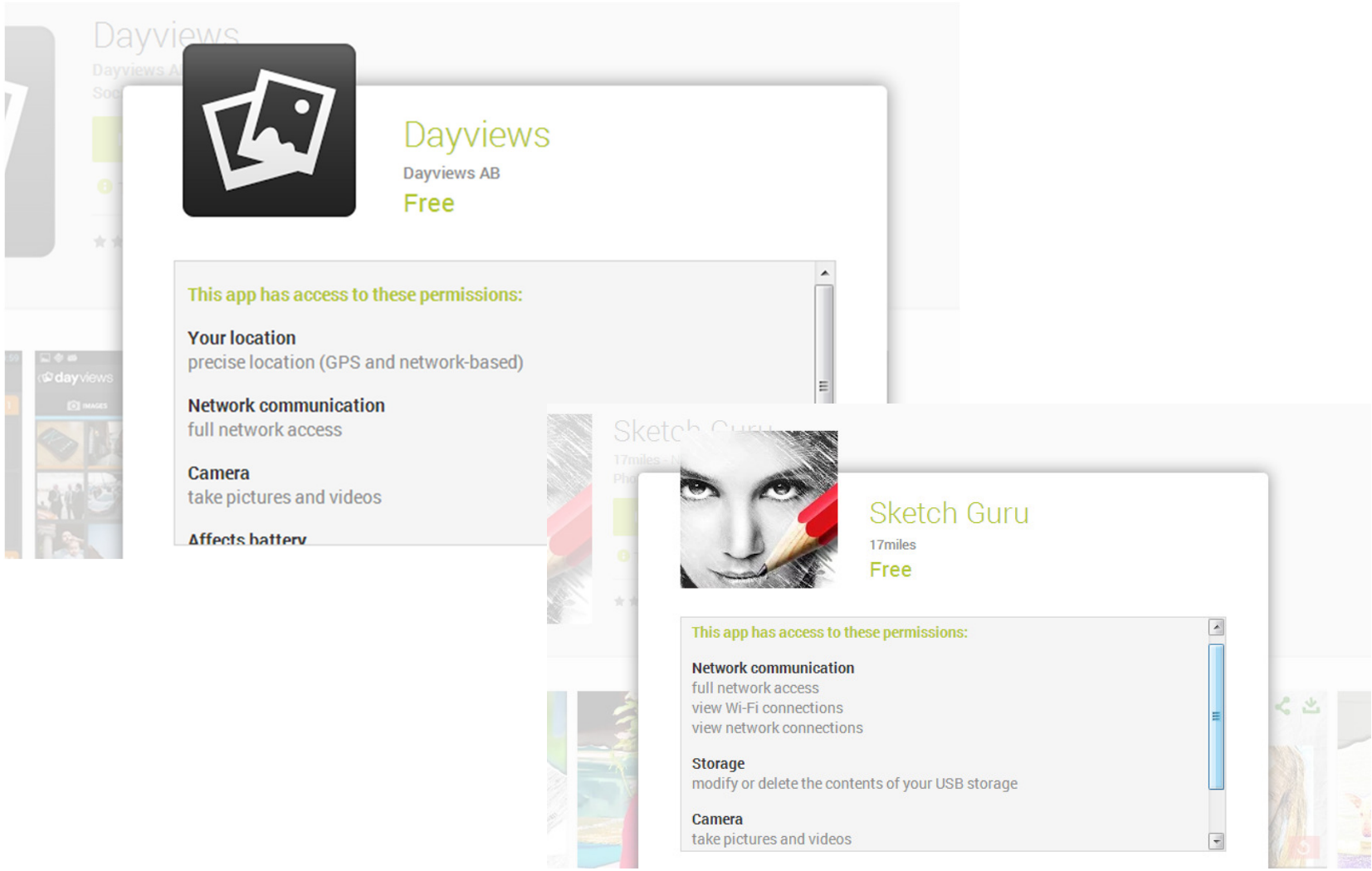
Language-based, Static Information Flow Control

Niklas Broberg (niklas.broberg@chalmers.se)

DAT147 Technical Writing in
Computer Systems and Networks

2014-09-04



What could possibly go wrong?

Access control won't do

- Apps need *legitimate access* to sensitive resources, to perform their intended benign task.
  - E.g. camera+network access to capture and post images to website.

- We need Information Flow (IF) control, to give *end-to-end guarantees* for how data is used.

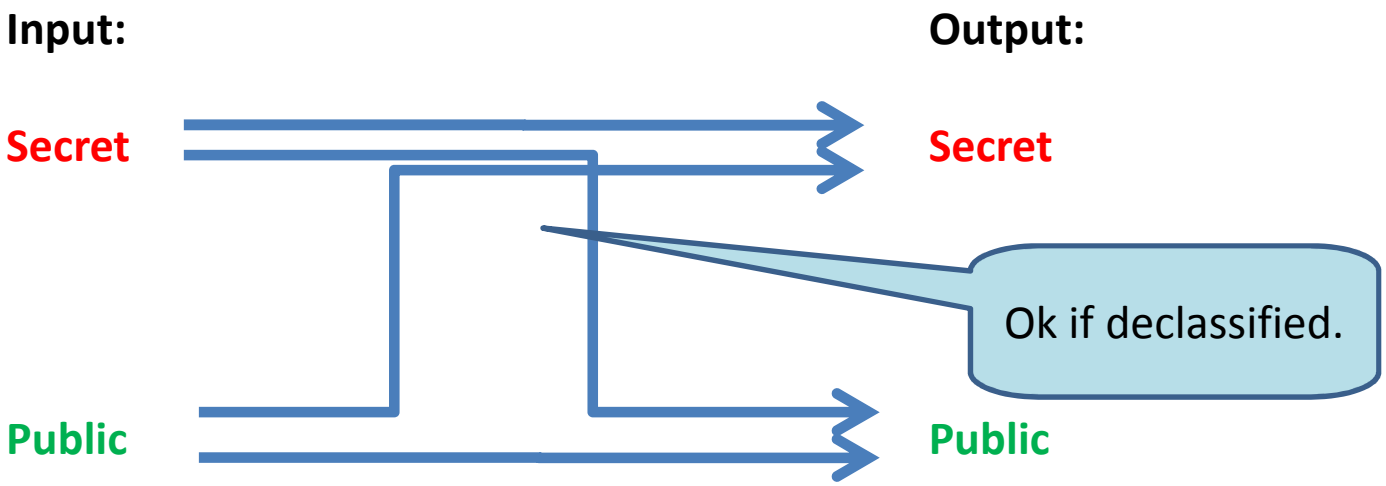
Non-interference won’t do

- Non-interference = strict separation of ”secret” and ”public” data.
  - Classic model of IF, Denning & Denning -77
  - Generally accepted to be too strict – we need possibility to *declassify* data.

- Example: Picture app can upload images, but only when I give my approval.

Declassification

- Declassification = making data ”non-classified”, i.e. releasing secret data as public.



Language-based IF Security

```
int x = 42 * ”Hello!”;
```

Cannot match type ’String’ with expected type ’int’.

```
int x = no_value.getValue();
```

Variable ’no_value’ may be uninitialized at call to ’getValue()’.

```
send_on_insecure_channel(
  super_secret_missile_launch_codes);
```

Data with policy {} (secret) passed to method expecting an argument with policy {Object x:} (public).

Language-based IF Security

- Use programming language techniques to address information flow control (IFC).
  - Static or dynamic analysis and verification
  - Specifically, using ”type” analysis for tracking information flow properties.

Paper I

- Dimensions and principles of Declassification
  - Andrei Sabelfeld and David Sands.
  - Computer Security Foundations (CSF), 2005.

- A survey paper on research within the domain of IFC, with a focus on *declassification*. Establishes much of today's terminology within the domain.

Paper II

- JFlow: Practical mostly-static information flow control.
  - Andrew C. Myers.
  - Principles of Programming Languages (POPL), 1999.

- Early, ground-breaking paper showing the practical viability of static IFC with declassification.

Paper III

- Paragon for Practical Programming with Information-Flow Control
  - Niklas Broberg, Bart van Delft and David Sands
  - Asian Symposium on Programming Languages and Systems (APLAS), 2013

- Recent paper showing state-of-the-art work using static IFC.