CoSMed: A Confidentiality-Verified Social Media Platform

Thomas Bauereiß

Armando Pesenti Gritti

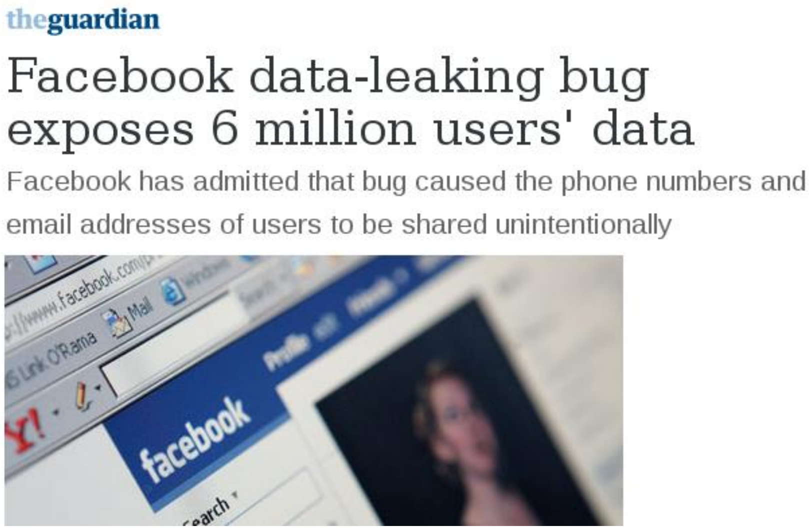
Andrei Popescu

Franco Raimondi

Middlesex
University
London

Introduction

- Security in web-based applications



theguardian

Facebook data-leaking bug exposes 6 million users' data

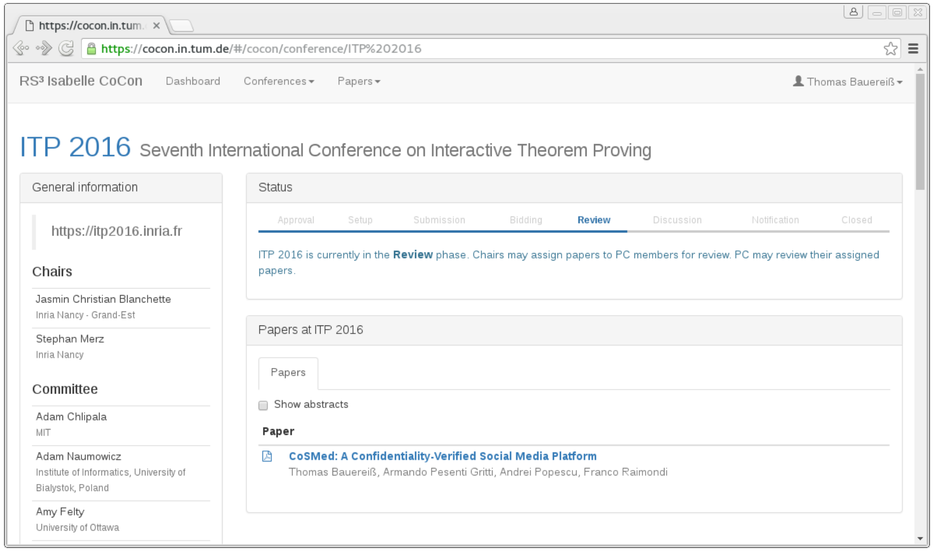
Facebook has admitted that bug caused the phone numbers and email addresses of users to be shared unintentionally

- Goal: Information flow control
  - not just access control!

Previous work

- Security framework: Bounded Deducibility Security (Kanav, Popescu, Lammich)
  - Highly expressive wrt. *what* information may be released and *when*
  - (Interactive) verification technique

- CoCon
  - Verified confidentiality of
    - papers,
    - reviews,
    - reviewer names,
    - discussions



ITP 2016 Seventh International Conference on Interactive Theorem Proving

General information

https://itp2016.inria.fr

Chairs

Jasmin Christian Blanchette
Inria Nancy - Grand-Est

Stephan Merz
Inria Nancy

Committee

Adam Chlipala
MIT

Adam Naumowicz
Institute of Informatics, University of Bialystok, Poland

Amy Felty
University of Ottawa

Status

ITP 2016 is currently in the **Review** phase. Chairs may assign papers to PC members for review. PC may review their assigned papers.

Papers at ITP 2016

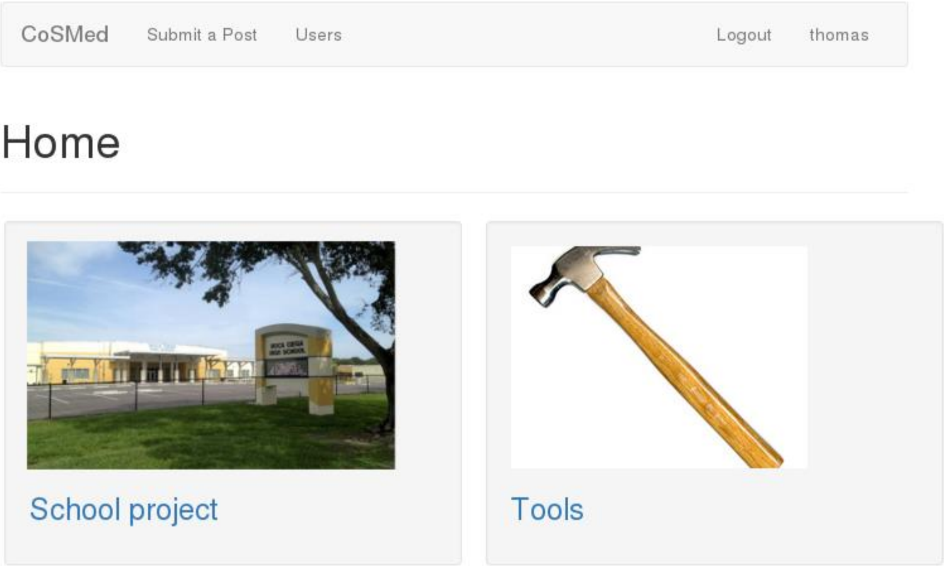
☐ Show abstracts

Paper

CoSMed: A Confidentiality-Verified Social Media Platform
Thomas Bauereiß, Armando Pesenti Gritti, Andrei Popescu, Franco Raimondi

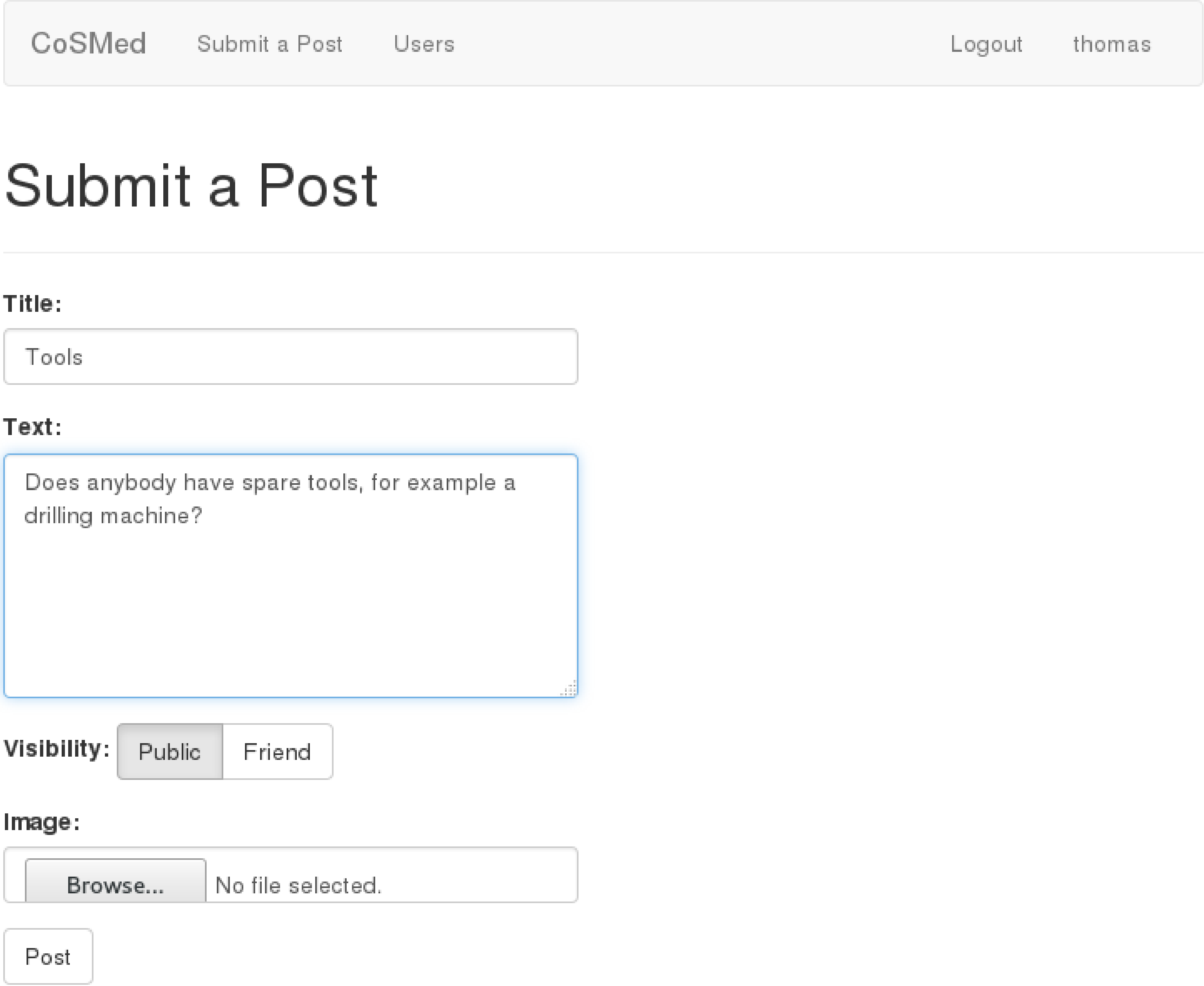
CoSMed

- Prototype social media platform



- Focus on confidentiality
- Tailored for needs of a charity organization

CARITAS
ANCHOR
HOUSE



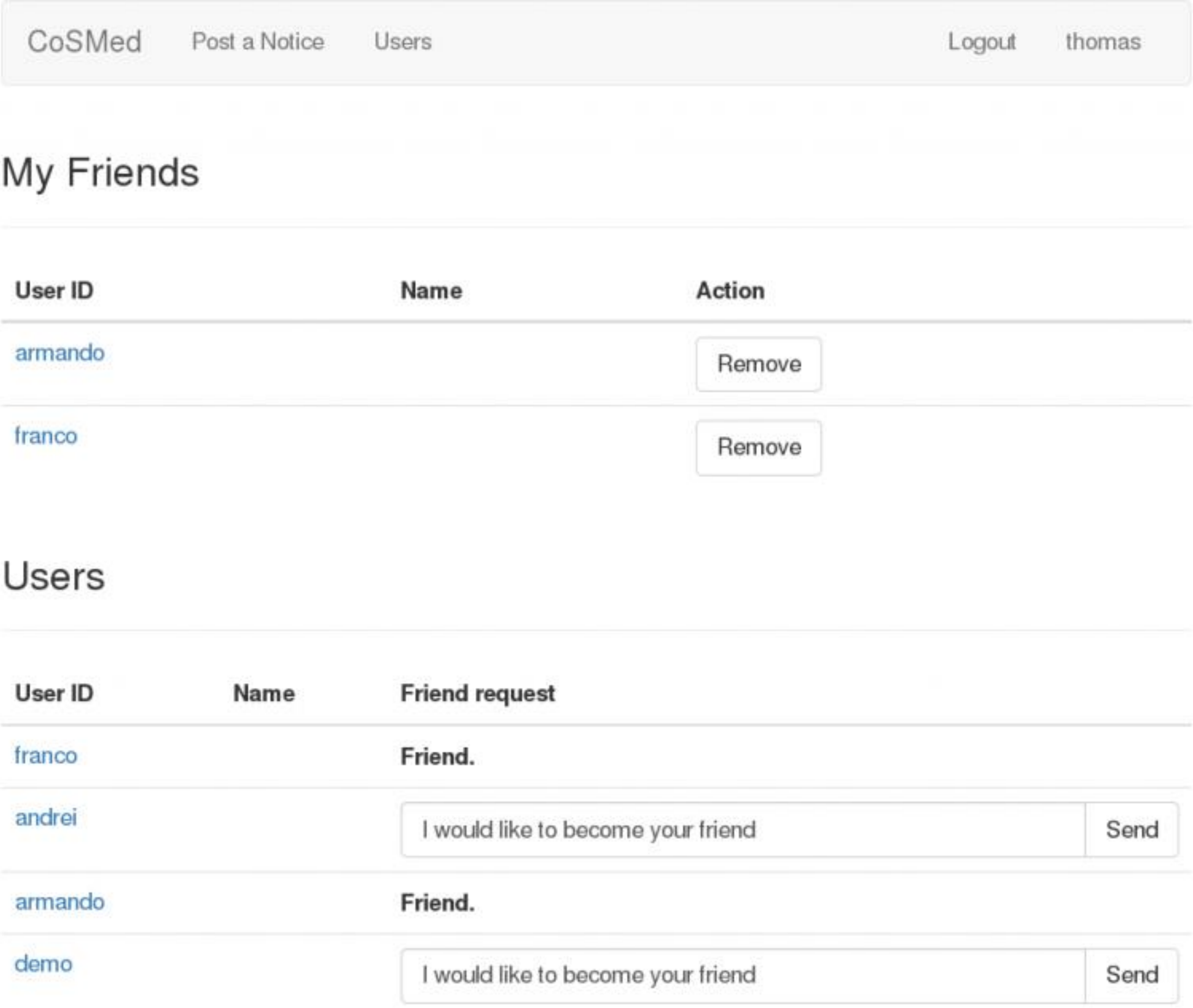
Submit a Post

Title: Tools

Text: Does anybody have spare tools, for example a drilling machine?

Visibility: [✓ Public] Friend

Image: No file selected.



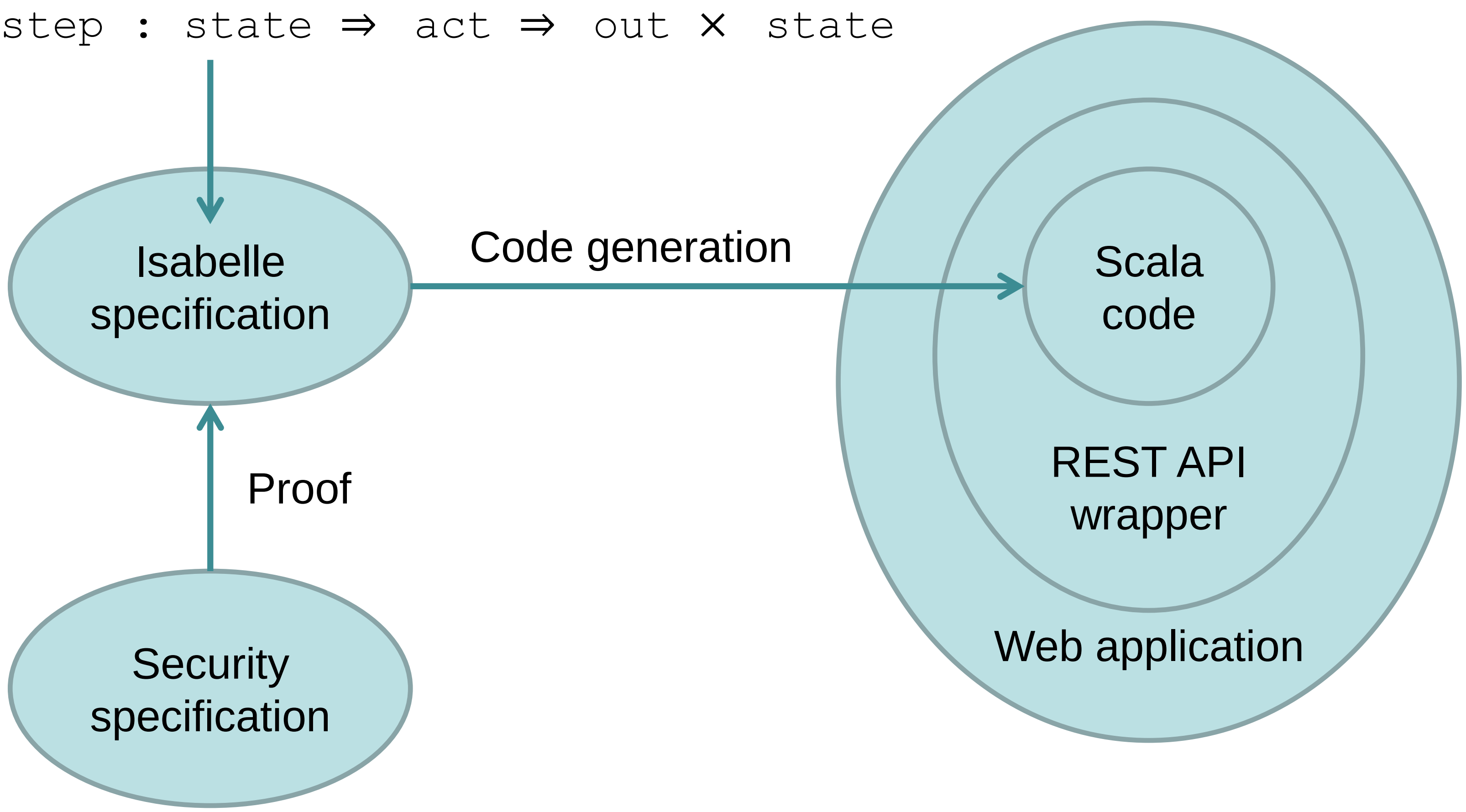
My Friends

User ID	Name	Action
armando		Remove
franco		Remove

Users

User ID	Name	Friend request
franco		**Friend.**
andrei		I would like to become your friend Send
armando		**Friend.**
demo		I would like to become your friend Send

System Architecture



`step : state ⇒ act ⇒ out × state`

Isabelle specification

Code generation

Scala code

REST API wrapper

Web application

Proof

Security specification

Security Requirements

- Confidentiality of
  - Friend-only posts
    - Text, image, and title updates
  - Friendship information
    - Who is friends with whom?

Bounded Deducibility Security

- Generalization of Nondeducibility (Sutherland, ‘86):

$$\forall t \in Sys, s \in List(Sec).$$
$$\exists t' \in Sys.\, O(t') = O(t) \wedge S(t') = s$$

  where

  - $Sys \subseteq List(Trans)$ is the set of possible execution traces of a system (i.e., sequences of system transitions)
  - $O : List(Trans) \rightarrow List(Obs)$ maps traces to observations
  - $S : List(Trans) \rightarrow List(Sec)$ maps traces to secrets

Bounded Deducibility Security

- Adding declassification:

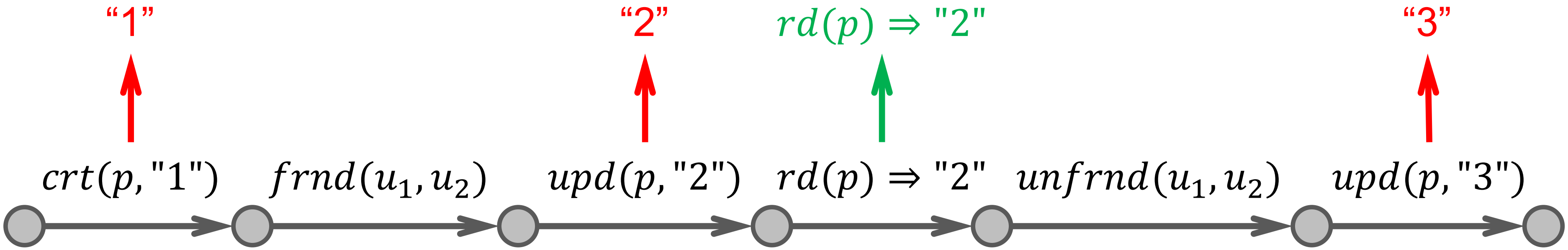
$$\forall t \in Sys, s \in List(Sec).\ (\boldsymbol{S(t), s}) \in \boldsymbol{B} \wedge \neg \boldsymbol{T(t)}$$
$$\longrightarrow (\exists t' \in Sys.\, O(t') = O(t) \wedge S(t') = s)$$

where

- $\boldsymbol{B} \subseteq List(Sec) \times List(Sec)$: declassification bound
  - Specifies which secrets have to be indistinguishable from which other secrets
- $\boldsymbol{T}$: declassification trigger
  - If T is true, secret information is allowed to be declassified

Post Confidentiality

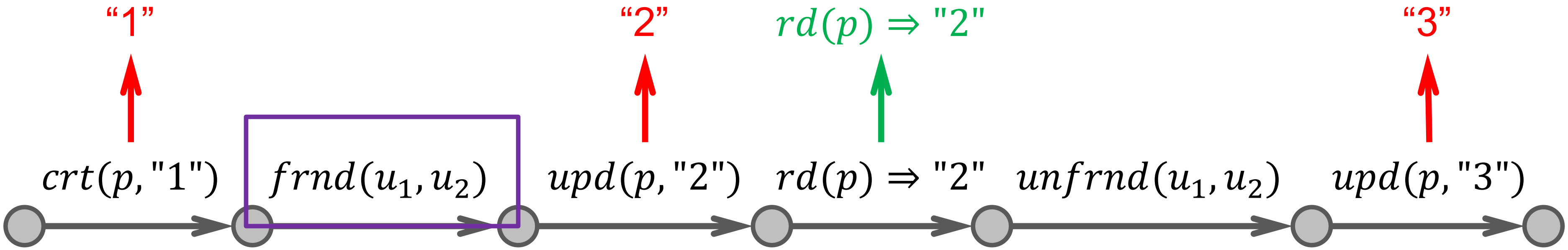
- Observations:
  - Actions (and outputs) performed by arbitrary but fixed set of users
- Secrets
  - Content updates of arbitrary but fixed post p



Post Confidentiality

- Declassification bound:
  - All secrets indistinguishable
- Declassification trigger:
  - Observer and post owner become friends or post becomes public

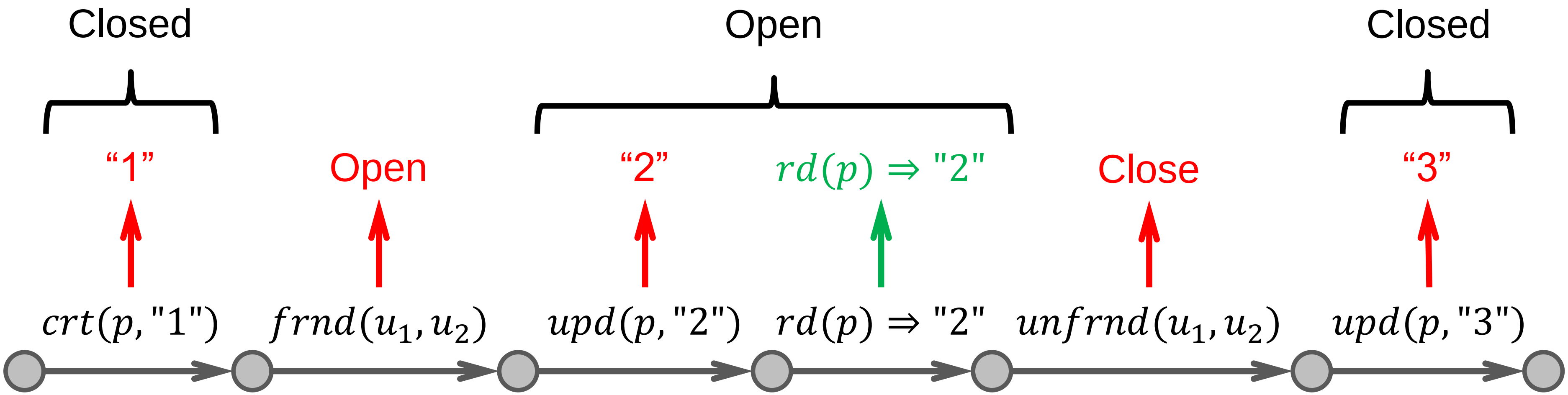
Too weak! What about “unfriending”?



Post Confidentiality

- Distinguish two phases
- Mark transitions

$$\mathrm{Sec} = \mathrm{Post\_Content} + \{\mathrm{Open}, \mathrm{Close}\}$$



Closed

Open

Closed

“1”

Open

“2”

$rd(p) \Rightarrow "2"$

Close

“3”

$crt(p, "1")$

$frnd(u_1, u_2)$

$upd(p, "2")$

$rd(p) \Rightarrow "2"$

$unfrnd(u_1, u_2)$

$upd(p, "3")$

Dynamic Declassification

Declassification bound for the closed phase:

$$BC(ul,\ ul')$$

Dynamic Declassification

... declassification bound for the open phase:

$BC(ul,\ ul')$ $BO(ul,\ ul)$

Dynamic Declassification

... iterated via mutual induction:

$$\boxed{B = BC}$$

$$BC(ul,\ ul') \qquad\qquad BO(ul,\ ul)$$

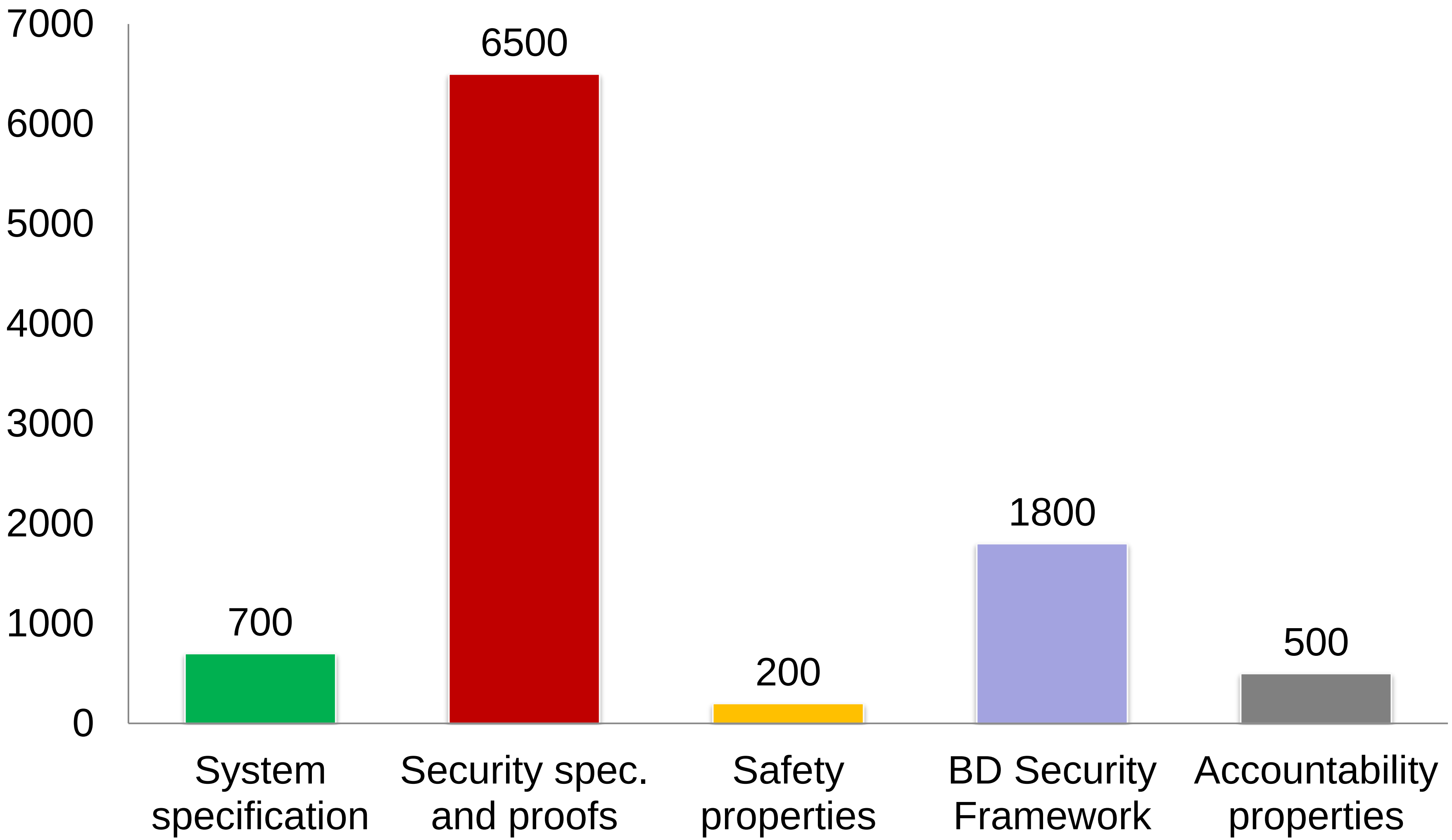
$$\frac{\text{last}\,ul = \text{last}\,ul' \qquad BO(sl, sl') \qquad \ldots}{BC(ul \cdot \text{Open} \cdot sl, ul' \cdot \text{Open} \cdot sl')}$$

$$\frac{BC(sl, sl')}{BO(ul \cdot \text{Close} \cdot sl, ul \cdot \text{Close} \cdot sl')}$$

Verification

- Unwinding
  - Construct alternative trace incrementally
  - Strategy for when and how to:
    - match observable transitions in both traces
    - insert/delete secret transitions as required by bound
  - “Unwinding relation” between original and alternative states and remaining secrets
  - Proof of unwinding conditions

Verification



Conclusion

- CoSMed:
  - https://cosmed.globalnoticeboard.com
  - Social media platform tailored for charity organization
  - Verified dynamic confidentiality requirements
  - Lesson learned for BD Security: declassification bounds incorporating dynamic triggers

- Next step: CoSMeDis
  - Extension of CoSMed to distributed system
  - Compositionality result for BD Security