Who Does the Autopsy? Criminal Implications of Implantable Medical Devices

by
Marc Goodman, Future Crimes Institute
goodman (at) futurecrimes.com

Abstract:

Rapid advances in medicine are increasingly enabling the integration of information technology with biology. Each year, tens of thousands of medical devices, including pacemakers, cardiac defibrillators and insulin pumps are being implanted into human beings around the world. While a small community of researchers has begun to pose critical questions about the privacy and security implications of incorporating computer technology into biological systems, little if any consideration has been given to the criminal opportunities created by doing so. Just as personal computers, credit cards, ATMs, mobile phones and SCADA systems have been subverted for criminal purposes, so too will implantable medical devices (IMDs). While IMDs have the potential to heal and save lives, they can also be exploited to commit crimes ranging from homicide to extortion. Heretofore law enforcement and criminal justice authorities have been absent from any substantive discussions regarding the highly disruptive future trends in medicine—an omission that must be remedied in order ensure public safety in the face of emerging, but imminent forms of criminal attack directed against medical technologies.

1. Introduction

Current and future innovations in medicine herald tremendous benefits for the sick and injured. Advances in a wide variety of scientific disciplines, including nanotechnology, robotics, synthetic biology, genomics, artificial intelligence and computer science, will save untold numbers of lives. To this end, health care systems around the world are rapidly adopting new forms of technology in an effort to improve patient outcome and to reduce costs, including the notable increase in the use of implantable medical devices (IMDs).

The range of available IMDs is ever expanding and includes cardiac pacemakers, defibrillators, cochlear implants, insulin pumps, neuro-stimulators and various drug delivery systems. In the States alone, over 2.5 million people rely upon IMDs to treat conditions ranging from cardiac arrhythmias to diabetes to Parkinson's disease.[1] According to a study by the Freedonia Group, demand for IMD's in the United States will increase 8.3% annually and will grow to a $48 billion dollar business by 2014.[2]

Initially, IMDs were stand-alone devices which did not frequently communicate with the outside world. Today, however, many of these devices are equipped with wireless technologies that allow for direct communication between the IMD and a base station controller, which itself connects via the Internet, mobile telephony or a landline phone to a medical care provider. These systems transfer data from the IMD to the base station via a variety of communications protocols, such as RFID or Bluetooth, and forward physiological information to medical practitioners for the purposes of monitoring and patient management. Some systems are send-only, such as blood glucose monitors, but others such as implantable cardiac defibrillators, are bidirectional and allow commands to be sent from a local controller to the IMD, causing the IMD to take a particular action, such as shocking the heart.

2. Past as Prologue: The Coming Criminal Subversion of IMDs

Criminals and terrorists have proven extremely adept at hacking and subverting any number of previously created technologies. Desktop computers have been targeted by computer viruses, credit card cryptographic algorithms have been reversed engineered, mobile smartphones are increasingly infected with malware, the Stuxnet worm effectively targeted energy industrial control systems and insurgents in Iraq successfully intercepted the video feed on a United States Department of Defense Predator drone.

Just as organized criminals have corrupted other forms of technology for personal gain, they will undoubtedly turn their attention to IMDs. Research has proved a number of viable attack vectors against IMDs. These range from software radio attacks to resource depletion

attacks.[3] [4] Using a variety of attack methodologies, researchers have been able to change IMD device settings, disable therapies and even deliver a command shock to an implanted pacemaker.

Many of the underlying communications technologies utilized by IMDs are notoriously insecure, with numerous documented successful exploits targeted against RFID, Bluetooth, GSM and wireless networking protocols.[5] [6] [7] [8] Moreover, as the overall number and diversity of devices communicate with IMDs increases, the resultant complexity and networking effect will complicate any efforts to secure the overall medical device ecosystem.

3. Crime Scenarios

There are any number of criminal offenses which might be perpetrated by targeting and attacking an IMD, with homicide being the most obvious concern. As demonstrated previously, a remote directive transmitted over the Internet could cause a command shock to be issued to a pacemaker, resulting in the sudden death of a targeted victim. In another example, an organized crime group, upon obtaining access to an IMD, might send an extortion email advising a victim that they had 1 hour to transfer funds to an overseas bank account or face shutdown of their IMD.

Of course the attack need not come from a far-away land nor from an unknown party. What might a disaffected spouse with criminal intent be able to accomplish? Armed with intimate details of a partner's medical condition, knowledge of how the IMD system worked and close-quarter access to all the relevant components, a live-in partner would be well-suited to perpetrate an attack if so motivated. With nearly 33% of all women murdered by somebody they know, women might be at particular risk for this type of attack.[9]

Moreover, as growth of IMDs increases to a more significant percentage of the population, it would be possible to target not just one person, but entire groups of individuals with a given IMD. For example, a sufficiently powerful electromagnetic pulse (EMP) could cause harm to large number of individuals with IMDs and instructions for building an EMP generator are widely available on the Internet.[10] Moreover, a criminal or terrorist organization could choose to launch a widespread critical infrastructure attack against hospital control systems and IMDs. According to researchers at the Oak Ridge National Laboratory, in both 2003 and 2009 respectively, the "Slammer" and "Conficker" worms had each successfully infected networked hospital systems responsible for monitoring heart patients.[11] Since the initial days of Slammer and Conficker, malware has since become even more sophisticated and a Trojan similar to Stuxnet, a highly specific and tailor-engineered piece of malicious code, could cause harm to numerous patients around the world simultaneously as a result of a zero-day exploit.

Though these scenarios may sound far-fetched, it is important to recall that criminals and terrorists have taken many draconian and anti-social actions in the past, from flying passenger jets into skyscrapers, to murdering thousands as part of ongoing narco-wars to prolific serial homicide involving acts of cannibalism. Therefore, it is not unreasonable to believe that as IMDs and other technologies become more prevalent that they will attract the attention of criminally motivated individuals or groups seeking to exploit them for financial gain, revenge or media attention alone.

While this article has focused on the criminal implications of IMDs, there are also a plethora of other concerns including significant potential privacy exploits wherein a device could provide a patient's private medical information to unauthorized parties. Furthermore, as location-based services become more prevalent, IMDs could also provide ongoing details of a patient's location around the clock, a feature that could be exploited to great effect by kidnappers, celebrity stalkers or even in domestic violence cases.

4. Building Bridges & Saving Lives

Heretofore law enforcement and criminal justice authorities have been absent from any substantive conversations regarding the integration of biology with technology. Yet given the rapidly increasing number of medical devices implanted each year, it is just a matter of time before these patients eventually die. When they do, they and their IMDs will arrive at the office of a medical examiner tasked with determining the cause of death in each case.

When the deceased begin to arrive, how will a coroner go about determining the cause of death?

Did the decedent with a pacemaker die of natural causes? Was this an accidental death due to an IMD malfunction? Was the device specifically targeted for criminal purposes? Or, was this a suicide wherein the patient himself subverted his own IMD to end pain and suffering, hoping that his family would receive life insurance funds for his apparent natural death? As modern medicine evolves and the proliferation of IMDs increases, one vital question must be answered: when a technologically-enhanced body shows up at the morgue, who will be capable of performing the autopsy?

Few if any police officers, prosecutors or coroners have studied biomedical engineering. It is also true that few biomedical engineers or physicians have studied forensic science or criminal justice. As increasing numbers of patients with IMDs arrive at the medical examiner's office, there will be a need, however, for both skill sets. Trained police investigators and corners will rely upon biomedical engineers for their expertise in attempting to forensically determine a cause of death. Conversely, device manufacturers and research scientists have limited understanding of the types of forensic evidence that would be required from an IMD to support a successful prosecution and conviction in case of criminal tampering.

5. Further Study

Implantable medical devices represent but one of an emerging breed of scientific breakthroughs being introduced into the healthcare delivery system. Nevertheless, they are by no means the only medical technology subject to malicious criminal attack. Other professional and consumer medical technologies such as telemedicine, m-health smartphone applications and robotic surgery, to name but a few, all incorporate similar underlying communications technologies and as such, may also be vulnerable to criminal attack in the future.

Further study is needed to delineate the best mechanisms of cooperation between criminal justice authorities, device manufacturers, researchers and the medical provider community. Moreover, additional research is required to determine the most appropriate way to educate the criminal justice and the medical-legal communities regarding potential criminal threat vectors against IMDs.

6. Conclusions

The time for both the medical and justice communities to come together and discuss the potential criminal threats against IMDs is now—before the next generation of IMDs is engineered and before widespread criminal attack methodologies are developed. Absent a seat at the table and additional training, who, if anybody at the medical examiner's office will be capable of performing the autopsy and determining the cause of death in cases involving IMDs? Who will be present from the criminal justice community to ensure that society's public safety interests are addressed?

There may be significant benefits for device manufacturers and medical researchers who choose to engage with criminal justice authorities on a proactive basis. Failure to do so, however, may result in a significant backlash and future draconian regulation, particularly after the first case of a documented homicide resulting from a criminally subverted IMD occurs. Moreover, the inclusion of law enforcement authorities in relevant discussions will enable them to share their unique perspectives and experience regarding criminal modus operandi, thereby creating an opportunity for manufacturers to engineer in security defenses up-front as a means of future crime prevention. Without formalized cooperative and information sharing mechanisms between justice and medical authorities, society may pay a heavy toll as new forms of criminal attacks against IMDs are developed and become widely disseminated.

References

[1] Leavitt, N. "Researchers Fight to Keep Implanted Medical Devices Safe From Hackers." *Computer* 43, no. 8 (2010): 11-14.

[2] See the Freedonia Group report, "Implantable Medical Devices US industry Forecasts for 2014 & 2019,"available at http://www.pharmaceutical-market-research.com/publications/medical_ devices /implantable_medical_devices.html.

[3] Halperin, D, T S Heydt-Benjamin, B Ransford, S S Clark, B Defend, W Morgan, K Fu, T Kohno, and W H Maisel. "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses." In 2008 IEEE Symposium on Security and Privacy. 2008.

[4] Hei, X, X Du, J Wu, and F Hu. "Defending Resource Depletion Attacks on Implantable Medical Devices.

[5] Newitz, A. "The RFID Hacking Underground: They Can Steal Your Smartcard, Jack Your Car, or Even Clone the Chip in Your Arm. And You Won't Feel a Thing. Five Tales From the Newest Cybercrime Frontier." WIRED-SAN FRANCISCO- 14, no. 5 (2006): 166.

[6] Loo, Alfred. "Technical Opinion: Security Threats of Smart Phones and Bluetooth." Commun. ACM 52 (2009): doi:10.1145/1467247.1467282. http://doi.acm.org/10.1145/1467247.1467282.
[7] Gold, S. "Why WPA Standards Won't Protect Your Network." Infosecurity 7, no. 1 (2010): 28-31.
[8] Bradbury, D. "Hacking Wifi the Easy Way." Network Security 2011, no. 2 (2011): 9-12.
[9] United States Bureau of Justice Statistics, available at http://bjs.ojp.usdoj.gov/content/homicide/intimates.cfm, accessed on 5 April 2011.
[10] See http://www.wikihow.com/Build-an-Emp-Generator for example, access on 4 April 2011.
[11] Leavitt, N. "Researchers Fight to Keep Implanted Medical Devices Safe From Hackers." Computer 43, no. 8 (2010): 11-14.

About the Author:

Marc Goodman is the founder of the Future Crimes Research Institute and the Security Advisor to Singularity University. Mr. Goodman has worked around the world on law enforcement and security matters and serves as a Senior Advisor to INTERPOL's Steering Committee on Information Technology Crime. He may be contacted at: goodman (at) futurecrimes.com.