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
- They just don’t work

(14) front door
(16) side door
Our Formalism and Passwords

- \( \text{allow} = P(e_1, e_2, e_3) = e_1 \lor (e_2 \land e_3) \)
  - \( e_1 = \text{knows password} \)
  - \( e_2 = \text{has an email address registered with the account} \)
  - \( e_3 = \text{can read email sent to that address} \)

- Stricter policy: \( \text{allow} = P_2(e_1, e_2, e_3, e_4) = e_4 \land P_1(e_1, e_2, e_3) \)
  - \( e_4 = \text{is human} \)

- Boolean operation \( \rightarrow \) will generalize
- Interpretation of policies that combine evidence
Framework for reasoning about trust

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

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

- $\text{edit1} = ((\text{quiz1}>70\% \land \text{peer}>50\%) \lor \text{passwdA}) \land \text{HIP}$
- $\text{edit2} = ((\text{quiz2}>90\% \land \text{peer}>75\%) \lor \text{passwdB}) \land \text{HIP}$

- $\text{read1} = \text{anybody}$
- $\text{read2} = (\text{peer}>20\%) \land \text{HIP}$
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