Almost everyone has seen a James Bond movie and has enjoyed all the intricate contraptions designed for 007. In today’s throes of mystery and intrigue, we might even envision a modern-day hacker tinkering with an influential, high-ranking official’s pacemaker to cause his or her ultimate demise. Research now seems to indicate that security concerns about implantable medical devices (IMDs) are not “Bond-ish”—they are real and potentially deadly.1,2 Even back in 2007, Vice President Dick Cheney’s cardiologist disabled the wireless functionality of his pacemaker because of just that fear.3

IMDs have been around since 1958. They include pacemakers, implantable cardiac defibrillators, insulin pumps, cochlear implants, and neurostimulators. In the US, they’re regulated by the Food and Drug Administration (FDA). However, over the years, there has been a lack of focus on issues surrounding possible cyberattacks that tamper with IMDs.5 We certainly have made advances in IMDs over the past six decades, especially in the areas of biocompatibility, structural design of devices and delivery systems, power management, and detection or wireless communication issues.3 We still need, however, to take a closer look at security issues relating to IMDs in the near future.

Current Trends
According to a new market research report,5 the nanotechnology in the medical devices market was valued at around US$5 billion in 2014 and expected to reach around US$8.5 billion by 2019. Every year, about 300,000 Americans receive wireless medical devices, including IMDs, such as pacemakers, glucose monitors, and pain pumps.6 The key question is, “Can these Internet-connected medical implants, like pacemakers, be hacked?” A new report in the journal Science suggests that this could be the case.3 Many of these devices connect with a hand-held controller over short distances using Bluetooth.3 According to the April 2015 issue of Communications of the ACM, Security and safety issues in the medical domain take many different forms. Examples range from purposely contaminated medicine to recalls of vascular stents, and health data breaches. Security risks resulting from intentional threats have only recently been confirmed, as medical devices increasingly use newer technologies such as wireless communication and Internet access. Intentional threats include unauthorized access of a medical device or unauthorized change of settings of such a device.7

In the coming years, more IMDs will be approved and used by patients. On 14 January 2015, the FDA approved the Maestro Rechargeable System, the first FDA-approved obesity device since 2007. According to the Centers for Disease Control and Prevention (CDC), one third of all US adults are obese (www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm430223.htm), suggesting a potentially broad user base.

Background
Cardiac implantable electronic devices (permanent pacemakers and

---

**Biological Warfare**

**Tampering With Implantable Medical Devices**

**Jay Liebowitz, Harrisburg University of Science and Technology**

**Robert Schaller, University of Pennsylvania**

---
implantable cardioverter defibrillators) are particularly appealing targets for cyberattacks due to the life-saving services that they provide and the complexity of their platforms. These devices utilize embedded software to monitor heart rates in patients with heart rhythm disorders. Randomized clinical trials have consistently shown benefits in certain patient populations, leading to a dramatic rise in implantation rates.8

Practitioners use commercial device programmers that communicate with these devices to extract clinical information, test particular features, and modify programming. Radio software makes it possible to communicate when in close proximity but without a direct connection. Recent advancements have allowed communication over the Internet to facilitate more expedient and efficient patient–physician communication, which has also resulted in financial savings. These same conveniences also make these devices more vulnerable to cyberattacks.

According to one study,9 secure system design for IMDs has the following challenges:

- **Battery life.** Security algorithms increase IMDs’ operation complexity and degrade the battery life dramatically.
- **Adaptability.** New countermeasures might be needed to combat new attacks, thus the IMD must be modifiable.
- **Availability.** IMDs should be available to a doctor for emergency treatment, even if that doctor wasn't previously authorized.
- **Reliability.** Security mechanisms should be robust enough to ensure system reliability.

Some security threats to IMDs fall into the categories of eavesdropping, impersonation, and jamming. Current approaches for dealing with these potential threats are through cryptography, external device deployment (pairing an external wearable device with the IMD), anomaly detection, and frequency hopping-spread spectrum (FHSS) and direct sequence-spread spectrum (DSSS) defenses.5

**Is There Still a Concern?**

So, the key question remains, “Can these IMDs be tampered with and hacked by others who aren’t supposed to have access?” In 2008, William Maisel, a Harvard Medical School cardiologist, co-authored a paper that indicated that hackers could reprogram an IMD without authorization.1 Using a commercial ICD programmer and a software radio, researchers were able to gain wireless access to a Medtronic defibrillator to garner personal patient data and enable potentially malicious therapy. Despite significant advantages (a team of researchers, expensive lab equipment, and close proximity to the device), they were able to show that potential security problems do exist.

The report encouraged IMD manufacturers to heed this warning and provide proper security precautions. Medtronic, Boston Scientific, and St. Jude Medical are the main manufacturers of defibrillators. Back in 2008, Medtronic (after seeing the report) said it was increasing the sophistication of the devices to make it difficult for outside tampering. Also, Boston Scientific said at that time that it used encryption in its defibrillators, and doubted its devices could be hacked.1

In 2013, Billy Rios and Terry McCorkle of Cylance reported a hard-coded password vulnerability affecting roughly 300 medical devices across approximately 40 vendors. Based on their research, the vulnerability could be exploited to potentially change critical settings or modify device firmware (https://ics-cert.us-cert.gov/alerts/ICS-ALERT-13-164-01).

A 2014 medical device cybersecurity workshop hosted by the FDA noted that “it’s only a matter of time before a patient is killed or injured due to a targeted cyberattack against a medical device—or even as the result of an unintentional cyber vulnerability.”10

Also, in 2014, the US Department of Homeland Security indicated that it was investigating about two dozen cases of suspected cybersecurity flaws in medical devices and hospital equipment that officials fear could be exploited by hackers.11

But while preemptive investigation in an effort to identify vulnerable firmware is one thing, criminal investigation after the fact is another. The medical examiner’s office does not necessarily have the expertise or resources to perform basic device interrogations, let alone the capability to conduct composite computer forensics investigations.

**What Still Needs to Be Done?**

It’s crucial to anticipate threats and create systems that are adequately protected. In addition to encouraging the industry to increase security, Maisel’s team also presented “zero-power” defenses (that is, defenses that don’t rely on the IMD’s battery but rather harvest power from external RF), including audible notifications warning a patient of tampering or requiring that an incoming signal be authenticated. Additional research aimed at defending such activity involved the creation of a “noise shield” that can block out certain attacks, the use of ultrasound waves to determine the distance between a transmitter and a
medical device to prevent remote attacks, and the development of a biometric heartbeat sensor to allow devices within a body to communicate with each other, keeping out external devices and signals.12-14 As with all evolving technologies, complex security systems must be balanced with ease of use for practitioners on a daily basis.

From an IT security perspective, this is certainly a new potential type of “biological warfare.” IMD manufacturers must find ways to better secure their devices from possible outside hacking by incorporating security technologies such as encryption, and the FDA needs to study this issue carefully. If not, people may certainly be able to get at “the heartbeat of America”!

References

Jay Liebowitz is the Distinguished Chair of Applied Business and Finance at Harrisburg University of Science and Technology. He previously was the Ordway Endowed Chair in Management and Technology at the University of Maryland University College, and full professor at Johns Hopkins University. Contact him at jliebowitz@harrisburgu.edu.

Robert Schaller is an assistant professor of clinical medicine at the Hospital of the University of Pennsylvania. He specializes in the treatment of heart rhythm disorders, including complex ablation therapy and implantation, and extraction of cardiac implantable electronic devices. Contact him at robert.schaller@uphs.upenn.edu.