An Empirical Investigation of Static and Polymorphic Tactile Stimuli's Effect on Habituation to Mitigate Cybersecurity Attacks

Javier J. Coto, Ph.D. Candidate

Yair Levy, Ph.D., Professor of IS & Cybersecurity

College of Computing and Engineering (computing.nova.edu)

Nova Southeastern University (NSU), Florida

NOVA SOUTHEASTERN UNIVERSITY | NSU Florida

Introduction

- Habituation can prevent users from adhering to security warnings like spear phishing emails, Secure Sockets Layer (SSL) warnings, or malware warnings (Akhawe & Felt, 2013; Anderson et al., 2016a; Anderson et al., 2016b; Neupane et al., 2014).
- Today users are still being consistently presented as the greatest weakness of any cybersecurity plan (Abraham & Chengalur-Smith, 2010; Anderson, 1993; Mahfuth et al., 2017; Neupane et al., 2014; Shingler & Boss, 2009; Stembert et al., 2015; Tsohou, et al., 2015).
- This study will use a neurological approach to investigate the effect of tactile stimuli in mitigating cybersecurity attacks vectors.

Research Problem

- The research problem that this study addresses is the increase in cyberattacks due to users' habituation to malware warnings that causes significant financial losses for organizations (Akhawe & Felt, 2013; Anderson et al., 2016a; Kaspersky, 2016; Neupane et al., 2014; Vance et al., 2017).

Background

- Groves and Thompson (1970) described habituation as a “decreased response to repeated stimulation” (p. 419).
- Emphasis needs to be placed on the user and attempt to understand human nature (Luo et al., 2011).
- Neupane et al. (2016) advised when studying cybersecurity that all future studies must investigate the effect of habituation.
- “A different approach is needed. Rather than approaching the problem solely from a traditional cryptography-based security framework, design must consider what humans do well and what they do not do well” (Dhamija et al., 2006, p. 590).

Background (Cont.)

- Users have been referred to as the weakest link in cybersecurity, malicious attackers routinely exploit users through social engineering tactics (Abraham & Chengalur-Smith, 2010; Mandiant, 2013).
- Anderson et al. (2016a) believed that habituation is a neurological issue. Moreover, according to Anderson et al. (2016a) "Through this phenomenon, warnings that were once salient become virtually unnoticeable, like familiar wallpaper" (p. 714).
- Vance et al. (2014) showed that self-reporting measuring instruments like surveys are not accurate for individuals to report their cybersecurity risk perceptions, instead cognitive Neuroscience applied to Information System (NeuroIS) tools should be used.
- The problem has been compounded due to the volume of non-essential notifications, sometimes very similar to the real warnings, this causes a generalization of habituation to all warnings (Vance et al., 2017).

Background (Cont.)

- Two main theories for Habituation
- Stimulus-Model Comparator Theory (Sokolov, 1963)
- Dual-Process Theory (Groves & Thompson, 1970).
- Both use Sokolov's (1963) mental model
- This study will directly measure the effects of habituation using multiple devices simultaneously while synchronized using an Event-Related Potential (ERP) to reduce mono-operationalization bias and construct validation (Dimoka et al., 2012).

Background (Cont.)

- Tugade and Engle (2004) recommend measuring Working Memory Capacity (WMC) on an individual level when investigating DPT.
- WMC is defined as "the number of items that can be recalled during a complex working memory task" (Tugade & Engle, 2004, p. 553).
- Moreover, Tugade and Engle (2004) explained when individuals are comparing mental models "WMC will determine whether a person has sufficient attention recourse to engage in controlled processing" (p. 560).
- WMC can be measured through task called complex span task (Baddeley & Hitch, 1974).

Background (Cont.)

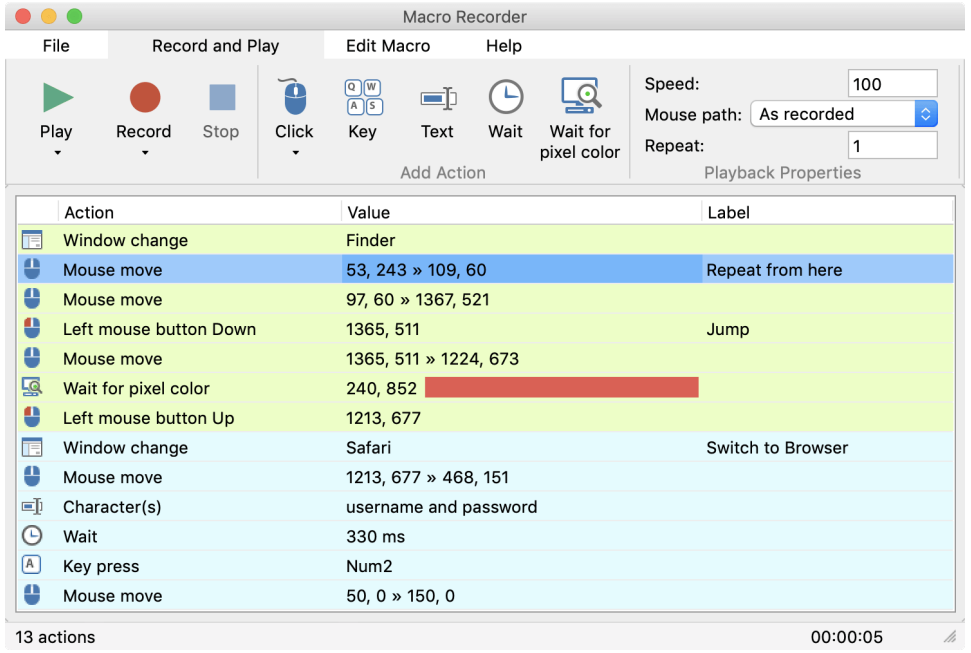
- Sunshine et al. (2009) investigated the effectiveness of SSL warnings by designing a multi-page warning system but found that users did not perform well at these tasks and often ignored the security warnings.
- Neupane et al. (2016) used a Functional Magnetic Resonance Imaging (fMRI) to study phishing and malware warnings, showing malware warnings had more brain activity than phishing warnings.
- Anderson et al. (2016a) who used an fMRI to study habituation with polymorphic image security warnings and animation security warnings, empirically showing reduction in RS.
- Anderson et al. (2016a) research extended Brustoloni and Villamarin-Salomon (2007) on context-sensitive guidance, which increased attention by using polymorphic dialogs.

Background (Cont.)

- EEG is used to measure the effects of habituation through Event-Related Potentials (ERPs) defined as "changes in electrical potential" (Grill-Spector et al., 2006, p. 16).
- The Event-Related Potential (ERP) record stimulus-specific Repetition Suppression (RS) defined as "the relative attenuation in neural signal evoked by the repeated occurrence of a stimulus" (Summerfield et al., 2008, p. 1004).

Background (Cont.)

- Anderson et al. (2015) relied on mouse cursor indicators to observe habituation, defined as "x, y coordinates and timestamp of each movement at a millisecond precision rate" (p. 2888) to calculate area under the curve, average speed and initial acceleration.
- "triangulate across measures" (Dimoka, 2012, p. 814).



Main Goal

- The main goal of this research study is to empirically assess through EEG data and mouse cursor indicators how tactile stimuli transmitted through a vibrating mouse would affect habituation, in the context of methodologies to mitigate the cybersecurity attacks vector. An added dimension of this study's goal is to empirically assess, through EEG data, the difference, if any, between static and polymorphic tactile stimuli effect on RS.

Research Questions

- The main research question that this study will address is:

  Are there any statistically significant differences in using tactile stimuli on RS and are there any statistically significant differences between polymorphic tactile stimuli and static tactile stimuli on reducing RS?

Research Questions (cont.)

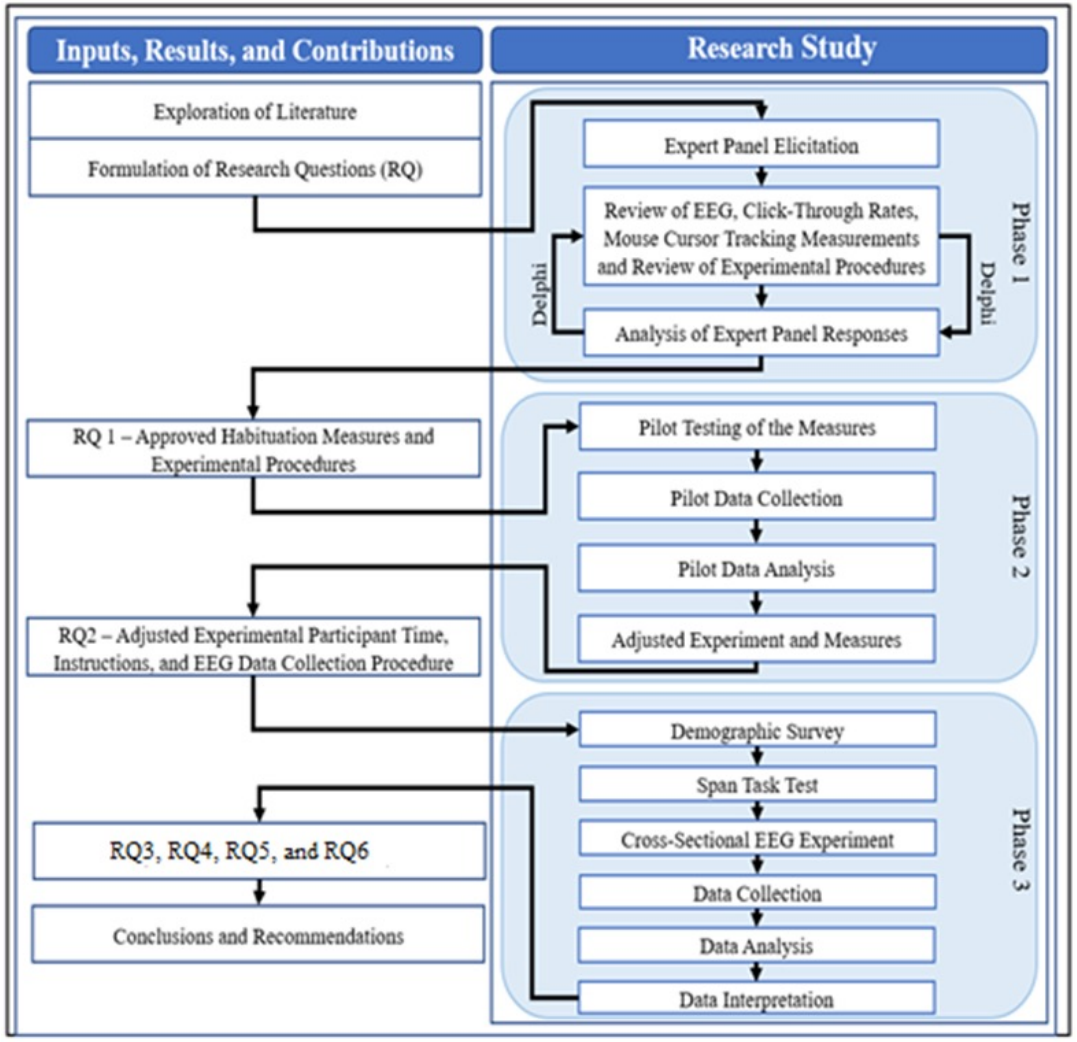
- RQ1: What are the experts' approved habituation measurements for EEG tactile and non-tactile stimuli, mouse cursor tracking, and the validation of the experimental participant task to capture habituation phenomenon?
- RQ2: What are the recommended results of pilot study for participants' time, instruction, and EEG data collection procedure?
- RQ3: Is there a significant impact of participants' working memory capacity as measured by span task test on their overall RS score?

Research Questions (cont.)

- RQ4: Are there any statistically significant mean differences on RS between tactile stimuli warnings and image warnings categories among participants?
- RQ5: Are there any statistically significant mean differences on mouse cursor indicator (area under the curve, initial acceleration, & average speeds) between tactile stimuli warnings and image warnings categories among participants?
- RQ6: Are there any statistically significant mean differences for RS when controlled for the categories of: (a) age, (b) gender, (c) number of speaking languages, (d) job type, (e) daily Internet usage, and (f) dominant hand orientation categories among participants?

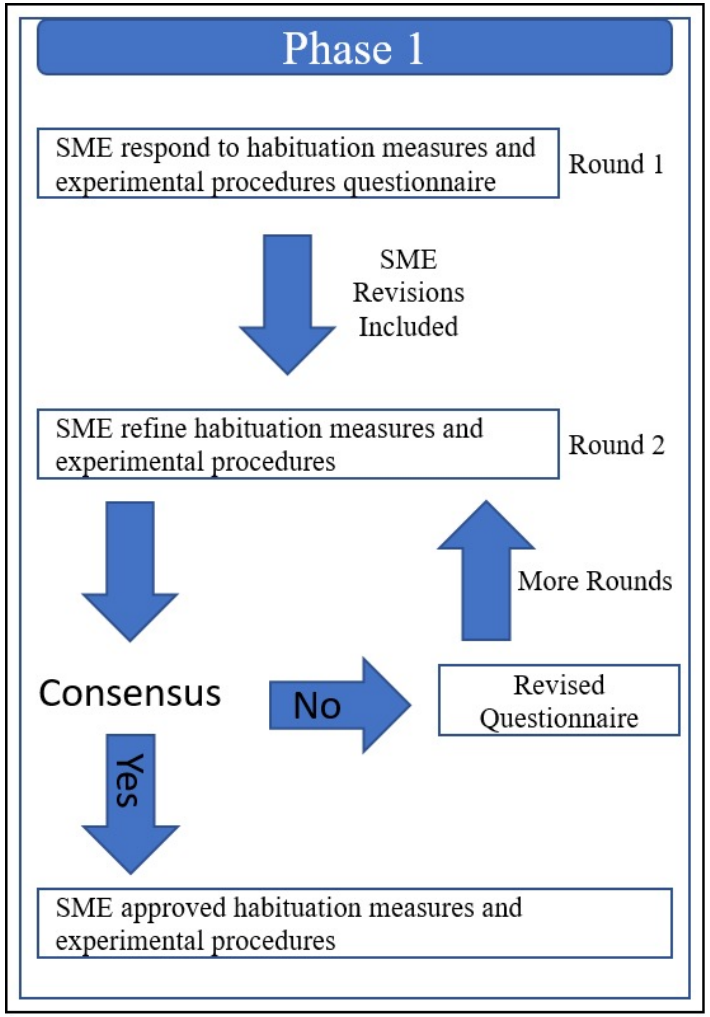
Research Design

- This study will have three phases:
  - Phase I: Subject Matter Experts (SMEs) will be surveyed using the Delphi technic
  - Phase II: A pilot study will be conducted
  - Phase III:
    - Demographic Survey
    - Span task test
    - Cross-sectional EEG experiment



Methodology – Phase I

- A SME panel of 15 to 30 experts will be established to review the measurements of the EEG headset, mouse cursor tracking metrics and the experimental procedures
- The Delphi methodology created in the 1950s by RAND Corporation to reach a consensus through multiply controlled feedback iterations to encourage and record debate amongst experts that may have different opinions (Dalkey & Helmer, 1963; Gordon & Glenn, 2009; Ramim & lichvar, 2014

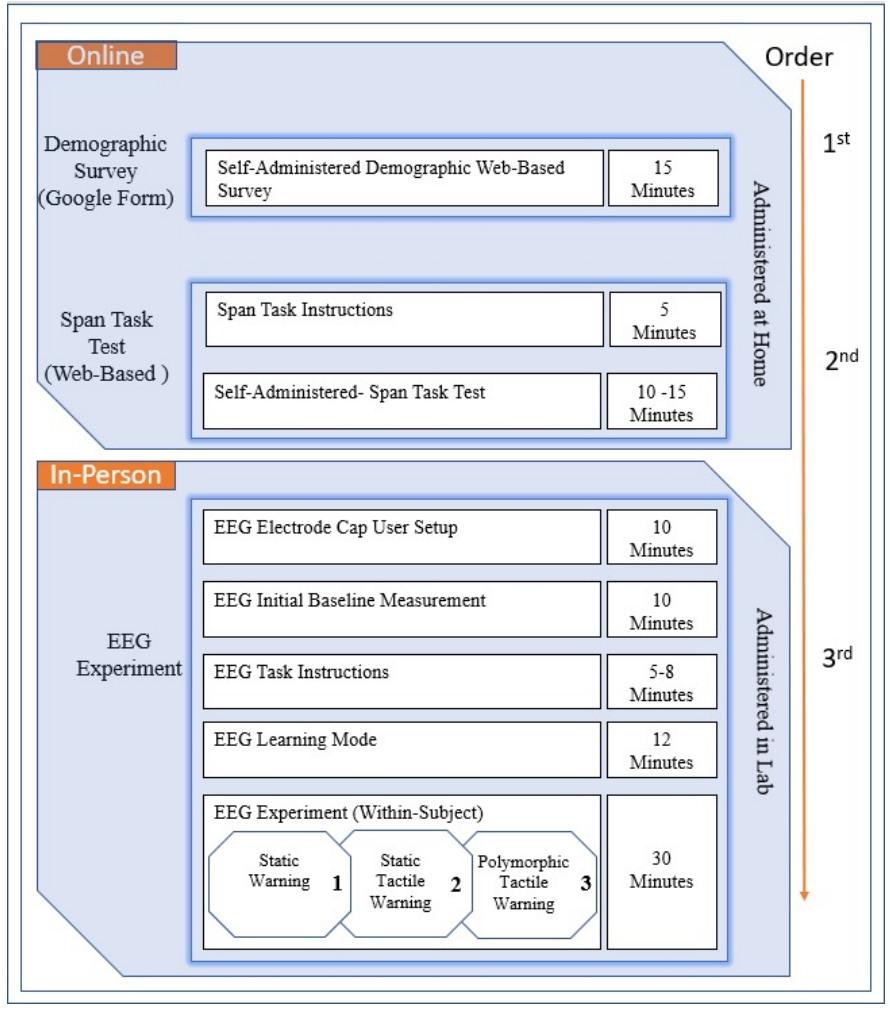


Methodology – Phase II

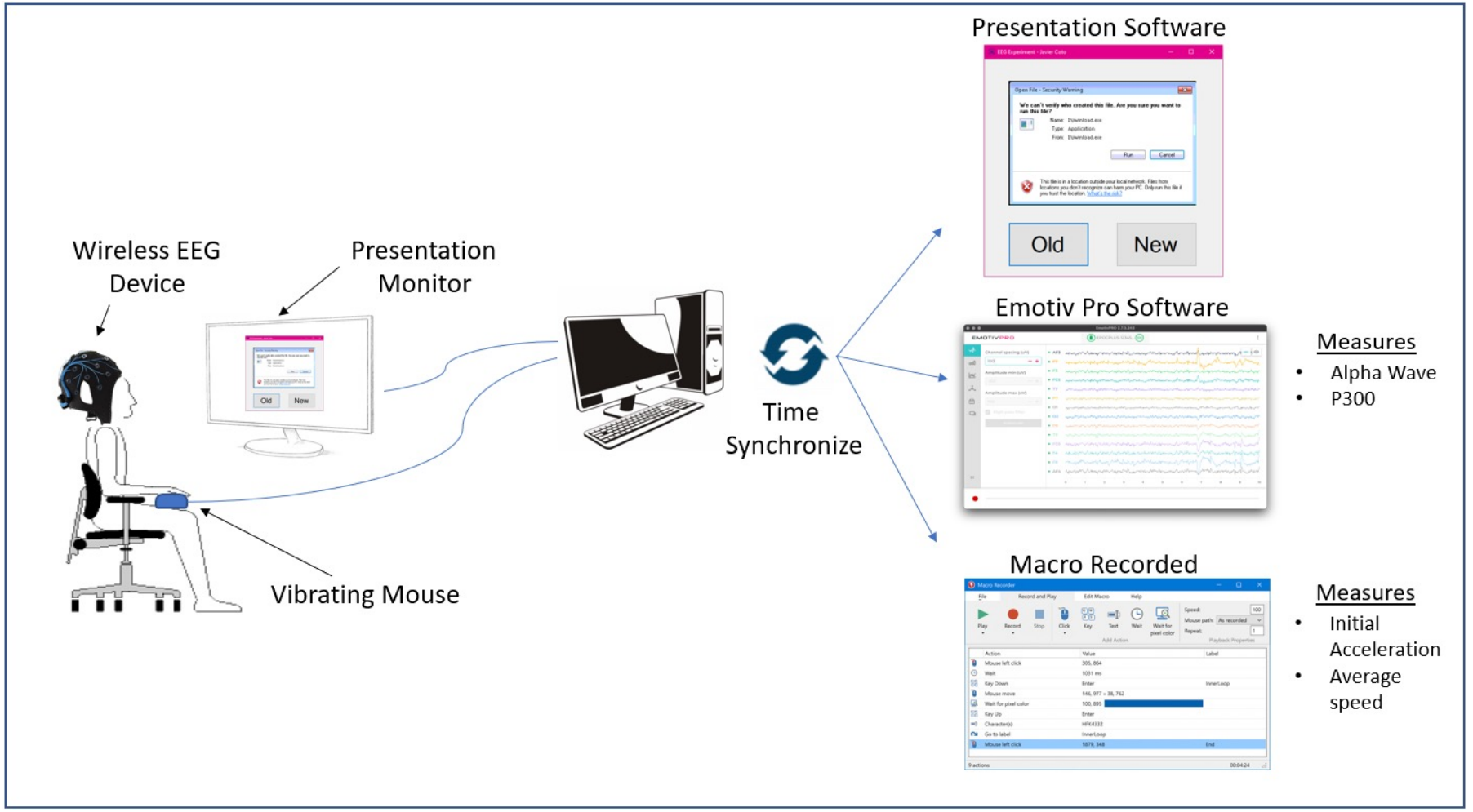
- Pilot study
- The outcome of the pilot study and data analysis will be used to refine and adjust all the experimental procedures and measures after the first real data is collected and analyzed.
- Verifies EEG electrode placement that correctly measures the brain area associated with habituation.
- Reenforces that the EEG Event-Related Potential (ERP) is capturing the intended data at the correct time and is synchronized with the warning stimuli prompt and the mouse indicator recording software.
- Ensures the mouse cursor tracking JavaScript program is capturing the correct data and is coordinated to the EEGs' ERPs.

Methodology - Phase III

- Online
  - Demographic survey
  - Attention Span test
- In-Person
  - EEG experiment
    - Administered in a mobile EEG lab
  - Data collection
  - Data analysis
  - Data interpretation

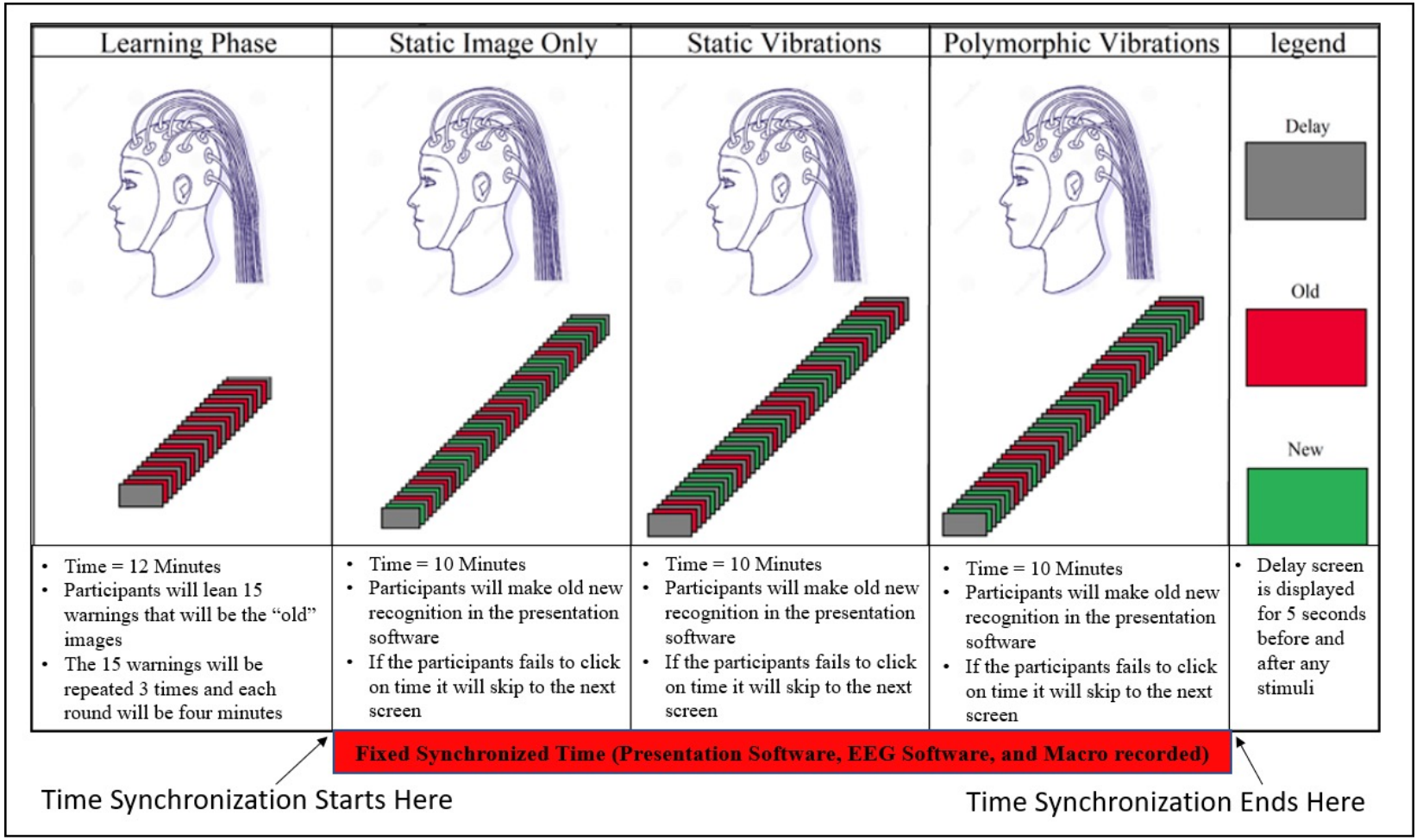


Methodology – Phase III (Cont.)



Methodology (Cont.)

- The EEG experiment consists of a learning phase followed by three 10-minute rounds where static images only, static tactile stimuli, and polymorphic tactile stimuli treatments will be tested



Methodology Summary

Variable	Measurements	Range	Source
Working memory capacity	Complex span task test score	0-100%	Chein & Morrison (2010) Tugade & Engle (2004) Baddeley & Hitch (1974)
Repetition suppression (RS)	Repetition suppression overall score (calculated by ERP's of fatigue model, sharpening model, or facilitation model)	0-100%	Riedl & Léger (2016) Vance et al. (2017) Vance et al. (2016) Grill-Spector et al. (2006) Summerfield et al. (2008)
Mouse cursor indicator	Area under the curve (greater AUC = greater attention) Initial Acceleration (lower Initial acceleration = greater attention) Average Speeds (lower average speed = greater attention)	0-100%	Anderson et al. (2015)

Experimental Design

- The data collection procedures will be quantitative
- Conducted as a cross-sectional lab experiment
- Unit of analysis of this study will be at the individual level
- 50 participants will be used, and three levels of treatments will be applied to each participant sequentially.

Validity and Reliability

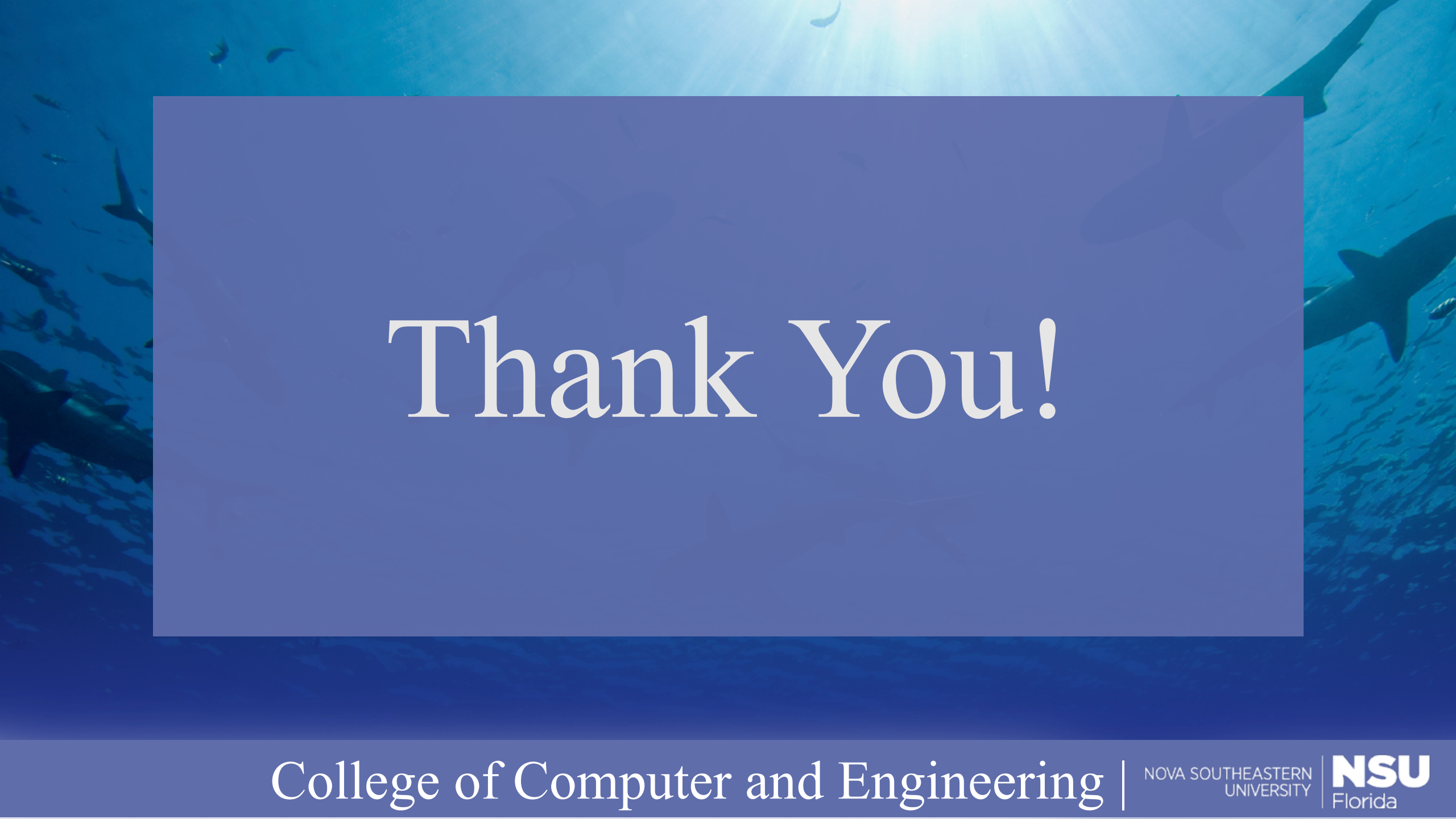
- **Internal validity**
  - This study attempts to increase the internal validity by adhering to Dimoka's (2012) recommendation of "triangulate across measures" (p. 814)
    - EEG Data
    - Mouse cursor indicators
      - Area Under the Curve (AUC)
      - Initial acceleration
      - Average speed
- **External validity**
  - The sample size of the study will be increased tenfold
  - SMEs will be used to confirm EEG measures
  - Rigorously attempted to follow the scholarly standards for the NeuroIS field (Brocke & Liang, 2014)

Discussion and Conclusions

- This study will answer the RQ in three phases
- The first phase refined the measurements and experimental procedures using SMEs following the Delphi methodology.
- The second phase consisted of a pilot study use to adjust further any measures, procedures, data collection, and participant's instructions
- The last phase, the experiment outcome will capture neurological data through an EEG machine for both static and polymorphic tactile stimuli and its effect on habituation to mitigate cybersecurity attacks

Limitations

- The setting used to simulate the phenomenon of habituation through a cross-sectional laboratory experiment
- The EEG headset with 32 electrodes, since most research grade EEG devices uses much more


Thank You!