Study finds hackers could use brainwaves to steal passwords

June 29 2017, by Tiffany Westry Womack

Credit: University of Alabama at Birmingham

Researchers at the University of Alabama at Birmingham suggest that brainwave-sensing headsets, also known as EEG or electroencephalograph headsets, need better security after a study reveals

hackers could guess a user's passwords by monitoring their brainwaves.

EEG headsets are advertised as allowing users to use only their brains to control robotic toys and video games specifically developed to be played with an EEG headset. There are only a handful on the market, and they range in price from $150 to $800.

Nitesh Saxena, Ph.D., associate professor in the UAB College of Arts and Sciences Department of Computer and Information Sciences, and Ph.D. student Ajaya Neupane and former master's student Md Lutfor Rahman, found that a person who paused a video game and logged into a bank account while wearing an EEG headset was at risk for having their passwords or other sensitive data stolen by a malicious software program.

"These emerging devices open immense opportunities for everyday users," Saxena said. "However, they could also raise significant security and privacy threats as companies work to develop even more advanced brain-computer interface technology."

Saxena and his team used one EEG headset currently available to consumers online and one clinical-grade headset used for scientific research to demonstrate how easily a malicious software program could passively eavesdrop on a user's brainwaves. While typing, a user's inputs correspond with their visual processing, as well as hand, eye and head muscle movements. All these movements are captured by EEG headsets. The team asked 12 people to type a series of randomly generated PINs and passwords into a text box as if they were logging into an online account while wearing an EEG headset, in order for the software to train itself on the user's typing and the corresponding brainwave.

"In a real-world attack, a hacker could facilitate the training step required for the malicious program to be most accurate, by requesting

that the user enter a predefined set of numbers in order to restart the game after pausing it to take a break, similar to the way CAPTCHA is used to verify users when logging onto websites," Saxena said.

The team found that, after a user entered 200 characters, algorithms within the malicious software program could make educated guesses about new characters the user entered by monitoring the EEG data recorded. The algorithm was able to shorten the odds of a hacker's guessing a four-digit numerical PIN from one in 10,000 to one in 20 and increased the chance of guessing a six-letter password from about 500,000 to roughly one in 500.

EEG has been used in the medical field for more than half a century as a noninvasive method for recording electrical activity in the brain. Electrodes are placed on the surface of the scalp to detect brain waves. An EEG machine then amplifies the signals and records them in a wave pattern on graph paper or a computer. EEG can be combined with a brain-computer interface to allow a person to control external devices. This technology was once highly expensive and used mostly for scientific research, like the production of neuroprosthetic applications to help disabled patients control prosthetic limbs by thinking about the movements. However, it is now being marketed to consumers in the form of a wireless headset and is becoming popular in the gaming and entertainment industries.

"Given the growing popularity of EEG headsets and the variety of ways in which they could be used, it is inevitable that they will become part of our daily lives, including while using other devices," Saxena said. "It is important to analyze the potential security and privacy risks associated with this emerging technology to raise users' awareness of the risks and develop viable solutions to malicious attacks."

One potential solution proposed by Saxena and his team is the insertion

of noise anytime a user types a password or PIN while wearing an EEG headset.

Provided by University of Alabama at Birmingham