Medina: Combining Evidence to Build Trust

Reasoning about trust without onions.

Johannes Helander

Ben Zorn

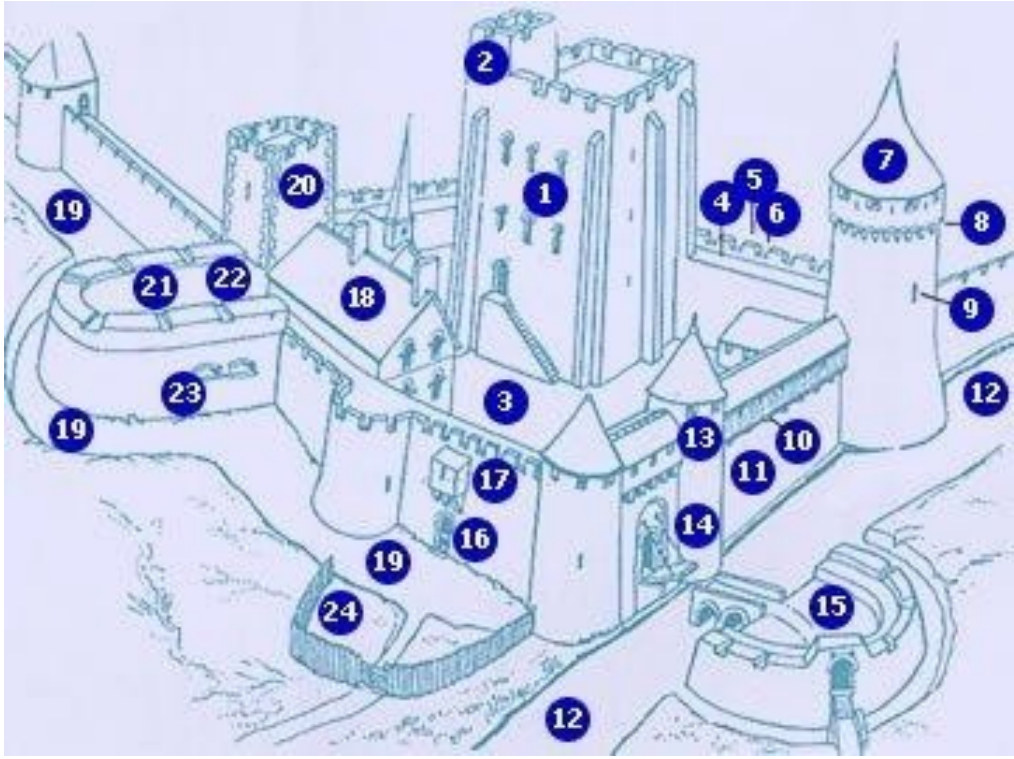
Microsoft Research

May 23, 2007

Oakland, WSP07

A Second Look at Passwords

- Not as strong as encryption would suggest
- Ad-hoc methodology
- Back-channels (e.g. password reset)
- Reuse of passwords
- Inconvenient to store



(14) front door
(16) side door

- They just don't work

Our Formalism and Passwords

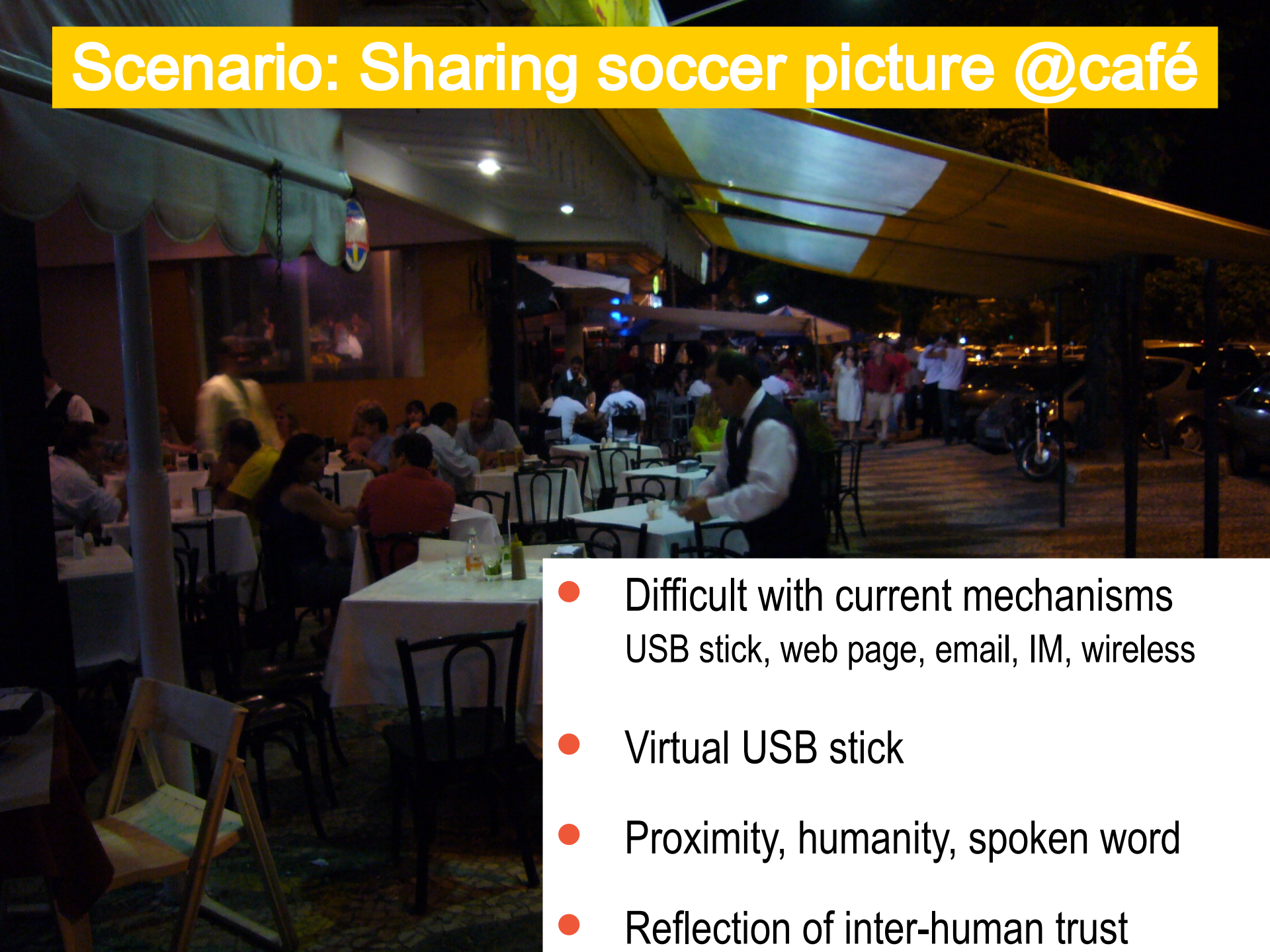
- allow = P(e1,e2,e3) = e1 | (e2 & e3)
  - e1 = knows password
  - e2 = has an email address registered with the account
  - e3 = can read email sent to that address
- Stricter policy: allow = P2(e1,e2,e3,e4) = e4 & P1(e1,e2,e3)
  - e4 = is human
- Boolean operation → will generalize
- Interpretation of policies that combine evidence

Framework for reasoning about trust

HIP, puzzle, biometric, proximity
peer rating, knowledge quiz

- Non-onion
- Time decay & integration
- Multiple sources of evidence
- Imprecise data

Scenario: Sharing soccer picture @café



- Difficult with current mechanisms
  USB stick, web page, email, IM, wireless
- Virtual USB stick
- Proximity, humanity, spoken word
- Reflection of inter-human trust

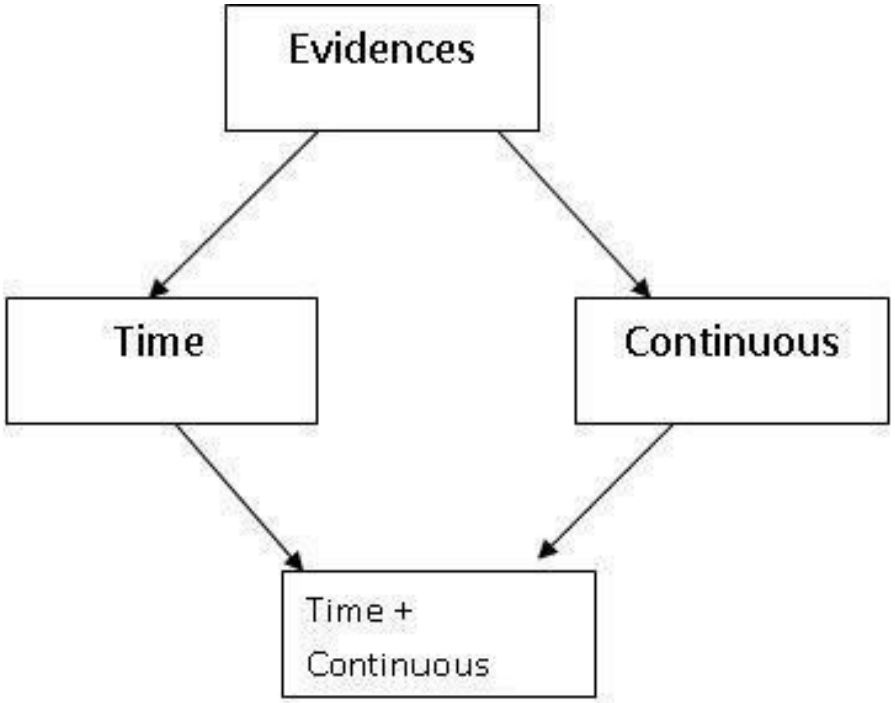
Scenario: Wiki access control

- Quizzes
- Ratings

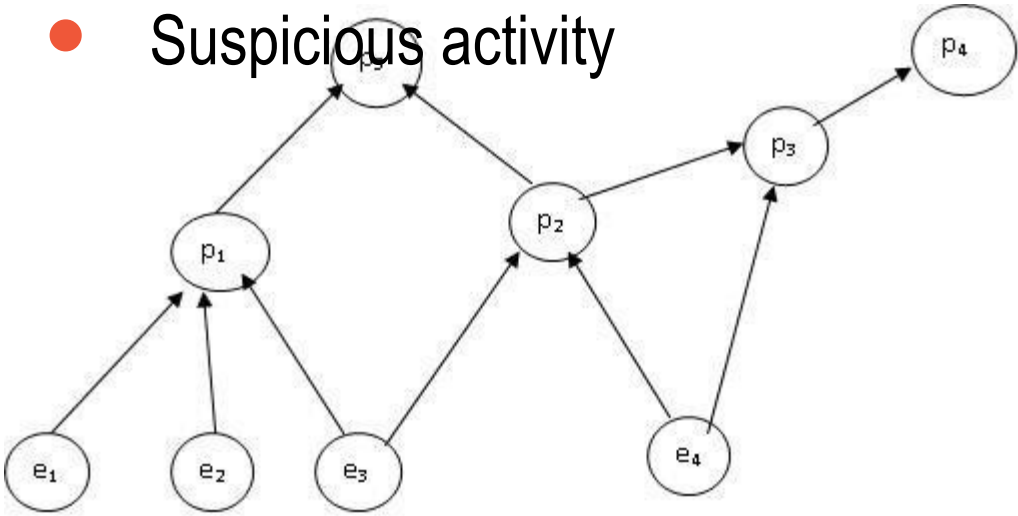
- edit1 = ((quiz1>70% & peer>50%) | passwdA) & HIP
- edit2 = ((quiz2>90% & peer>75%) | passwdB) & HIP

- read1 = anybody
- read2 = (peer>20%) & HIP

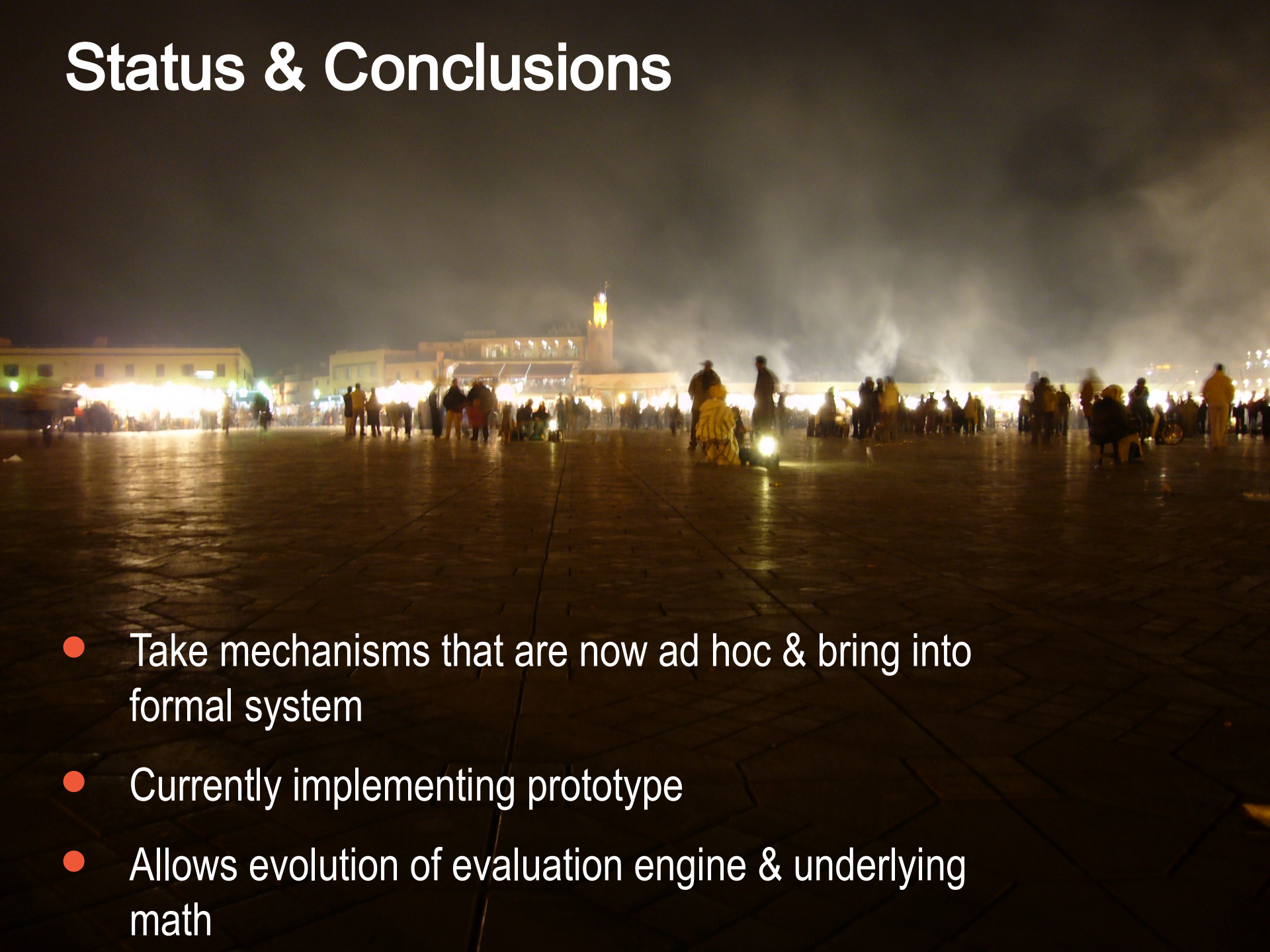
Adaptive Trust Evaluation



- Stochastic process?
- Decay
- Filters
- Credit history
- Suspicious activity



Status & Conclusions



- Take mechanisms that are now ad hoc & bring into formal system
- Currently implementing prototype
- Allows evolution of evaluation engine & underlying math