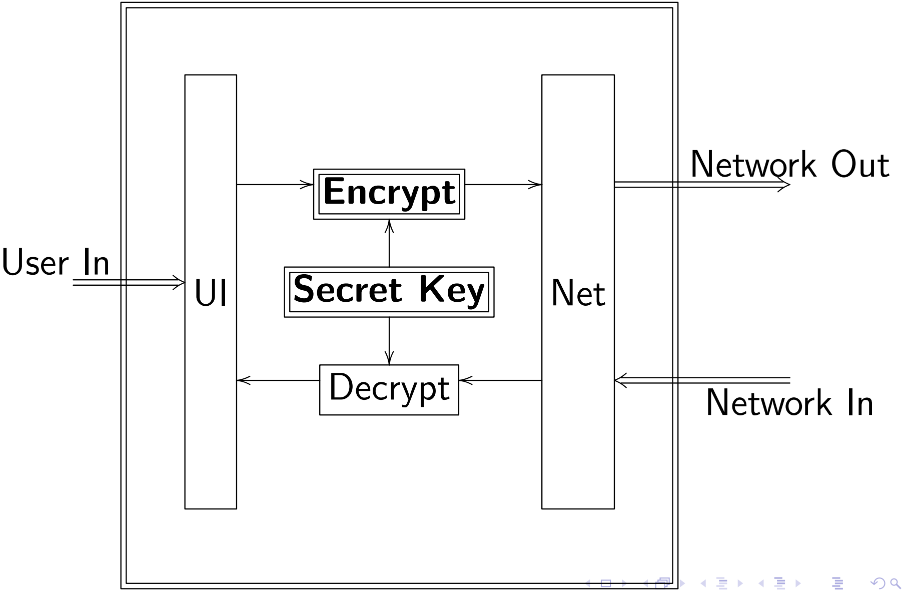
Our Idea

- Design expressive language allowing:
    - enforcement of fine-grained security policies
    - little to no runtime overhead
    - correctness proofs (everything is better with more proofs!)

Our Project: A Proof of Concept

- Framework & Password Manager
- Implemented in Coq
- Based on compile-time enforced modularity and parametricity
- Demo: `https://andersk.scripts.mit.edu/pwmgr/demo`

Example Specification



Future Work

- termination proofs ⟶ absolute running time
    - lack of timing side-channels in the presence of malicious untrusted code
    - currently, we only handle timing side-channels under the assumption of quick code
- more modular termination / timing proofs
- more applications