Human-aware Science of Security

M. Bashir, K. Keefe, M. Noureeddine and W. Sanders
The Science of Security

• Current state of security research
  1. Find a vulnerability
  2. Fix it!
  3. Introduce a new vulnerability or find another one
  4. Fix it! Go to 3.

• We need to study cyber security as a science
  – It’s not just a practice

• We need to model and analyze security systems
  – How secure is a system? Under which conditions?

• Design systems that are resilient to known as well as unknown threats or attacks
The Problem

• According to the IBM security services report (2004), 95% of investigated security incidents involve human error.
• Human users are regarded as the weakest link in the cyber security loop
• “The problem exists between the chair and the keyboard” (PEBCAK)
• We need to design and evaluate security systems with humans in the loop
• An area often understudied in design of security systems
In the Literature

• Two trends in human-aware security: Modeling and Usable security

1. Modeling:
   • Introduce a model of human decision in analogy with the central bank problem in economics [Beautement09]
   • Introduce security ontologies to define information and applications where human factors are vulnerabilities (based on some standards) [Parkin09]

2. Usable security: Design of human-centric security systems
   • Researchers noted usability issues since 1975 (Saltzer and Schroeder: “psychological acceptability”)
   • Most of the work focused on authentication and email encryption
Our Approach

• Include models of human decision making in models of security systems
• Evaluate the security (as well as performance) of systems in light of the uncertainty of human behavior
• Current research: Human Influenced Task Oriented Process (HITOP) formalism
• Goal: Use techniques from human factors, behavioral economics, human computer interaction (HCI), to design accurate models of human behavior
Human Influenced Task Oriented Process (HITOP)

• We defined the HITOP\cite{Eskins11} formalism
  – Model human actions as a set of tasks
  – Assumption: Humans tend to maximize local utilities
  – Define “human decision points” (HDP) where human decisions are important
  – In a HDP, human either willing to perform security action or not
  – Willingness related to local utility function\cite{Eskins11}

• We are looking to evaluate the accuracy of HITOP in modeling human decisions
Case Study

• We will evaluate HITOP through a model of a nuclear power plant, influenced by Stuxnet
Methodology

• Investigate literature in usable security, human factors, human computer interaction, etc.
• Determine the variables that alter human behavior in favor of poor security decisions
• Devise a model that allows us to simulate such decisions
• Design a system model, an attacker model and a human user model
• Use a simulation tool (Mobius) to evaluate the security (performance) of the system in light of all these variables
Relation to SoS

• Understanding and studying security systems is incomplete without considering human factors

• Understanding and modeling human behavior can help in
  – The assessment of the security of implemented systems
  – The design of new systems that are resilient to threats introduced by human elements
References

