Headset EEG hacking gives new meaning to PINheads

August 22 2012, by Nancy Owano

(Phys.org) -- Researchers at the Usenix Security conference earlier this month demonstrated a way to get into your brain and learn facts that you don't want to reveal. Using a commercial off-the-shelf brain-computer interface, the researchers created a custom program designed to find out personal data such as address and PIN. The study, "On the Feasibility of Side-Channel Attacks with Brain-Computer Interfaces," is by Ivan Martinovic, Doug Davies, Mario Frank, Daniele Perito, Tomas Ros, and Dawn Song. The authors point out that it is just such a commercial off the shelf brain computer interface—costing a few hundred dollars—that can run the brain-hacking show.

"Consumer-grade BCI devices are available for a few hundred dollars and are used in a variety of applications, such as video games, hands-free keyboards, or as an assistant in relaxation training," according to the study. "There are application stores similar to the ones used for smart phones, where application developers have access to an API to collect data from the BCI devices," they note. As the security risks involved in using consumer-grade BCI devices have not been studied, and the impact of malicious software with device access unexplored, the team had their work cut out for them.

After having a look at the devices' security implications, they have concluded that the technology can be turned against people to reveal information the victims assume is secret.

Brain-computer interfaces, or BCIs, have been used in medical settings,

involving expensive equipment, but the researchers concerned themselves with cheaper, commercial devices. (For example, Emotiv offers an Emotiv EPOC described as a high resolution, neuro-signal acquisition and processing wireless neuroheadset for $299 and NeuroSky offers inexpensive BCI "neuroscience headsets" with a company motto, "brain wave sensors for everybody.")

The researchers, who are from the universities of Oxford and Geneva and University of California, Berkeley, tested their mind-reading program using an Emotiv EEG device on 28 participants.

The subjects did not know their brains were being used to extract private information; they were only told that they were going to participate in an experiment involving the privacy implications of using gaming EEG devices.

After carrying out a number of experiments, they showed the feasibility of using a cheap consumer-level BCI gaming device to partially reveal private information of the users. By analyzing EEG signals in their experiments, they were able to detect which of presented stimuli were related to the user's private information—credit cards, PIN numbers, persons known to the user, and user's residence.

The team said, "We show that the entropy of the private information is decreased on the average by approximately15% to 40% compared to random guessing attacks."

Their work was supported by National Science Foundation grants, Intel ISTC for Secure Computing, and the Carl-Zeiss Foundation.

More information: www.usenix.org/conference/usen … -computer-interfaces