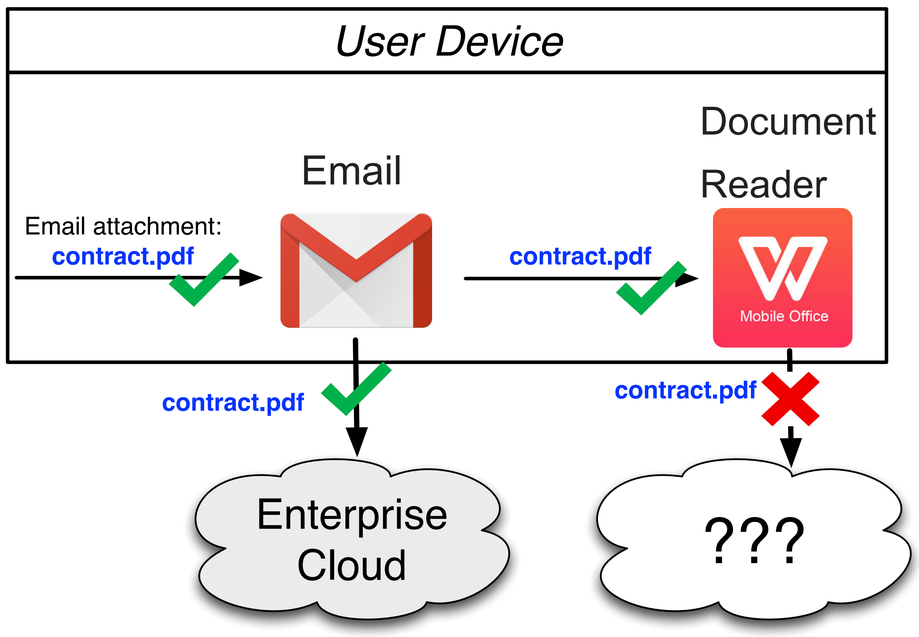
Resilient Architectures

Practical Secrecy Enforcement on Modern Commodity Platforms

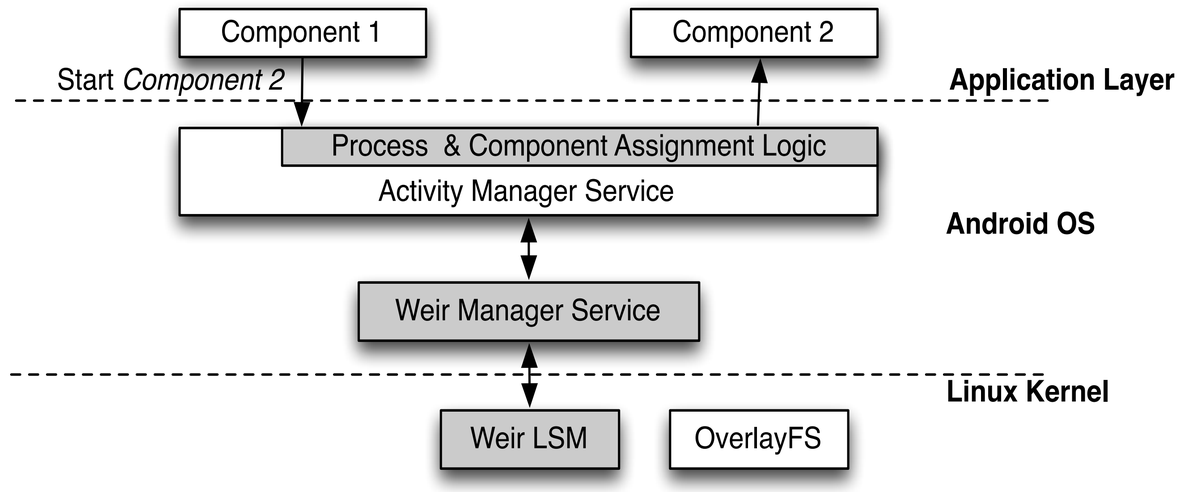
Adwait Nadkarni
Benjamin Andow
Dr. William Enck

Your Data is protected; but is it *secure*?

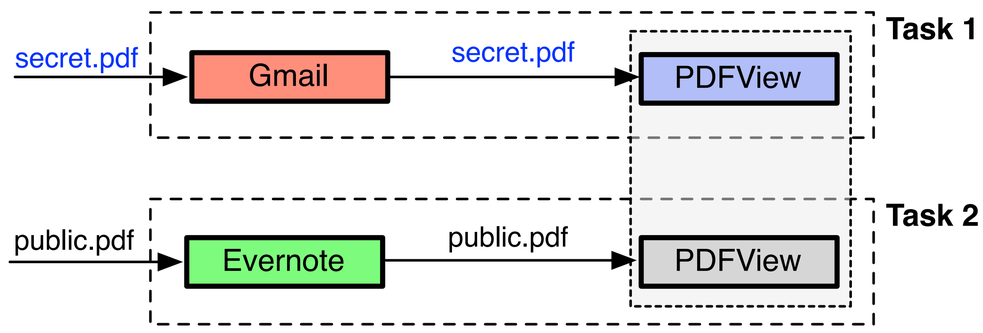


- Need information flow control (IFC)
- **Problem:** Practical IFC is hard (security vs practicality)
  - ***What*** to track? (process vs object)
  - **How** to track (explicit vs implicit)

Implementation



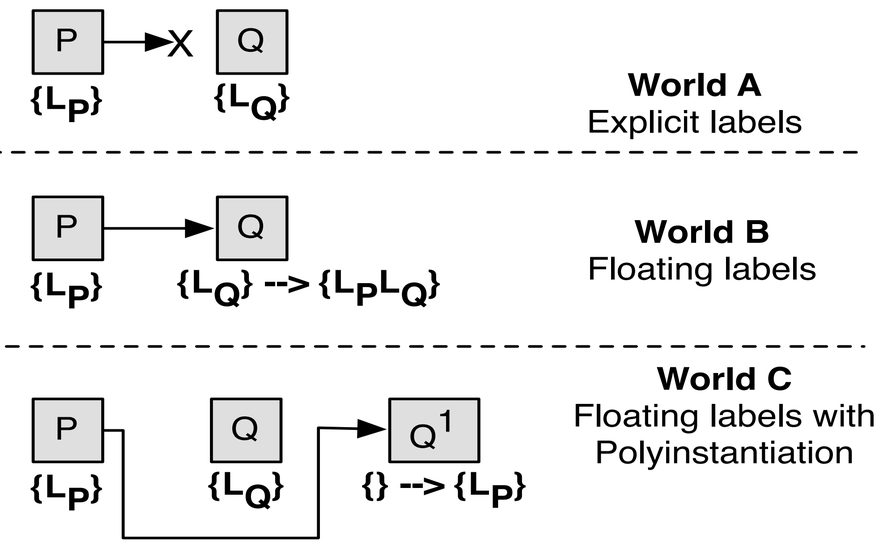
Benefits



- Backwards compatible with unmodified applications
- Transparent to applications

Technical Approach

- Use **context sensitive** floating labels
  - Polyinstantiate processes, files, applications in the *caller's security context.*



- *Advantages:*
  - Precise and secure process labeling
  - Secure application of implicit tracking.

Open Questions

We know how to design and enforce security policies (Aquifer [CCS'13], Weir (USENIX'16))

- How to *specify* the security policy?
  - Data is user-specific, so are policies.
  - Security context:
    - ***What*** to protect?
    - ***How*** to protect it?

Source code:

http://wspr.csc.ncsu.edu/weir/

Contact: Adwait Nadkarni **(anadkarni@ncsu.edu)**