BioSpectrum
the business of Bio & Health Sciences
ASIA EDITION

Research shows vulnerability of brain hacking for memory manipulation

05 November 2018 | News

Vulnerabilities exist in the connected software and hardware and these need to be addressed if we are to be ready for the threats that lie ahead, according to a new report by researchers from Kaspersky Lab and the University of Oxford Functional Neurosurgery Group.

Singapore - In the future, cyberattackers may be able to exploit memory implants to steal, spy on, alter or control human memories. And while the most radical threats are several decades away, the essential technology already exists in the form of deep brain stimulation devices. Scientists are learning how memories are created in the brain and can be targeted, restored and enhanced using such implantable devices. However, vulnerabilities exist in the connected software and hardware and these need to be addressed if we are to be ready for the threats that lie ahead, according to a new report by researchers from Kaspersky Lab and the University of Oxford Functional Neurosurgery Group.

The researchers combined practical and theoretical analysis to explore the current vulnerabilities in implanted devices used for deep brain stimulation. Known as implantable pulse generators (IPGs) or neurostimulators, these devices send electrical impulses to specific targets in the brain for the treatment of disorders such as Parkinson's disease, essential tremor, major depression, and obsessive–compulsive disorder. The latest generation of these implants comes with management software for both clinicians and patients, installed on commercial-grade tablets and smartphones. The connection between them is based on the standard Bluetooth protocol.

The researchers found a number of existing and potential risk scenarios, each of which could be exploited by attackers. These include:

- Exposed connected infrastructure – the researchers found one serious vulnerability and several worrying misconfigurations in an online management platform popular with surgical teams that could lead an attacker to sensitive data and treatment procedures.
- Insecure or unencrypted data transfer between the implant, the programming software, and any associated networks could enable malicious tampering of a patient’s or even of whole groups of implants (and patients) connected to the

same infrastructure. Manipulation could result in changed settings causing pain, paralysis or the theft of private and confidential personal data.

- Design constraints as patient safety takes precedence over security. For example a medical implant needs to be controlled by physicians in emergency situations, including when a patient is rushed into a hospital far from their home. This precludes use of any password that isn't widely known among clinicians. Further, it means that by default such implants need to be fitted with a software 'backdoor'.

- Insecure behavior by medical staff – programmers with patient-critical software were found being left with default passwords, used to browse the internet or with additional apps downloaded onto them

Addressing these vulnerable areas is key, because the researchers estimate that over the coming decades, more advanced neurostimulators and a deeper understanding of how the human brain forms and stores memories, will accelerate the development and use of such technology and create in new opportunities for cyberattackers.

Within five years, scientists expect to be able to electronically record the brain signals that build memories and then enhance or even rewrite them before putting them back into the brain. A decade from now, the first commercial memory boosting implants could appear on the market – and, within 20 years or so, the technology could be advanced enough to allow for extensive control over memories.

New threats resulting from this could include the mass manipulation of groups through implanted or erased memories of political events or conflicts; while 'repurposed' cyberthreats could target new opportunities for cyberespionage or the theft, deletion or 'locking' of memories (for example, in return for a ransom).

Commenting on the results of the investigation, Dmitry Galov, junior security researcher, Global Research and Analysis Team, Kaspersky Lab said, "Current vulnerabilities matter because the technology that exists today is the foundation for what will exist in the future. Although no attacks targeting neurostimulators have been observed in the wild, points of weakness exist that will not be hard to exploit. We need to bring together healthcare professionals, the cybersecurity industry and manufacturers to investigate and mitigate all potential vulnerabilities, both the ones we see today and the ones that will emerge in the coming years."

Laurie Pycroft, doctoral researcher in the University of Oxford Functional Neurosurgery Group added: "Memory implants are a real and exciting prospect, offering significant healthcare benefits. The prospect of being able to alter and enhance our memories with electrodes may sound like fiction, but it is based on solid science the foundations of which already exist today. Memory prostheses are only a question of time. Collaborating to understand and address emerging risks and vulnerabilities, and doing so while this technology is still relatively new, will pay off in the future."