



Brainjacking: Implant Security Issues in Invasive Neuromodulation

Laurie Pycroft¹, Sandra G. Boccard¹, Sarah L.F. Owen³, John F. Stein², James J. Fitzgerald¹, Alexander L. Green¹, Tipu Z. Aziz¹

Key words

- Brainjacking
- Cybersecurity
- Deep brain stimulation
- Hacking
- Implantable medical device
- Implantable pulse generator
- Medical device security
- Neurosecurity
- Neurosurgery

Abbreviations and Acronyms

DBS: Deep brain stimulation
ET: Essential tremor
FDA: US Food and Drug Administration
ICD: Impulse control disorder
IPG: Implantable pulse generator
NAcc: Nucleus accumbens
OCD: Obsessive-compulsive disorder
PD: Parkinson disease
STN: Subthalamic nucleus

From the ¹Oxford Functional Neurosurgery, University of Oxford, John Radcliffe Hospital, Headington; ²Department of Physiology, Anatomy, and Genetics, Sherrington Road; and ³Department of Applied Health and Professional Development, Oxford Brookes University, Headington Campus, Oxford, United Kingdom

To whom correspondence should be addressed:
 Laurie Pycroft, M.Sc.
 [E-mail: laurie.pycroft@nds.ox.ac.uk]

Citation: *World Neurosurg.* (2016) 92:454–462.
<http://dx.doi.org/10.1016/j.wneu.2016.05.010>

Journal homepage: www.WORLDNEUROSURGERY.org

Available online: www.sciencedirect.com

1878-8750/\$ - see front matter © 2016 Elsevier Inc. All rights reserved.

INTRODUCTION

The concept of altering human conscious experience and behavior with unauthorized manipulation of implanted electronic devices dates back to science fiction literature of the 1980s, when authors began to speculate about the advantages and pitfalls offered by hypothetical electronic neural implants.^{1,2} Until recently the risk of neurological implants being used against their users was firmly in the realm of fantasy. However, the increasing sophistication of invasive neuromodulation, coupled

The security of medical devices is critical to good patient care, especially when the devices are implanted. In light of recent developments in information security, there is reason to be concerned that medical implants are vulnerable to attack. The ability of attackers to exert malicious control over brain implants (“brainjacking”) has unique challenges that we address in this review, with particular focus on deep brain stimulation implants. To illustrate the potential severity of this risk, we identify several mechanisms through which attackers could manipulate patients if unauthorized access to an implant can be achieved. These include blind attacks in which the attacker requires no patient-specific knowledge and targeted attacks that require patient-specific information. Blind attacks include cessation of stimulation, draining implant batteries, inducing tissue damage, and information theft. Targeted attacks include impairment of motor function, alteration of impulse control, modification of emotions or affect, induction of pain, and modulation of the reward system. We also discuss the limitations inherent in designing implants and the trade-offs that must be made to balance device security with battery life and practicality. We conclude that researchers, clinicians, manufacturers, and regulatory bodies should cooperate to minimize the risk posed by brainjacking.

with developments in information security research and consumer electronics, has resulted in a small but real risk of malicious individuals accessing implantable pulse generators (IPGs). Unauthorized access to IPGs could cause serious harm to the patients in whom the devices are implanted.

This review summarizes the current literature on the plausibility and potential impact of this risk, identifies possible physiologic mechanisms of attack, and highlights trade-offs inherent in IPG design that provide exploitable vulnerabilities. In doing so we aim to increase awareness of neurological implant security and thereby stimulate discussion of defensive measures. Other than a very brief review from 2009,³ this article is the first to address medical implant information security threats in detail from a neurological/neurosurgical perspective.

For the purposes of this review, unauthorized control of an electronic brain implant will be referred to as “brainjacking,” analogous to the hijacking of a vehicle. The term neurosecurity is used to

refer to defense mechanisms protecting neurological implants from subversion.³

PLAUSIBILITY AND RISK OF BRAINJACKING

More than 100,000 patients worldwide have received deep brain stimulation (DBS), predominantly for movement disorders.⁴ This number is only likely to increase in the future as DBS shows promise for treating a wide range of neurological and psychiatric conditions.^{5,6} More speculatively, DBS and similar implants have been proposed as a potential tool for enhancing cognition in healthy individuals^{7–9} and as a method of correcting “abnormal moral behavior.”¹⁰ Factors contributing to the increasing prevalence of DBS include reductions in treatment cost, increasing demand in newly industrialized countries, aging populations in more economically developed countries, and ongoing improvements in IPG design.¹¹

With increasingly widespread adoption of these intracranial neuromodulation

techniques comes greater opportunity for individuals with a high degree of technical competence to use the technology for malicious purposes. Information technology security researchers have demonstrated the potential for exploitation of the security limitations of implantable medical devices, with potentially severe consequences.

At present, 2 implantable medical devices have been exploited publicly—insulin pumps and implantable cardiac defibrillators. In 2011, Jay Radcliffe, a security researcher and diabetic, used publicly available device information and an inexpensive consumer-grade microprocessor with radiofrequency transmitter to bypass the security of an insulin pump, and outlined a potentially lethal method of attack.¹² This work was extended by Barnaby Jack, who demonstrated unauthorized control over an insulin pump at a distance of 90 m without prior knowledge of the device serial number, a limitation of Radcliffe's earlier attack.¹³ Jack further demonstrated unauthorized and potentially lethal control over an implantable defibrillator,¹⁴ a risk first outlined in 2008 by academic research.¹⁵ As a result of this work, the U.S. Food and Drug Administration (FDA) has issued a safety warning on the risks of inadequate medical device security¹⁶ and public workshops have been undertaken in collaboration with industry to address the issue.^{17,18} Most recently, the FDA has warned about intrusion vulnerabilities in a continuous external drug pump.¹⁹ Furthermore, the U.S. Department of Homeland Security has issued an alert regarding the unacceptable risks associated with using hard-coded (unchangeable) passwords in medical devices.²⁰

Unauthorized access to implants can be lethal—deliberate misuse of an insulin pump (albeit not by electronic exploitation) has been reported in at least 1 murder²¹ and U.S. Vice President Dick Cheney reportedly had the wireless telemetry on his impulse control disorder (ICD) device disabled during his time in office for fear of political assassination.²² Wireless exploitation of implants is also likely to be subtle. Device failures are a somewhat common eventuality²³ and diagnostics after failure of the device are rarely performed. Even if an attack were detected, tracking

down the attacker would be a highly challenging task.

Attacks could be made for a variety of reasons including blackmail, malice against an individual, or manipulation of a politically notable individual. The motive need not even be rational. In 2008 a website for epilepsy sufferers was attacked using flashing images designed to trigger seizures,²⁴ with the attackers' apparent motivation being amusement.

Similar security issues have been brought forth in the automobile industry, particularly in the wake of high-profile proof-of-concept hacks of several major vehicle brands.²⁵ The security research community has released a set of guidelines, the Five Star Automotive Cyber Safety Program,²⁶ the principles of which may be translatable to neurosecurity design.

The information technology community has given some degree of recognition to medical implant information security vulnerabilities, as detailed in *Secure implant design*, but the topic has only been discussed seriously in the biomedical literature recently²⁷⁻²⁹ and there are no detailed discussions of the risks specific to neurological implants beyond a single forward-thinking but brief review published several years ago.³

METHODS OF ATTACK

Once attackers have successfully breached security on a device, they have several options for brainjacking their victim. Stimulation parameters including voltage/current, frequency, pulse width, and electrode contact can be altered to change the effect of stimulation.³⁰ These potential attacks are unlikely to be directly lethal, but may cause serious harm and distress. The accompanying list is not exhaustive and, as the variety and complexity of invasive neuromodulation therapies increases, the potential methods of attack grow in number. Several of these attack strategies are highly speculative and could require a degree of physical or informational access that is unrealistic for most attackers. Clinicians should nevertheless be aware of these possibilities, especially as the complexity of neural implants increases, with a concomitant increase in the complexity and variety of available

attack vectors. See [Table 1](#) for an overview of potential attacks.

Blind Attacks

The most straightforward attacks rely on no patient-specific knowledge on the part of the attacker (i.e., the attacker is "blind"). Simply turning off the stimulation would result in a loss of therapeutic effect. If temporary, this would typically be no more than an annoyance as the patient would be able to reinitiate stimulation, although sudden cessation of stimulation can cause serious "rebound" symptoms in a variety of disorders including Parkinson disease (PD), essential tremor (ET), and obsessive-compulsive disorder (OCD).³¹⁻³⁴ More invasive attacks would allow permanent disabling of an IPG, necessitating surgical replacement of the device, with concomitant surgical risks and expenses.

Repeated interrogation of an implanted device can deplete the battery prematurely.³⁵ In the case of traditional nonrechargeable IPGs, this will result in reduced device lifespan. In the case of rechargeable models, repeated overdraining of the battery can result in the device disabling itself to avoid potential catastrophic failure (depending on IPG model). Battery damage would also necessitate IPG replacement.

Although these forms of brainjacking would be unpleasant, their lasting effects would likely be minor. It would, however, be possible to induce tissue damage as a result of increasing pulse width and voltage. The firmware of most IPGs is designed to lock out dangerous stimulation parameters under normal usage, but an attacker may be able to subvert these limits. Typical parameters for DBS induce minimal tissue damage,³⁶⁻³⁸ but feline in vivo data indicate that tissue damage can occur at high charge densities,^{39,40} with extrapolation from these data providing an estimate of safe stimulation parameters.⁴¹ The effects of such electrically induced lesions would vary depending on location and extent of damage, but could result in serious disability.

Finally, an attacker could seek to gain information from the target's implant in a passive or active manner,²⁷ (i.e., by passively "listening" for information transmitted during normal operation or actively accessing the device to receive information). Most IPGs store some

Table 1. Summary of Attack Types

Attack Category	Attack Type	Condition	Potential Harms
Blind	Switching off IPG	Any	Denial of stimulation; rebound effects
	Draining battery		Denial of stimulation; rebound effects; IPG damage
	Overcharge stimulation		Tissue damage
	Data theft		Violation of patient privacy; facilitation of further attacks
Targeted	~10 Hz STN stimulation	PD	Hypokinesia/akinesia
	GPI electrode contact change	PD	
	Increase voltage/decrease frequency ViM stimulation	ET	Exacerbated tremor
	Increased frequency PAG/PVG stimulation	Pain	Increased pain
	Increased frequency VPL/VPM stimulation	Pain	
	STN electrode contact change	PD	Impulse control disorders; alteration of affect
	NAcc electrode contact change	OCD	Alteration of affect
	NAcc stimulation control	OCD, depression	Alteration of reward processing; operant conditioning

ET, essential tremor; GPI, internal globus pallidus; IPG, implantable pulse generator; NAcc, nucleus accumbens; OCD, obsessive-compulsive disorder; PAG/PVG, periaqueductal/periventricular gray matter; PD, Parkinson disease; STN, subthalamic nucleus; ViM, ventral intermediate thalamic nucleus; VPL/VPM, ventroposterior lateral/medial thalamic nucleus.

identifiable information including patient name, diagnosis, and physician details; all IPGs, by necessity, store information regarding stimulation parameters. Acquiring this information may be an ends in itself or may form the first stage of one of the targeted attack strategies detailed later.

Targeted Attacks

More elaborate attacks could make use of implanted electrodes to alter behavior and cognition by modifying stimulation parameters based on some degree of pathophysiologic knowledge of the patient. Increasing or decreasing stimulation frequency has a substantial impact on the efficacy of DBS for several indications, in some cases reversing the positive effects of stimulation. Alteration of voltage or pulse width changes the volume of tissue activated,^{30,42} which may diminish the treatment effect or induce unpleasant off-target effects by stimulating surrounding structures. Changing the electrode contact(s) used for stimulation would enable off-target structures to be stimulated directly, resulting in variable effects depending on electrode location and surgical approach used.⁴³ With the development of directionally selective electrodes, currently being introduced into clinical use,⁴⁴ the intended increase

in precision of on-target stimulation could also afford attackers more sophisticated control over malicious off-target stimulation.

These attacks may require sophisticated knowledge of the patient's clinical condition, making them more challenging to perform, although the effects are potentially more desirable from some attackers' perspective. A dedicated attacker may be able to acquire medical records by breaching medical databases, social engineering, or simple attacks. Even without medical knowledge of the patient, scanning up and down stimulation parameters could enable an attacker to empirically determine settings that cause distress.

Impairing Motor Function

Movement disorders are the most common indications for DBS, with >100,000 patients estimated to have undergone DBS for PD alone.⁴ In PD and ET there is potential for an attacker to subvert IPG function to impair motor control. In patients receiving DBS of the subthalamic nucleus (STN) for PD, stimulation at a frequency of ≥ 130 Hz typically results in desired clinical outcomes,⁴⁵ whereas 5–10 Hz or ~ 20 Hz stimulation can significantly exacerbate bradykinetic/akinetic symptoms.^{46–49} Similar effects have been reported in DBS of the internal globus pallidus for PD,

wherein switching to more dorsal electrode contacts resulted in pronounced akinesia.⁵⁰ Given these data, an attacker may substantially impair motor function by altering basic stimulation parameters, thereby increasing the patient's parkinsonian symptoms beyond baseline levels. A similar potential attack exists for patients with ET and DBS of the ventral intermediate nucleus, wherein low frequency, high voltage stimulation can significantly exacerbate tremor symptoms.⁵¹

Inducing Pain

DBS is an effective treatment for a wide range of chronic pain disorders, with most established techniques showing efficacy for focal pain,⁵² and emerging targets showing promise in the treatment of whole-body pain syndromes.^{53,54} The periventricular/periaqueductal gray matter and the ventral-posterolateral/ventral-posteromedial nuclei of the sensory thalamus are the most frequently targeted regions. In clinical practice, these nuclei are stimulated at low frequency to alleviate pain, but higher frequency stimulation, above ~ 70 Hz, is reported to increase painful sensations.^{54,55} Alteration of stimulation frequency in this manner by an attacker could induce severe pain in these patients.

Altering Impulse Control

ICDs, involving behavioral problems such as hypersexuality and pathologic gambling, are a relatively common problem in patients with PD and are particularly strongly associated with the use of dopaminergic agonists.^{56,57} In clinical practice, STN-DBS offers a mechanism for reduction of dopaminergic medication, thereby assisting in the management of ICDs.^{58,59}

Several case reports indicate that inappropriate electrode contact selection can induce a range of disturbances in impulse control. Mania, hypersexuality, and pathologic gambling have been linked with specific electrode contacts.⁶⁰⁻⁶³ The precise effects of a given contact will depend on many factors—individual anatomic variation, surgical approach taken, other stimulation parameters—but it appears plausible that disruption of impulse control could be achieved in at least a subset of patients by switching of electrode contact. An attacker may be able to disrupt the clinician-set stimulation parameters and thereby remove protection from, or even induce, ICDs.

Modifying Emotion and Affect

Alteration of emotional processing and affect can occur during DBS, either as a side-effect or as part of the intended stimulation effects. Dysfunction of emotional behavior has been noted in several case reports of patients receiving STN-DBS for PD, including pathologic crying,⁶⁴⁻⁶⁶ inappropriate laughter,⁶⁷ and affective lability,⁶⁸ likely due to off-target stimulation. Undesirable off-target emotional effects have also been observed in patients receiving DBS of the nucleus accumbens (NAcc) for OCD, notably strong sensations of fear and panic with concomitant autonomic arousal.⁶⁹⁻⁷¹ Deliberate stimulation of inappropriate electrode contacts by an attacker may, therefore, induce personally and socially undesirable emotional changes, which would likely be highly distressing for a patient and their loved ones.

Modulating Reward Processing

Perhaps the most concerning attack strategy feasible using currently implanted neural devices involves the use of operant conditioning to exert substantial control

on a patient's behavior. As noted previously, the NAcc is the target of stimulation in several emerging DBS indications, including depression, OCD, and anorexia. Currently the number of patients undergoing NAcc-DBS is small, although this number may increase if one or more indications prove to be clinically viable.

The enhancement/attenuation of positive reinforcement effected by NAcc stimulation has been well demonstrated in humans and other animals,^{72,73} and is a core component of the rationale for its value as a target in such a broad range of conditions.⁷⁴⁻⁷⁶ Sufficient control on the IPG could enable use of operant conditioning to modify the behavior of the victim, potentially reinforcing harmful behaviors. This strategy would require more sophistication on the part of the attacker than required by most of the attacks discussed previously. One would need continuous control on the IPG for an extended period of time, along with a means of surveillance of the victim. It would be feasible for the attacker to use a wireless relay device placed near the victim to remove the need to be in close physical proximity, but placing this device without detection would have its own challenges.

SECURE IMPLANT DESIGN

Several design constraints exist that necessitate trade-offs between neurosecurity and other desirable features of IPGs. These trade-offs and challenges, along with specific methods of attack and desirable security features for future devices, have been discussed in greater detail elsewhere,^{27-29,77-79} therefore this section will only consider the factors most relevant to clinical practice—battery life and practicality.

Telemetric adjustment of IPG settings provides substantial benefits in terms of the flexibility and usability of the device,²⁷ but also provides mechanisms by which the device may be subverted. At present, IPG telemetry has relied on near-field transcutaneous wireless communication between the implanted device and proprietary IPG-specific external telemetry devices, using several dedicated frequency bands, under the control of either the clinician or the patient. The newest IPGs use consumer-grade wireless communication protocols, such as Bluetooth, and in

the longer term, device manufacturers are considering using communication over transmission control protocol/internet protocol (TCP/IP), enabling remote telemetric control and/or software updates of IPGs over the Internet. In addition, manufacturers are shifting from proprietary external hardware programmers (which are expensive to design, manufacture, and update) to proprietary software running on consumer devices such as tablets and smartphones.

Unfortunately, proprietary and consumer protocols have drawbacks. Proprietary systems typically attempt to make use of “security through obscurity” (i.e., maintaining secrecy about software/hardware design to thwart potential attackers), which is unreliable.⁷⁹ Proprietary designs are also typically less open to security researchers due to manufacturers’ reluctance to disclose trade secrets to third parties, which increases the challenge of uncovering security flaws. This challenge is exacerbated by the risk of lawsuits brought against legitimate security researchers for disclosing design flaws under legislation such as the Digital Millennium Copyright Act, as discussed in a recent guidance statement made by the Electronic Frontier Foundation to the FDA.⁸⁰ Conversely, popular consumer protocols are widely adopted and understood, potentially lowering the barrier of entry to attackers.

Emerging IPG technology will provide opportunities and pitfalls in terms of neurosecurity. One potential example is “closed-loop” or “adaptive” DBS, wherein physiologic signals are used to alter stimulation profiles on the fly, without any intervention from patients or clinicians. These systems may plausibly be more resilient to brainjacking attempts, as the decreased requirements for human intervention would facilitate the use of less easily accessible programming methods than current IPG user interfaces, thereby increasing security without a concomitant decrease in system utility. Conversely, however, the increased complexity of closed-loop systems may provide additional surfaces for attackers to exploit. Certain experimental closed-loop systems use wireless interfaces between sensor, controller, and stimulation components.^{81,82} Use of such a design would effectively turn neuromodulation into a

Supervisory Control and Data Acquisition (SCADA) system. By maliciously influencing such a system's input, it is possible to influence output parameters and thereby alter stimulation—a process that has been demonstrated to have a devastating effect in several real-world SCADA systems, most famously the Iranian nuclear fuel centrifuges that were damaged by malware called Stuxnet.⁸³

Several potential security solutions exist, although, as detailed, many are subject to limitations. Specific solutions include improved auditing,⁸⁴ rolling code cryptography,⁷⁷ server-based cryptographic key management,²⁸ formal verification of device software,⁸⁵ proximity-based authentication,^{86,87} and “communication cloaker” or “shield” wearable devices that mediate secure communication between programmer and implant.^{88,89} For more detail, see Camara et al.²⁷

It is the responsibility of IPG manufacturers to carefully trade-off between clinical demands, ergonomics, and neurosecurity. Designing any secure digital system is difficult and, as discussed, IPG design presents several unusual challenges that are not easily solved without causing problems elsewhere in the system. Neuromodulation is a rapidly evolving field and it is difficult to predict future innovations, therefore any regulatory approach to solving problems of neurosecurity must carefully balance information security risks with the risk of impeding technological development through application of inflexible rules. Manufacturers and regulators should endeavor to ensure that, when security flaws are found, researchers are able to disclose these flaws in a safe and timely manner without undue legal impediments.⁸⁰

Battery Life

Most IPGs currently in use rely on a non-rechargeable battery, which can last anywhere from <1 year to a decade, depending on IPG model and stimulation parameters,⁹⁰ necessitating surgery to explant and replace the depleted device. Given the risks and distress associated with surgery, manufacturers attempt to maximize the life of the battery by using the highest capacity cells that are feasible and by minimizing power drain resulting from the electronic systems.

A substantial portion of energy usage is taken up by the stimulation itself and is,

therefore, unavoidable, but the rest is devoted to maintaining the function of the internal electronics of the device—micro-processor(s), memory, and wireless communication system. Most potential security improvements involve increased power drain from 1 or more of these components, or the inclusion of additional components that would contribute to energy usage. Cryptographic systems require extraprocessing power to encrypt/decrypt data,⁷⁹ improved auditing requires more memory to be of value, and frequent software verification would result in increased wireless communications. Rechargeable IPGs are becoming increasingly popular and reduce the importance of battery life somewhat, but the limited charge/discharge cycles available to each battery and the desire to maximize time between charging still necessitate a careful approach to power management. Future closed-loop DBS systems may reduce power consumption in comparison to traditional IPGs,⁹¹ thereby freeing up more energy to be used for security systems.

Practicality

A crucial design consideration for any security system is the human factor. Human error is a major cause of security failures across many domains of information technology⁹² and ergonomics is an important secondary concern in the development of medical devices.⁹³ If a security system requires too much time and effort on the part of patients and clinicians, there is risk that it will remain unused or, potentially worse, that it will be improperly used and thereby provide a false sense of security. Furthermore, in a medical context, ease-of-use and open access can be critical for proper treatment.

Most of the security solutions that would be implemented on the implantable device would not impact considerably on the practicality of the system. A little extra time setting up proper security protocols during the initial programming stage is acceptable and, with adequate training, may be implemented reliably. Problems are more likely to happen with additional devices being added to the system, especially if patients are expected to use these devices constantly. Cloaker and shield devices have been proposed.^{88,89} These are external electronic devices that provide an

additional layer of security between the implant and other devices that are trying to communicate with it. These would likely provide a substantial improvement to system security, but would risk being underused due to the inconvenience of carrying around additional devices. Excessively burdensome security systems may even cause nonadherence to treatment, resulting in re-emergence of a patient's symptoms. This inconvenience may be attenuated by integration of the security systems into consumer-grade electronic devices (e.g., by enabling a patient's smartphone to act as a communications hub),⁷⁸ but using consumer devices in this manner increases yet more security concerns.

Device manufacturers are beginning to offer telemetric control of neural implants using consumer devices. Several IPGs currently on the market offer integration with smartphone or tablet-type devices. This development may provide substantial benefits in terms of user friendliness and reduced clinical visits. However, enabling access to implants with Internet-enabled consumer electronics risks attackers exploiting security flaws in these devices and thereby indirectly accessing and subverting implants. Remote network access vastly increases the availability of devices to attackers, making attacks easier and therefore more attractive. A 2015 FDA warning addressed security vulnerabilities in a network-accessible drug pump,¹⁹ demonstrating the risks associated with Internet-enabled medical devices. This issue of network security in healthcare is discussed in detail in a recent article by Independent Security Evaluators.⁹⁴

Notably, allowing wireless access to implants in this manner would enable over-the-air firmware updates, which are not currently implemented in any model of IPG. This would facilitate the patching of security holes (increasingly important for the longer lasting rechargeable IPGs), but would also leave devices open to injection of counterfeit firmware updates.⁹⁵ Firmware serves to control the hardware of embedded medical devices, such as IPGs, therefore any alteration to it would enable substantial changes to the function of the device, beyond the changes that are possible through the user interface. For example, although the user interface on most IPGs will prevent

the setting of stimulation parameters capable of causing tissue damage (as discussed in the section on Blind attacks), alteration of firmware may be able to bypass these restrictions, enabling attackers to cause lesions. Allowing IPGs to connect to the Internet routinely would increase the probability of such illegitimate firmware modification by allowing attackers to access the devices remotely instead of requiring them to be in close proximity.

Manufacturers must carefully weigh these factors when deciding whether wireless interfacing is suitable for a given implantable device. An important consideration is the context under which updates can take place and the authorizations necessary. It may be preferable to prevent updates being made over the Internet and instead require an authorization mechanism that is only available in a clinical setting.

Another key concern is the accessibility of neural implants in case of emergency. Clinicians may be presented with an unconscious or otherwise noncommunicative patient whose implant they must access to provide effective treatment, but are unable to do so due to security measures. Thus, the device must have an emergency mode, which leaves open a potential attack vector, meaning that designing such a mode is a technical challenge.²⁷ Similar considerations must be made with regard to patient programming modes. It is valuable for patients to be able to access their own implants and change stimulation parameters to some degree at home, but allowing too great a degree of control by the patient programmers enables easy access for attackers or misuse by patients.

CONCLUSIONS

Use of implanted neuromodulation is still a relatively new field, but has already had a great impact on the treatment of several severe neurological disorders. The future of this field is highly promising and, contingent on positive outcomes in clinical trials and gradual reductions in hardware cost, it is probable that these devices will only become more popular. This popularity is also contingent on factors, such as public acceptance and reliability of implanted neurostimulators, both of

which could be substantially negatively impacted by failures in device security.

It bears repeating that this neurosecurity threat is still likely theoretical. We were not able to identify any evidence that the scenarios detailed have ever been attempted. Nevertheless, we believe that the issues discussed in this article indicate that brainjacking is a potentially serious threat warranting serious discussion before any real-world harms occur. As a result of the paucity of work specifically addressing brainjacking, there are several areas of investigation that may prove fruitful.

First, as this review is merely a first step toward more rigorous discussion of neurosecurity issues, there are doubtless several as-yet unidentified potential attack strategies. The focus of the present article has been on IPGs for DBS but epilepsy monitoring systems, sensory prosthetics, brain-computer interfaces, and other emerging neurotechnologies, are all likely to have device-specific opportunities and challenges worthy of study. Detailed threat modeling may prove to be useful in identification of the most effective strategies for minimizing neurosecurity related risk. Stakeholders should collaborate to quantify the expected risk of brainjacking to facilitate development of mitigation strategies.

Second, more resources should be put into development of novel mechanisms to enhance neurosecurity, along with appropriation of mechanisms used in other fields. It may be valuable to develop codes of best practice for neurosecurity, or to formulate overall guidelines for medical device security that can be tailored to the specific requirements of neural implants. Any such code should be formulated to encourage cooperation between stakeholders and be sufficiently flexible to adapt to the rapid pace of change in neurological implant design. Device manufacturers must strive to improve on recent advances, ensuring that security concerns are considered throughout the design process and not relegated to an afterthought, and should cooperate with security researchers who seek to responsibly disclose design flaws. Regulatory bodies must balance use of their powers to encourage good neurosecurity practices with the risk of impairing real-world security through overly burdensome

regulations. Given that neurosecurity is not an immediate concern, there is sufficient time for manufacturers and regulatory agencies to carefully consider methods of risk mitigation. Although there is a responsibility for manufacturers to make their devices secure, the expected value of any novel security features should be carefully weighed against other clinically relevant factors, and innovation should not be unduly stifled by the demands of neurosecurity.

Third, given the unique challenges presented by brainjacking, further research into its implications beyond purely biomedical considerations may be valuable. The philosophical implications of exerting control on another human being in this manner are potentially quite profound and deserving of detailed analysis. Similarly, the legal and economic implications may be substantial, especially if greatly increased proliferation of neurotechnology is to be expected.

Finally, publicizing these risks among clinicians and patients may be an important means of minimizing risks. Even if it were possible to implement a perfect security design, the human element of a system almost always presents a tempting target for attackers. Clinicians should educate themselves about the basics of information security and be mindful of the risks of brainjacking when evaluating faulty implants or caring for high-profile patients. Hospital staff should also be aware of social engineering techniques used by attackers to gain privileged information and should have at least a basic understanding of how to minimize neurosecurity risk. Patients should have some degree of awareness of particularly risky behaviors to avoid, although any discussion of this topic should avoid undue alarm and emphasize the extremely low probability of any individual patient being targeted by electronic attacks.

In writing this article, we are aware that the information contained herein could be used by an attacker to engage in one of the attacks. This is a risk we take seriously, but we believe that the benefits of publicizing this topic outweigh the increased danger. The physiologic mechanisms that we describe are all easily accessible in scientific journals and any intellectually capable attackers could do their own research. The main challenge for an

- after stimulation of the motor thalamus in a case of chorea-acanthocytosis. *Neurology*. 2002;59:1982-1984.
37. Haberler C, Alesch F, Mazal PR, Pilz P, Jellinger K, Pinter MM, et al. No tissue damage by chronic deep brain stimulation in Parkinson's disease. *Ann Neurol*. 2000;48:372-376.
 38. Henderson JM, Pell M, O'Sullivan DJ, McCusker EA, Fung VSC, Hedges P, et al. Post-mortem analysis of bilateral subthalamic electrode implants in Parkinson's disease. *Mov Disord*. 2002;17:133-137.
 39. Yuen TG, Agnew WF, Bullara LA, Jacques S, McCreery DB. Histological evaluation of neural damage from electrical stimulation: considerations for the selection of parameters for clinical application. *Neurosurgery*. 1981;9:292-299.
 40. McCreery DB, Agnew WF, Yuen TG, Bullara L. Charge density and charge per phase as cofactors in neural injury induced by electrical stimulation. *IEEE Trans Biomed Eng*. 1990;37:996-1001.
 41. Shannon RV. A model of safe levels for electrical stimulation. *IEEE Trans Biomed Eng*. 1992;39:424-426.
 42. McIntyre CC, Butson CR, Maks CB, Noecker AM. Optimizing deep brain stimulation parameter selection with detailed models of the electrode-tissue interface. *Conf Proc IEEE Eng Med Biol Soc*. 2006;1:893-895.
 43. Boccard SGJ, Fernandes HM, Jbabdi S, Van Hartevelt TJ, Kringelbach ML, Quaghebeur G, et al. Tractography study of deep brain stimulation of the anterior cingulate cortex in chronic pain: key to improve the targeting. *World Neurosurg*. 2016;86:361-370.e1-3.
 44. Green AL, Aziz TZ. Steering technology for deep brain stimulation. *Brain*. 2014;137(Pt 7):1854-1856.
 45. Birdno MJ, Grill WM. Mechanisms of deep brain stimulation in movement disorders as revealed by changes in stimulus frequency. *Neurotherapeutics*. 2008;5:14-25.
 46. Timmermann K, Wojtecki L, Gross J, Lehrke R, Voges J, Maarouf M, et al. Ten-hertz stimulation of subthalamic nucleus deteriorates motor symptoms in Parkinson's disease. *Mov Disord*. 2004;19:1328-1333.
 47. Fogelson N, Kuhn AA, Silberstein P, Limousin P, Hariz M, Trottenberg T, et al. Frequency dependent effects of subthalamic nucleus stimulation in Parkinson's disease. *Neurosci Lett*. 2005;382:5-9.
 48. Eusebio A, Chen CC, Lu CS, Lee ST, Tsai CH, Limousin P, et al. Effects of low-frequency stimulation of the subthalamic nucleus on movement in Parkinson's disease. *Exp Neurol*. 2008;209:125-130.
 49. Rizzone M. Deep brain stimulation of the subthalamic nucleus in Parkinson's disease: effects of variation in stimulation parameters. *J Neurol Neurosurg Psychiatry*. 2001;71:215-219.
 50. Krack P, Pollak P, Limousin P, Hoffmann D, Benazzouz A, Le Bas JF, et al. Opposite motor effects of pallidal stimulation in Parkinson's disease. *Ann Neurol*. 1998;43:180-192.
 51. Kuncel AM, Cooper SE, Wolgamuth BR, Clyde MA, Snyder SA, Montgomery EB, et al. Clinical response to varying the stimulus parameters in deep brain stimulation for essential tremor. *Mov Disord*. 2006;21:1920-1928.
 52. Bittar RG, Kar-Purkayastha I, Owen SL, Bear RE, Green A, Wang S, et al. Deep brain stimulation for pain relief: a meta-analysis. *J Clin Neurosci*. 2005;12:515-519.
 53. Boccard SGJ, Fitzgerald JJ, Pereira EAC, Moir L, Van Hartevelt TJ, Kringelbach ML, et al. Targeting the affective component of chronic pain: a case series of deep brain stimulation of the anterior cingulate cortex. *Neurosurgery*. 2014;74:628-635 [discussion: 635-637].
 54. Boccard SGJ, Pereira EAC, Aziz TZ. Deep brain stimulation for chronic pain. *J Clin Neurosci*. 2015;22:1537-1543.
 55. Pereira EAC, Aziz TZ. Neuropathic pain and deep brain stimulation. *Neurotherapeutics*. 2014;11:496-507.
 56. Weintraub D, Siderowf AD, Potenza MN, Goveas J, Morales KH, Duda JE, et al. Association of dopamine agonist use with impulse control disorders in Parkinson disease. *Arch Neurol*. 2006;63:969-973.
 57. Weintraub D, Koester J, Potenza MN, Siderowf AD, Stacy M, Voon V, et al. Impulse control disorders in Parkinson disease: a cross-sectional study of 3090 patients. *Arch Neurol*. 2010;67:589-595.
 58. Gee L, Smith H, De La Cruz P, Campbell J, Fama C, Haller J, et al. The influence of bilateral subthalamic nucleus deep brain stimulation on impulsivity and prepulse inhibition in Parkinson's disease patients. *Stereotact Funct Neurosurg*. 2015;93:265-270.
 59. Zurowski M, O'Brien JD. Developments in impulse control behaviours of Parkinson's disease. *Curr Opin Neurol*. 2015;28:387-392.
 60. Kulisevsky J, Berthier ML, Gironell A, Pascual-Sedano B, Molet J, Parés P. Mania following deep brain stimulation for Parkinson's disease. *Neurology*. 2002;59:1421-1424.
 61. Raucher-Chéné D, Charrel C-L, de Maindreville AD, Limosin F. Manic episode with psychotic symptoms in a patient with Parkinson's disease treated by subthalamic nucleus stimulation: improvement on switching the target. *J Neurol Sci*. 2008;273:116-117.
 62. Herzog J, Reiff J, Krack P, Witt K, Schrader B, Müller D, et al. Manic episode with psychotic symptoms induced by subthalamic nucleus stimulation in a patient with Parkinson's disease. *Mov Disord*. 2003;18:1382-1384.
 63. Smeding HMM, Goudriaan AE, Foncke EMJ, Schuurman PR, Speelman JD, Schmand B. Pathological gambling after bilateral subthalamic nucleus stimulation in Parkinson disease. *J Neurol Neurosurg Psychiatry*. 2007;78:517-519.
 64. Wojtecki L, Nickel J, Timmermann L, Maarouf M, Südmeyer M, Schneider F, et al. Pathological crying induced by deep brain stimulation. *Mov Disord*. 2007;22:1314-1316.
 65. Low HL, Sayer FT, Honey CR. Pathological crying caused by high-frequency stimulation in the region of the caudal internal capsule. *Arch Neurol*. 2008;65:264-266.
 66. Okun MS. Pseudobulbar crying induced by stimulation in the region of the subthalamic nucleus. *J Neurol Neurosurg Psychiatry*. 2004;75:921-923.
 67. Krack P, Kumar R, Ardouin C, Limousin P, McVicker JM, Benabid AL, et al. Mirthful laughter induced by subthalamic nucleus stimulation. *Mov Disord*. 2001;16:867-875.
 68. Wojtecki L, Timmermann L, Groiss SJ, Elben S, Reck C, Südmeyer M, et al. Long-term time course of affective lability after subthalamic deep brain stimulation electrode implantation. *Neurocase*. 2011;17:527-532.
 69. Okun MS, Mann G, Foote KD, Shapira NA, Bowers D, Springer U, et al. Deep brain stimulation in the internal capsule and nucleus accumbens region: responses observed during active and sham programming. *J Neurol Neurosurg Psychiatry*. 2007;78:310-314.
 70. Shapira NA, Okun MS, Wint D, Foote KD, Byars JA, Bowers D, et al. Panic and fear induced by deep brain stimulation. *J Neurol Neurosurg Psychiatry*. 2006;77:410-412.
 71. Sousa MB, Reis T, Reis A, Belmonte-de-Abreu P. New-onset panic attacks after deep brain stimulation of the nucleus accumbens in a patient with refractory obsessive-compulsive and bipolar disorders: a case report. *Rev Bras Psiquiatr*. 2015;37:182-183.
 72. Heath RG. Electrical self-stimulation of the brain in man. *Am J Psychiatry*. 1963;120:571-577.
 73. van Kuyck K, Gabriëls LA, Cosyns PR, Arckens L, Sturm V, Rasmussen SA, et al. Behavioural and physiological effects of electrical stimulation in the nucleus accumbens: a review. *Acta Neurochir Suppl*. 2007;97(Pt 2):375-391.
 74. Delaloye S, Holtzheimer PE. Deep brain stimulation in the treatment of depression. *Dialogues Clin Neurosci*. 2014;16:83-91.
 75. Kocacik E, Temel Y, Höllig A, Falkenburger B, Tan SK. Current perspectives on deep brain stimulation for severe neurological and psychiatric disorders. *Neuropsychiatr Dis Treat*. 2015;11:1051-1066.
 76. Park RJ, Godier LR, Cowdrey FA. Hungry for reward: how can neuroscience inform the development of treatment for anorexia nervosa? *Behav Res Ther*. 2014;62:47-59.
 77. Raghunathan A, Jha NK. Hijacking an insulin pump: security attacks and defenses for a diabetes therapy system, 2011 IEEE 13th International Conference on E-Health Networking, Applications and Services. Columbia, MO: IEEE; 2011:150-156.

78. Zhang M, Raghunathan A, Jha NK. Trustworthiness of medical devices and body area networks. *Proc IEEE*. 2014;102:1174-1188.
79. Burleson W, Clark SS, Ransford B, Fu K. Design challenges for secure implantable medical devices. DAC '12 Proceedings of the 49th Annual Design Automation Conference; Pages 12-17; ACM New York, NY.
80. Doctorow C, McSherry C. Comments of Electronic Frontier Foundation. Postmarket management of cybersecurity in medical devices; draft guidance for Industry and Food and Drug Administration staff. Available at: https://www.eff.org/files/2016/04/22/electronic_frontier_foundation_comments_cybersecurity_in_medical_devices_.pdf. Published 2016. Accessed May 30, 2016.
81. Rhew H-G, Jeong J, Fredenburg JA, Dodani S, Patil P, Flynn MP. A wirelessly powered log-based closed-loop deep brain stimulation SoC with two-way wireless telemetry for treatment of neurological disorders, 2012 Symposium on VLSI Circuits (VLSIC). IEEE. 2012;70-71.
82. Grahn PJ, Mallory GW, Khurram OU, Berry BM, Hachmann JT, Bieber AJ, et al. A neurochemical closed-loop controller for deep brain stimulation: toward individualized smart neuromodulation therapies. *Front Neurosci*. 2014;8:169.
83. Kushner D. The real story of Stuxnet. *IEEE Spectrum*. Available at: <http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>. Published 2013. Accessed May 30, 2016.
84. Hansen JA, Hansen NM. A taxonomy of vulnerabilities in implantable medical devices. Proceedings of the Second Annual Workshop on Security and Privacy in Medical and Home-Care Systems - SPIMACS '10. New York: ACM Press; 2010:13.
85. Li C, Raghunathan A, Jha NK. Improving the trustworthiness of medical device software with formal verification methods. *IEEE Embed Syst Lett*. 2013;5:50-53.
86. Rasmussen KB, Castelluccia C, Heydt-Benjamin TS, Capkun S. Proximity-based access control for implantable medical devices. Proceedings of the 16th ACM Conference on Computer and Communications Security - CCS '09. New York: ACM Press; 2009:410.
87. Kim Y, Lee WS, Raghunathan V, Jha NK, Raghunathan A. Vibration-Based Secure Side Channel for Medical Devices. Proceedings of the 52nd Annual Design Automation Conference on - DAC '15. New York: ACM Press; 2015:1-6.
88. Denning T, Fu K, Kohno T. Absence makes the heart grow fonder: new directions for implantable medical device security. Conference proceedings published by USENIX association from the 3rd conference on Hot Topics in Security (2008); USENIX Association Berkeley, CA
89. Gollakota S, Hassanieh H, Ransford B, Katabi D, Fu K. They can hear your heartbeats: non-invasive security for implantable medical devices. Available at: <http://groups.csail.mit.edu/netmit/wordpress/wp-content/themes/netmit/papers/secureimd-sigcomm2011.pdf>. Accessed May 30, 2016.
90. Stewart CDM, Eljamel S. Prediction of implantable pulse generator longevity in deep brain stimulation: limitations and possible solutions in clinical practice. *Stereotact Funct Neurosurg*. 2011;89:299-304.
91. Little S, Pogossyan A, Neal S, Zavala B, Zrinzo L, Hariz M, et al. Adaptive deep brain stimulation in advanced Parkinson disease. *Ann Neurol*. 2013;74:449-457.
92. Kraemer S, Carayon P, Clem J. Human and organizational factors in computer and information security: pathways to vulnerabilities. *Comput Secur*. 2009;28:509-520.
93. Stone R, McCloy R. Ergonomics in medicine and surgery. *BMJ*. 2004;328:1115-1118.
94. Independent Security Evaluators. Securing hospitals: a research study and blueprint. Available at: https://securityevaluators.com/hospitalhack/securing_hospitals.pdf. Published 2016. Accessed May 30, 2016.
95. Kim Y, Lee W, Raghunathan A, Raghunathan V, Jha NK. *Implantable Biomedical Microsystems*. New York: Elsevier; 2015.

Conflict of interest statement: The authors would like to thank the Norman Collisson Foundation and NIHR Oxford Biomedical Research Centre for funding this work.

Received 8 January 2016; accepted 5 May 2016

Citation: World Neurosurg. (2016) 92:454-462.

<http://dx.doi.org/10.1016/j.wneu.2016.05.010>

Journal homepage: www.WORLDNEUROSURGERY.org

Available online: www.sciencedirect.com

1878-8750/\$ - see front matter © 2016 Elsevier Inc. All rights reserved.



WORLD NEUROSURGERY is indexed in:

- Current Contents/Clinical Practice
- BioSIS
- MEDLINE/PubMed
- ISI/BioMed
- Science Citation Index
- Excerpta Medica
- SCOPUS

For more information, visit www.WORLDNEUROSURGERY.org