Brainjacking: implant security issues in invasive neuromodulation

Laurie Pycroft, MSc., Sandra G. Boccard, PhD., Sarah L.F. Owen, DPhil., John F. Stein, FRCP, James J. Fitzgerald, FRCS(SN), Alexander L. Green, FRCS(SN), Tipu Z. Aziz, FMedSci

PII: S1878-8750(16)30272-8
DOI: 10.1016/j.wneu.2016.05.010
Reference: WNEU 4071

To appear in: World Neurosurgery

Received Date: 8 January 2016
Revised Date: 4 May 2016
Accepted Date: 5 May 2016

Please cite this article as: Pycroft L, Boccard SG, Owen SLF, Stein JF, Fitzgerald JJ, Green AL, Aziz TZ, Brainjacking: implant security issues in invasive neuromodulation, World Neurosurgery (2016), doi: 10.1016/j.wneu.2016.05.010.

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.
Brainjacking: implant security issues in invasive neuromodulation

Author names and affiliations

Laurie Pycroft, MSc.1; Sandra G. Boccard, PhD.1; Sarah L.F. Owen, DPhil.2; John F. Stein, FRCP; James J. Fitzgerald, FRCS(SN)1; Alexander L. Green, FRCS(SN)1; Tipu Z. Aziz, FMedSci1

1: Oxford Functional Neurosurgery, University of Oxford, Level 6, West Wing, John Radcliffe Hospital, Headington, Oxford, UK, OX3 9DU

2: Department of Physiology, Anatomy, and Genetics, Sherrington Road, Oxford, UK, OX1 3PT

3: Department of Applied Health and Professional Development, Oxford Brookes University, Headington Campus, Oxford, UK, OX3 0BP

Correspondence should be addressed to Laurie Pycroft
Email: laurie.pycroft@nds.ox.ac.uk   Tel: +44 (0) 7788804011

Author contributions statement

LP, JJF and TZA developed the core concept of the review.

LP wrote the manuscript and identified the security risks specific to DBS.

SGB, SLFO, JFS, JJF, ALG, and TZA all reviewed the manuscript several times and provided extensive feedback and suggestions for rewrites based on their areas of expertise.

Keywords

Deep Brain Stimulation; Hacking; Implantable Pulse Generator; Implantable medical device; Cybersecurity; Medical device security; Neurosecurity; Brainjacking; Neurosurgery

Highlights

• Current state of information security of neurological implants is reviewed
• Specific risks associated with brain implant hacking (“brainjacking”) are identified
• Trade-offs between security and function of brain implants is discussed
• Recommendations are made for improving future security of neurological implants
Introduction

The concept of altering human conscious experience and behaviour via unauthorised 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 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).

Unauthorised 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 physiological mechanisms of attack, and highlights trade-offs inherent in IPG design that provide exploitable vulnerabilities. In doing so we aim to raise 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, unauthorised 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 defence mechanisms protecting neurological implants from subversion\(^3\).

Plausibility and risk of brainjacking

Over 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 behaviour” \(^10\). Factors contributing to the increasing prevalence of DBS include reductions in treatment cost, increasing demand in newly industrialised countries, ageing 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.

To date, two implantable medical devices have been exploited publicly – insulin pumps and implantable cardiac defibrillators. In 2011, Jay Radcliffe, a security researcher and diabetic, utilised 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 unauthorised control over an insulin pump at a distance of 90 metres without prior knowledge of the device serial number, a limitation of Radcliffe’s earlier attack \(^13\). Jack further demonstrated unauthorised 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 FDA has issued a safety warning over the risks of inadequate medical device security \(^16\) 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 United States Department of Homeland Security has issued an alert regarding the unacceptable risks associated with using hard-coded (unchangeable) passwords in medical devices \(^20\).
Unauthorised access to implants can be lethal – deliberate misuse of an insulin pump (albeit not via electronic exploitation) has been reported in at least one murder\textsuperscript{21} and US Vice President Dick Cheney reportedly had the wireless telemetry on his ICD disabled during his time in office for fear of political assassination\textsuperscript{22}. Wireless exploitation of implants is also likely to be subtle – device failures are a somewhat common eventuality\textsuperscript{23} and post-failure device diagnostics 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\textsuperscript{24}, with the attackers’ apparent motivation being amusement.

Similar security issues have been raised in the automobile industry, particularly in the wake of high-profile proof-of-concept hacks of several major vehicle brands\textsuperscript{25}. The security research community has released a set of guidelines, the “Five Star Automotive Cyber Safety Program”\textsuperscript{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 recently\textsuperscript{27–29} 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\textsuperscript{3}.

**Methods of attack**

Once an attacker has successfully breached security on a device, they have several options for brain-jacking their victim. Stimulation parameters including voltage/current, frequency, pulse width, and electrode contact can be altered in order to change the effect of stimulation\textsuperscript{30}. These potential
attacks are unlikely to be directly lethal, but may cause serious harm and distress. The list below 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 re-initiate stimulation, although sudden cessation of stimulation can cause serious “rebound” symptoms in a variety of disorders including Parkinson’s 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 non-rechargeable IPGs, this will result in reduced device lifespan; in the case of rechargeable models, repeated over-draining of the battery can result in the device disabling itself in order to avoid potential catastrophic failure (depending on IPG model). Battery damage would also necessitate IPG replacement.

Although the above 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\textsuperscript{36–38} but feline \textit{in vivo} data indicate that tissue damage can occur at high charge densities\textsuperscript{39,40}, with extrapolation from these data providing an estimate of safe stimulation parameters\textsuperscript{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\textsuperscript{27}, i.e. by passively “listening” for information transmitted during normal operation or actively accessing the device to receive information. Most IPGs store some 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 below.

**Targeted attacks**

More elaborate attacks could make use of implanted electrodes to alter behaviour and cognition by modifying stimulation parameters based on some degree of pathophysiological 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 (VTA)\textsuperscript{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\textsuperscript{43}. With the development of directionally selective electrodes, currently being introduced into clinical use\textsuperscript{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 via breaching medical databases, social engineering, or simple attacks as discussed above. 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 over 100,000 patients estimated to have undergone DBS for PD alone. In both 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, whereas 5-10 Hz or ~20 Hz stimulation can significantly exacerbate bradykinetic/akinetic symptoms. 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. 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 ET patients with DBS of the ventral intermediate nucleus, wherein low frequency, high voltage stimulation can significantly exacerbate tremor symptoms.

Inducing pain

DBS is an effective treatment for a wide range of chronic pain disorders, with most established techniques showing efficacy for focal pain, and emerging targets showing promise in the treatment of whole-body pain syndromes. The periventricular/periaqueductal grey matter (PVG/PAG) and the ventral-posterolateral/ventral-posteromedial nuclei of the sensory thalamus (VPL/VPM) are the
most frequently targeted regions. In clinical practice, these nuclei are stimulated at low frequency to alleviate pain, but higher frequency stimulation, above \(^\sim 70\) 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

Impulse control disorders (ICDs), involving behavioural problems such as hypersexuality and pathological gambling, are a relatively common problem in patients with PD and are particularly strongly associated with the use of dopaminergic agonists\(^{56,57}\). In normal 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 pathological gambling have been linked with specific electrode contacts\(^{60-63}\). The precise effects of a given contact will depend on a variety of factors – individual anatomical variation, surgical approach taken, other stimulation parameters, etc. – but it appears plausible that disruption of impulse control could be achieved in at least a subset of patients via 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 behaviour has been noted in several case reports of patients receiving STN-DBS for PD, including pathological 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\textsuperscript{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 over a patient’s behaviour. As noted above, 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 rise if one or more indications proves to be clinically viable.

The enhancement/attenuation of positive reinforcement effected by NAcc stimulation has been well demonstrated in humans and other animals\textsuperscript{72,73} and, indeed, is a core component of the rationale for its value as a target in such a broad range of conditions\textsuperscript{74–76}. Sufficient control over the IPG could enable use of operant conditioning to modify the behaviour of the victim, potentially reinforcing harmful behaviours. This strategy would require an even greater level of sophistication on the part of the attacker than required by most of the attacks discussed above. One would need continuous control over the IPG for an extended period of time, along with a means of surveillance over 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 bring 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\textsuperscript{27–29,77–79}, therefore this section will 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\textsuperscript{27}, but also provides mechanisms by which the device may be subverted. To date, 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 clinician or patient. The newest IPGs utilise consumer-grade wireless communication protocols such as Bluetooth, and in the longer-term, device manufacturers are considering utilising communication over TCP/IP, enabling remote telemetric control and/or software updates of IPGs over the internet. Additionally, 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, both 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 in order to thwart potential attackers, which is unreliable\textsuperscript{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\textsuperscript{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 physiological 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 utilise wireless interfaces between sensor, controller, and stimulation components\textsuperscript{81,82}; use of such a design would effectively turn neuromodulation into a Supervisory Control and Data Acquisition (SCADA) system. By maliciously influencing the such a system’s input, it is possible to influence output parameters and thereby alter stimulation – a process that has been demonstrated to devastating effect in several real-world SCADA systems, most famously the Iranian nuclear fuel centrifuges that were damaged by malware called Stuxnet\textsuperscript{83}.

Several potential security solutions exist although, as detailed below, many are subject to limitations. Specific solutions include improved auditing\textsuperscript{84}, rolling code cryptography\textsuperscript{77}, server-based cryptographic key management\textsuperscript{28}, formal verification of device software\textsuperscript{85}, proximity-based authentication\textsuperscript{86,87}, and “communication cloaker” or “shield” wearable devices that mediate secure communication between programmer and implant\textsuperscript{88,89}. For more detail, see Camara et al. (2015)\textsuperscript{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 below, 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, so 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 endeavour 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.\textsuperscript{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,\textsuperscript{90} necessitating surgery to explant and replace the depleted device. Given the risks and distress associated with surgery, manufacturers attempt to maximise the life of the battery by using the highest-capacity cells that are feasible and by minimising 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 – microprocessor(s), memory, and wireless communication system. Most potential security improvements involve increased power drain from one or more of these components, or the inclusion of additional components that would contribute to energy usage. Cryptographic systems require extra processing power to encrypt/decrypt data,\textsuperscript{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 maximise 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,\textsuperscript{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 technology and ergonomics is an important secondary concern in the development of medical devices. 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 upon 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 arise 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 – 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 under-utilised due to the inconvenience of carrying around additional devices. Excessively burdensome security systems may even incentivise non-adherence 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, but using consumer devices in this manner raises 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 via 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\textsuperscript{19}, demonstrating the risks associated with internet-enabled medical devices. This issue of network security in healthcare is discussed in detail in a recent paper by Independent Security Evaluators\textsuperscript{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\textsuperscript{95}. Firmware serves to control the hardware of embedded medical devices such as IPGs, so 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, while the user interface on most IPGs will prevent the setting of stimulation parameters capable of causing tissue damage (as discussed in “Blind attacks”, above), 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 here is the context under which updates can take place and the authorisations necessary; it may be preferable to prevent updates being made over the internet and instead require an authorisation 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 non-communicative 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. Similar considerations must be made with regards 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 via 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 above have ever been attempted. Nevertheless, we believe that the issues discussed in this paper indicate that brainjacking is a potentially serious threat that warrants 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 towards more rigorous discussion of neurosecurity issues, there are doubtless several as-yet unidentified potential attack strategies. The focus of the present paper 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 modelling may prove to be useful in identification of the most effective strategies for minimising neurosecurity related risk. Stakeholders should collaborate to quantify the expected risk of brainjacking in order 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 utilised 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 upon 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. While 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 over 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, publicising these risks among clinicians and patients may be an important means of minimising risks. Even if it were possible to implement 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 minimise neurosecurity risk. Patients should have some degree of awareness of particularly risky behaviours to avoid, although any discussion of this topic should avoid undue alarm and emphasise the extremely low probability of any individual patient being targeted by electronic attacks.

In writing this paper, we are aware that the information contained herein could be used by an attacker to engage in one of the attacks described above. This is a risk we take seriously, but we believe that the benefits of publicising this topic outweigh the increased danger. The physiological mechanisms that we describe are all easily accessible in scientific journals and any intellectually capable attacker could do their own research; the main challenge for an attacker is in accessing the implanted devices, not in deciding what to do once access is achieved. Furthermore, as discussed above, the current risk of brainjacking is low. The examples given in this paper are intended to illustrate attacks that could be made even with our current, relatively crude, level of neurotechnology. It is better to consider this issue seriously now, rather than in a several years’ time when the sophistication of these implants is far greater, as would be the harm that an attacker may cause by subverting them.

The advantages offered by integrating electronics with the human nervous system are substantial and the rapid development of this area suggests even greater things to come in the future. As with many emerging technologies, these advances are not without risks and pitfalls. The histories of both
information security and medicine have amply demonstrated that prevention is better than cure, so
let us apply these lessons to neurosecurity while the situation remains relatively tractable.

Funding and acknowledgements

The authors would like to thank the Norman Collisson Foundation and NIHR Oxford Biomedical
Research Centre for funding this work. Thanks to B. Cheeran, A. Dwyer, A. Gillespie, H. Maslen, P.
Nye, A. Sandberg, and T. Siepmann for feedback and support.
References


71. Sousa MB, Reis T, Reis A, Belmonte-de-Abreu P. New-onset panic attacks after deep brain


Table 1: Summary of attack types

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

Abbreviations: ET, essential tremor; GPi, internal globus pallidus; IPG, implantable pulse generator; NAcc, nucleus accumbens; OCD, obsessive-compulsive disorder; PAG/PVG, periaqueductal/periventricular grey matter; PD, Parkinson’s disease; STN, subthalamic nucleus; ViM, ventral intermediate thalamic nucleus; VPL/VPM, ventroposterior lateral/medial thalamic nucleus
Abbreviation list

DBS = Deep Brain Stimulation
ET = Essential Tremor
GPi = internal Globus Pallidus
ICD = Impulse Control Disorder
IPG = Implantable Pulse Generator
NAcc = Nucleus Accumbens
OCD = Obsessive-Compulsive Disorder
PAG = Periaqueductal Grey matter
PVG = Periventricular Grey matter
PD = Parkinson’s Disease
STN = Subthalamic Nucleus
VPL = Ventroposterior Lateral thalamic nucleus
VPM = Ventroposterior Medial thalamic nucleus
VTA = Volume of Tissue Activated
Disclosure – conflict of interest

As corresponding author I, Laurie Pycroft, am not aware of any conflicts of interest among any of the authors relevant to this review article.