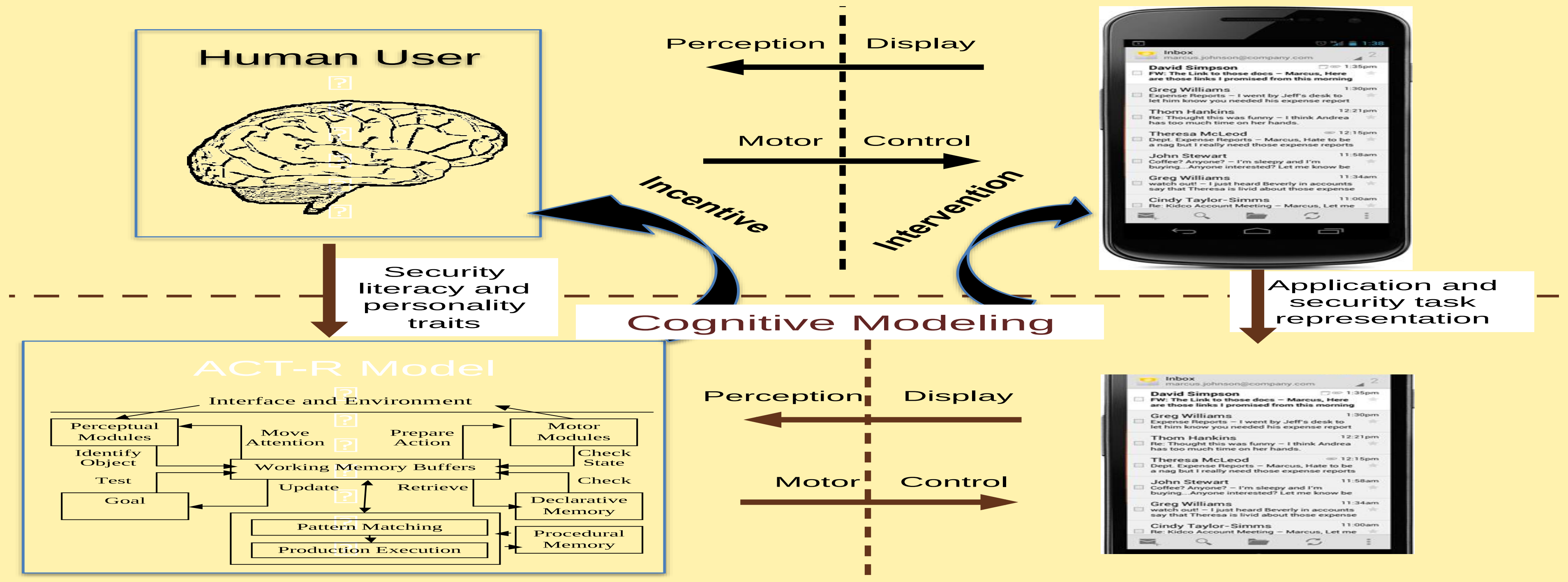
Modeling Security/Incentive Behaviors

Anton Dahbura, Xiangyang Li, Johns Hopkins University Information Security Institute

Nathan Bos, Johns Hopkins University Applied Physics Laboratory

- Analytical Cognitive Modeling (CogM) architectures can effectively capture user security behaviors, as well as the mechanisms of incentives and interventions
- In so doing, they promote designs tuned to human's sometimes sub-optimal or irrational preferences and tendencies.



Approach

- ***Benchmark Cognitive Modeling Architectures for Security Behavioral Modeling***
- ***Augment Security and Incentive Modeling Capabilities***
- ***Model Users in Single Task and Multi-Tasking Security Applications***
- ***Calibrate and Validate Cognitive Security Modeling with Human Subject Testing Studies***

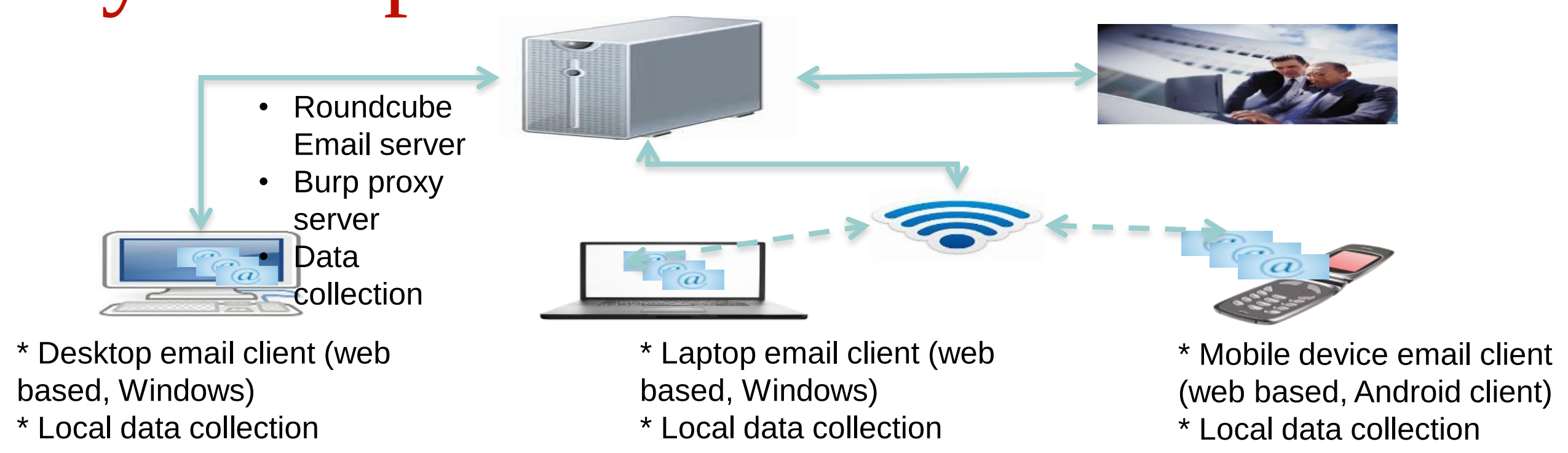
Modeling Methodology Study

- A higher-level model, which takes advantage of existing CogM constructs, is determined to be critical to the success through a literature review.
- Incentives and interventions are modifications to realities of production rules, knowledge chunks, and their associated semi-symbolic values.

A Pilot User Study

- 10 participants went through 40 emails through think aloud method.
- PC and mobile clients were used.
- Data collection was tested for classification effectiveness and platform difference.

Empirical Study Set-up


Roundcube Email server
Burp proxy server
Data collection
* Desktop email client (web based, Windows)
* Local data collection
* Laptop email client (web based, Windows)
* Local data collection
* Mobile device email client (web based, Android client)
* Local data collection

An User Study on Intervention and Incentive

- Participants classify emails of three phishing tells.
- Targeted training based on performance is given.
- Financial reward is introduced in treatment group.

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11th 2017
Arlington, VA

JOHNS HOPKINS UNIVERSITY