Securing the Open Softphone

Kickoff Colloquium
September 1, 2010

The Promise of Ubiquitous Communication and Computation

- **Unrestrained collaboration in groups large and small**
- **Examples:**
  - Crime-reporting with protection from corruptible authorities (when police are potentially corrupt)
  - Political organizing without (state-owned?) media filters
  - Real-time traffic monitoring
  - Disaster relief
- **Problems:**
  - How do you get valid information
  - In a way that preserves individual privacy
  - In a way that gives people a reason to participate
  - (no privacy $\Rightarrow$ no participation)
  - (no validity $\Rightarrow$ data pollution $\Rightarrow$ no participation)

Privacy - more than confidentiality

- **a general concern, decomposable into**
  - confidentiality of contents of communication (TLS)
  - freedom from traffic analysis (Tor for IP, ?)
  - freedom from query analysis (private information retrieval)
  - confidentiality of location (?)
  - ? (?)

- **softphone-related particular challenges**
  - location, location, location!
  - always-with-human and multifaceted (entertaintment/payment/work/play/love): surveillance like never before

Information Reliability & Integrity

Also a general concern with various aspects:

- **Validity of reports or shared information**
  - reputation-based, ground-truth checkable,…
- **User authentication**
  - using password, sensors, proximity, anonymous credentials,…
- **Reliable distributed data management**
  - p2p-based, best-effort vs. 100% accuracy,…
- **Dynamic group formation**
  - based on user registration/revocation, access controlled,…

- **Non-solution for <u>any</u> of the above:**
  - Register every cell phone to a name, punish for bad communication

What's different (given all this prior work)

- **Promises** (not available on PCs):
  - *High mobility*
  - *Opportunistic networking*
  - *Rich sensing*
  - *Always-on*
  - *Peer-to-peer* (wifi/bluetooth) and infrastructure mode

- **Challenges** (not the same as PCs):
  - *Computing constraints* (e.g., for evaluation of sensory data or running heavy protocols): memory, speed, power
  - *Fixed protocols* at the phone network layer that are both privacy unfriendly and insecure
  - *Central control* (large companies/government regulation) that may be unaligned with user incentives