University at Buffalo
Department of Industrial and Systems Engineering
School of Engineering and Applied Sciences

Ph.D. Dissertation Defense

Mental Models for Cybersecurity: A Formal Methods Approach

Adam M. Houser, Candidate

Failures in complex systems often result from problematic interactions between different system components, including human users. Furthermore, system complexity means that designers may fail to anticipate component interactions, particularly where rare and undesirable human-automation interaction can significantly impact safe and effective system operation. Problematic and often unanticipated interactions may be driven in part by the mental models of system users, where incongruencies between user mental models---which can drive the actions users take within a given system---and functional system characteristics can lead to unsafe or inappropriate operational states. The ramifications of these incongruencies are particularly important for cybersecurity, where unanticipated system states can lead to software vulnerabilities, data leaks, or system failure.

While human factors engineers have developed powerful methods for exploring the performance of complex systems, traditional strategies for investigating human-automation interaction can be difficult to use, time-consuming, and may not be robust to the discovery of unanticipated events. One potential solution is the use of formal methods, a well-defined collection of mathematical languages and techniques used to prove whether system models do or do not support desirable properties. The exhaustive statespace search capabilities of model checking, a formal methods technique, can help analysts identify system conditions regardless of their rarity.

Our work extends formal mental modeling techniques with cybersecurity-specific concepts and computer security folk models to explore and discover unanticipated human-automation interactions resultant from mismatches between mental models and system characteristics that can lead to computer security failures. Two cases are used in this investigation. The first explores configuration errors committed by users of a popular cloud data storage service, using a formal modeling framework to explore the actions that users take and describe the vulnerabilities of users with certain mental models to particular security configuration settings. The second case extends the initial generic framework by integrating folk modeling concepts in cybersecurity applications. We investigate a phishing email attack example, then use our findings to describe how users with different folk models could commit potentially dangerous actions depending on threats posed by malicious emails.

In this dissertation, we describe our method and demonstrate its capabilities using both cases described above. We also discuss our research contributions and explore possibilities for future research.

Date | Time | Place: **Friday, May 25th, 10:00am, Bell 341**

Committee: **Matthew L. Bolton, Ph.D. (Chair); Ann M. Bisantz, Ph.D.; Jun Zhuang, Ph.D.**