

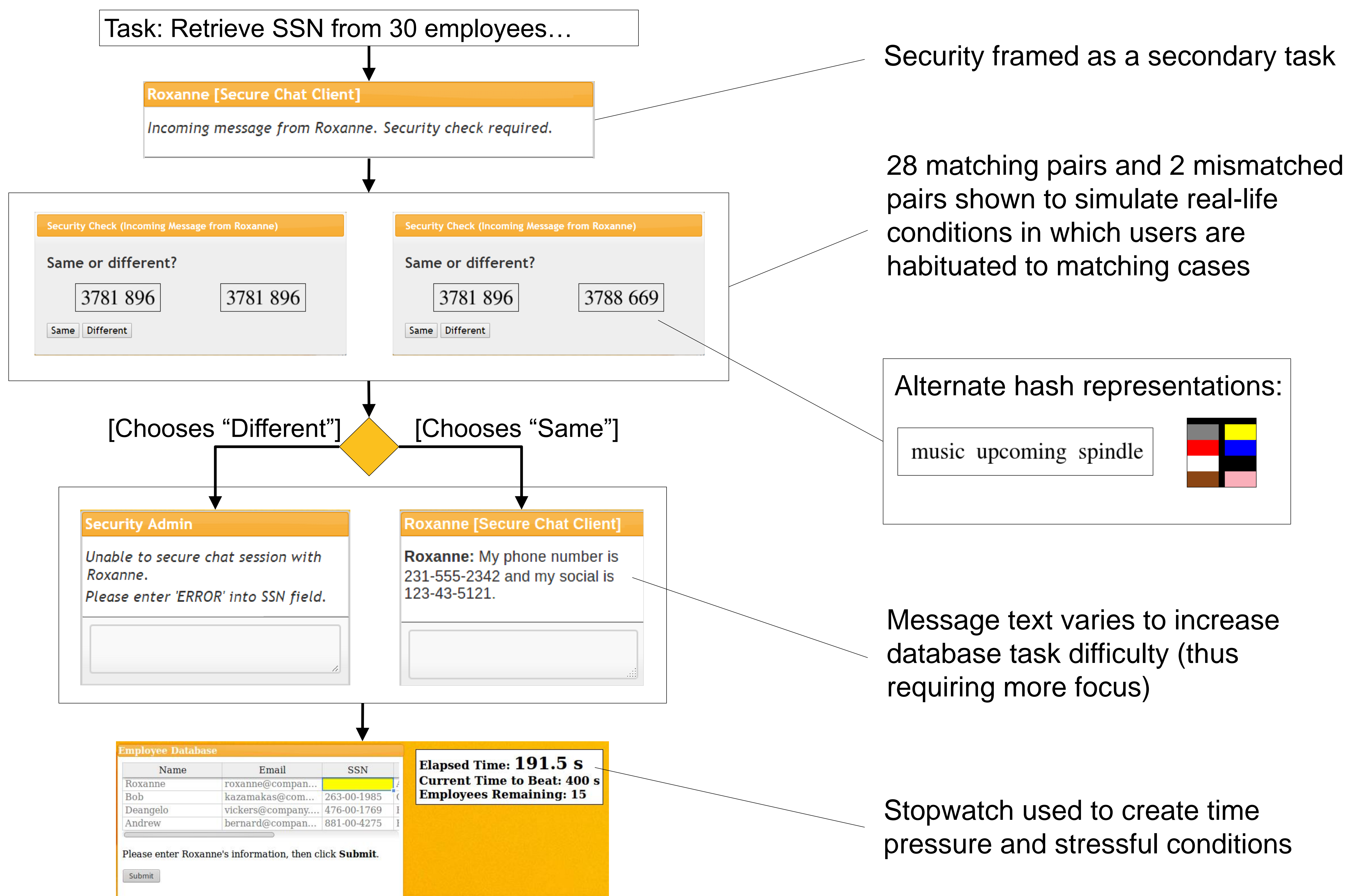
A Framework for Comparative Usability Studies on Secure Device Pairing

Achal Channarasappa, Pranita Ramakrishnan, Joshua Tan, Jeremy Thomas

Motivation

- Device pairing methods can be used to establish secure communication channels
- These methods often require visually comparing a pair of hash representations
- Different pairing methods may vary in usability (time required, accuracy of comparisons)
- Comparative studies on pairing methods may have diminished ecological validity if pairing is the primary focus

Experimental Framework



Future Work

- Add support for additional types of factors
 - User interaction mode (e.g., Compare & Select)
 - Incorporate multiple devices (e.g., smartphones)
 - Representation variations (e.g., fonts)
- Modify activity to facilitate usability studies on public key fingerprint verification methods

