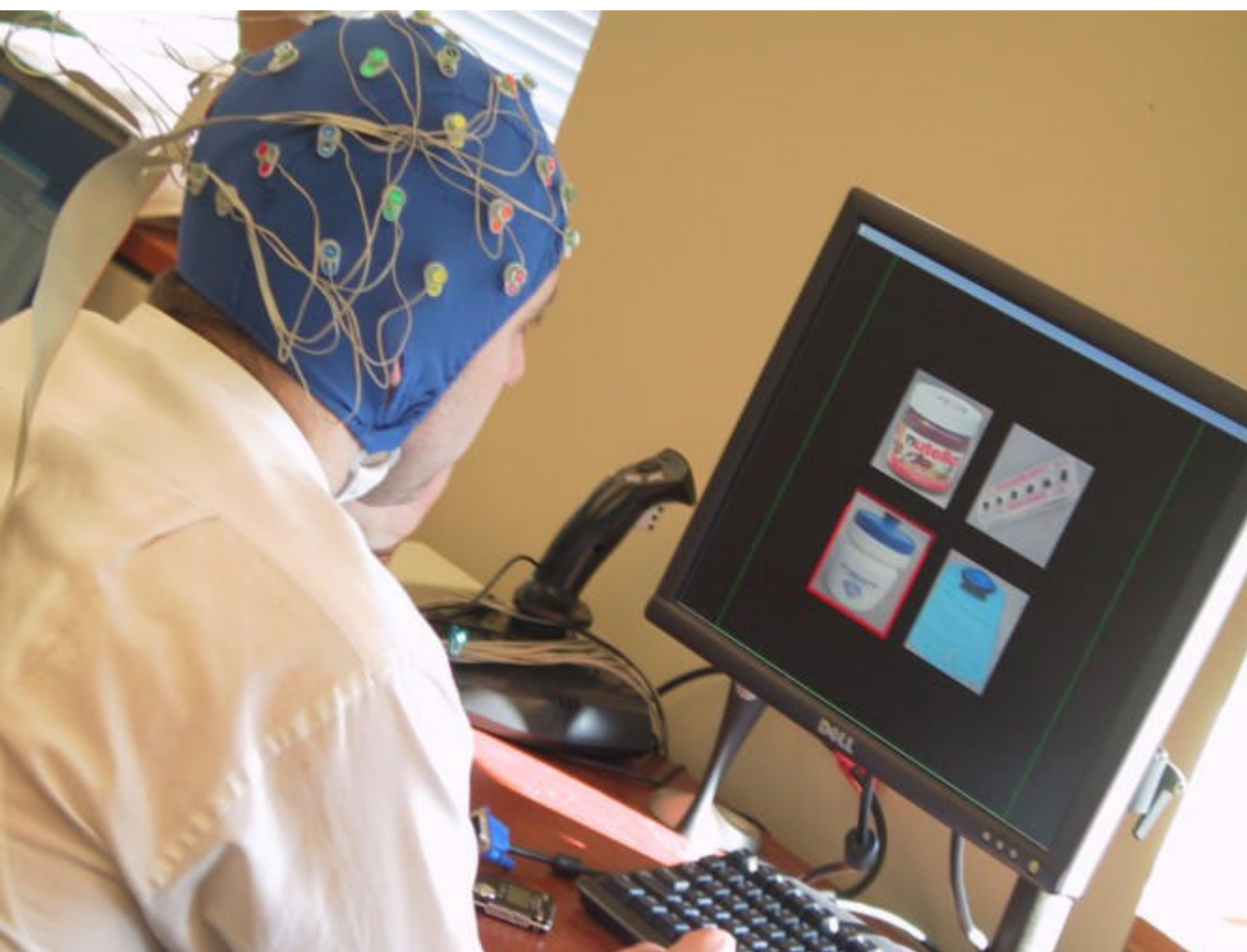


The Next Hacking Frontier: Your Brain?

By [Hadley Leggett](#)  July 9, 2009 | 12:59 pm | Categories: [Biotech](#), [Brains and Behavior](#), [Ethics](#)



Hackers who commandeer your computer are bad enough. Now scientists worry that someday, they'll try to take over your brain.

433
diggs

[digg it](#)

In the past year, researchers have developed technology that makes it possible to use thoughts to [operate a computer](#), [maneuver a wheelchair](#) or even [use Twitter](#) — all without lifting a finger. But as neural devices become more complicated — and go wireless — some scientists say the risks of “brain hacking” should be taken seriously.

“Neural devices are innovating at an extremely rapid rate and hold tremendous promise for the future,” said computer security expert Tadayoshi Kohno of the University of Washington. “But if we don’t start paying attention to security, we’re worried that we might find ourselves in five or 10 years saying we’ve made a big mistake.”

Hackers tap into personal computers all the time — but what would happen if they focused their nefarious energy on neural devices, such as the deep-brain stimulators currently used to treat Parkinson’s and depression, or electrode systems for

controlling prosthetic limbs? According to Kohno and his colleagues, who published their concerns July 1 in [Neurosurgical Focus](#), most current devices carry few security risks. But as neural engineering becomes more complex and more widespread, the potential for security breaches will mushroom.

For example, the next generation of implantable devices to control prosthetic limbs will likely include wireless controls that allow physicians to remotely adjust settings on the machine. If neural engineers don't build in security features such as encryption and access control, an attacker could hijack the device and take over the robotic limb.

"It's very hard to design complex systems that don't have bugs," Kohno said. "As these medical devices start to become more and more complicated, it gets easier and easier for people to overlook a bug that could become a very serious risk. It might border on science fiction today, but so did going to the moon 50 years ago."

Some might question why anyone would want to hack into someone else's brain, but the researchers say there's a precedent for using computers to cause neurological harm. In November 2007 and March 2008, malicious programmers [vandalized epilepsy support websites](#) by putting up flashing animations, which caused seizures in some photo-sensitive patients.

"It happened on two separate occasions," said computer science graduate student Tamara Denning, a co-author on the paper. "It's evidence that people will be malicious and try to compromise peoples' health using computers, especially if neural devices become more widespread."

In some cases, patients might even want to hack into their own neural device. Unlike devices to control prosthetic limbs, which still use wires, many deep brain stimulators already rely on wireless signals. Hacking into these devices could enable patients to "self-prescribe" elevated moods or pain relief by increasing the activity of the brain's reward centers.

Despite the risks, Kohno said, most new devices aren't created with security in mind. Neural engineers carefully consider the safety and reliability of new equipment, and neuroethicists focus on whether a new device fits ethical guidelines. But until now, few groups have considered how neural devices might be hijacked to perform unintended actions. This is the first time an academic paper has addressed the topic of "neurosecurity," a term the group coined to describe their field.

"The security and privacy issues somehow seem to slip by," Kohno said. "I would not be surprised if most people working in this space have never thought about security."

Kevin Otto, a bioengineer who studies brain-machine interfaces at Purdue University, said he was initially skeptical of the research. "When I first picked up the paper, I don't know if I agreed that it was an issue. But the paper gives a very compelling argument that this is important, and that this is the time to have neural engineers collaborate with security developers."

It's never too early to start thinking about security issues, said neural engineer Justin Williams of the University of Wisconsin, who was not involved in the research. But he stressed that the kinds of devices available today are not susceptible to attack, and that fear of future risks shouldn't impede progress in the field. "These kinds of security issues have to proceed in lockstep with the technology," Williams said.

History provides plenty of examples of why it's important to think about security before it becomes a problem, Kohno said. Perhaps the best example is the internet, which was originally conceived as a research project and didn't take security into account.

"Because the internet was not originally designed with security in mind," the researchers wrote, "it is incredibly challenging — if not impossible — to retrofit the existing internet infrastructure to meet all of today's security goals." Kohno and his colleagues hope to avoid such problems in the neural device world, by getting the community to discuss potential security problems before they become a reality.

"The first thing is to ask ourselves is, 'Could there be a security and privacy problem?'" Kohno said. "Asking 'Is there a problem?' gets you 90 percent there, and that's the most important thing."

Via [Mind Hacks](#)