Neurosurg Focus 27 (1):E7, 2009

Neurosecurity: security and privacy for neural devices

Tamara Denning, B.S., Yoky Matsuoka, Ph.D., and Tadayoshi Kohno, Ph.D.

Department of Computer Science and Engineering, University of Washington, Seattle, Washington

An increasing number of neural implantable devices will become available in the near future due to advances in neural engineering. This discipline holds the potential to improve many patients' lives dramatically by offering improved—and in some cases entirely new—forms of rehabilitation for conditions ranging from missing limbs to degenerative cognitive diseases. The use of standard engineering practices, medical trials, and neuroethical evaluations during the design process can create systems that are safe and that follow ethical guidelines; unfortunately, none of these disciplines currently ensure that neural devices are robust against adversarial entities trying to exploit these devices to alter, block, or eavesdrop on neural signals. The authors define "neurosecurity"—a version of computer science security principles and methods applied to neural engineering—and discuss why neurosecurity should be a critical consideration in the design of future neural devices. *(DOI: 10.3171/2009.4.FOCUS0985)*

Key Words • neural engineering • computer security • neurosecurity • implantable device

A 2007 WHO report indicated that neurological disorders—such as injury, spina bifida, stroke, encephalitis, multiple sclerosis, Parkinson disease, and Alzheimer disease—affect up to 1 billion people worldwide.[21] Unlike traditional approaches that stress accommodation of the needs of the neurologically affected via drug interventions or intrusive and costly home or hospital care, neural engineering combines cutting-edge technologies to develop a proactive role in understanding more about how the nervous system works, in order to provide rapid, complete, and effective treatment, rehabilitation, and assistance. These technologies can allow patients to experience more freedom and independence in their daily lives than ever before.

The possibility of controlling electromechanical systems via neural signals opens up an enormous application space. There is exciting potential to enhance people's well-being: can we make paralyzed limbs usable again? Can we leverage early diagnoses of neural disease to prevent the onset? Can we use neural signals to operate remote robotic systems in dangerous, time-sensitive environments, thereby preserving human lives? And what about enhancing human capabilities? The military might want to use neural engineering to allow combat personnel to function at a higher level than the average human capabilities; others might want to enhance an elderly brain by allowing it to function like a young, healthy brain—beyond what is possible by traditional therapy. Technologies such as these are not fantasy; they are already funded research.

Standard engineering and medical practices seek to ensure that neural engineering systems are safe for the patient to use. Neuroethics, on the other hand, strives to ensure that the therapies produced by neural engineering follow certain ethical guidelines and respect the sanctity of the individual.[11] To date, neither of these approaches considers how a neural device might be appropriated to perform unintended actions that are unethical or unsafe. In this paper we define "neurosecurity" and discuss related challenges that will arise as neural engineering technologies continue to evolve. In addition, we discuss why neurosecurity must be a critical consideration in the design of future neural devices.

Defining Neurosecurity

Computer security and privacy is a field within computer science dedicated to the design and engineering of technologies so that they behave as intended, even in the presence of malicious third parties who seek to compromise the operations of the device. These malicious parties are often called hackers, attackers, or adversaries. Three of the standard goals in computer security are confidentiality, integrity, and availability: an attacker should

Abbreviation used in this paper: DBS = deep brain stimulator.

not be able to exploit the properties of a device to learn private information (confidentiality); an attacker should not be able to change device settings or initiate unauthorized operations (integrity); and an attacker should not be able to disable a device altogether and render it ineffective (availability). We define neurosecurity as the protection of the confidentiality, integrity, and availability of neural devices from malicious parties with the goal of preserving the safety of a person's neural mechanisms, neural computation, and free will.

Neurosecurity is not a critical concern for current neural engineering devices, which have limited deployment outside of research environments or are self-contained systems; however, unless appropriate safeguards are considered early in the design of the neural devices that will be deployed within 5–20 years, security and privacy concerns could become critical. We view it as the community's responsibility to assess and develop technical approaches for mitigating these threats—before any serious risks manifest. We base our argument on several facts. First, security vulnerabilities have already been found in implanted medical devices. In our past research, we experimentally demonstrated that a hacker could wirelessly compromise the security and privacy of a representative implantable medical device: an implantable cardiac defibrillator introduced into the US market in 2003. Specifically, our prior research found that a third party, using his or her own homemade and low-cost equipment, could wirelessly change a patient's therapies, disable therapies altogether, and induce ventricular fibrillation (a potentially fatal heart rhythm).[10] Although we only conducted our experiments using short-range, 10-cm wireless communications, and although we believe that the risk of an attack on a patient today is very low, the implications are clear: unless appropriate safeguards are in place, a hacker could compromise the security and privacy of a medical implant and cause serious physical harm to a patient.

We believe that some future hackers—if given the opportunity—will have no qualms in targeting neural devices. We have already seen examples of malcontents and vandals using computers in an attempt to cause physical harm to patients: in both November 2007 and March 2008 individuals placed flashing animations on epilepsy support websites, causing some patients with photosensitive epilepsy to experience seizures.[9,17] In the context of a neural device, there is an added risk that these vandals can take advantage of neural plasticity to make longer-term alterations to a person's neural computation. There have also been cases of illegal self-prescription in which patients tried to use their own implantable medical devices to cause themselves harm.[1] Patients with neural devices may self-prescribe in an attempt to enhance their performance, increase their level of pain relief, or overstimulate the reward centers in the brain.

Our stance is based on the experiences of the computer security community in other domains. The Internet is a prime example of the consequences of designing a system without giving due consideration to security and privacy: the Internet was created in simpler times. Its creators and early users shared a common goal—they wanted to build a network infrastructure to hook all the computers in the world together so that as yet unknown applications could be invented to run there. All the players, whether designers, users, or operators, shared a consistent vision and a common sense of purpose.[5]

When the Internet was originally designed and built as a research project, security was not a critical concern. Yet, as we all know, security concerns on the Internet are now a daily issue. Furthermore, because the Internet was not originally designed with security in mind, it is incredibly challenging—if not impossible—to retrofit the existing Internet infrastructure to meet all of today's security goals. Realizing this, the National Science Foundation initiated a major long-term research initiative targeted at creating a new, global Internet, predicated on the assumption that the best solution may be to start over from scratch, incorporating security into the system's design from the beginning.[7] We have seen similar situations arise in other contexts, such as electronic voting.[12]

We are at a similar stage in the evolution of neural engineering as we were at the Internet's inception: neurosecurity is not an issue today, but it could be an important concern in the future. The consequence of a neurosecurity breach can be far worse than a breach in the Internet's security; instead of protecting the software on someone's computer, we are protecting a human's ability to think and enjoy good health. Rather than wait for these concerns to manifest—at which point it may be too late to retrofit security into mature designs—we must begin to consider neurosecurity now.

Exploring Neurosecurity

We expect neural devices to follow several technological trends that will—if realized—serve to increase neurosecurity risks. The first trend is the use of wireless communications. Existing implantable medical devices, such as the latest generation of pacemakers and implantable defibrillators, can wirelessly send and receive signals up to a range of 5 m. Wireless communications are a valuable convenience in clinical settings and surgical environments. In the home, these implantable devices can connect to a wireless bedside monitor and provide nonintrusive monitoring while the patient sleeps. Wireless communication capabilities for neural devices are similarly attractive.[19] Some of the neural devices that are being developed in research labs today can already connect wirelessly to external computers. It is easy to imagine that it might also be desirable to set up home monitors for patients with neural devices. In the future we can also expect multiple implants within a patient's body to be wirelessly interconnected; for example, neural signals from the motor cortex could be wirelessly transmitted to a robotic prosthetic leg. Another trend is the increase of complexity: as the components used in neural systems become more complex, more integrated, and influence a larger set of neurons, it will become harder to identify and defend against all potential security vulnerabilities.

To ground this discussion, we give several examples of how neurosecurity concerns could manifest in neural devices. We present examples from the forefront of to-

day's neural engineering research and discuss how they might be subject to neurosecurity concerns. We wish to stress that the neurosecurity issues we identify below are based on current hypotheses of how these devices may evolve over time. For each of the technologies below, we give examples of how they relate to the 3 tenets of neurosecurity: confidentiality, integrity, and availability.

Prosthetic Limbs

Significant innovation is occurring in the realm of neurally controlled prosthetic limbs.[3,4,13,14,18,20–23] We hypothesize that future prosthetic limb systems will allow physicians to connect wirelessly to a neural implant to adjust settings. These future systems must guard against a hacker trying to hijack these signals to take control of the robotic limb or give erroneous movement feedback to the patient (integrity). The attacker does not need to be near the patient—the attacker only needs to have attack hardware placed near the patient. The attacker could also infect the patient's biotech components with a digital virus. The patient can also be the attacker and try to modify the settings on his or her own prosthetic limb—perhaps with the intention of overriding mechanical safety settings to gain extra strength or interfering with limb feedback to eliminate the ability to sense pain.

These prosthetic systems must also guard against hackers trying to prevent the patient from using the limb, particularly since this can occur while he or she is running, driving, or climbing stairs (availability). In addition, these systems should prevent a hacker from remotely eavesdropping on the wireless signals and collecting private information about the patient's activities (confidentiality). Such confidentiality attacks could range from learning what keys a person's prosthetic limb is typing on a keyboard to a person's intended movements—before those movements have taken place.

Deep Brain Stimulator

Some neural engineering devices are designed to stimulate regions of the brain itself. Current-generation DBSs have had success treating Parkinson disease, chronic pain, and other medical conditions.[6,8,16] The security vulnerabilities in today's devices are probably minimal; however, as future DBSs become more ubiquitous, technologically capable, and address broader clinical needs, neurosecurity will become a more pressing issue. For example, patients may attempt to self-prescribe elevated moods or increased activation of reward centers in the brain, whereas hackers may attempt to program the stimulation therapy maliciously (integrity). The hacker's strategy does not need to be too sophisticated if he or she only wants to cause harm; it is possible to cause cell death or the formation of meaningless neural pathways by bombarding the brain with random signals. Alternatively, a hacker might wirelessly prevent the device from operating as intended (availability). We must also ensure that DBSs protect the feelings and emotions of patients from external observation (confidentiality). Furthermore—if he or she is receiving treatment for a socially sensitive condition such as depression—a patient might also want to prevent a wireless hacker from detecting the presence of the DBS.

Cognitive Function Augmentation

Another branch of neural engineering research rehabilitates cognitive function by using neural engineering to bridge damaged brain tissue; an example of this is memory augmentation.[2] Several neurosecurity concerns may arise as these technologies transition from research studies to real deployments in patients with Alzheimer and other diseases. A hacker should not be able to alter the settings of the device wirelessly to stimulate the brain in an unsafe manner or to interfere with the normal formation of memories (integrity); for example, a hacker should not be able to cause disproportionately intense memories or cause unimportant things to become long-term memories. As noted above, the plasticity of the brain can cause spurious electrical signals to make long-term alterations to the brain's normal function.

Because these technologies will be intimately connected to a patient's cognitive functions, we must ensure that future technological advances do not unintentionally jeopardize the privacy of an individual's mind (confidentiality). For example, if it is possible to determine whether a patient is familiar with something by wirelessly eavesdropping on the implant's signals, then neurosecurity dictates that the implant should be designed to conceal this information; otherwise, the patient could be forced to reveal potentially private information. Last, we must ensure that a hacker cannot simply disable the device, thereby causing unexpected gaps in a patient's memory (availability).

Conclusions

Cutting-edge neural devices are being tested to gauge their ability to withstand physical perturbation;[15] it is now time to consider their ability to withstand security perturbation. Our interest in neurosecurity is not to protect the clinical devices of today, where patient risk is low, but to assure that neural devices are designed to withstand future risks. Without such foresight and attention, we worry that unexpected but serious neurosecurity issues may arise with future neural devices. In this paper we define neurosecurity and introduce some key concepts that may shape the area.

Neurosecurity will probably face technical challenges that are dramatically different from those of traditional computer security applications. It is easy to ask a computer user to make security decisions in response to pop-up windows; in contrast, it would be difficult to ask the users of neural devices to make rapid meta-decisions about their own brains. Furthermore, the consequence of a breach in neurosecurity—where human health and free will are at stake—is very different from a breach in computer security, where the victim is a computer on a desk. Due to the elegant yet little-understood plasticity of the neural system, changes made by hackers could have irreversible effects on human performance and cognition. By focusing on neurosecurity issues early, we hope to ensure that future neural devices are not only safe, effective,

and ethically designed, but that they are also robust in the face of adversaries attempting to co-opt their operations to perform unintended, unsafe actions.

Disclosure

Financial support was received through an Alfred P. Sloan Research Fellowship awarded to Dr. Kohno. No portion of this paper has been presented or published previously.

References

1. Associated Press: **FDA: Insulin Pumps Linked to Deaths, Injuries in Teens**, 2008 (http://www.foxnews.com/story/0,2933,354133,00.html) [Accessed 14 March 2009]
2. Berger TW, Ahuja A, Courellis SH, Deadwyler SA, Erinjippurath G, Gerhardt GA, et al: Restoring lost cognitive function. **IEEE Eng Med Biol Mag 24:**30–44, 2005
3. Chapin JK: Using multi-neuron population recordings for neural prosthetics. **Nat Neurosci 7:**452–455, 2004
4. Chapin JK, Moxon KA, Markowitz RS, Nicolelis MA: Realtime control of a robot arm using simultaneously recorded neurons in the motor cortex. **Nat Neurosci 2:**664–670, 1999
5. Clark DD, Wroclawski J, Sollins KR, Braden R: Tussle in cyberspace: defining tomorrow's internet. **IEEE/ACM Trans Networking 13**:462–475, 2005
6. Coffey, RJ: Deep brain stimulation for chronic pain: Results of two multicenter trials and a structured review. **Pain Medicine 2:** 183–192: 2008
7. Computing Research Association: **NSF Future Internet Network Design Informational Meeting**, 2007 (http://www.cra.org/nsf.find/information.november) [Accessed 14 March 2009]
8. Deuschl G, Schade-Brittinger C, Krack P, Volkmann J, Schafer H, Botzel K, et al: A randomized trial of deep-brain stimulation for Parkinson's disease. **New Engl J Med 355:** 896–908, 2006
9. Ertl B: **Hooligans Attack Epilepsy Patients During Epilepsy Awareness Month**, 2007 (http://www.pr.com/press-release/60959) [Accessed 14 March 2009]
10. Halperin D, Heydt-Benjamin TS, Ransford B, Clark SS, Defend B, Morgan W, et al: Pacemakers and implantable cardiac defibrillators: software radio attacks and zero-power defenses, in IEEE (ed): **IEEE Symposium on Security and Privacy**. Los Alamitos: IEEE Computer Society Conference Publishing Services, 2008, pp 129–142
11. Illes J: **Neuroethics: Defining the Issues in Theory, Practice and Policy**. New York, NY: Oxford University Press USA, 2005
12. Kohno T, Stubblefield A, Rubin AD, Wallach DS: Analysis of an electronic voting system, in IEEE (ed): **IEEE Symposium on Security and Privacy**. Los Alamitos: IEEE Computer Society Conference Publishing Services, 2004, pp 27–40
13. Lucas L, DiCicco M, Matsuoka Y: An EMG-controlled hand exoskeleton for natural pinching. **J Robot Mechatron 16:**482–488, 2004
14. Matsuoka Y, Afshar P, Oh M: On the design of robotic hands for brain machine interface. **Neurosurg Focus 20(5)**:E3, 2006
15. Mavoori J, Jackson A, Diorio C, Fetz E: An autonomous implantable computer for neural recording and stimulation in unrestrained primates. **J Neurosci Methods 148:**71–77, 2005
16. Mayberg H, Lozano A, Voon V, McNeely H, Semionwicz D, Hamani C, et al: Deep brain stimulation for treatment-resistant depression. Neuron 5: 651[en dash]660, 2005
17. Poulsen K: Hackers assault epilepsy patients via computer, in **Wired.** March 28, 2008 (http://www.wired.com/politics/security/news/2008/03/epilepsy) [Accessed 14 March 2009]
18. Santucci DM, Kralik JD, Lebedev MA, Nicolelis MAL: Frontal and parietal cortical ensembles predict single-trial muscle activity during reaching movements in primates. **Eur J Neurosci 22:**1529–1540, 2005
19. Schwartz AB, Cui XT, Weber DJ, Moran DW: Brain-controlled interfaces: movement restoration with neural prosthetics. **Neuron 52:**205–220, 2006
20. Serruya MD, Hatsopoulos N, Paninski L, Fellows M, Donoghue J: Instant neural control of a movement signal. **Nature 416:**141–142, 2002
21. Stein RB, Mushahwar V: Reanimating limbs after injury or disease. **Trends Neurosci 28:**518–524, 2005
22. Taylor DM, Tillery SH, Schwartz AB: Direct cortical control of 3D neuroprosthetic devices. **Science 296:**1829–1832, 2002
23. Velliste M, Perel S, Spalding MC, Whitford AS, Schwartz AB: Cortical control of a prosthetic arm for self-feeding. **Nature 453**:1098-1101, 2008
24. World Health Organization: **World Health Statistics 2007**. 2007 (http://www.who.int/whosis/whostat2007/en/index.html) [Accessed 14 March 2009]

Manuscript submitted March 15, 2009.
Accepted April 16, 2009.

Address correspondence to: Tadayoshi Kohno, Ph.D., Department of Computer Science and Engineering, Box 352350, University of Washington, Seattle, Washington 98195-2350. email: yoshi@cs.washington.edu.