Distributed System Security via Logical Frameworks

Lujo Bauer * **Frank Pfenning †** **Michael K. Reiter †‡***

† Department of Computer Science
‡ Department of Electrical & Computer Engineering
*** CyLab**
Carnegie Mellon University

Access Control Today

- **Physical**
  - Physical keys
  - Identification cards
  - Access cards and tokens
- **Computer**
  - Username and password
  - Biometrics
  - Smart cards
  - Kerberos, Passport, …
- **Weaknesses of current methods**
  - Limited expressiveness
  - Poor cross-domain interoperability

Converged Mobile Devices ("Smartphones")

- **Converged mobile devices ("smartphones")**
  - Match wireless telephony to evolved OS or application environments
  - Include the ability to download data to local storage, run applications, and store user data beyond PIM capabilities
  - Leaders: Nokia, Motorola, Sony Ericsson, RIM, Samsung

- **Converged device market nearly doubled in 2003 [IDC]**
  - Market shows "significant growth and future promise"
  - ~10,000,000 shipped worldwide in 2003, but should inherit mobile phone market—over **500,000,000** shipped in 2003
  - Compound annual growth rate of ~86% projected through 2007
- **In the not-too-distant future, every person will have at least one**

A Universal Access-control System

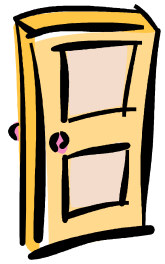
- **Goal: to use smartphones to intelligently control environment**
  - In particular, utilize smartphone as a universal access-control device
- **Your smartphone will permit you to do things better ...**
  - Office door unlocks as you approach it, computer logs you in, etc.
- **... And to do things you could not do before**
  - Delegate authority seamlessly and with fine granularity
- **Enabling technologies**
  - Logic-based access control
  - Proof-carrying authorization
  - Logical frameworks

- I would like to borrow a book from Mike's office.

Jon

Jon's phone

D208 (Mike's office)



- Mike's students may enter Mike's office.
- Mike's admin may act on Mike's behalf at CMU.
- Mike's wife may act on Mike's behalf always.

Mike

Mike's phone

- Only Mike has the authority to enter his office, but he may delegate it to others.

Logic-Based Access Control

[Lampson, Abadi, Burrows & Wobber 1992; ...]

- **Access control system can be modeled by a formal logic**
  - Allows formal reasoning about the capabilities and limitations of the system
  - Provides for separation of mechanism from policy
- **Logic might consist of**
  - Strings — Mike, Jon, HH.D208
  - Channels — 0x4C892BD... (public key)
  - Compound principles — Jon **as** Student, Device **for** Mike
  - Statements — Jon **says** Goal(HH.D208,…), Jon **speaksfor** Mike.students, **delegates**(Mike, Mike.students, Goal(...))

Logic-based Access Control Cont'd

- **Logic contains inference rules for reasoning about statements**
- **Example: Reasoning about belief**

A says F ≡ ?

$$\frac{\textit{pubkey} \text{ signed } \textit{fmla}}{(\text{name } (\textit{pubkey})) \text{ says } \textit{fmla}} \qquad \frac{F}{A \text{ says } F}$$

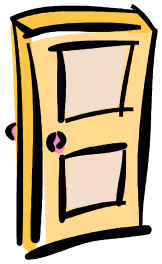
$$\frac{A \text{ says } F \qquad A \text{ says } (F \rightarrow G)}{A \text{ says } G}$$

```
Jon says
   Goal(CMU.HH.D208.open)
```

Jon's phone

Jon

D208
(Mike's office)



```
Delegates(Mike,Mike.students,
   Goal(CMU.HH.D208.open)
∀F: Delegates(Mike,
   Mike.Admin, Goal(CMU.F))
Mike.Wife speaksfor Mike
```

Challenge:

```
Mike says
   Goal(CMU.HH.D208.open)
```

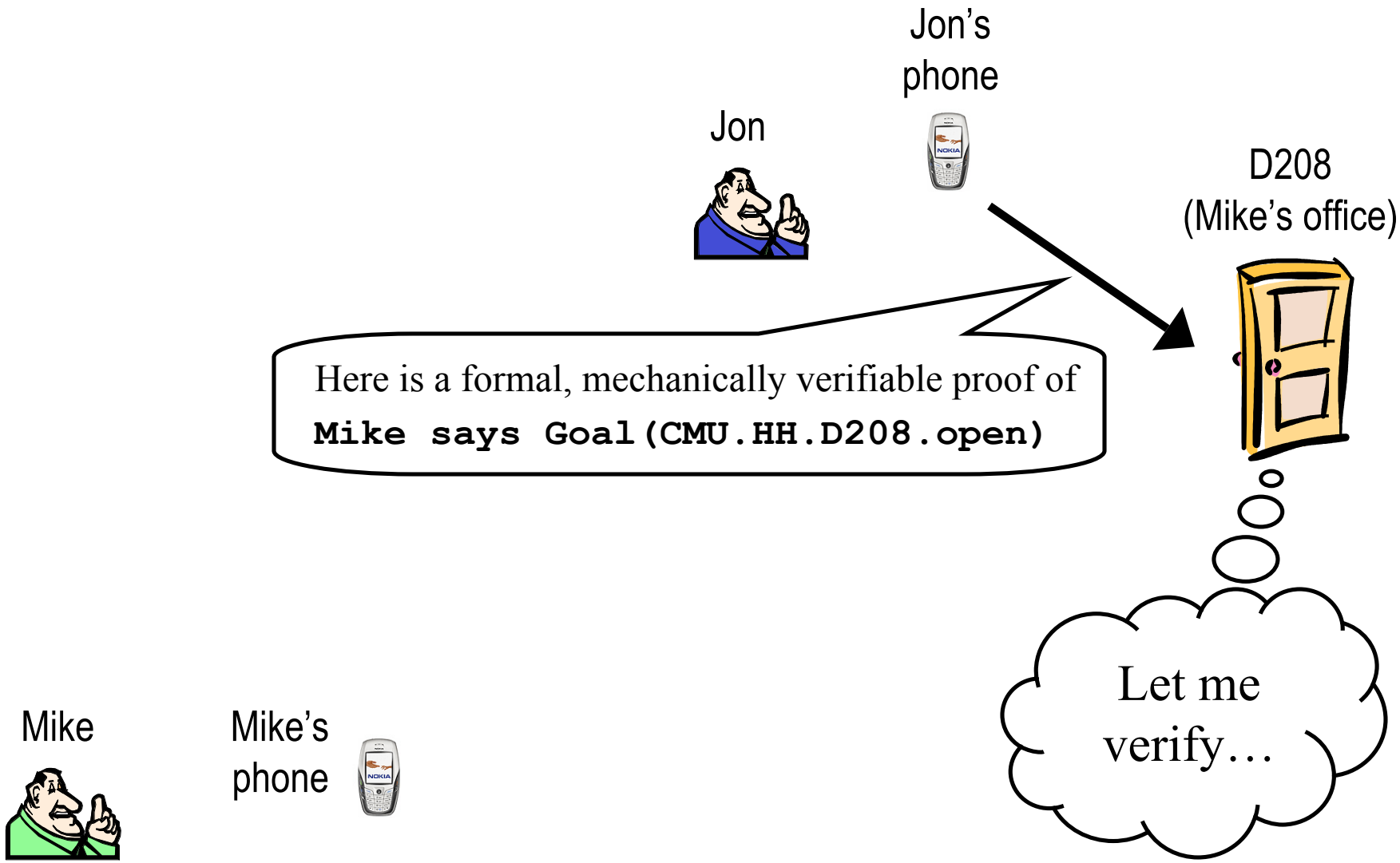
Mike

Mike's phone

Proof-carrying Authorization (PCA)

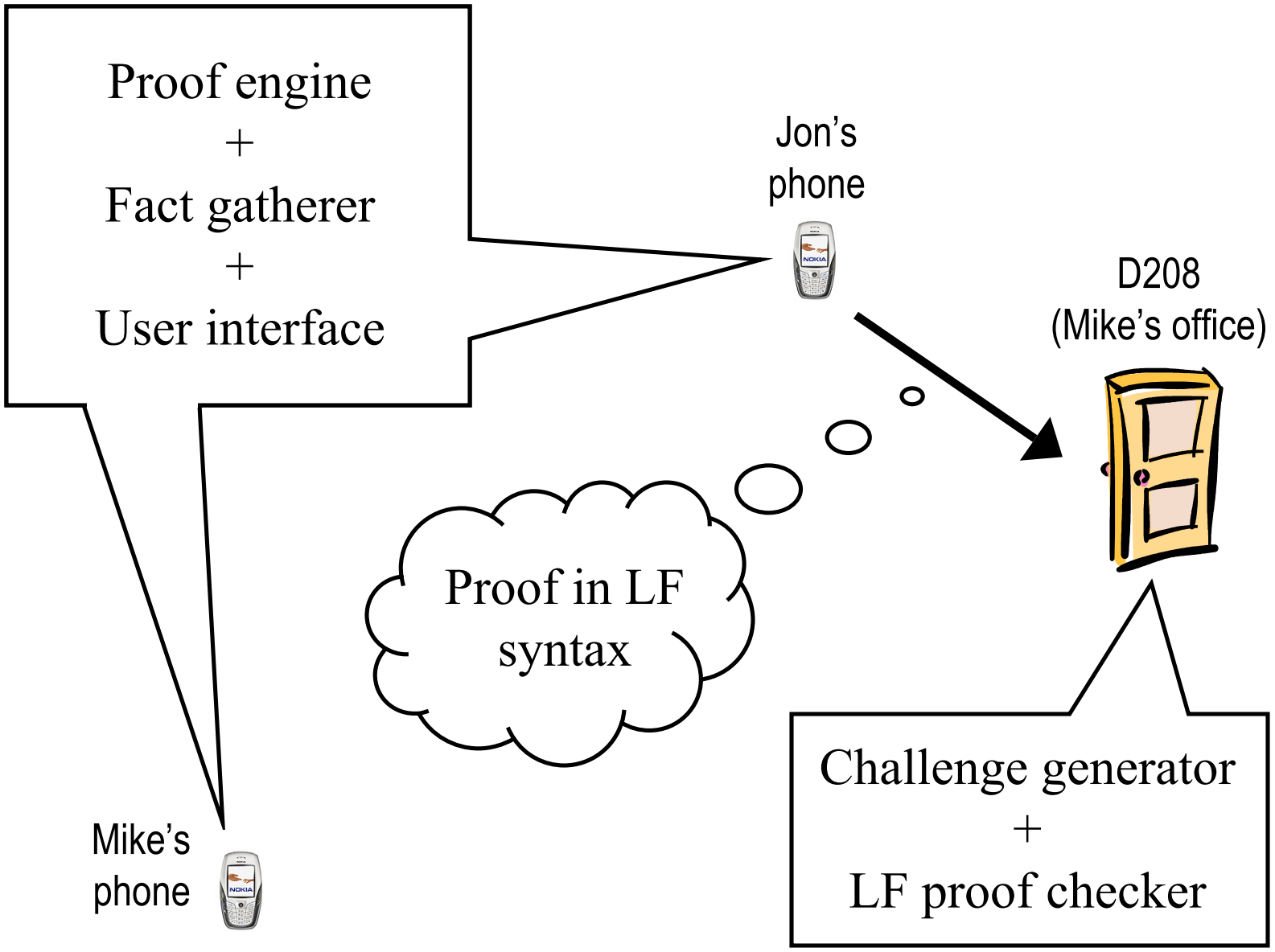
- **A language and paradigm for developing interoperable security logics**
- **Resolves tension between generality and expressivity of access-control logics**
- **Server uses higher-order logic**
  - General, undecidable logic
  - Proof checking decidable
- **Client uses application-specific logic**
  - Application-specific operators defined in higher-order logic
  - Inference rules defined (and proven) as lemmas
  - Proof generation decidable

Proof-carrying Authorization (PCA)



Gap Between Model & Implementation

- **Observation: The implementation may behave differently from the model**
- **Problem: Does the model prove anything about the actual implementation?**
- **(Partial) Solution: Integrate logical framework in implementation**
  - Components of the logic and logical framework are core pieces of the system's data structures and protocols
  - Use standard, well-studied technology: LF



Challenges: Access Control

- **Constraining unintended consequences**
  - Participants may utter contradictory or overly general statements
- **Scalable and automated proof-generation strategies**
  - Human assistance not always possible
- **Resource-constrained mobile devices**
  - Proof-generation can be partitioned to take advantage of powerful, non-mobile infrastructure
- **Privacy concerns**
  - Every authorization and delegation explicitly encoded
  - Credentials can be observed
- **Capture resilience**
  - A stolen device should not reveal the credentials stored on it

Challenges: Logical Frameworks

- **More expressive frameworks allow us to describe a larger number of realistic scenarios**
- **Concurrent Logical Framework (CLF)**
  - Combination of linear logic, type theory, and monads
  - Directly supports the specification of distributed and concurrent systems
- **Specifying system architecture (policies, protocols, proofs) in the enhanced framework**