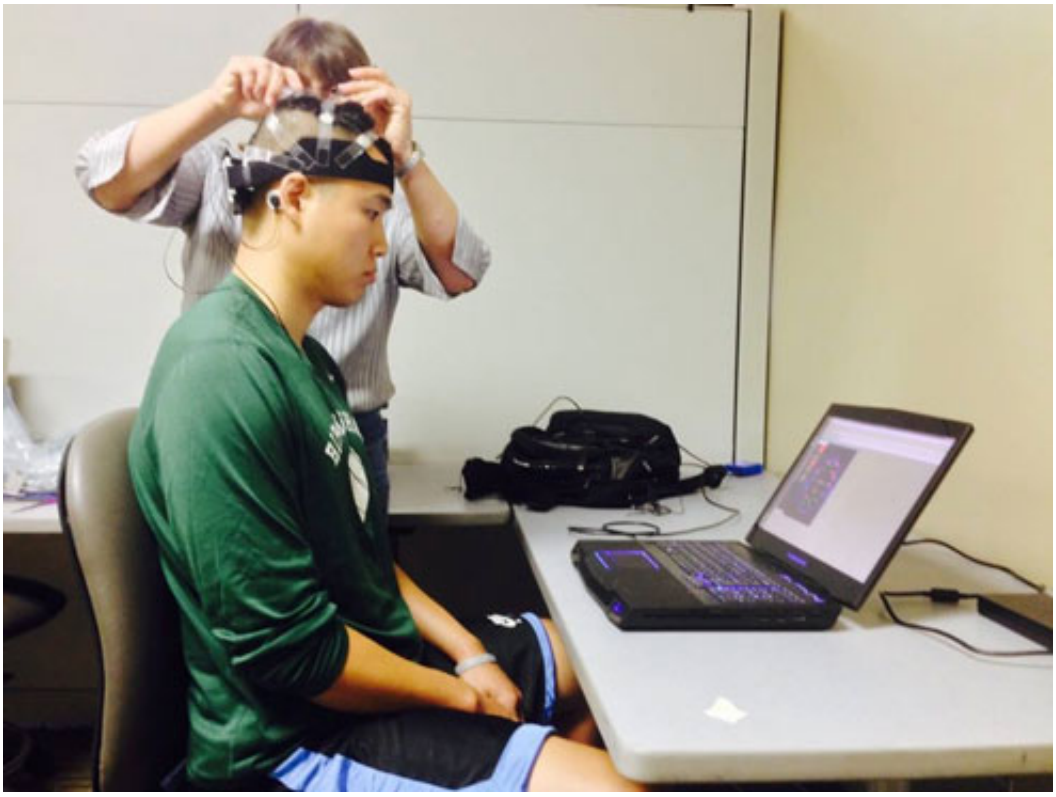
Research studies cyberattacks through the lens of EEG and eye tracking

October 23 2015



Setting up: The research team sets up an EEG headset for measurement of brain signals.

University of Alabama at Birmingham researchers have conducted a study that provides new insights on users' susceptibility to, and capability to detect, cyber-criminal attacks such as malware and phishing attacks.

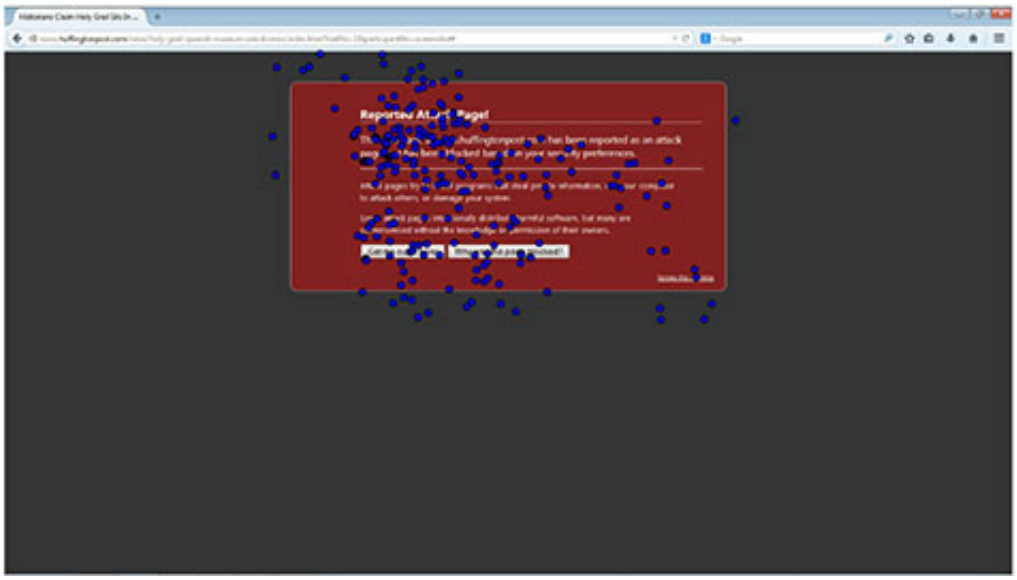
The study analyzed users' brain activity and eye gaze movements as they were subjected to these attacks. This new research was presented at the 2015 ACM Conference on Computer and Communications Security last week in Denver.

This study from researchers within the UAB College of Arts and Sciences Department of Computer and Information Sciences and Center for Information Assurance and Joint Forensics Research was based on the knowledge that detecting malware and phishing attacks are user-centered functions, but little is understood about the user behavior underlying these tasks.

There is some prior knowledge on this topic regarding users' performance in these security tasks, but UAB's research took the work to the next level by studying users in a near-reality setting and evaluating more than one neurophysiological measure during a single study.

Researchers took a three-dimensional approach to this study by looking at what the users' task performance was through evaluating how they process the tasks of detecting cyberattacks with neural activity, which was captured using electroencephalogram, or EEG, cognitive metrics and with eye gaze patterns, which were captured using an eye-tracker.

The evaluation process tested users on phishing attacks, which use malicious email to collect personal and financial information, as well as Web-based malware attacks, which deploy software to infect computers with viruses while users browse the Web.



Gaze patterns: The flow of fixations plotted on the screen, showing where participants held their eye gaze during the first warning trial.

"By looking at these three measures together, we were able to show that users do not spend enough time analyzing key phishing indicators, and often fail at detecting phishing attacks even when they are mentally engaged in the task and subconsciously processing real sites differently from fake sites," said Nitesh Saxena, Ph.D., the director of the Security and Privacy In Emerging computing and networking Systems (SPIES) lab and associate professor of computer and information sciences at UAB. "Under malware attacks, we found the opposite to be true. Users were found to be frequently reading, possibly comprehending and eventually heading the message embedded in the malware warning (such as the one provided by common browsers)."

"Overall, the way users respond to and process malware warnings is good news," said UAB graduate student Ajaya Neupane, co-author of the article with Saxena. "The gaze patterns show that users are reading the warnings, the neural activity shows that users are undergoing high

workload and are highly engaged when warnings were displayed, and the task accuracy shows that users heed warnings a large majority of the time."

Also, for phishing attacks, a direct correlation was found between the users' attention control, which is considered a personality trait, measured via a paper-and-pencil test, and how accurate they were at detection.

"We believe that means the users' susceptibility to phishing attacks is a function of their personality traits," Saxena said. "The more attentive they are by nature, the more likely they are to detect the phishing attacks."

These results give researchers the foundation upon which to begin designing mechanisms that will use real-time neural and eye-gaze features that can automatically infer a user's alertness state, and determine whether or not the user's response should be relied upon. Most interestingly, the insight that users' brains can subconsciously detect phishing attacks, even though users themselves may fail at detecting them, can be used to build future automated phishing detection mechanisms based on neural activity.

"We can begin thinking about developing ways to automatically detect whether users are attentive or inattentive, and whether they subconsciously detected a phishing attack," Neupane said. "Our research suggests that combining neural and ocular features might provide a robust detection system, which would result in higher user security measures."

Provided by University of Alabama at Birmingham