SPICE: A Software Tool for Bridging the Gap Between End-user's Insecure Cyber Behavior and Personality-traits

Anjila Tamrakar(atamraka@uno.edu), Justin D Russell(jrusse10@iastate.edu), Irfan Ahmed(irfan@cs.uno.edu), Golden G. Richard III(golden@cs.uno.edu), Carl F. Weems(cweems@iastate.edu)

Greater New Orleans Center for Information Assurance at the University of New Orleans

Introduction

Problem:

- For security purposes, technical controls alone are insufficient due to human role.
- People can be misled to perform activities that make their system vulnerable to attacks.
- no proper tool to study the variations of insecure cyber behavior across individuals with different personality traits.

Motivation:

- Recognition of characteristic personality trait such as trait anxiety and unemotional callousness assists in understanding the threat in cyber system that arise from user behavior
- Helps leveraging a number of fields such as identification of incentives, anti-habituation mechanisms, discovering motivators of insider threat etc.

Solution:

- A flexible tool "SPICE" to explore relationship between cyber security and personality trait that can add to improve security posture.

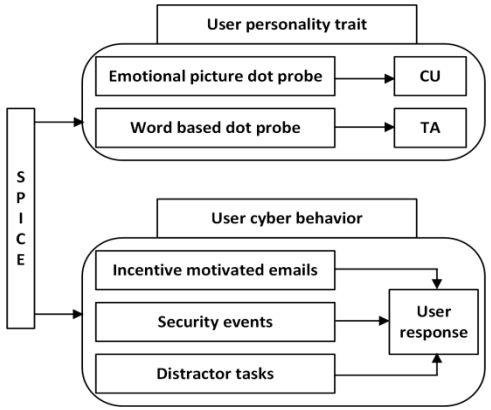
Goal:

- psychometric analysis of insecure end user behavior

How?

- study two sides: cyber behavior and personality trait of end user

System Overview



CU – callous unemotional trait

TA- trait anxiety

Phase I : User personality trait

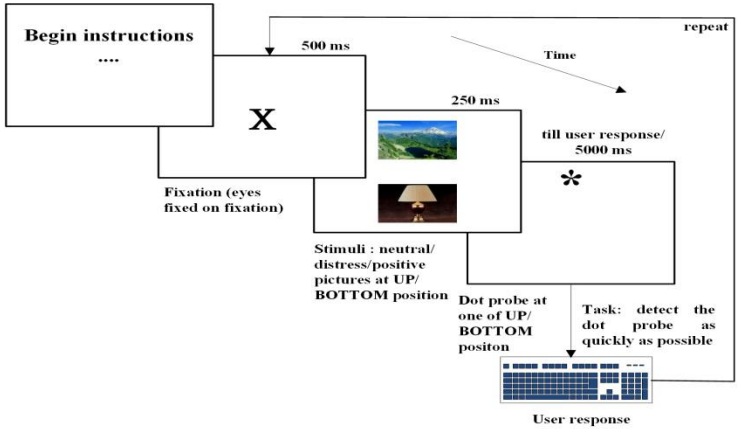


Figure 2: Emotional picture dot probe

Possible picture pairings: neutral-positive/distress and vise-versa, neutral-neutral

Measures:

- Distress Attentional Facilitation Index
- Positive Attentional Facilitation Index

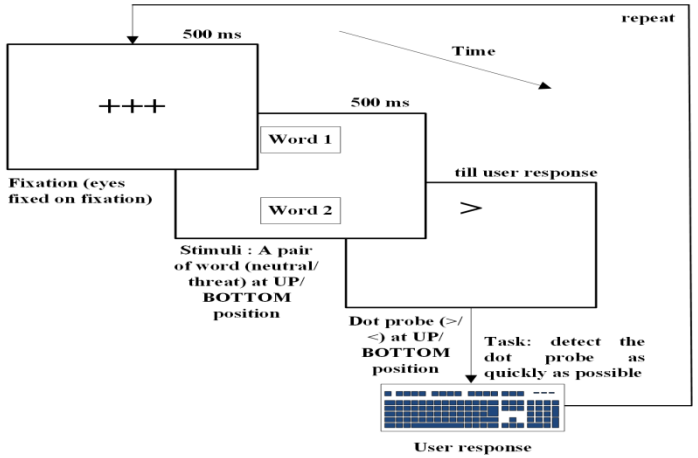


Figure 3: Word based dot probe

Possible word pairings: neutral-threat and vise-versa

Measures:

- Threat Bias Index

Phase II : User cyber behavior

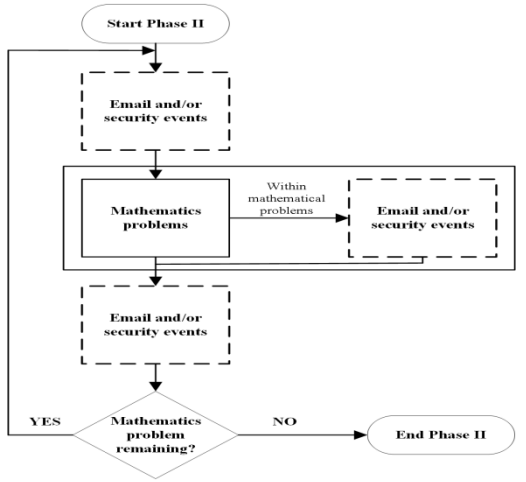


Figure 4: Abstract flow diagram of phase II

- Dotted rectangular box represents may or may not occur events
- Mathematical task act as distractor task
- Emails and/or security events may appear before, after and/or during each mathematical problems

Security events:

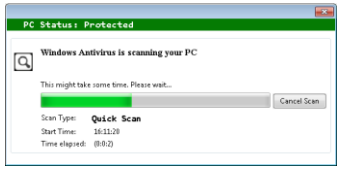


Figure 5: Anti-virus scan

Capture end user's intent towards anti-virus scan

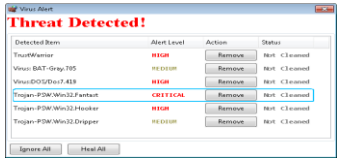


Figure 6: Virus alert

capture how end user acts with informed severity level of virus

Figure 7: Java update

Capture end user software update habits

Phase II : User cyber behavior

Security events:

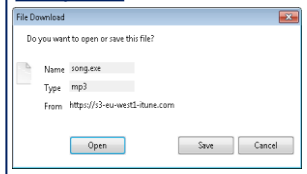


Figure 8: Download interface

Capture end user un/attendance during download

Email:

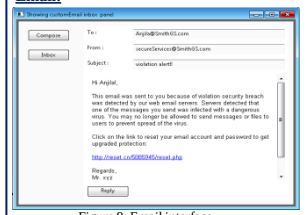


Figure 9: Email interface

Capture propensity to be victim

- SPICE captures cyber user behavior through basic but tangible simulated system events

Pros and Cons

Tool Flexibility:

- Human readable tag based scripts
- Easy customization and manipulation of experiment as required

Benefits:

- First tool to have psychological measure and cyber behavior integrated in same software
- Can be used for large scale data collection
- possibilities of various novice study from the data captured during experiment
- Cost minimization as no hardware is used for psychometric analysis

Limitation:

- Not an online tool
- Limited pool of user interfaces that can be chosen to use in experiment
- No analysis on collected data, experimenter needs to analyze the data himself

SPICE – Software Package for Investigating Computer Experiences