Implantable Hacking Devices: An Undetectable Threat to Electronics Security.

Hack Miami/ Caveo Security/ Torchlit Studios

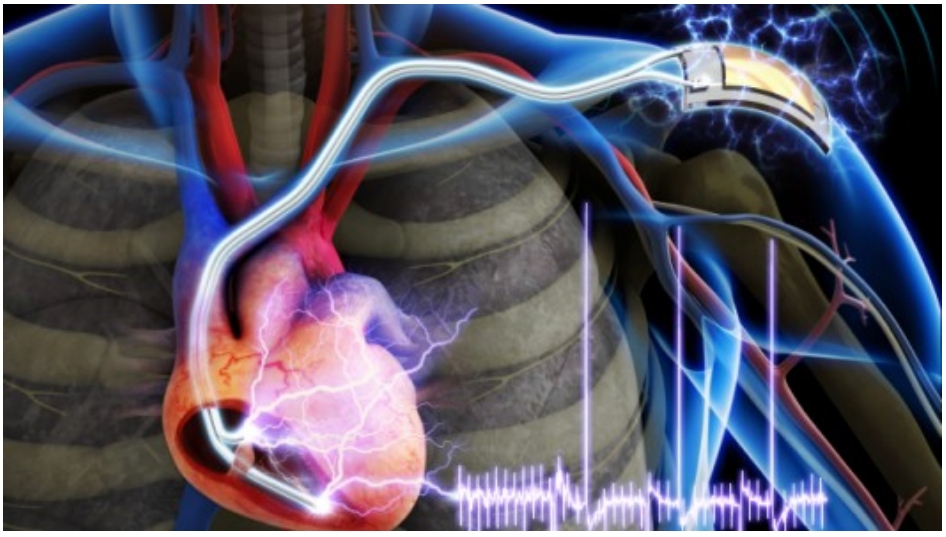
Author:
Seth Wahle

2-8-2015

Abstract: Implantable electronic devices will allow hackers to breach the security of networks, infrastructure and personal electronics. These purpose built implantable devices will be nearly undetectable via currently available personnel scanning and searching devices and techniques. For proof of concept an implantable near-field communications chip was used to compromise Android devices. This simple device could however be used to compromise a wide array of devices and systems.

Introduction: With electronics technology advancing in its current direction, It will soon be logistically feasible for purpose built circuits to be implanted in the human body for the purpose of breaching various security measures. This is attributed to several factors including advancement in implanted power generation, miniaturization and cost reduction of integrated circuits, and the commercialization of implantable devices.

The medical industry has been long searching for ways to eliminate the need to do repetitive surgeries to replace the batteries in pacemakers. New Flexible Piezoelectric nanogenerators have been developed, tested, and human trials are underway. These thin film nanogenerators are implanted in the patients shoulder and generate power to recharge the pacemakers battery with every movement. Even the blood vessels expanding and contracting below the generator is enough to generate a charge, this means that the generator is capable of maintaining the battery as long as the person is alive.



Caveo Security
a cyber security defensive action company

hackmiami

Next, the miniaturization and cost reduction of integrated circuits will make highly capable electronics of an implantable size affordable to the masses. Due to an influx in both the application specific integrated circuit (ASIC) and the field programmable gate array (FPGA) in recent years, the cost of producing compact, energy efficient, yet powerful electronics has been steadily decreasing. This is exceedingly evident in the mobile and embeded computing markets. This will lay the ground work for new implantable hacking devices to be a feasible production. Even now scientists have been able to produce RFID tracking devices small enough tot track the whereabouts of bee's in effort to find the cause of decreasing bee populations. The tracking device illustrated is able to track a bee at a distance of about 10ft and was manufactured by hand. They estimate that through integration of the circuit in to a silicon wafer and machine production, they could significantly reduce the size, weight, and electrical consumption of the device.

Finally, There is a movement towards the commercialization of implantable devices. This has been spurred by a “bio-hacker” movement. Companies such as Grindhouse Wetwear and Dangerous-things.com have already begun producing and selling implantable devices and self implant kits. Tim Cannon of Grindhouse Wetwears even went as far as to implant a custom cellphone sized circuit in to his forearm to track his own biomedical data. While these companies have yet to be scrutinized by any legal regulations, they have taken it upon themselves to attempt to meet or exceed the regulations of the standing medical and body modifications markets. There is a current and growing demand for these implantable devices. I personally know of over 500 people who currently have devices similar to the one used in this demonstration implanted in their hands already. If I can figure out that I can subvert certain security protocols and practices using my device, then it is only a matter of time before they explore the idea as well.

Caveo Security
a cyber security defensive action company

hackmiami

Electronics and medical technology have advanced to a point where low energy electronic devices can now be implanted in the body. A hacker equipped with with an implanted device can undetectably take remote control of any NFC (near field communications) enabled android phone. This experiment serves as a proof of concept to an implantable device being used as an attack vector.

Implantable Device Specifications: For this experiment a 13.56Mhz ISO and NFC type 2 compliant NTAG216 RFID chip-set, with a 7 byte UID and 888 bytes of read/write memory was encapsulated in a Schott 8625 Bio-glass capsule and implanted In to the hand between the thumb and index finger. When implanted the device is nearly visually undetectable and does not trigger metal detectors.

Implant Wound	Well healed
	

Implementation: To test this concept a well known exploit was implemented in a new way. The Implanted device was encoded to trigger the android phone to access an HTTP download link. This link downloads a Metasploit meterperator .APK file (android reverse TCP). The meterperator, once installed and run on the android phone, opens contact to the metaspliot multi-handler installed on a virtual private server. The metasploit multi-handler allows the attacker to remotely control functions of the android phone including taking pictures from the front and back camera, receiving the GPS location of the phone, downloading and uploading files to the SD card , and giving the attacker a remote shell to execute commands.

Results: The implanted device successfully triggers the download of the malicious file on all tested NFC compliant android phones, with NFC transmission enabled. With the file downloaded and installed, remote control of the phones was successfully established and all features of the phone are remotely controllable and files can be downloaded from the phone. However, in order to use the attack vector to against an unwitting victim limitations of the system would have to be overcome via social engineering or additional system development.

Limitations: The malicious .APK file loses connection to the remote server when the phone goes in to its locked mode or if the phone is rebooted. This could be overcome by rewriting the file to run as a background service that starts on boot. The .APK file must manually installed and phone settings to allow installation of untrusted sources is necessary to make the system work. This can be overcome through social engineering, or providing the malicious .AKP file with Google play signatures, and using an additional exploit to cause a forced installation.

Conclusion: This experiment clearly demonstrates the viability of implantable devices as an attack vector as well as the lack of security in the NFC protocol. While NFC was targeted for this experiment, as ASIC technology advances and becomes less expensive to produce, more capable implantable hacking devices could be developed.