

Grand Challenge #4

Preserving Individual Agency in Cyberspace

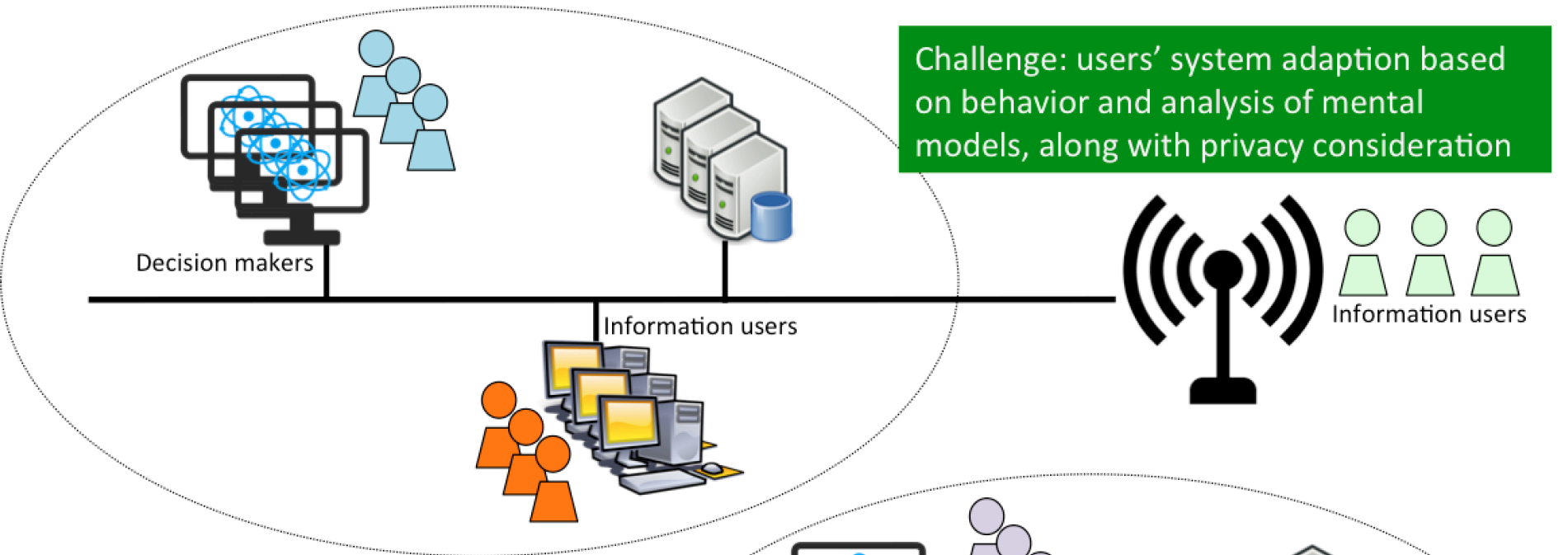
Shuyuan Mary Ho

Florida State University

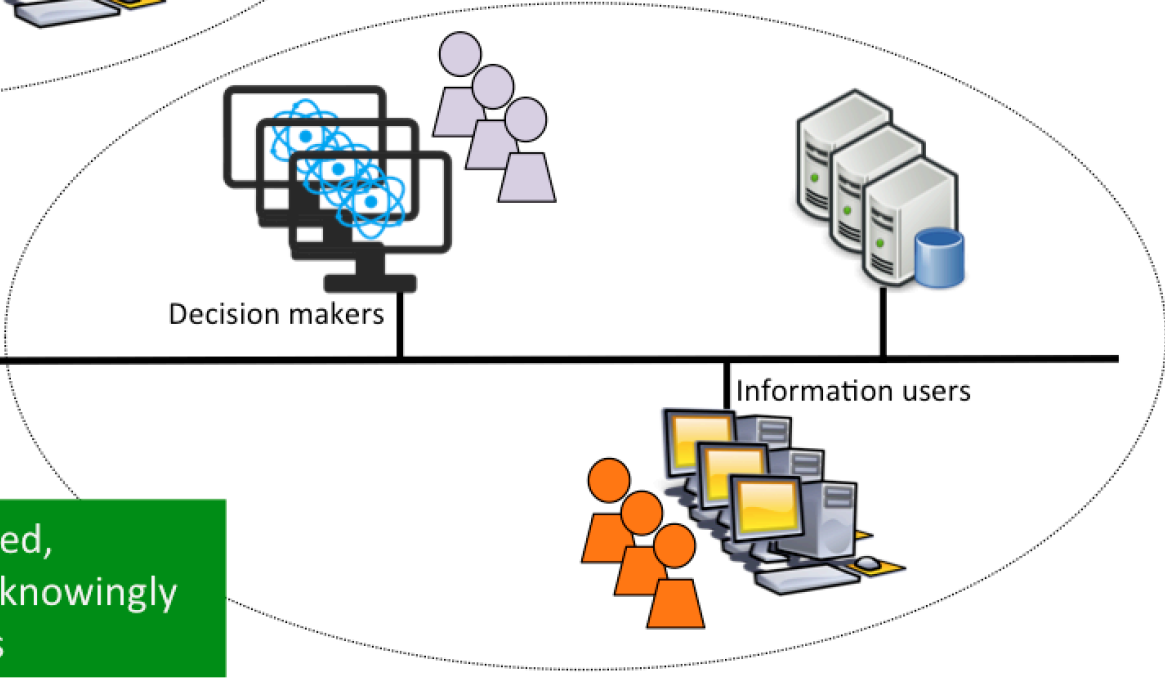
Executive Summary

- Incorporation of human activity in systems design
 - requires consideration of mental models accompanied with various abilities, cognition, situation awareness, and simultaneously the preservation of privacy.
 - Key agents:
 1. Decision makers e.g., C-suites officers, administrators
 2. Information users
 3. Adversaries

Challenge: users' system adaption based on behavior and analysis of mental models, along with privacy consideration



Challenge: users' personal data captured, intercepted and owned by others—unknowingly susceptible to comprise by adversaries



Grand Challenge

- Is it possible to attain *seamless cybersecurity*?
- The design and development of a usable infrastructure requires considerations of privacy, usability of information, as well as information integrity, control and assurance.
- This grand challenge requires HCI research and experimentation to investigate the identification and incorporation of the **mental models** into **systems design** and **development**.
- These models include personalization, usability and accessibility to foster and enable communication while guarding against the possible penetration of adversaries with authorized access.

Grand Challenge

- How do we incorporate and augment communication in systems infrastructure that can assist in systems development and usability design to meet the collective and individual needs of human agents with many varieties of **technical**, **cognitive**, **sensory** or **physical** abilities, while at the same time **preserving privacy** as personal data is banked by a 3rd party agency, with a notion to incorporate preventive mechanisms against the possible threat of the **conversion of human agents** from trusted users to adversaries?

Recommendations for Research Agenda and Research Program

1. The usability and useable security considerations of systems' adaptation that incorporate various **mental models** at *technical*, *cognitive*, *sensory* and *physical* domains to address the problems of identifying **negligent users** and **human errors** against **phishing attacks**, as well as **unintentional consequences** from mis-utilization of the systems.
2. The governance of information should consider the **seamless credibility** of individual entities. As personal data is being collected by the organizations (whether in the cloud-based or proprietary environment), sensitive and elevated consideration of individuals' rights, ownership and quality of information should be included and modeled so as to ensure and preserve privacy against the **monitoring threats by the ill-intentioned adversaries**.