Computer Security for the Home User

Adele Howe, Indrajit Ray and Zinta Byrne

National Science Foundation
WHERE DISCOVERIES BEGIN

Colorado State University

The home computer user is an important but poorly understood factor in computer security. Most security strategies are not as effective as they might be because they are not tailored to a user's perceptions and needs and may exceed the users' resources (time, money, knowledge).

Psychology

Relatively little is known about how home computer users view security threats and their own risk and how their perceptions influence their behavior. Our subjects studies assess factors that influence user behavior in security situations.

Policy Capturing Study

Approach:

- Assessed users' responses to security threats:
  - availability,
  - integrity,
  - confidentiality,
  - unwitting accomplice

- 16 on-line vignettes
- 60 young adults (18-29 yrs) & 44 older adults (50+ yrs)
- Asked about perceived risk, vulnerability and intention to click on links

Findings:

- All threats increased ratings of risk and vulnerability
- More computer knowledge led to weighing integrity threats more
- Gender & age influenced perceptions of risk
- Subjects' recognition of vulnerability in high threat conditions resulted in lower intention to click on links

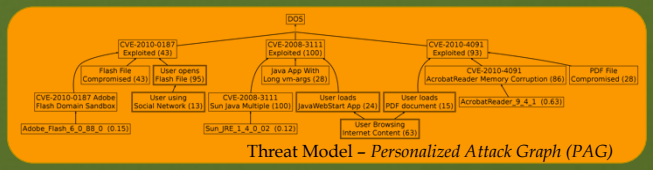
Studying how people view their security vulnerability and risk

Current/Future Work in Psychology

- Pilot interview study of common computer activities, perceptions of threats and demographics
- Study of trade-offs people consider in deciding to engage in Internet activities and insecure behaviors
- Simulation study of in situ user behavior to see whether results vary and to expand types of scenarios

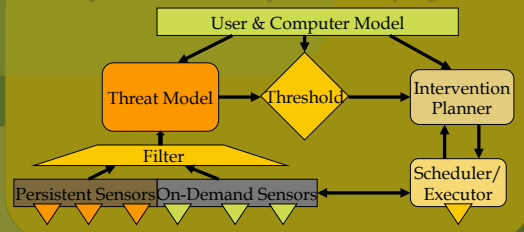
Security

Personalized Attack Graphs (PAG) extend the attack graph to model single computers and their users. Nodes represent system state (vulnerability status, computer configuration, changes due to user/attacker actions) and have a conditional probability given its predecessors. Edges model state transitions.

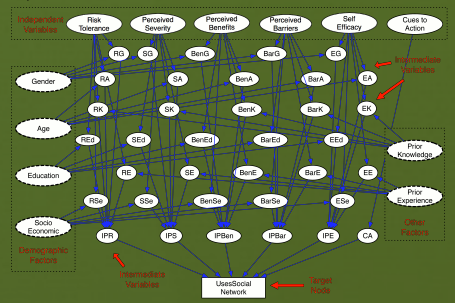


Threat Model – *Personalized Attack Graph (PAG)*

Proposed Home Computer Security Agent



User studies (ours and others) identified how different human characteristics influence user activities that lead to more or less secure systems.
A *Bayesian User Profile* relates the factors to compute probability of actions. The probabilities are computed when a PAG is instantiated for a user/system. Our model is based on Chester Claar's model of home computer users (2011 Ph.D. thesis at Utah State).



Computing Probability of User Reading Email

Artificial Intelligence

Attack paths are the possible ways a system can be compromised. Threats are modeled as the paths from leaves to root in our PAG.
Goal: Find multiple attack paths
Approach:

1. Convert the PAG to PDDL, a planning language
2. Create algorithm to generate *all alternative* attack paths

Our algorithm (S-A*) finds multiple attack paths of increasing complexity.

Study: Algorithmic Trade-offs in Generating Alternatives

Procedure:

1. Implement 4 algorithms: state based A*, action based A*, hybrid and random walk
2. Run on 5 benchmark domains
3. Compare on coverage, solution diversity, search cost and solution quality

Findings:

Coverage: All produce unique solutions

Diversity: RWS and HS-A* produce the most diverse solutions

Search Cost: H-A* finds solutions faster, all algorithms find best results early

Quality: A*s produce the best quality

Planning for identifying likely threats & promising interventions

Current/Future Work in AI

- Incorporate security quality metrics:
  - Cost of attack
  - Likelihood of Attack
  - Cost of intervening
  - Utility of performing suspect action
- Search over a Pareto front of attack paths
- Extend to generating interventions
- Design home computer security agent

Current/Future Work in Security

- Automated generation of PAG
  - Reduce errors and improve timeliness of updates
  - Information extraction using machine learning to generate patterns
- Intervention strategies
  - Actions to prevent or repair security breaches that take into account
    - the user's desired level of security and utility
    - results of psychological studies

Systematizing knowledge of user factors that influence behavior & personalizing security to match actions to each user/computer

Recent Publications

"The Psychology of Security for the Home Computer User" 2012 IEEE Symposium on Security & Privacy
"Perceptions of Internet Threats: Behavioral Intent to Click Again" 2012 Society for Industrial & Organizational Psychology Conference
"Using Planning for a Personalized Security Agent" AAAI-2012 Workshop on Problem Solving Using Classical Planners

Graduate Students

Current: Mark Roberts, Margozata Urbanska, Kyle Sandell
Past: Kyla Dvorak, Joshua Liff, Janet Weidert

http://www.cs.colostate.edu/psysec/