University of New Orleans

ScholarWorks@UNO

University of New Orleans Theses and Dissertations

Dissertations and Theses

Summer 8-10-2016

SPICE: A Software Tool for Studying End-user’s Insecure Cyber Behavior and Personality-traits

Anjila Tamrakar
University of New Orleans, atamraka@uno.edu

Recommended Citation

Tamrakar, Anjila, "SPICE: A Software Tool for Studying End-user’s Insecure Cyber Behavior and Personality-traits" (2016). *University of New Orleans Theses and Dissertations*. 2236.
https://scholarworks.uno.edu/td/2236

SPICE: A Software Tool for Studying End-user's Insecure Cyber Behavior and Personality-traits

A Thesis

Submitted to the Graduate Faculty of the
University of New Orleans
In partial fulfillment of the
Requirements for the degree of

Master of Science
in
Computer Sciecne
Concentration in Information Assurance

by

Anjila Tamrakar
BS in Computer Engineering, Tribhuvan University, 2012

in the
Department of Computer Science

August, 2016

Dedication

This thesis work is dedicated to my mum and dad. Thank you for your love and constant support.

Acknowledgements

I am very fortunate to have graduate degree from The University of New Orleans, for which I would like to thank my supervisors Dr. Irfan Ahmed and Dr. Golden G. Richard, especially for their constant support and guidance throughout the study. They are the most incredible supervisors, mentors and motivators that I have ever met.

I would like to extend my appreciation to Dr. Carl F. Weems and Justin David Russell from Iowa State University, my mentor and coworker, whom I had opportunity to work and grow with. I would also like to thank my thesis committee member Dr. Adlai DePano for serving as a member of my thesis committee. His comments and guidance were very helpful to me during my writing.

To all my friends and family members, thank you for understanding and encouragments in many ways.

This work is only the beginning of my journey.

This research was supported by the National Science Foundation, Grant NSF-1358723

Contents

List of Figures

List of Tables

Abbreviations

SPICE	**S**oftware **P**ackage for **I**nvestigating **C**omputer **E**xperiences
CA	**Ca**llous Unemotional Trait
TA	**T**rait **A**nxiety

Abstract

Insecure cyber behavior of end users may expose their computers to cyber-attack. A first step to improve their cyber behavior is to identify their tendency toward insecure cyber behavior. Unfortunately, not much work has been done in this area. In particular, the relationship between end users cyber behavior and their personality traits is much less explored [27]. This paper presents a comprehensive review of a newly developed, easily configurable, and flexible software SPICE for psychologist and cognitive scientists to study personality traits and insecure cyber behavior of end users. The software utilizes well-established cognitive methods (such as dot-probe) to identify number of personality traits, and further allows researchers to design and conduct experiments and detailed quantitative study on the cyber behavior of end users. The software collects fine-grained data on users for analysis.

Keywords: Software Psychology, Cyber-psychology, Psychometrics, Personality traits, Cyber security, Human factors, Test-bed

Chapter 1

Introduction

End users are prone to insecure cyber behavior that may lead to compromise the integrity, availability or confidentiality of their computer systems. For instance, they turn off firewall, disable auto-patching software, or be the victim of social engineering attack (for phishing, drive by download etc.). The current efforts on improving the cyber behavior of end users are mostly limited to education, training, and awareness campaign that do not have long-lasting impact on user behavior. The technical controls are also enforced to improve certain aspects of user behavior such as maintaining strong password, use of encryption etc. but they cannot be applied generically such as to effectively prevent user to respond phishing emails, open suspicious attachments, or download and run executable from anonymous source. The challenge in securing such insecure point governed by end user's behavior is unique in that the focus is on applications used by end users and their renderings of user interface.

The authors believe that a first step to an effective solution is to study end users who have high tendency toward insecure cyber behavior. In particular, personality factors such as anxiety, and callousness may affect end user's cyber security behavior [25]. Thus, it is imperative to explore any reliable relationship among personality traits and cyber behavior of end users that can help in developing user-centric mechanisms for maintaining the proper security postures of end users. For example, automatically generating variants of user interfaces and alert system that tap individual psychological traits might prevent users from engaging in insecure cyber behavior unintentionally. This relationship is fruitful and allows us to understand factors involving high security-risk users who are prone to involve in insecure cyber environment on individual basis.

Unfortunately, current research has been both theoretically and methodologically limited [28] with no significant state of the art research linking personality and cyber security, and warrants more research efforts to understand the complex relationship between the deeply rooted aspects of the cyber security and psychology. Such research is often dependent on reliable software tools to conduct experiments on end users.

This paper presents a comprehensive review of SPICE (Software Package for Investigating Computer Experiences) a newly developed, script based, and easily customizable software tool that is capable of capturing personality traits and intriguing cyber behavior of end users. SPICE is designed and developed by the authors with the goal of allowing researchers to study the relationship of cognitive and personality factors with the cyber behavior involving the risk and propensity of either being victimized, or victimizing other individuals while using different software applications (such as email, flash etc.). This paper mainly illustrates the design and configurations of the tool.

To the authors best knowledge, SPICE is the first tool designed to study the relationship between personality traits and secure/insecure cyber behavior of end users. It provides a framework to conduct experiments in a graphical based environment. The research on the subject is particularly useful to adapt software interfaces, warnings, and messages in accordance with personality traits to improve the security posture of end users.

The rest of the paper is organized as follows: Chapter 2 explains the background while Chapter 3 describes the overview of the proposed tool SPICE. Chapter 4 details the methods of the identification of the personality traits of end users while Chapter 5 presents the description, and method of identification of insecure cyber behavior of the users. Chapter 6 discusses the customization features of SPICE followed by Chapter 7 that discusses the data captured by SPICE at its various phases. Chapter 8 presents the related work and Chapter 9 concludes our discussion on SPICE and also lists the future work.

Chapter 2

Background

Insecure cyber behavior results into the risk of information exposure, financial loss etc. McBride et al. noted that due to the substantial loss guided by the actions of insider employees, it is crucial to maintain the information systems and keep them on check [18]. This suggest us that there is relationship between the computer users, their behaviors, actions and the security vault of that system. The insecure behavior is defined as any event or action that has security related adverse effect in which there is loss of information confidentiality, disruption of information or system integrity, disruption or denial of system availability, or violation of any computer security policies. The end users prone to insecure cyber behavior may lead to compromise the confidentiality, integrity and availability (CIA Triad) of their computer systems. For instance, they turn off firewall, disable auto-patching software, or be the victim of social engineering attack (for phishing, drive by download etc.) which eventually results in violation of CIA Triad.

McBride et al. [18] also notes that only technical controls as a single measure being unsuccessful, many organizations use a range of behavioral controls such as security education, training, awareness campaigns (SETA) and so on to prevent insider abuse. The damage due to computer security misdemeanors is motivating people to take protective approach. The technical side to the security while is crucial, the computer security also depends upon the individuals security behavior. For example: In an organization, system administrators are responsible for most technical controls such as setting up firewalls and servers, but this alone is not comprehensive security approach. Users are responsible for practicing secure behaviors such as choosing and using appropriate passwords, use of encryption etc. Besides, technical controls are not effective in preventing users from variety of discrepancies like respond to phishing emails, open suspicious attachments or download and run executable from anonymous source etc.

Study of behavioral, personality and cognitive factors in the field of cyber security can contribute a lot towards cyber security. This interdisciplinary study lets researches better understand the risk in cyber systems that come from the behaviors and action of end users [18]. Thus, such related research and study can help leverage the field of cyber security in a number of ways including identification of incentives and anti-habituation mechanisms for maintaining proper security postures, discovering motivators, indicators of insider threat etc. Thus, it is imperative to explore any reliable relationship among personality traits and cyber behavior of end users that can help in developing user-centric mechanisms for maintaining the proper security postures of end users. For example, automatically generating variants of user interfaces and alert system that tap individual psychological traits that might correspond to learning and awareness and prevent users from engaging in insecure behavior unintentionally thereby reducing the effects of end user point cyber-attacks. Knowledge and techniques used in psychology can aid inherently towards understanding motivations in cyber-crime from attackers point of view while understand the characteristics of people having personality traits that mostly get victimized on the other side. The collaboration of these two divergent but yet related field may have potential to answer many interesting queries. For example: personality and characteristics profiling of a virus writer, analysis of virtual crime and so on.

For effective security, users need to make conscious decision and action. Security concerned users have an influential attitude and behavior towards being more security conscious. It is important to know what factors of users own the nature of personality that influence users security behavior. However, there is little theoretical grounded empirical research in the field of information security research on the behavior aspect of individual secure/insecure computer practices. Studying the end users, their personality traits and their underlying behavior towards cyber security can be an initial step towards solving the gap between understanding relation between cyber security and psychology.

Motivated by such needs to somehow narrow the gap, we tried to cultivate a prototype computing environment where the data necessary to study such can be generated. It is possible to gain more insights on those concerns only when a reliable and transparent tool is there that can provide reliable and validated output. Through this tool SPICE, we aim to contribute towards narrowing such gap by providing better tool and data (output of that tool) by applying psychometrics as supported by Haque et al. [8].

Chapter 3

SPICE Overview

Figure 3.1 illustrates an overall infrastructure of SPICE. It consists of two distinct phases: First phase identifies personality traits of end users, and the second phase examines the secure/insecure cyber behavior of end users. SPICE employs emotional picture dot probe and word based dot probe methodology to attend two personality traits: Callous Unemotional (CU) and Trait Anxiety (TA).

To evaluate user's cyber behavior, SPICE engages end user in a hypothetical scenario to perform several tasks such as checking emails, and solving accounting/mathematical problems. Furthermore, SPICE is configured to trigger number of cyber tasks involving decision-making on user side for depicting cyber behavior. The tasks include running antivirus scan, ignoring phishing emails, and respond to virus alerts. SPICE captures the user's responses in the background.

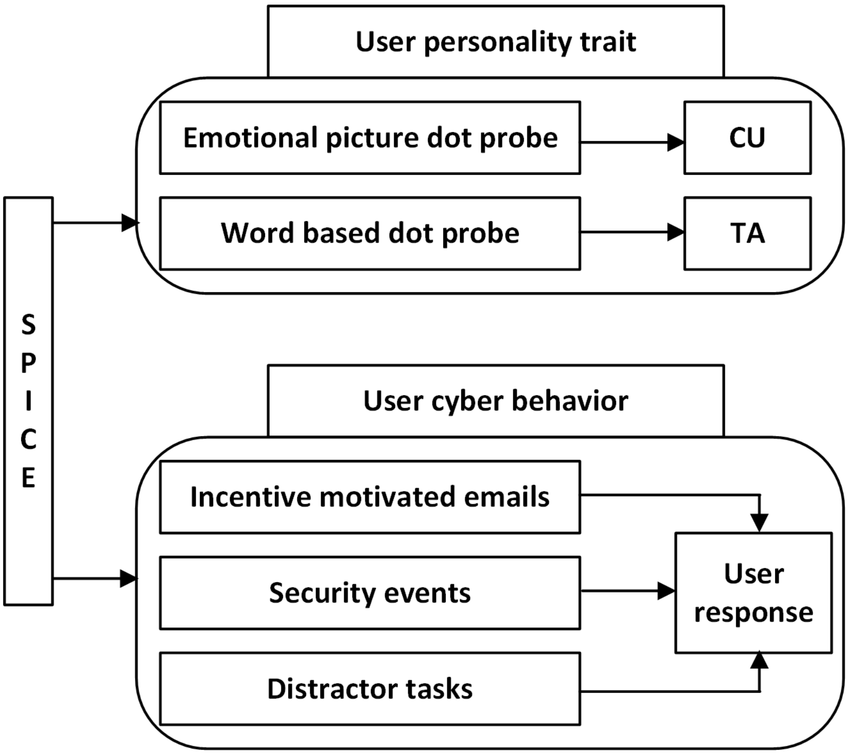


Figure 3.1: Overall architecture of *SPICE*.

Chapter 4

Identification of Personality Traits of End Users

A consistent finding in psychology is that people vary in their preferences and degrees of attention paid to visually presented stimuli which prime behavioral action and memory. Detection of these preferences and responses can be measured by latencies in responding to a visual stimuli presented via a graphical user interface. These latencies are associated with personality traits such as TA and CU. The major work of this paper is based on the principle idea that there are particular cognitive preferences and personality factors that may be associated with secure/insecure cyber behavior and may be important risk or protective factor in cyber security like attentiveness to security prompts, openness to perpetrating insider attacks, or susceptibility to social engineering attacks etc.

4.0.1 Personality Traits

Personality traits are widely studied in the field of psychology. Research in psychology suggests that personality characteristics such as Trait Anxiety and Callous Unemotional can play a significant role in providing insights about susceptibility to cyber-attacks such as social engineering attacks, propensity to commit insider threat.

The current version of SPICE supports two personality traits: trait anxiety (TA), and callousness (CU). The traits are chosen for the initial version because of their significance to risk or protective factor in cyber security such as attentiveness to security prompts, openness to perpetrating insider attacks, or susceptibility to social engineering attacks.

4.0.1.1 Callous Unemotional

Callous unemotional trait is characterized by lack of empathy, guilt and exhibit uncaring attitudes and behavior towards other's feelings [14]. The individuals having callous and unemotional traits may have a tendency for committing cybercrimes because of lack of sympathy for victim or personal connection to their organization [11]. Picture dot probe developed by Kimonis and his colleagues[14] was used to access CU

4.0.1.2 Trait Anxiety

Trait anxiety (TA) is characterized by feeling of stress, worry and discomfort. Given the links between anxiety and susceptibility to social pressure, the individuals having anxiety may have a tendency for succumbing to cyber-attacks such as social engineering attacks [15]. But conversely, it can also be a protective factor in increasing rule following and conscientiousness [10], thereby reducing the risk that user will be an attacker. In order to access TA, attentional probe task developed by Cognition and Emotion Laboratory at the University of Western Australia [22] was used. We call it word dot probe task for easy recall through out the paper.

4.0.2 Dot-probe Task

This section discusses the techniques used by SPICE to identify personality traits of end users. SPICE uses dot-probe task to identify trait anxiety, and callous-unemotional trait. Biases in selective attention cause individual differences in emotional vulnerability [32] that are used to determine callous unemotional trait [13] and trait anxiety [3]. Dot-probe task [17] is a low cost and non-invasive method for assessing selective attention as compared to psychophysiological measures [12].

Dot-probe task presents a pair of stimuli on computer screen to capture attentional bias towards emotional cues. It is iterative, and consists of a sequence of three steps: 1) 500 milliseconds of fixation is presented at the center of the screen to reset the attention from the last iteration. 2) Fixation disappears and two stimuli in the screen aligned vertically equidistant from the center of screen appears for 250 milliseconds (picture dot probe) or 500 milliseconds (word dot probe).. (3) Both stimuli disappear and a probe appears in the position of one of the stimuli.

The users are instructed to concentrate on the fixation when the task starts. This serves the purpose of balancing the users attention from attending up or down position from the previous task in the loop. After the probe is presented on the screen, the user responses by pressing a preset key designated to represent the corresponding stimulus position on the screen such as i or e for upper and m orx for lower position in SPICE. The users task is the hit the key that corresponds to the probe shown in the screen as fast as possible.

The time taken by the user to respond after the probe has been presented on the screen is called latency. Shorter probe detection latency for one stimulus over the other indicates the selective attentional bias towards the attended stimulus. Faster the probe detected by the user, its more likely that the users attention was biased towards the stimuli that was located in the same position as the probe. The latency in response time is used to calculate the facilitation index. It is noteworthy that the durations in millisecond and presentation of content on the computer screen are standard, and validated by past research [21].

Dot probe task is very popular method in the field of psychology to access personality trait such as TA, CU etc. based on biases in the selection of attention on the presented visual stimuli (e.g. pictures, words) on individual basis. The number of variations exists in instrumenting the dot-probe task. However, the basic methodology of the task is fairly consistent (as discussed above). The dot probe task described here was developed using primary slides taken from the International Affective Picture System [16].This section further discusses the implementation of two variants of the dot-probe task in SPICE i.e. picture dot-probe, and word dot-probe tasks.

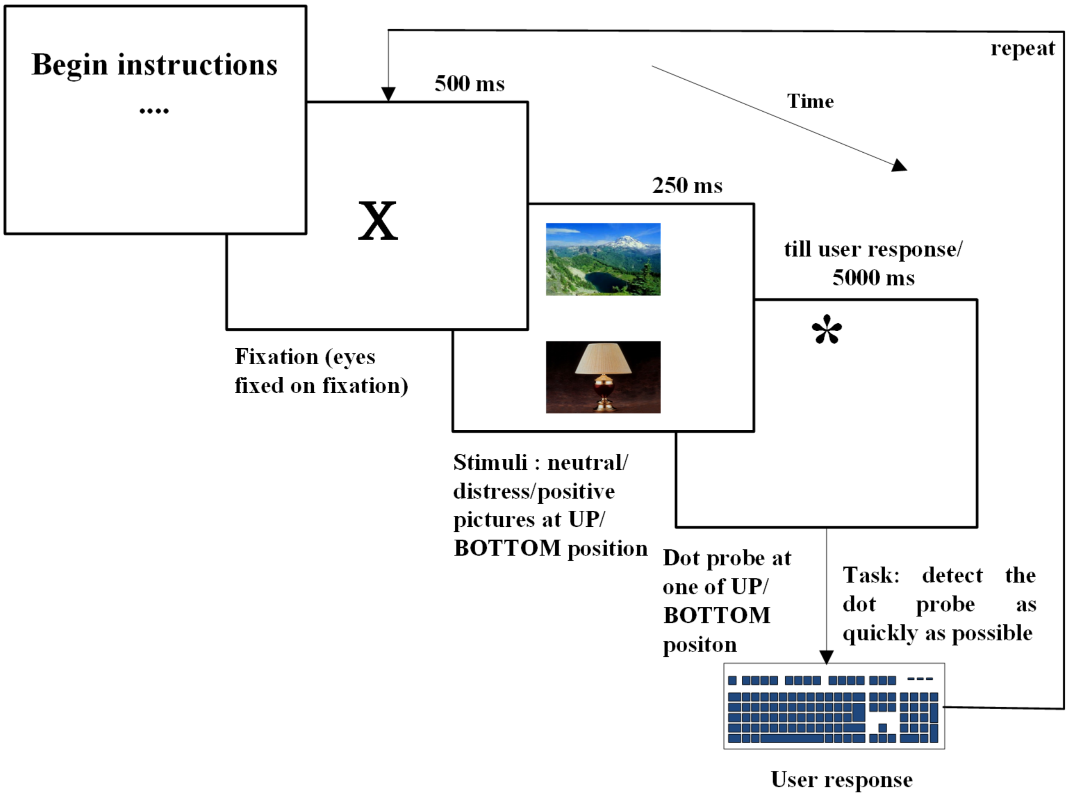


Figure 4.1: Illustration of Picture Dot-probe Task

4.0.2.1 Pictures Dot-probe Task

The picture dot-probe task is used for assessing callous unemotional trait. It involves a sequence of steps as illustrated in Figure 4.1. The task begins with the presentation of a fixation, followed by emotional pictures displayed number of times simultaneously in pairs on a computer screen. The pictures represent various emotional content including positive emotion (e.g. a child's happy face), neutral emotion (e.g. fork, and lamp), and distress, pain, and suffering (e.g. a crying child). The pictures are then followed by a probe (*).

When the probe appears on the screen, the user is supposed to indicate the location of the probe with the preset keys of the keyboard. For instance, the default keys in SPICE are 'i' or 'e' and 'm' or 'x' to indicate the upper and lower positions on the screen respectively. SPICE records the user's response time, and whether the user has indicated the location of the probe correctly. The user has to respond in 5 seconds. Otherwise, it is assumed that the response is incorrect. In the calculation of facilitation index, the incorrect responses are discarded and are considered as failure to attend the task. The dot-probe task is performed iteratively to capture substantial data on user's response.

The data is further processed to compute distress and positive facilitation indices as follows [21]. The incorrect responses are not included in the calculation.

Distress Attentional Facilitation Index

$$(Y) = 1/2[((N \uparrow) - (D \uparrow)) + ((N \downarrow) - (D \downarrow))] \tag{4.1}$$

Positive Attentional Facilitation Index

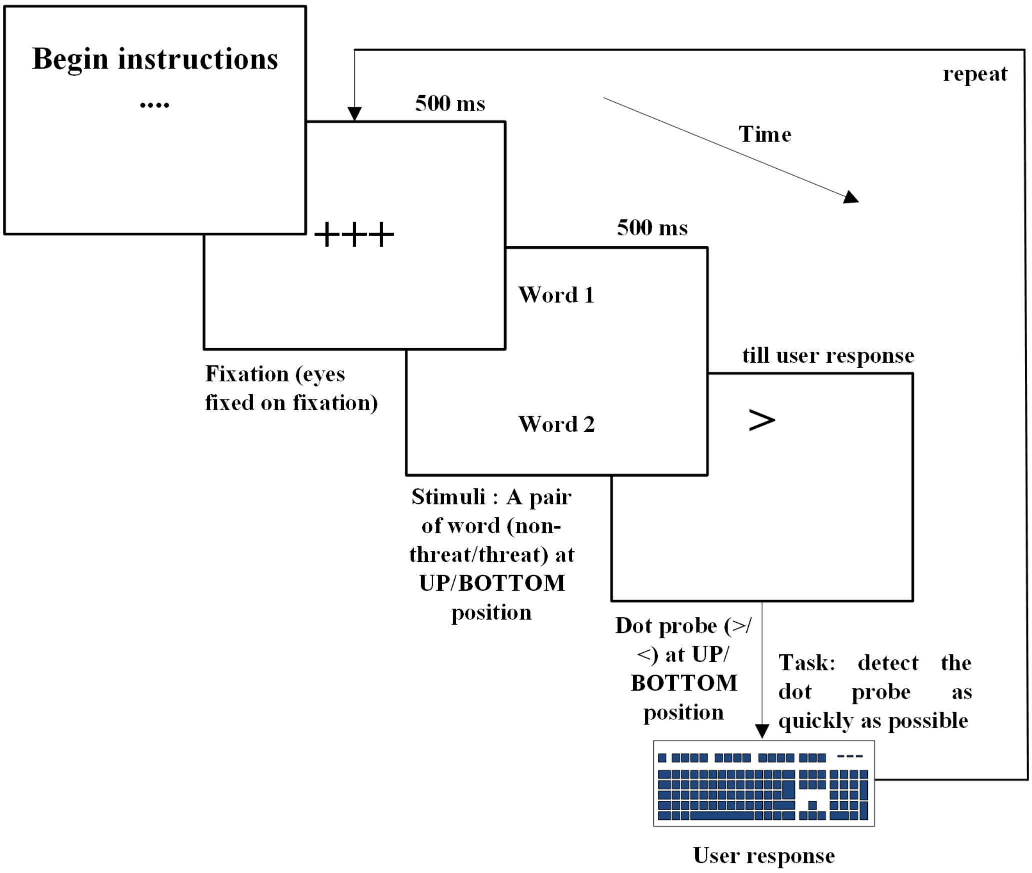
$$(Y) = 1/2[((N \uparrow) - (P \uparrow)) + ((N \downarrow) - (P \downarrow))] \tag{4.2}$$

Where, N ↑ = only neutral picture appear on the screen, with the dot probe replacing the top picture (Probe top); D↑= distressing picture on top, probe on top; N↓ = only neutral picture appear on the screen, probe on bottom; D↓= distressing picture on bottom, probe on bottom; P↑= positive picture on top, probe on top; P↓= positive picture on bottom, probe on bottom.

*All variables are mean response time

The distress/positive attentional facilitation index is mean latencies to detect probe that appear in the location of neutral picture to the location of distress/positive picture and indicate a bias to attend to distress/positive content respectively. They are calculated by subtracting the average response time to probe replacing neutral stimulus in neutral-neutral pairings.

SPICE has a feature to provide training session aside from trials for a dot-probe task. Training allows users to get some hands-on experience before testing session. In training session, users are allowed to participate in the task to make them familiar with their assigned task and are presented with feedbacks for incorrect response. The response is correct if the user responses with the key that corresponds to the position of probe else it is incorrect. For example: If the probe appeared at the UP position, the user is supposed to hit 'i'/'e' failure to which shows red incorrect symbol in the screen which informs user about incorrect response. The first session is always training session followed by multiple trial sessions. The users are allowed to take break



Begin instructions
....
500 ms
repeat
Time
+++
500 ms
Word 1
Fixation (eyes fixed on fixation)
till user response
Word 2
>
Stimuli : A pair of word (non-threat/threat) at UP/BOTTOM position
Dot probe (>/<) at UP/BOTTOM position
Task: detect the dot probe as quickly as possible
User response

Figure 4.2: Illustration of Word Dot-probe Task

in between each session. While the foremost training task makes user familiar to the task, trial sessions are recorded for user response to calculate their attentional biases.

The default settings of SPICE use one set of sixteen pairs of pictures in training, and 4 sets in testing, each having 24 pairs of pictures. For uniformity, SPICE uses equal number of emotional and neutral pictures in both training and testing sessions.

4.0.2.2 Word Dot probe Task

Word dot-probe task is used to assess trait anxiety. It works on the fact that the individuals with anxiety have shorter response time to probe for mild threat words such as fear. Figure 4.2 illustrates the sequence of steps for a word-probe task. The task begins with the presentation of fixation i.e. the symbol (+++), which is followed by displaying a pair of words aligned vertically on computer screen. The words used for the task are generally categorized into threat and non-threat words. The task is concluded with a probe either '<' or '>' replacing one of the words on screen. When the probe appears on the screen, the user is supposed to indicate the type of the probe quickly. SPICE records the response time, and whether the user has identified the probe correctly.

Similar to picture-probe task, SPICE allows users to experience a training session before trials and data collection. The default settings use one set of 10 pairs of words for training, and two sets for testing, each having 96 pairs of words. The task is performed several times to capture substantial data on user's response.

The data is then processed to calculate threat bias index (TBI) as follows.

Threat Bias Index

$$(Y) = ((NT) - (T)) \tag{4.3}$$

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.

The threat bias index is calculated by subtracting the average response time on probe replacing non-threat word to probe replacing threat word. In the above calculation, the positive value of TBI represents selective attention to threat and negative value represents attentional avoidance of threat [5].

Chapter 5

Secure/Insecure Cyber Behavior of End Users

End users (i.e. humans) are considered the weakest link in cybersecurity [1]. Their insecure cyber behavior may lead to compromise the integrity, availability, and confidentiality of a computer system. SPICE is a well-equipped platform to design experiments for understanding secure/insecure cyber behavior of end users. It provides a hypothetical skeleton scenario that can embed different cyber activities for end users with the opportunity to perform insecure cyber behaviors. SPICE captures users activities to identify their tendency towards insecure cyber behavior. This section discusses the scenario along with several preconfigured cyber tasks in SPICE such as checking emails, applying computer updates, and scanning computer with antivirus program.

5.1 Definition of Secure/Insecure Cyber Behavior

It is challenging to define a clear distinction between secure and insecure cyber behavior. Generally, a secure cyber behavior is described in terms of good security practices that reduce the risk of cyber attacks. Some examples include downloading software or software patches only from trusty websites, maintaining strong and distinct passwords for login credentials, keeping password completely secret, timely updating software patches, and using only secure and trusty network [23].

5.2 Identification of secure/insecure cyber behavior

We intend to simulate a real world cyber-environment to study the users behavior in computer related tasks. By the means of capturing how the end user interact with the given user interfaces and programs, it is possible to analyze this behavior. It is often necessary to design this simulation environment in such a way that it mirages the real world environment so as to collect data without interfering the users. For an example: specifically in cyber environment, we cannot present an interface very new in design and still want user to behave like the one that they have been habituated to. However, simulating everything is not our goal. Instead we simulate only those user interfaces that can provide us insight about the cyber behavior of the user such as ability to harm others, decide to take risks or be benign, follow security etc. We also assume hypothetical scenario where user's task is to respond to the given scenario as described below.

5.2.1 Hypothetical (Skeleton) Scenario

SPICE uses multi-tasking approach in a hypothetical scenario to assess the cyber behavior of end users in a dynamic, busy and robust working environment. The current version of SPICE has following built-in scenario to present to users.

"Imagine you just got a new job in accounting for a firm and a new colleague shows you software designed to track technology advances at your old company. Part of your new job is to monitor stock of the old company so your new company can respond, as you work in accounting. The main part of your work is accounting so you will also need to solve math problems. Periodically, you will need to respond quickly to emails and periodically you will be alerted to when you need to focus on stock quotes."

According to the scenario, as part of the job, user performs three main tasks: 1) solving accounting/ mathematical problems, 2) monitoring the stock prices of the competitor companies, and 3) responding to emails quickly. SPICE provides a graphical user interface for the user to perform the tasks.

5.2.1.1 Accounting/Mathematics Problems

Some incentives (in terms of points) are attached with the number of mathematical problems. To get more incentives, the user needs to solve more problems within time-constraints. The problems are designed based on the established work of Hopko et al. [9]. Figure 5.1a shows a graphical interface presenting a mathematics problem to user.

5.2.1.2 Stock Market Ticker

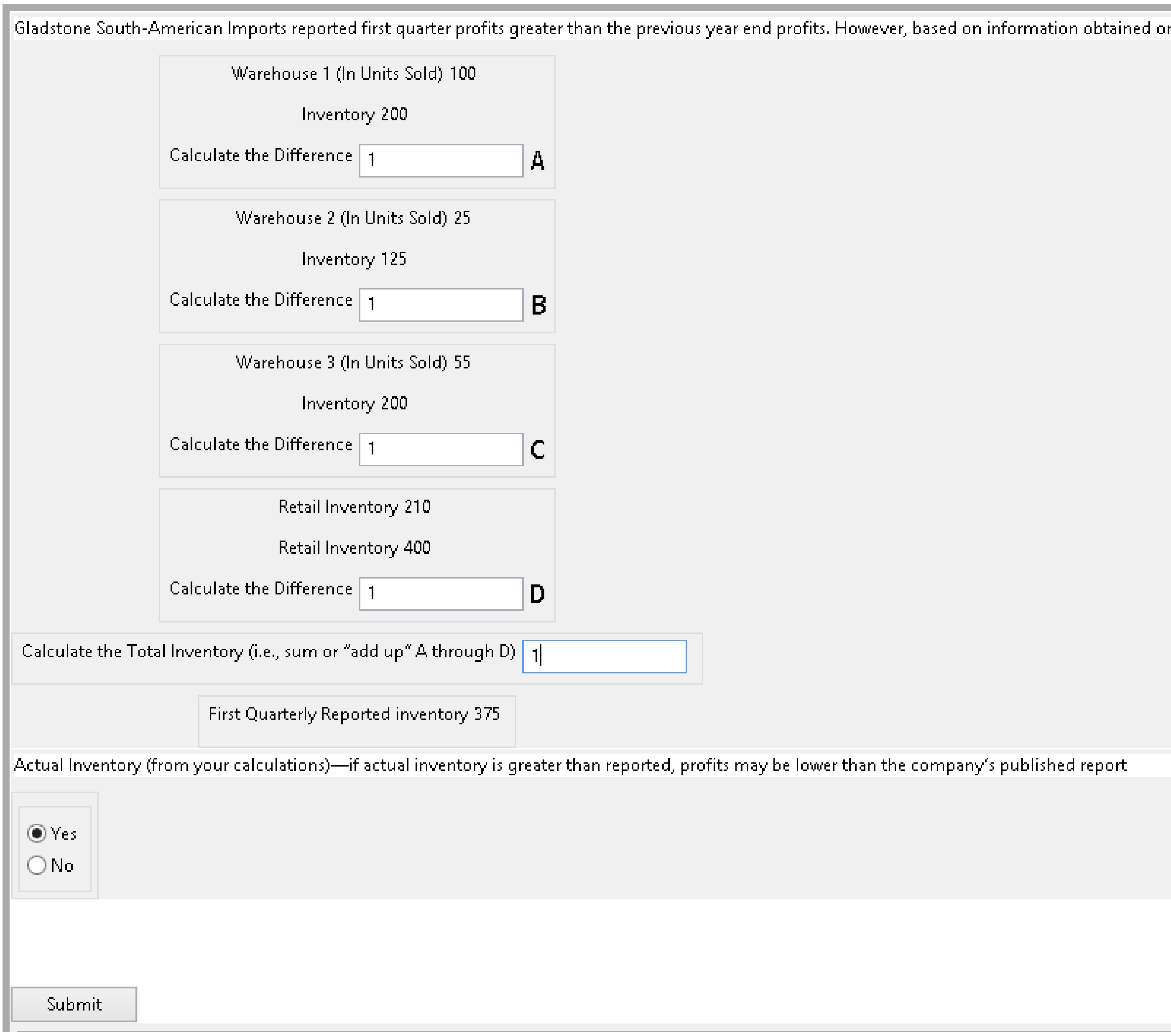
SPICE shows a moving stock-market ticker to distract the users from their accounting job. The ticker interface (shown in Figure 5.1b) is a small box attached under the interface of mathematics problem. The information displayed on the ticker can be used in number of ways while designing an experiment. For instance, the user can be asked to simply report the information to an upper management or to make the scenario complex, the information can be used to provide hints to users for solving mathematical problems.

5.2.1.3 Email

As part of the job, emails are periodically presented to users as another distraction from accounting job. SPICE provides a basic email interface (shown in Figure 5.2) to respond to emails. The interface displays the header information of incoming emails. If the user clicks on the header entry, it opens up the basic HTML content of the email. Furthermore, SPICE can be configured to add/remove the functionalities of replying and deleting emails in the interface.

5.2.2 Cyber Tasks

SPICE allows configuring/embedding cyber tasks to trigger during the normal operations of a user's job in a scenario. To study insecure cyber behavior of end users, the tasks are security



Gladstone South-American Imports reported first quarter profits greater than the previous year end profits. However, based on information obtained or

Warehouse 1 (In Units Sold) 100

Inventory 200

Calculate the Difference 1 A

Warehouse 2 (In Units Sold) 25

Inventory 125

Calculate the Difference 1 B

Warehouse 3 (In Units Sold) 55

Inventory 200

Calculate the Difference 1 C

Retail Inventory 210

Retail Inventory 400

Calculate the Difference 1 D

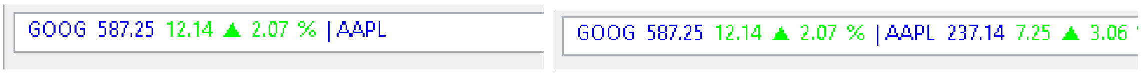
Calculate the Total Inventory (i.e., sum or "add up" A through D) 1

First Quarterly Reported inventory 375

Actual Inventory (from your calculations)—if actual inventory is greater than reported, profits may be lower than the company's published report

● Yes
○ No

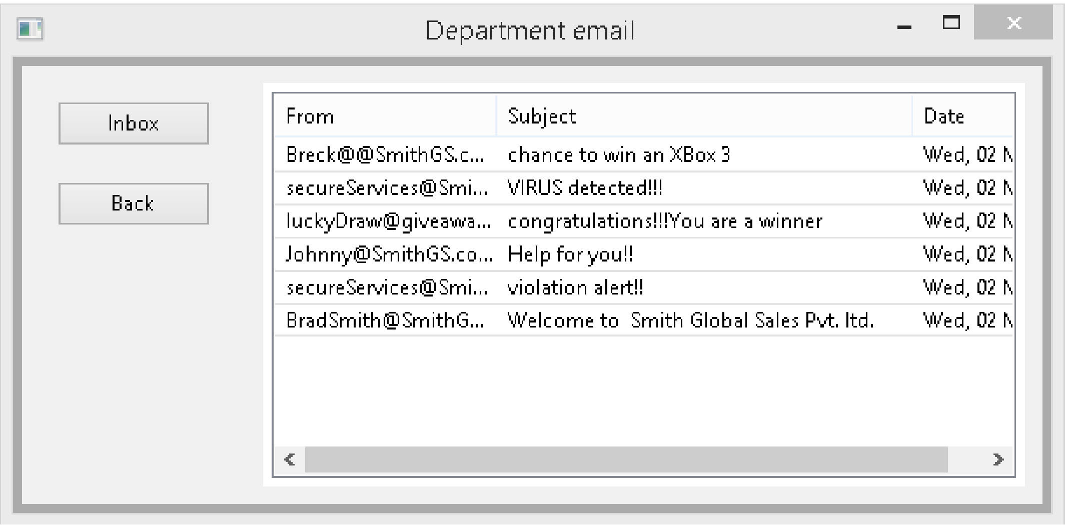
FIGURE 5.1A: User interface for mathematics problem.



GOOG 587.25 12.14 ▲ 2.07 % | AAPL

GOOG 587.25 12.14 ▲ 2.07 % | AAPL 237.14 7.25 ▲ 3.06

FIGURE 5.1B: User interface for Stock market ticker.



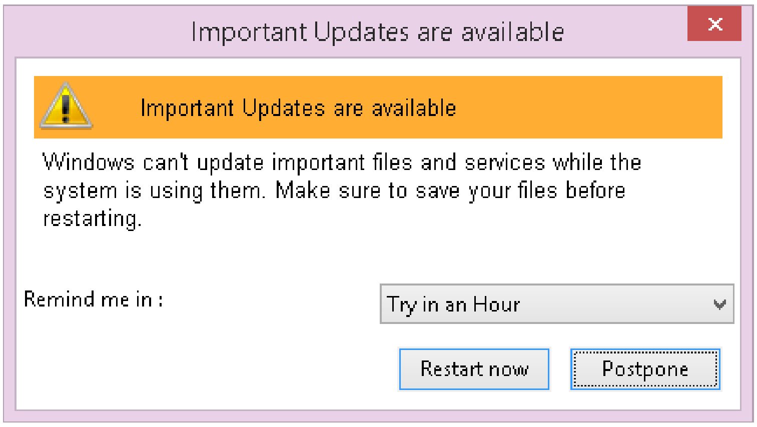
From	Subject	Date
Breck@@SmithGS.c...	chance to win an XBox 3	Wed, 02 N
secureServices@Smi...	VIRUS detected!!!	Wed, 02 N
luckyDraw@giveawa...	congratulations!!!You are a winner	Wed, 02 N
Johnny@SmithGS.co...	Help for you!!	Wed, 02 N
secureServices@Smi...	violation alert!!	Wed, 02 N
BradSmith@SmithG...	Welcome to Smith Global Sales Pvt. ltd.	Wed, 02 N

FIGURE 5.2: Email Interface showing header information of incoming emails

events that may either lead to compromise the security of a system or avoid cyber attacks such as antivirus scanning, and software updates. The tasks are configured as graphical user interfaces such as messages and dialogue boxes that are presented to user for response. For instance, to perform antivirus scanning, a dialogue box appears on screen asking user to start, defer or cancel the scanning. When user responds to the box, SPICE records the user response, and hides the box. It is noteworthy that SPICE does not react on user response to execute the presented tasks. The authors believe that further pursuing the user response is unnecessary for accomplishing the goal of exploring user intent on different cyber events. SPICE is already configured with several cyber tasks covering variety of security events described as follows:

5.2.2.1 Software Update

This task allows user to install new software updates/patches. It is a common situation often experienced by an end user, and is critical to prevent software exploitation [29] . If a computer system is not patched, and a known vulnerability exists in the system, it is highly likely that the system will be compromised [4]. This task captures the user attitude towards applying software/system updates. Figure 5.3a, 5.3b and 5.3c presents three different examples of graphical interfaces in SPICE for updating computer system/software. They are inspired from real world situations on system update, flash player updates and Java. Updating the system signifies that the user is conscious on security aspect of the system. People usually neglect software and



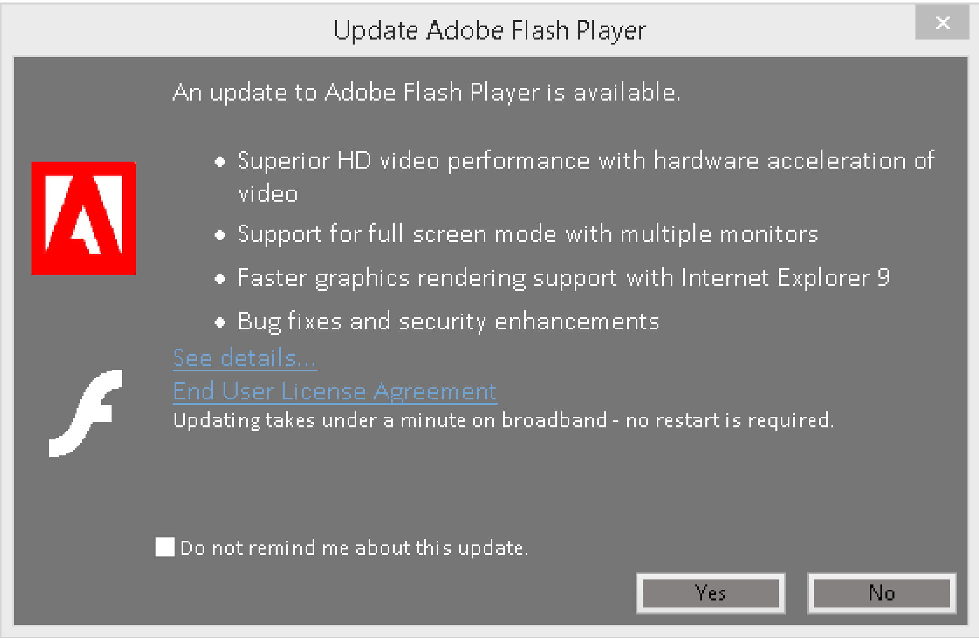
Important Updates are available

Important Updates are available

Windows can't update important files and services while the system is using them. Make sure to save your files before restarting.

Remind me in : Try in an Hour

FIGURE 5.3A: User Interface for System Updates.



Update Adobe Flash Player

An update to Adobe Flash Player is available.

- Superior HD video performance with hardware acceleration of video
- Support for full screen mode with multiple monitors
- Faster graphics rendering support with Internet Explorer 9
- Bug fixes and security enhancements

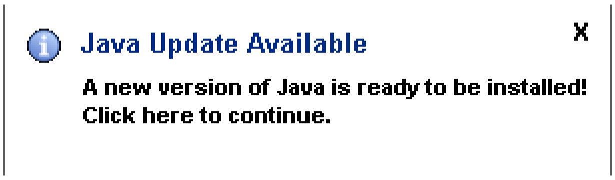
See details...

End User License Agreement

Updating takes under a minute on broadband - no restart is required.

□ Do not remind me about this update.

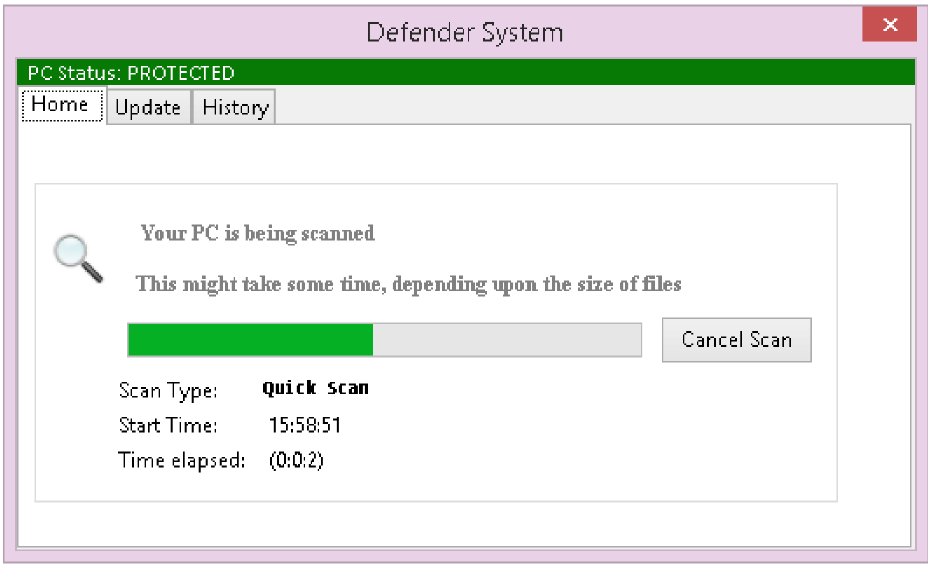
FIGURE 5.3B: Flash player update interface.



Java Update Available

A new version of Java is ready to be installed! Click here to continue.

FIGURE 5.3C: Java update interface.



Your PC is being scanned

This might take some time, depending upon the size of files

Scan Type: Quick Scan
Start Time: 15:58:51
Time elapsed: (0:0:2)

FIGURE 5.4: Anti-virus user interface

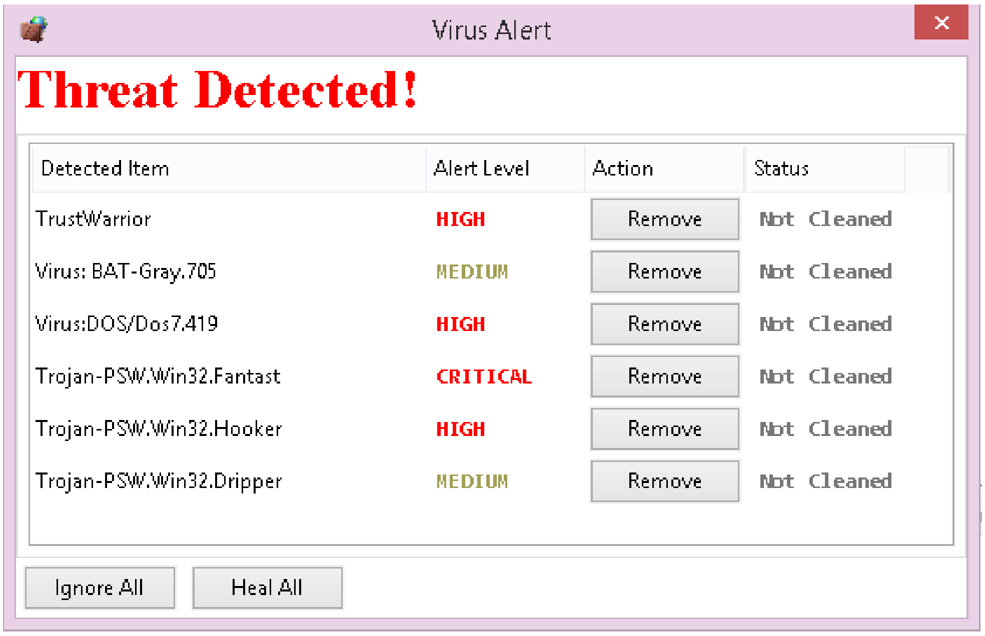
system update. The user beliefs and understanding about update is out of our scope and hence we capture only the user action on update user interface.

5.2.2.2 Anti-virus Scanning

This task allows user to cancel an on-going malware-scanning process. The scanning assesses the contents of a computer hard disk for identifying malicious document and executable files. The task captures user preference of either letting the scanning-process complete or cancelling the process. It is presented to user as a dialogue box (refer to Figure 5.4) consisting of a progress bar representing the completion level of the scanning process, and a Cancel Scan button allowing user to cancel the scanning process. If user presses the button, another dialogue box appears with Yes/No options confirming user's action on canceling the scanning process.

5.2.2.3 Virus Alert

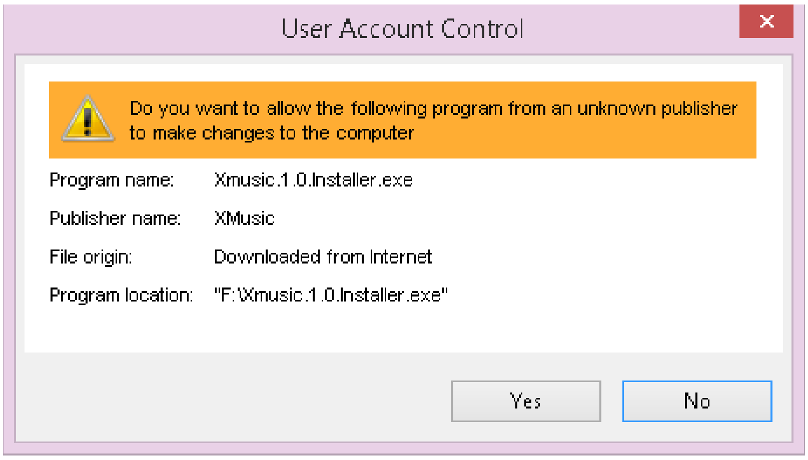
This task captures user's reaction on a virus alert. It allows user to either remove or ignore viruses from a computer system reported by an antivirus software. The task presents a list of viruses in an alert interface (refer to Figure 5.5) where each entry shows a severity level of virus, and a button for removing the virus from the computer. We believe that the user may not be



Threat Detected!

Detected Item	Alert Level	Action	Status
TrustWarrior	HIGH	Remove	Not Cleaned
Virus: BAT-Gray.705	MEDIUM	Remove	Not Cleaned
Virus:DOS/Dos7.419	HIGH	Remove	Not Cleaned
Trojan-PSW.Win32.Fantast	CRITICAL	Remove	Not Cleaned
Trojan-PSW.Win32.Hooker	HIGH	Remove	Not Cleaned
Trojan-PSW.Win32.Dripper	MEDIUM	Remove	Not Cleaned

FIGURE 5.5: Virus alert user interface.



Do you want to allow the following program from an unknown publisher to make changes to the computer

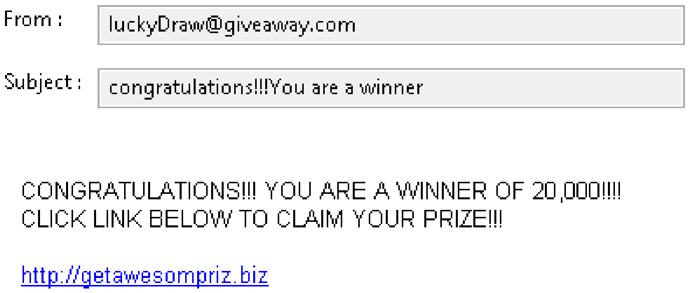
Program name:	Xmusic.1.0.Installer.exe
Publisher name:	XMusic
File origin:	Downloaded from Internet
Program location:	"F:\Xmusic.1.0.Installer.exe"

FIGURE 5.6: Suspicious download pop-up window.

familiar with the names of viruses and malwares in the wild. Thus, the severity levels : critical, high, medium, and low help user make informed decision.

5.2.2.4 Drive-by download

This task examines user for being attentive while downloading files from Internet. It presents a suspicious dialogue box (refer to Figure 5.6) asking permission from user to download a file that is an executable with .exe extension, and from an anynomous source. The task mimics a



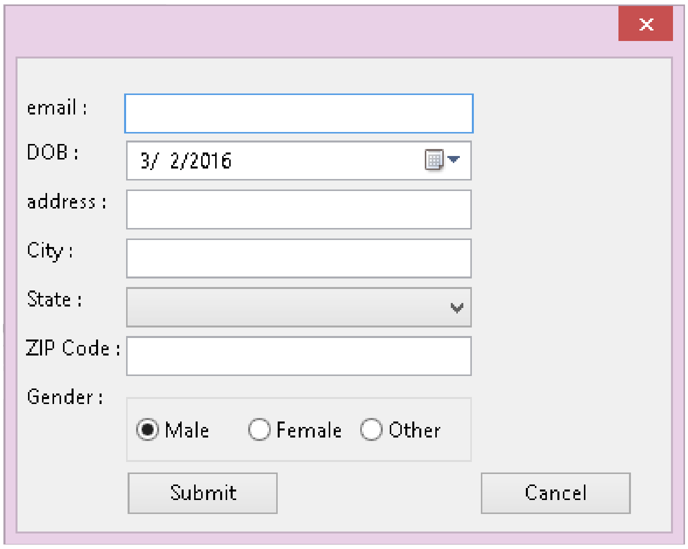
From : luckyDraw@giveaway.com

Subject : congratulations!!!You are a winner

CONGRATULATIONS!!! YOU ARE A WINNER OF 20,000!!!!
CLICK LINK BELOW TO CLAIM YOUR PRIZE!!!

http://getawesompriz.biz

FIGURE 5.7A: Scam email posing as lucky draw award.



email :

DOB : 3/ 2/2016

address :

City :

State :

ZIP Code :

Gender : ● Male ○ Female ○ Other

FIGURE 5.7B: The interface for stealing personal information such as email, date of birth (DOB), mailing address, city, state, zip code, gender.

part of drive-by download scenario a popular attack that leads user to click on a web link, and download a file (often an executable) [6].

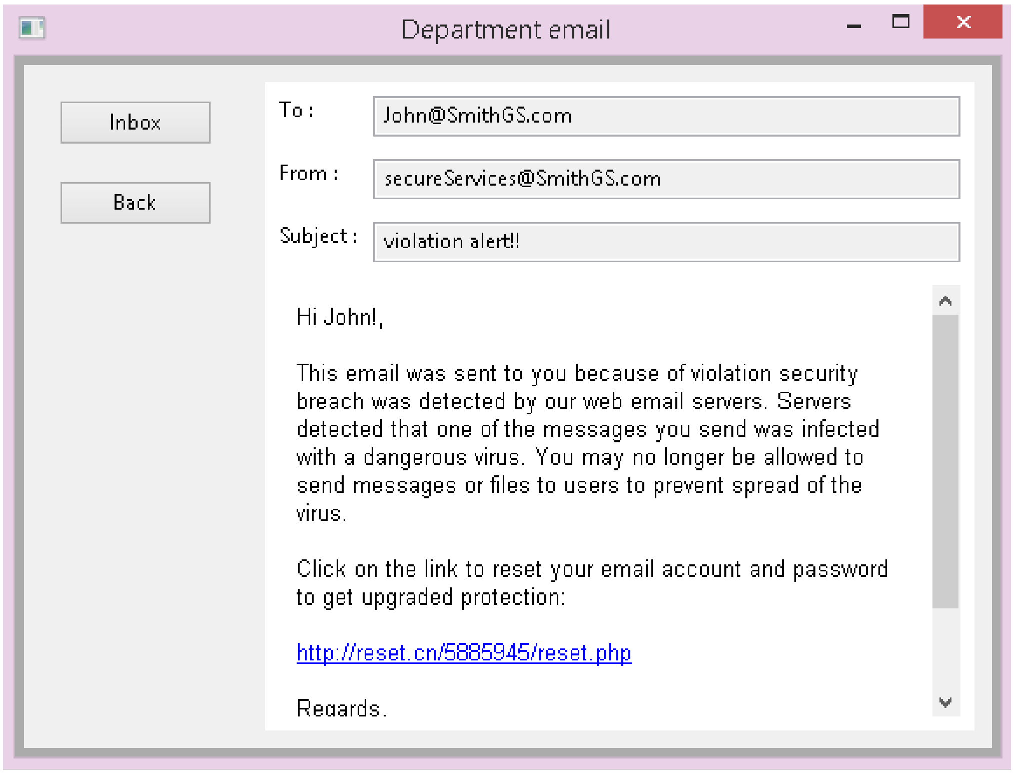
5.2.2.5 Phishing and Hacking

SPICE provides an email interface to check incoming emails. Phishing emails and hacking are two email models present in SPICE at the time of this writing. Phishing email minutiae about propensity of being victimized while hacking email distinguishes tendency to victimize others.

Greetings [user]

[email message]

[link]



To : John@SmithGS.com

From : secureServices@SmithGS.com

Subject : violation alert!!

Hi John!,

This email was sent to you because of violation security breach was detected by our web email servers. Servers detected that one of the messages you send was infected with a dangerous virus. You may no longer be allowed to send messages or files to users to prevent spread of the virus.

Click on the link to reset your email account and password to get upgraded protection:

http://reset.cn/5885945/reset.php

Regards,

FIGURE 5.7C: Scam email seemingly coming from IT Department.

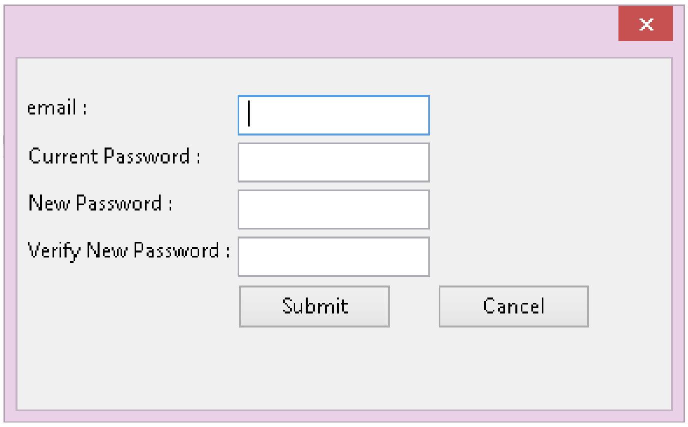
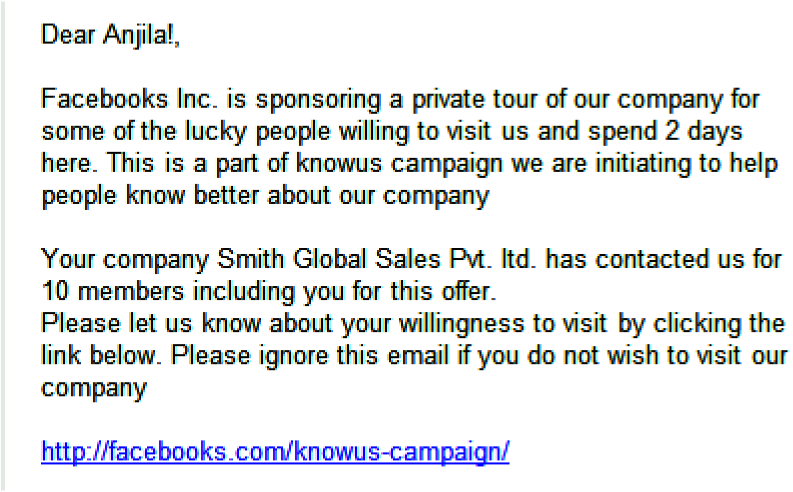


FIGURE 5.7D: The interface for stealing email ID and passwordshown after clicking the link in Figure 5.7c.



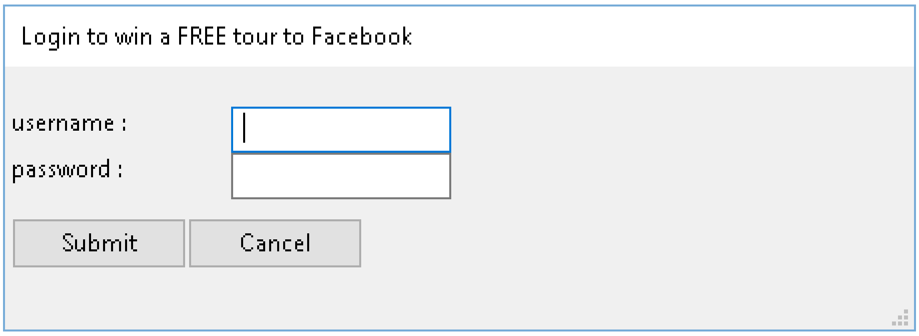
Dear Anjila!,

Facebooks Inc. is sponsoring a private tour of our company for some of the lucky people willing to visit us and spend 2 days here. This is a part of knowus campaign we are initiating to help people know better about our company

Your company Smith Global Sales Pvt. ltd. has contacted us for 10 members including you for this offer.
Please let us know about your willingness to visit by clicking the link below. Please ignore this email if you do not wish to visit our company

http://facebooks.com/knowus-campaign/

Figure 5.7e: Scam email luring user to click the link posing as a fake facebook company.



Login to win a FREE tour to Facebook

Figure 5.7f: Scam email in figure requesting for Facebook email and password.

The above format represents the email presented to the user in SPICE. The idea is to trick or lure user to click the link somehow and identify user potential to engage in secure and insecure cyber behavior. It is important to note that we do not phish or hack any entity in SPICE but rather provide just the simulation of all those activities.

With phishing and hacking email, information about users propensity to involve in activities like hacking other to gain benefits, blindly trusting in computing, revealing private information can be gathered. Exploitation based message such as luring to gain prize, instilling fear about security violation and provide fake link to reset password immediately are some examples of phishing email while providing link to access insider information on competitor company is an instance of hacking email.

Phishing emails are very popular among cyber criminals. They send fraudulent emails that appear to come from legitimate source (e.g. your university. Company you work at, big enterprise etc.) and take advantage of fear, desire to help, desire to gain [2] to gain private information such as passwords, credit card information etc. SPICE leverages email to launch phishing attack on user such as theft of password and personal information. It captures user's response of either ignoring phishing emails or becoming a victim of phishing. SPICE allows configuring email contents, introducing web links in emails, and redirecting the links to access locally configured interfaces for data entry. Following are three distinct phishing scenarios preconfigured in SPICE.

Scenario 1: User receives an email stating that he has won a big cash prize in a lucky draw. The email further instructs the user to fill out a form accessible through a web link. Figure 5.7a and Figure 5.7b show the email, and the form asking for personal information such as date of birth (DOB), mailing address, and zip code. **Scenario 2**: User receives an email stating that a stealthy virus has been detected, and all employees are required to update their passwords of the company's email service via a given web link in the email as shown in Figure 5.7c. Figure 5.7d shows the interface for stealing email ID and passwords. **Scenario 3**: User receives an email seemingly coming from Facebook stating that the user has a chance to win a visit of Facebook headquarter as a part of Know Us campaign. The user is required to login to facebook page via a given web link in the email. Figures 5.7e and 5.7f show the email contents, and the interface accessible via the link for stealing the username and password of the user's Facebook account.

Hacking emails are those emails that are presented to the user with the capability to hack others to gain information about others in dishonest/illegal way. For example: a new colleague shows you software designed to track stock prices at another competitor company that will help to get hints to solve mathematics problem in fast paced manner.

As part of experimental design, SPICE has a configuration option that ensures that user always opens emails. However, it does not interfere in user's response while user is checking emails. Furthermore, SPICE can be configured to generate emails utilizing user's personal information such as first name in salutation. This functionality is particularly useful to cater social engineering attacks.

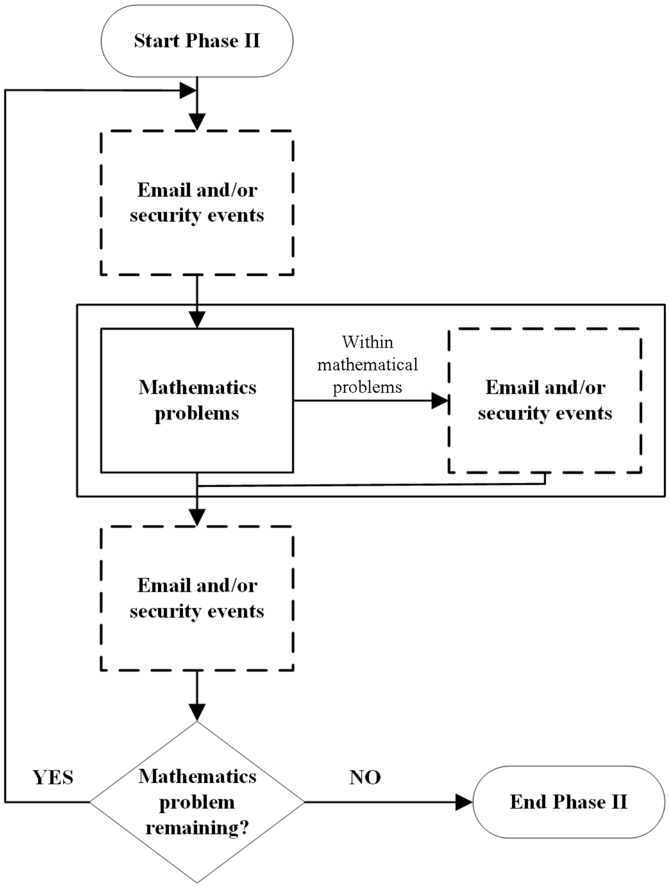

Start Phase II
Email and/or security events
Mathematics problems
Within mathematical problems
Email and/or security events
Email and/or security events
YES
Mathematics problem remaining?
NO
End Phase II

FIGURE 5.8: Synergy (in flow diagram) among the tasks in hypothetical scenario and cyber tasks. Dotted box represent optional events. Email and/or security events may appear before, after and/or during mathematics problem.

5.2.3 Synergy among Hypothetical-scenario Tasks and Cyber Tasks

SPICE configures two types of tasks: cyber tasks, and the tasks in a hypothetical scenario. Once the tasks are configured, SPICE further allows configuring the sequence of the tasks. A task can be configured to appear before, after or during a current task. This functionality provides more control over the design of an experiment, and also ensures that all the participants in an experiment go through the same sequence of tasks thereby, making the results more comparable. Figure 5.8 illustrates the synergy among the tasks in a preconfigured hypothetical scenario (described in section 5.2.1), and the cyber tasks (including security events). The main task from the scenario is to solve mathematical problems, monitor the ticker presenting stock market information, and informing upper management of his organization about certain stock market events through email. Occasionally, user experiences cyber tasks related to security events that may appear anytime while user is performing tasks from the scenario.

Chapter 6

Software Customization

Customizability is one of the important features in SPICE. It is easy to modify the contents and manage flow of occurrence of different events for the design of the experiment. In this section, we discuss about scripting and how we can customize different aspects of the tool.

6.0.1 Scripting

SPICE employs a tag-based, customizable scripting for configuring the experimental environment. Every task is configured and represented by a script including dot-probe, and cyber tasks. For example, the script for the emotional dot probe follows the following pattern as shown in Listing 6.1.

```
1.      <dot-probe>
2.      <block>0</block>
3.      <up> neu98.jpg,neu2190.jpg,   </up>
4.      <up-type> Neutral, Neutral,   </up-type>
5.      <down> neu62.jpg,neu43.jpg,... </down>
6.      <down-type> Neutral, Neutral,   </down-type>
7.      <probe-position>Down, Up,   </probe-position>
8.      </dot-probe>
```

Listing 6.1: Picture dot probe script

Line 1 represents the start of dot probe and line 8 represents the corresponding end tag. 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.

```
1.      12XXXX
2.      <tag> WELCOME_EMAIL</tag>
3.      <from>  FROM </from>
4.      <to> To </to>
5.      <subject> SUBJECT </subject>
6.      <dialog> DIALOG_ID</dialog>
7.      <message> EMAIL_TEXT
8.      </message>
```

Listing 6.2: Script for an email

Listing 6.2 represents a short email script. Line 1 represents a email ID, which must be start with 12, and has the format 12XXXX (e.g. 12000). Tags in Line 6 are for inserting a link to a dialog box. When a user clicks on the link, the dialog box will appear. SPICE binds a user interface/dialog to a link in an email through a unique dialog box ID. The ID is defined in a separate dialog box scripting used to configure the user interface of a dialog box. The tags in Line 3, 4, and 5 are used to mention sender, and recipient's email addresses, and the subject of an email respectively. An email message is written between the tags in lines 7 and 8.

6.0.2 Event Sequencing

SPICE allows managing the order of occurrence of different events/tasks in a list. Listing 6.3 illustrates an example of the list (referred to as flow-order), in which the tasks such as emails, cyber tasks, and mathematical problems are presented to the user. According the list, the tasks can occur before, or after mathematical problems (M). Furthermore, the tasks can be configured to trigger during mathematical problems through a separate variable i.e. maths_sec_events.

```
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"]
```

Listing 6.3: Order of the occurrence of events

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
"software-update", "virus-alert", "flash-update", "Java-update", "anti-virus-scan" are security events

6.0.3 Other software parameters

SPICE provides number of other software parameters to configure fine-grained details of a task. Listing 6.4 covers some important parameter along their brief description and default values.

```
1.      General Configuration
        a.      write-log: True
        b.      startLevelNumber:1
2.      Picture-probe-configuration
        a.      fixation-interval:500
        b.      image-interval:250
        c.      probe-interval:500
        d.      idle-response-time:5000
3.      Word-probe-configuration
        a.      fixation-interval:500
        b.      word-interval:250
        c.      probe-interval:500
4.      Email configuration:
        a.      Company-name: Smith Global Sales Pvt. ltd.
        b.      Company-email: @SmithGS.com
        c.      Name: user
```

LISTING 6.4: Configuration parameters

Write-log in 1a provides an option to write log about each event in the software while 1b instructs the tool to start from the specific phase for example: 1 to start from the picture dot-probe, 3 to start the tool from word based dot-probe, 5 to start the tool from the phase to identify insecure behavior. The configuration parameters in the picture and word based dot-probe provides the time period in millisecond for which fixation, pair of stimuli and probe needs to be presented to the user. The configuration in 4a and 4b provides the email and company name which represents the company the user is working for as per the hypothetical situation. Similarly, 4c provides the option to specify the name to whom the emails will be directed to. For example: if the name provided in the configuration file is John, then the email contain will be Hello John, ... But this can be kept empty to skip name in the email in which case, generic email will be generated for example Hello, .

Chapter 7

Data Collection

SPICE records user's response on each task in CSV (comma separated value) files. This section discusses the fields and their plausible values stored in the files.

7.0.1 Identification of Personality Traits of End Users

SPICE uses picture, and word-based dot-probe tasks to identify anxiety, and callousness. A user has to go through a large number of dot-probe tasks spread over multiple intervals to complete an experiment. SPICE records detailed information about each probe-task including pictures or words displayed on computer screen, and user's response time on a probe. Tables 7.1 and 7.2 present the fields (used in CSV files), their brief descriptions, and possible values.

7.0.2 Insecure Cyber Behavior of End Users

This section discusses the data fields for cyber tasks. It is worth mentioning that SPICE allows tagging data for improving data visualization, and analysis. For instance, Virus-alert interface can be configured with tags such as VIRUS_ALERT_HEAL_ALL, VIRUS_ALERT_IGNORE_ALL, and VIRUS_ALERT_CLOSE to represent the user actions on the interface i.e. remove, or ignore viruses, or close virus alert window. This functionality allows a non-technical person to do the data analysis efficiently.

Table 7.1: Data fields (in a CSV file) for picture probe task.

Field	Explanation	Possible Value
Block No	One block can contain a number of dot probe task like training block contains 16 picture pairs	e.g. 0 is considered training block
Current No	Task sequence number within each block	abc
DisplayCode	code for what is being displayed in the screen	FIXATION \PROBE-UP \PROBE-DOWN \PICTURE
DisplayTime	Time for which DisplayCode is displayed in the screen	Time in milliseconds
PictureUPType	Type of image in UP position	Positive \negative \neutral
PictureDOWNType	Type of image in DOWN position	Positive \negative \neutral
IsCorrect	Does the position of probe and user's key press match	0 (for NO) and 1 (for YES)
Latency	Latency of user response to the dot probe	Time in milliseconds

Table 7.2: Data fields (in a CSV file) in word probe task.

Field	Explanation	Possible Value
DisplayCode	code for what is being displayed in the screen	e.g. FIXATION \PROBE-UP \PROBE-DOWN \WORD
DisplayTime	Time for which DisplayCode is displayed in the screen	Time in milliseconds
PROBE_POSN	Which word type the probe replaces	PINP(Probe in Neutral word position) and PITP (Probe in threat word position)
ThreatWord	Threat word	ambulance \attack etc.
NeutralWord	Neutral word	chair \kite etc.
CurrentProbe	current probe	>\<
IsCorrect	Does probe match user's response	1 (CurrentProbe and Response match) else 0
Latency	Latency of user response to the dot probe	Time in milliseconds

Furthermore, SPICE keeps track of hierarchical tasks, which are generated when one task spawns another task during execution. It maintains a unique ID for each task to record parent-child relationship in a hierarchical task. Table 7.3 shows the data captured during the identification of insecure user behavior.

Table 7.3: Data capture during identification of insecure behavior.

Field	Explanation	Possible Value
Parent ID	Parent of the current event	-1 if no parent
DisplayTime	Time for which DisplayCode is displayed in the screen	Time in milliseconds
Math ID	ID of presented mathematical problem	13XXXX
Email ID	ID of presented email	12XXXX (e.g. 120000)
Email Tag	Email tag configured in email script	e.g. WELCOME_EMAIL
Dialog ID	ID of the dialog presented	5XXXXX (e.g. 500000)
Dialog Tag	Tag for the dialog	e.g. VIRUS_ALERT
response	Users actions on presented event/dialog	e.g. VIRUS_ALERT_CLOSE
Response code	Unique code for each response	e.g. code for VIRUS_ALERT_CLOSE = 12
Start time	Time when event/dialog are presented on screen	System time
End time	Date when the experiment started	system date
Date	Tag for the dialog	e.g. VIRUS_ALERT

Chapter 8

Related work

Cyberpsychology is an emerging area in psychology [31], [30]. SPICE is an effort to provide a cybersecurity-focused tool for research in this field. None of the existing software focuses on integrating concepts in psychology and cognitive science (such as personality traits) with the cybersecurity behavior of end users. For instance, Inquisit [19] , e-prime [24], and DirectRT [7] are popular tools for designing, testing and demonstrating psychological tests and experiments. However, they have limited capability of designing experiments on cybersecurity behavior [26].

More recently, Neupane et al. [20] presents a study on measuring users's security behavior with their underlying neural activity. The study focuses on users ability to distinguish between a legitimate and a phishing website, and observe security (malware) warnings. The brain activities are measured through functional Magnetic Resonance Imaging (fMRI) scanning. E-prime software is used for a limited purpose of presenting visual and auditory stimuli to users and recording their response time. Since E-prime does not support cybersecurity tasks, the tasks are performed on real environment.

Chapter 9

Conclusion and Future work

We 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.

SPICE is fully configurable software to add variety of cyber tasks, and the tasks from number of different hypothetical scenarios. However, it has currently limited preconfigured tasks (described in this paper). As part of future work, we will add more interfaces, and introduce variety of scenarios. Also, we will extend the tool to make it functional on web in order to supporting experimentation on large scale.

Bibliography

[1] Allen and Malcolm. Social engineering a means to violate a computer system. *SANS Institute, InfoSec Reading Room*, 2006.

[2] I. U.-K. Base. *What are phishing scams and how can I avoid them?*, 2015 (accessed February 18, 2016).

[3] A. T. Beck and D. A. Clark. An information processing model of anxiety: Automatic and strategic processes. *Behaviour research and therapy*, 35(1):49–58, 1997.

[4] N. by Symantec. *Why Security Updates Are Vital*, 2015 (accessed July 23, 2015).

[5] M. Colin, Y. S. Lih, M. R. Elizabeth, and W. C. Lynlee. Internet-delivered assessment and manipulation of anxiety-linked attentional bias: Validation of a free-access attentional probe software package. *Behavior Research Methods*, 39(3):533–538, 2007.

[6] M. Cova, C. Kruegel, and G. Vigna. Detection and analysis of drive-by-download attacks and malicious javascript code. *Proceedings of the 19th international conference on World wide web*, pages 281–290, 2010.

[7] Empirisoft. *Direct RT (Version 2014)*, 2014 (accessed December 18, 2015).

[8] S. T. Haque, S. Scielzo, and M. Wright. Applying psychometrics to measure user comfort when constructing a strong password. *Symposium On Usable Privacy and Security (SOUPS 2014)*, pages 231–242, 2014.

[9] 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.

[10] J. W. Jencks and D. L. Burton. The role of trait anxiety in reducing the relationship between childhood exposure to violence or victimization and subsequent violent behavior among male delinquent youth. *International journal of offender therapy and comparative criminology*, 57(8):985–995, 2013.

[11] E. R. Kimonis, B. Cross, A. Howard, and K. Donoghue. Maternal care, maltreatment and callous-unemotional traits among urban male juvenie offenders. *Journal of youth and adolescence*, 42(2):165–177, 2013.

[12] E. R. Kimonis, P. J. Frick, L. C. Munoz, and K. J. Aucoin. Can a laboratory measure of emotional processing enhance the statistical prediction of aggression and delinquency in detained adolescents with callous-unemotional traits? *Journal of abnormal child psychology*, 35(5):773–785, 2007.

[13] E. R. Kimonis, P. J. Frick, L. C. Munoz, and K. J. Aucoin. Callous-unemotional traits and the emotional processing of distress cues in detained boys: Testing the moderating role of aggression, exposure to community violence, and histories of abuse. *Development and psychopathology*, 20(02):569–589, 2008.

[14] 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.

[15] P. A. Kosten, L. M. Scheier, and J. L. Grenard. Latent class analysis of peer conformity: Who is yielding to pressure and why? *Youth & Society*, page 0044118X12454307, 2012.

[16] P. J. Lang, M. M. Bradley, and B. N. Cuthbert. International affective picture system (iaps): Technical manual and affective ratings. *NIMH Center for the Study of Emotion and Attention*, pages 39–58, 1997.

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

[18] M. McBride, L. Carter, and M. Warkentin. *The Role of Situational Factors and Personality on Cybersecurity Policy Violation*, 2012 (accessed December 3, 2015).

[19] Millisecond. *Inquisit*, (accessed July 23, 2015).

[20] A. Neupane, M. L. Rahman, N. Saxena, and L. Hirshfield. A multi-modal neurophysiological study of phishing detection and malware warnings. pages 479–491, 2015.

[21] U. of New Orleans-Department of Psychopathology Laboratory. *Emotional Pictures Dot-Probe Task*, 2014 (accessed December 13, 2015).

[22] T. U. of Western Australia-Cognition and E. L.-D. of Psychology. *Attentional Probe Task*, (accessed December 18, 2015).

[23] U.-C. Publications. *Before You Connect a New Computer to the Internet*, 2015 (accessed December 18, 2015).

[24] W. E. Schneider and A. Zuccolotto. A.(2002). e-prime user's guide. pittsburgh, pa: Psychology software tools.

[25] J. Shropshire, M. Warkentin, A. Johnston, and M. Schmidt. Personality and it security: An application of the five-factor model. *AMCIS 2006 Proceedings*, page 415, 2006.

[26] C. Stahl. Software for generating psychological experiments. *Experimental Psychology*, 53(3):218–232, 2006.

[27] G. F. Thomas, S. R. Kuper, K. M. Thomas, E. W. Armbrust, and M. W. Haas. Understanding the user can be a tool for cyber defense. Technical report, DTIC Document, 2012.

[28] M. Warkentin and R. Willison. Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*, 18(2):101, 2009.

[29] R. Wash, E. J. Rader, K. Vaniea, and M. Rizor. Out of the loop: How automated software updates cause unintended security consequences. *SOUPS*, pages 89–104, 2014.

[30] R. West. The psychology of security. *Communications of the ACM*, 51(4):34–40, 2008.

[31] B. K. Wiederhold. The role of psychology in enhancing cybersecurity. *Cyberpsychology, Behavior, and Social Networking*, 17(3):131–132, 2014.

[32] J. M. G. Williams, F. N. Watts, C. MacLeod, and A. Mathews. *Cognitive psychology and emotional disorders.* John Wiley & Sons, 1988.

Vita

The author Anjila Tamrakar was born in Kathmandu, Nepal. She received her Bachelors degree in Computer Engineering from Tribhuvan University in 2012. She joined the University of New Orleans Computer Science graduate program to pursue a MS degree with concentration in Information Assurance. This research work was funded by NSF and was conducted under the supervision of Dr. Irfan Ahmed, Dr. Golden G. Richard and Dr. Carl Weems in 2015/2016.