Grand Challenge

Empower users to make informed security decisions that are visible, controllable, and understandable while maintaining trustworthy and autonomous agency

- Problems: User are forced to make security decisions without appropriate information, and security suggestions are made without understanding of users' context and abilities
- Difficult?
  - Lack of appropriate understanding of the consequences of security actions
  - Difficult to gauge user intent
  - No one-size-for-all approach
  - Limited cognitive resources
  - Security is secondary and conflicting to primary tasks
  - Security threats are ubiquitous (IoT, fake news, social media disclosure)

- Barriers:
  - Users do not adopt security behavior
  - Do not understand contextual factors
  - Insufficient communication of consequences of security action
  - Environmental cues are noisy, complex and abstract
  - IT makes security a primary task
- Progress possible?
  - Machine learning algorithms (e.g., nudges and recommender systems) allow
    - Security to be personalized to users
    - model contextual factors
  - Mental models/ interventions empower users to make informed decisions
  - Ability to create interactive social systems to facilitate cooperative and stewarded actions (e.g., allow experts to help non-experts)
  - Identification of cues from the environment
  - Identification of specific user “strengths”

- People?
  - Lorrie Cranor
  - Rick Wash
  - Emily Rader
  - Angela Sasse
  - Jason Hong
  - Gordon Hull
  - Bart Knijnenburg
  - Jim Blythe
  - Sauvik Das

- Research Programs?
  - To encourage users to think and adopt security behavior (against phishing, fake news on social media, application permission, password, IoT security adoption) at every level (individual, organizational, societal)
  - Human-in-the-loop security/ variable autonomy security
  - Grassroots effort on shared responsibility and security norms at societal or national level