WRAP-UP

Protocols, UIs, Usage

- Security & Privacy Protocols for Mobile Phone

- Security & Privacy UIs for Mobile Phones

- Security & Privacy Issues Through Mobile Phone Use

Mobile Privacy & Security Protocols

- Deployment Costs!
- Ease of Use (Interaction Required for Protocol Use)
- Performance
- Resources (Energy, User Costs, Attention)
- User Perception of Security
- Awareness of User of Security Issues, Requirements

- Opp: Trusted Device
- Scalability?
- Multi-Channel
- Fuzziness (Does it add value?)
- Opp: Use of Sensors!
- Location!

Mobile Privacy & Security UIs

- Usability
- Understandability
- Intuitiveness
- Simplicity
- Willingness to Configure & Use
- Unobtrusiveness
- Device Diversity!
- Multi-Modality
- Situatedness (Challenge & Opp.)

- Scalability (How many interactions per hour?)
- Threat Awareness
- Resources (I/O, e.g., Small Screen, Keys)
- Sensors, alternative Input Modalities, Biometrics
- Shoulder Surfing Protection
- Social Compatibility, Acceptability

Privacy & Security Implications Through Mobile Phone Usage

- Exert Control (force legal compliance)
- Source of Control (Socially, Technologically)
- Location-Awareness
- Social compliance
- Implications of Use Through Software Capabilities
- Trust (vs. Laptop, PC)

- Source of cultural change!
- New Vulnerabilities (e.g., Bluejacking, Denial of Energy Attack, „Zombie my phone")
- Logging
- Availability of Sensors (e.g., Camera, Microphone?) to Others