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

Anjila Tamrakar[1], Justin D. Russell[2], Irfan Ahmed[1], Golden G. Richard III[1], Carl F. Weems[2]
[1]University of New Orleans, 2000 Lakeshore Dr. New Orleans, LA - 70122
[2]Iowa State University, Ames, IA - 50011
atamraka@uno.edu, jrusse10@iastate.edu, {irfan, golden}@cs.uno.edu, cweems@iastate.edu

## ABSTRACT

End users are prone to insecure cyber behavior that may lead them to compromise the integrity, availability or confidentiality of their computer systems. For instance, replying to a phishing email may compromise an end user's login credentials. Identifying tendency toward insecure cyber behavior is critically important to improve cyber security posture and thesis of this paper is that the susceptibility of end-users to be a victim of a cyber-attack may be predicted using personality traits such as trait anxiety and callousness.

This paper presents an easily configurable, script-based software tool to explore the relationships between the personality traits and insecure cyber behaviors of end users. The software utilizes well-established cognitive methods (such as dot probe) to identify a number of personality traits for a user and further allows researchers to design and conduct experiments through customizable scripting to study the end-users' insecure cyber behaviors. The software also collects fine-grained data on users for analysis.

## Keywords

Software Psychology; Personality traits; computer security; Human factor; Test-bed

## 1. INTRODUCTION

Current efforts on improving the secure cyber behavior of end users are mostly limited to education, training, and awareness campaigns that do not tend to have long-lasting impacts on user behavior. Technical controls are also enforced to improve certain aspects of user behavior, such as maintaining strong passwords and the use of encryption, but these have no impact on other issues, such as effectively preventing users from responding to phishing emails, or downloading and running executable from anonymous sources.

A first step to an effective solution is to study end users who have greater tendencies toward insecure cyber behavior. In particular, exploring any reliable relationship among personality traits and cyber behavior of end users can help in developing user-centric mechanisms for maintaining their proper cyber security postures. For example, automatically generating variants of user interfaces and alerting systems that tap individual psychological traits might prevent users from engaging in insecure cyber behavior unintentionally.



*CODASPY'16 March 09-11, 2016, New Orleans, LA, USA*



ACM ISBN 978-1-4503-3935-3/16/03.
DOI: http://dx.doi.org/10.1145/2857705.2857744

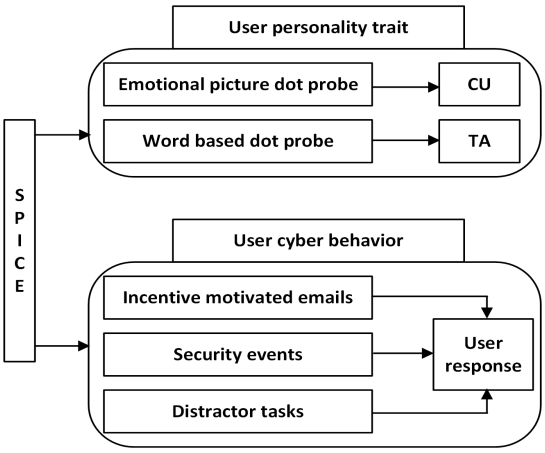


**Figure 1: Overall architecture of *SPICE*.**

In this paper, we propose SPICE (Software Package for Investigating Computer Experiences) - a script based, easily customizable research tool for acquiring data on an end-user's personality traits, and (in)secure cyber behavior. As shown in Figure 1, SPICE currently utilizes dot-probe tasks to identify two personality traits, trait anxiety (TA), and callousness unemotional trait (CU). It further creates a multistage simulated scenario (using configuration parameters, and customizable scripts) involving both distraction and routine tasks such as accounting, monitoring of stock rates, responding to an email, and updating software. Some tasks allow a user to opt into an insecure behavior such as providing a web link in an email to click. To the author's best knowledge, SPICE is the first tool designed to study the relationship between personality traits and cyber security behavior of end users.

## 2. PERSONALITY TRAITS

### 2.1 Anxiety and Callousness

Psychology researchers note that degree of attention and preferential biasness towards visually presented stimuli are associated with personality traits [4] such as TA and CU that may be important risk or protective factors in cyber

security. A consistent finding in psychology proposes that individuals who tend towards CU traits are more likely to commit cybercrimes as a result of lacking sympathy for victims or personal connections with an organization [2]. Similarly, TA may be a vulnerable factor in users succumbing to attacks such as social engineering, given links between anxiety and neuroticism. On the other hand, TA also may be a protective factor in improving rule-following and conscientiousness.

Personality traits have been widely studied with standardized sets of self-report and interview based questions. Predispositions for attending to, processing, and biasness towards stimuli can be identified with dot probe technology.

## 2.2 Dot Probe Task

This method [3] involves presentation of a fixation symbol ("X") at the center of the computer screen, then simultaneous presentation of stimuli (e.g. a pair of picture, words) on the computer screen (e.g. one on the top, one on bottom), immediately followed by removal of stimuli and presentation of a probe (e.g."*" or "<" / ">") in the location of one of the stimuli. The theory behind this assessment technique is that the faster the probe is detected, the more likely the participant was attending to the stimulus that was located in the same position as the probe. Therefore, shorter probe detection latencies for one category of stimuli over another indicate a selective attention bias towards the category with the shorter probe detection latency. Biases in the selection of attention cause individual differences in emotional vulnerability and are usually used in determining callous unemotional trait and trait anxiety. The main purpose of this task in our software architecture is to collect the independent variable attentional facilitation and threat bias index.

### 2.2.1 Emotional Picture dot probe task

The stimuli presented in this task are pictures representing distress, positive and neutral content with possible stimuli pairings: neutral-neutral, distress-neutral, positive-neutral. Callous-unemotional individuals have been shown to demonstrate shorter detection latencies for images of pain, distress and sufferings than non-callous individuals. The distress and positive facilitation index is calculated as follows:

Distress Attentional Facilitation Index

$$(Y) = 1/2[((N\uparrow) - (D\uparrow)) + ((N\downarrow) - (D\downarrow))] \quad (1)$$

Positive Attentional Facilitation Index

$$(Y) = 1/2[((N\uparrow) - (P\uparrow)) + ((N\downarrow) - (P\downarrow))] \quad (2)$$

Where, N $\uparrow$ = only neutral picture appear on the screen, with the dot probe behind the top picture (Probe top); D$\uparrow$= distressing picture on top, probe on top; N$\downarrow$ = only neutral picture appear on the screen, probe on bottom; D$\downarrow$= distressing picture on bottom, probe on bottom; P$\uparrow$= positive picture on top, probe on top; P$\downarrow$= positive picture on bottom, probe on bottom.

*All variables are mean response time

The distress/positive attentional biases are the mean latencies to detect probes that appear in the location of the neutral picture to the location of the distress/positive picture and indicate a bias to attend to distress/positive content respectively. The task consists of a block of practice stimuli (16 picture pairs) followed by 4 blocks of test stimuli (24 picture pairs each). The user is assisted to take a break between each block.

### 2.2.2 Word based dot probe task

The stimuli presented in this task are a pair of words of negative and neutral type, in a vertically aligned fashion succeeded by presentation of fixation ("+++") and followed by probe (">" or "<") at the location of one of the word pair. Individuals with anxiety have shorter probe detection latencies for mild threat stimuli (a word like 'fear'). The task consists of the practice block (10 pairs of words) followed by two blocks of 96 pairs of words each. The threat bias index (TBI) is calculated as follows:

Threat Bias Index

$$(Y) = ((NT) - (T)) \quad (3)$$

Where, T= median response time to probes presented in the position of the threat word; NT= median response time to probes presented in the position of the non-threat word.

# 3. INSECURE CYBER BEHAVIOR

Simulating a real world environment is crucial to capture user behaviors in a related, immersive scenario. However, simulating every aspect of a situation is obviously impossible. Instead of simulating everything, we designed our tool to capture a user's cyber behavior in the context of general but important security related activities that can capture user's intentions to harm others/take risks/be secure/be meticulous. We present users with the hypothetical situation that they are acting as a new employee in an accounting firm after having a similar experience in another company. We present a multi-tasking environment where user has to participate in various parallel tasks listed below:

1. Solve accounting problems (mathematics problems)
2. Monitor stock prices of competitors' companies and respond to market updates
3. Attend to emails and respond as quickly as possible
4. Attend to various system-related security events, such as software updates, antivirus scanning, etc.

These parallel tasks tend to keep the user busy and encourage their normal behaviors even in the testing scenario.

## 3.1 Mathematical problems

Mathematical problems are based on the established work by Hopko et al [1] and we present them as a distractor task to the user. As per our hypothetical situation, the more mathematical problems a user solves correctly, the more compensation is provided, which presents mathematical problems as a major task. Thus users are not aware of the intention to capture their secure/insecure cyber behavior. In the process of solving mathematical problems, other tasks (emails and security events) interrupt the user. The interrupting task may be related, such as emails that on responding may provide a hint to solve a subsequent mathematical problem, resulting in more incentive. Other unrelated task such as security events may also appear as interrupting tasks. Thus we provide an incentive-motivated environment but the user can opt to choose or not to participate in those cases.

## 3.2 Security events

SPICE present varying user interfaces related to security that tap users' knowledge and tenacity to victimize others/be victimized, maintain security postures like keeping

their system updated and safe etc. These user interfaces are presented before, after or during solving mathematical problems. Followings are the security events presented to the user:

1. Software updates like Flash update, Java update
2. Anti-virus scan
3. Virus alert
4. Drive by download

## 3.3 Emails

Email represents a strong communication factor in any working environment. We present emails of various nature ranging from company welcome emails to incentive-motivated emails and random advertising emails. The user response towards these helps us gather knowledge about the users' propensity to participate in potentially unethical behavior. For example: email from colleagues offering a link to hack other company illegally; emails from adversaries asking employees to reset their username and passwords; emails from random persons sending a link to receive reward etc. These clearly demonstrate user's intentions based on their actions and responses.

In our tool, we present the option to force a user to at least open the email but we leave all other decisions to the user. This can be employed to illustrate that emails are important; otherwise the emails may not be attended to at all, especially given our scenario where incentives are related to the mathematical problems that are presented.

## 3.4 Stock market ticker

We show a ticker displaying information about the stock market. The user may need to keep track of the stock market while solving the mathematical problems. This is one of the other distractor tasks used in our tool.

# 4. SOFTWARE CUSTOMIZATION

Customizability is one of important feature in SPICE. It is easy to modify the contents and manage flow of occurrence of different events for the design of the experiment.

## 4.1 Scripting

SPICE employs a tag-based, customizable scripting for configuring the experimental environment. A tag-based script follows the basic rules and patterns as shown below.

1. *<dot-probe>*
2. *<block>0</block>*
3. *<up> neu_img_1.jpg,neg_img_2.jpg, ...</up>*
4. *<up-type> Neutral, Neutral, ...</up-type>*
5. *<down> neg_img_1.jpg,pos_img_1.jpg, ...</down>*
6. *<down-type> Neutral, Neutral, ...</down-type>*
7. *<probe-position>Down, Up, ...</probe-position>*
8. *</dot-probe>*

Line 1 and 8 represents the start and end tag of dot probe. Line 2 represents the block number. Lines 3/5 represent the list of images to be shown in the top/bottom positions on the screen during the task while lines 4/6 are the types of images in lines 3/5. The tags used are predefined tags and in between the tags are content that is customizable by the user. We use a similar tag-based script for word-based dot probe, emails, and mathematical problems.

## 4.2 Event sequencing

In a simulated scenario, the tool allows managing the order of occurrence of different events. Flow order is maintained as a simple list as shown below that describes the order in which the emails, security events and mathematical problems are presented to the user.

*Flow-order*=["Email-120000", "M", "software-update", "virus-alert", "M", "Email-120002-f"]
*maths_sec_events*=[["flash-update", "Java-update"], ["Email-120003-f", "Email-120004-f","anti-virus-scan"]]

Where, $M$ = mathematical problem,
*Email-XXXXXX* = email with id XXXXXX from email script,
*Email-XXXXXX-f* = email with id XXXXXX from email script with force feature, and
*"software-update", "virus-alert", "flash-update", "Java-update", "anti-virus-scan"* are security events.

Security events and emails can occur before or after mathematical problems as depicted in *Flow-order*. Similarly, emails and security events can also occur within each mathematical problem, which is maintained in a separate variable as *"maths_sec_events"*. *maths_sec_events* is a double array that represents the event within each mathematical problem.

# 5. CONCLUSION

We have presented SPICE, an easily configurable, script-based software tool to explore the relationships between the personality traits and insecure cyber behaviors of end users. SPICE is designed to capture data detailing the personality traits and cyber behaviors of a large population of users, to create data sets that will be helpful in studying the variations of cyber behavior across different personality types.

# 6. ACKNOWLEDGMENTS

The authors would like to thank CNS-SaTC for the support by NSF-1358723

# 7. REFERENCES

[1] D. R. Hopko, D. W. McNeil, C. Lejuez, M. H. Ashcraft, G. H. Eifert, and J. Riel. The effects of anxious responding on mental arithmetic and lexical decision task performance. *Journal of Anxiety Disorders*, 17(6):647–665, 2003.

[2] E. R. Kimonis, P. J. Frick, J. L. Skeem, M. A. Marsee, K. Cruise, L. C. Munoz, K. J. Aucoin, and A. S. Morris. Assessing callous–unemotional traits in adolescent offenders: Validation of the inventory of callous–unemotional traits. *International journal of law and psychiatry*, 31(3):241–252, 2008.

[3] C. MacLeod, A. Mathews, and P. Tata. Attentional bias in emotional disorders. *Journal of abnormal psychology*, 95(1):15, 1986.

[4] S. P. Tipper and J. Driver. Negative priming between pictures and words in a selective attention task: Evidence for semantic processing of ignored stimuli. *Memory & Cognition*, 16(1):64–70, 1988.