Quantitative Security Metrics with Human in the Loop

Mohammad Noureddine, Ken Keefe,
William H. Sanders and Masooda Bashir
University of Illinois at Urbana Champaign

Motivation

- Human users are regarded as the weakest link in cyber-security (95% of security incident involved human error)
- HCI and usable security: design human centered security systems
- Attackers are still making use of human vulnerabilities to compromise systems

Research Goals

- Understand the behavior and decision making of human users
- Identify the variables affecting human behavior and decision making
- Accurately model the behavior of human users in the context of cyber-security
- Develop a simulation tool to incorporate system models, human models as well as adversary models
- Develop case studies to evaluate our models and the underlying tool

Human Behavior

- Users often do not consider themselves to be at risk
- Security is not a priority for users; people tend to sacrifice security in favor of performance
- Home and work conditions affect people's ability to make sound decisions
- Some cognitive and personal factors also have important on people's decisions
- Some variables affecting security decision making:

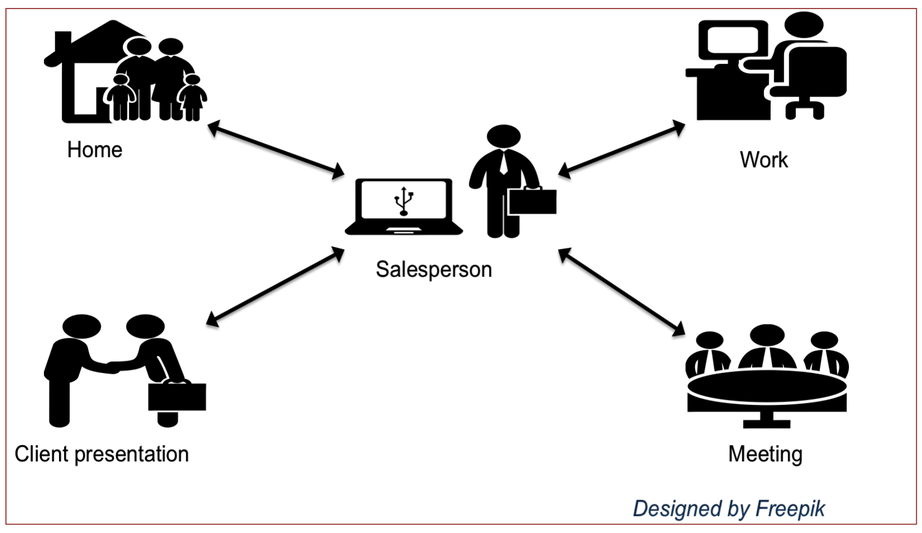
Category	Variables
Business process and environment	Experience; training; duties; security policy; workload; email load; security culture; deadlines
Cognitive factors	Risk and security assessment; stress; fatigue; lack of attention
Personal factors	Age; culture

HITOP

- Human-Influenced Task-Oriented Process (HITOP) formalism
- Modeling formalism for rational human decision makers (users, system administrators, etc.)
- Human participants make security decision by maximizing local utility
- Utility functions includes variables representing training, experience, positive work experiences, etc.

Case Study

- We are modeling an engineering firm trying to protect important information assets using HITOP
- Participants are engineers, customer representatives, sales representatives and system administrators
- An attacker will try and exploit human vulnerabilities to compromise the firm's assets
- For example, a salesperson moves information between home, work, client presentations and corporate meetings, as shown below



Future Work

- Relax the rational behavior assumption in HTIOP
- Develop a more accurate model of human behavior and decision making
- Incorporate such models into the Mobius framework, a tool for modeling and simulation of complex systems
- Design more case studies to evaluate our approach

http://hot-sos.org/

The Science of Security initiative is funded by the National Security Agency.