Malware in Men - will you be protected?

Babu Nath Giri
McAfee Avert Labs, Bangalore

About Author

Babu Nath Giri is Malware Researcher at McAfee Avert Labs, Bangalore.
Contact Details: c/o McAfee India Software India Pvt. Ltd., Pine Valley 2nd Floor, Embassy Golf Links Business Park, Intermediate Ring Road, Bangalore 560071, India, phone +91-80-6656-9626, fax +91-80-6656-9099, e-mail babu@avertlabs.com

Keywords

Computer Threats, Malware, Bionics, Cyborgs, Cybernetics, Pacemakers, Wearable Computers, Body Area Networks, Personal Area Network

Malware in Men - will you be protected?

Abstract:

Computers continue to increase their influence in many aspects of today's society, and that trend shows no signs of slowing down. We see computers in almost all walks of life, from satellites to cell phones, and from cars to coffee machines. Years ago people entered computers to operate and repair them; today, in contrast, computers are starting to enter humans.

As computers become faster, smaller, and wireless, wearable or implanted devices are gaining in popularity. These very portable computers are particularly useful in the area of medicine. Implantable devices such as pacemakers and hearing aides save and improve lives. Wearable devices—particularly consumer electronics such as MP3 players—have been popular for several years. Today we have MP3 jackets, head-mounted displays, and wrist-worn PCs. The comfort and mobility of these devices is compelling; however, because these are still computers, we also face the problems of the security and stability of these devices.

One excellent study on the security and privacy of implantable devices was done by Daniel Halperin et al (Daniel Halperin, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S.Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, William H. Maisel, 2008). We've also read a fine study on the security issues of some popular consumer electronics, such as MP3 players and video streaming devices, by T. Scott Saponas et al. (T. Scott Saponas, Jonathan Lester, Carl Hartung, and Tadayoshi Kohno 2006). The two studies demonstrate that these devices are vulnerable to malicious attacks. In this paper we will look at the big picture of wearable and implanted devices with security in mind. We will also discuss the possibility of such malware arising in the future.

Introduction

One of the biggest developments in the 20th and 21st centuries has been the computer and the field of computer science. Computers have taken over as a major part in all walks of modern life. We see computers everywhere and in everything these days, from toasters to satellites. It is hard to imagine life without computers in the present era. Computers have been a boon to us in many fields, including medicine, communications, education, entertainment, and commerce.

Computers have become so advanced that we even have miniature microprocessors or electrical circuits placed within human bodies. For example, a digital video camera replaced the eyes of a blind man; electrical signals were processed by a microcomputer and then transmitted to the nerves in the visual cortex by way of electrodes, giving the patient an archaic but effective vision as bright dots that resemble a stadium display[1].

As computer circuitry becomes smaller and smaller and as scientists gain more knowledge about interfacing with the human system, there will be more electronics embedded in our bodies. It is safe to assume that in the future, bionic parts in humans might be common. Computers have come a long way from the time when humans entered computer systems to operate and repair them; to today, when computers are now entering humans.

[1] http://jp.senescence.info/thoughts/cybernetics.html

Computers and the Internet have transformed the way we work and live, yet they are not without their share of problems. Computer viruses, worms, and Trojans plague us today. With the advent of the Internet there has been an increase in maliciousness in this field, causing disturbances and loss of critical resources. These computer threats have spread to all devices and areas where computers or software are used.

Is this device wearable?

This could be one of the questions you'll ask in the future when you buy an electronic device. As we have seen, more and more devices are getting personal, so wearable is not hard to imagine. If we look to the past, we notice many devices that can be termed wearable. One was the Sony Walkman and later the CDman. These inventions revolutionized the music industry and the way in which people listened to music. The history of wearable devices dates back to at least the 12th century [2] with the invention of eyeglasses[3]. More recent developments in wearable devices are mostly electronic in nature. These devices fit into a few general categories, such as entertainment, communications, monitoring, medical, etc.

Today the most common wearable devices are mobile phones, PDAs, MP3 players, wireless earplugs, etc. These are relatively unobtrusive when compared with devices such as MP3 jackets[4], head-mounted displays[5], and wrist-worn PCs[6]. There is also work underway on "smart" textiles, with integrated electronics (Friedrich Gustav Wachter 2006).

Electronic devices are not just wearable today, but have gone beneath the conceivable human surface. Devices are implanted inside human bodies—for monitoring various medical conditions such as heart disorders, for example see study by G. Tröster (G. Tröster 2004). Does this mean we are becoming cyborgs?

Definition: Cyborgs are a combination of human and mechanical and/or electric systems. Essentially using nonliving parts to enhance some body function(s) or add a new function(s)[7,8].

Cyborgs are not just science fiction. They are gradually becoming a reality. According to some definitions, many of us qualify as cyborgs. People using artificial limbs, pacemakers, and lenses, among other things, are considered cyborgs in some circles because they use external machinery to enhance their functions[7]. More sophisticated machinery is arriving, including computer-assisted artificial limbs and hearing. In the area of limbs, an onboard computer in an amputee's new leg is improving the symmetry of the person's gait across a wide range of walking speeds[9]. Cochlear

[2] http://www.media.mit.edu/wearables/lizzy/timeline.html

[3] http://en.wikipedia.org/wiki/Eyeglasses

[4] http://www.mp3blue.de/english/frameset_e.htm

[5] http://inventorspot.com/teleglass_t3-f_video_eyeglasses_HMD_Japan

[6] http://www.zypad.com/zypad/wearablecomputers.aspx?pg=Zypad%20WL%201000

[7] http://www.usp.nus.edu.sg/cpace/cyborg/haraway/definition.html

[8] http://www.sjsu.edu/faculty/butryn/cyborg.htm#Selected%20academic%20sources

[9] http://www.bmj.com/cgi/content/full/323/7315/732

implants[10] have been instrumental in restoring hearing to people who have difficulty. There are implants planned that will use 3D digital technology and microprocessors to analyze incoming sounds[11]. A spinal cord stimulation system has been developed to reduce pain; these systems also include a surgically implanted device[12]. Implants don't stop there; these are just some of the most successful implementations of human-machine coexistence.

That coexistence holds a lot of promise for patients with vision loss, though this may not happen in the near future. There is research in progress to restore vision to the blind. All of this research is based on implants of microelectronics into the patient's eye. One line of research by MIT scientists involves implanting a microchip in the patient's eye and sending signals to it from a miniature camera[13].

Wearable devices play a far greater role in the area of health care. Miniaturization of electronic devices and advances in wireless connectivity has allowed health care units to maintain a constant watch on a patient's condition [14](A. Tura, M. Badanai, D. Longo, L. Quareni 2003).

With so many devices on or in our bodies the next logical step for a technologist is to connect them using a network for data collection and resource management.

BAN, PAN in a man

Two types of networks have emerged to connect wearable devices on humans for various applications:

- Body-area networks [15](BANs) are used mainly to connect wearable device on one body
- Personal-area networks [16](PANs) connect devices within a close range

These two networks are or will be used for various applications. BANs also come in wireless versions (WBANs), which make them more useful. Combining wearable devices and WBAN has provided many opportunities in the area of health care [17] (Guest Editorial Introduction to the Special Section on M-Health 2004).

WBANs collect data from many sensors on the body, gather them into a central resource, and then transmit this data. Because we will wear or carry several devices—MP3 player, pacemaker, and others—on our bodies, we need a mechanism to control and coordinate all these devices. Traditionally this has been the task of a network operating system.

[10] http://www.nidcd.nih.gov/health/hearing/coch.htm

[11] http://www.columbuswired.net/Health/bionichearing_062801.htm

[12] http://www.controlyourpain.com/index.cfm?langid=1

[13] http://web.mit.edu/newsoffice/1995/microchip-0213.html

[14] http://www.artificialvision.com/newpubs/wearable_healthcare/cached.html

[15] http://www.wirelessnetdesignline.com/
199500635;jsessionid=JAWLLZ4NX5BI0QSNDLQCKH0CJUNN2JVN?printableArticle=true

[16] http://www.networkworld.com/details/468.html

[17] http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=552302

Personal attacks: the malware angle

Once the data is on the wires or in the air, it is susceptible to both innocent and malicious interference. Because the network will use proven and widely available technologies in the final stage of the transfer, this could lead to eavesdropping on the data. You can imagine the potential seriousness of data theft. A person's medical data, for example, will appeal to health insurance companies and pharmaceutical companies. The insurance firms can collect this data and use it later to target these specific customers. The pharmaceutical firms, on the other hand, could use this data in real time to display ads on WBAN-supported devices such as PDAs or personal computers.

The network is skin deep

You have heard about "shivers running up your spine," so don't be surprised in the near future if someone talks about "data running up your spine." One technology under development lets devices use human skin to transmit data across the body.

The initial research using human skin as a data path was done at the IBM Almaden Labs by Thomas Zimmerman[18], who used a very tiny amount of current to transmit the data. The labs built their own transmitters and receivers to work on this technology. Microsoft has also done research in this area and has come up with a method to transmit data and power to devices attached to the human body[19].

Red Tacton, arguably the first practical system of this sort, was built by Japanese communications company NTT[20]. It uses a different technology to transmit data through the skin and does not require the transmitter or the receiver to be in contact with the skin.

I've got you under my skin: the malware angle

Skin-transfer technology will enable people to transfer data just by touching someone or being in contact with a device. That means the data is constantly exposed and makes the system vulnerable to many threats. Because we are often in crowds, it may not always be possible for us to choose with whom we have physical contact. This could lead to surreptitious data tapping. Systems such as Red Tacton allow devices to receive data even when they are not touching, which makes these systems very vulnerable to data thieves.

There are many other situations in which physical contact with devices will be necessary. Some of these applications identify users without having them show ID, just by getting the data off their skin. These situations can lead to malicious devices that could serve as bugs. Door handles and car doors, for example, could operate as silent data thieves. It might be possible not only to retrieve data from such situations but also to inject data into someone.

Heart attacked

Of all implantable devices the most popular and widely used are pacemakers and defibrillators.

Definition: A pacemaker is a small device that is placed under the skin of your chest or abdomen to help control abnormal heart rhythms. This device uses electrical pulses to prompt the heart to beat at a normal rate[21].

[18] http://www.almaden.ibm.com/cs/user/pan/pan.html

[19] http://arstechnica.com/news.ars/post/20040622-3915.html

[20] http://www.taipeitimes.com/News/biz/archives/2005/03/20/2003247076

Definition: An implantable cardioverter defibrillator [22](ICD) is a small device that is placed in your chest or abdomen. This device uses electrical pulses or shocks to help control life-threatening, irregular heartbeats, especially those that could lead the heart to suddenly stop beating (sudden cardiac arrest). If the heart stops beating, blood stops flowing to the brain and other vital organs. This usually causes death if it is not treated in minutes.

These devices are critical in maintaining a stable condition in patients' hearts. Since its invention, the pacemaker has involved into a more sophisticated device. Now pacemakers come with a wireless transmitter that replays data about the patient's heart condition and also programs the pacemaker itself.

Like all other devices with data in the air, even the pacemakers and ICD are vulnerable to hackers. Daniel Halperin et al. discuss the defenses for such threats in their paper (Daniel Halperin, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S.Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, William H. Maisel, 2008).The paper shows that these attacks are possible. A zero-day attack could prove very harmful or fatal because their targets are life critical. These devices don't have the leeway of time that traditional information and digital devices have to recover from these attacks.

You can run but you can't hide

Consumer electronics is full of wearable devices, which come in all shapes, sizes, and uses. One of the most widely used consumer wearable electronics is the MP3 player. Along with the success of Apple's iPod, there are a number of MP3 players in the market. Sales of MP3 players are expected to quadruple in 2009[23]. Apple's iPod, for one, is not just a music player—it has many more applications.

A recent addition to this list of applications is the Nike iPod sports kit. This is a device used by runners to measure and record their distance and pace. The communication between the shoe and the iPod is wireless, and this is vulnerable to hacks. As most of these consumer electronics go wireless they also become vulnerable to attacks. T. Scott Saponas et al. in "Devices That Tell on You: Privacy Trends in Consumer Ubiquitous Computing" say it is possible for somebody to hack a Nike iPod sports kit and track the person using it (T. Scott Saponas, Jonathan Lester, Carl Hartung, Tadayoshi Kohno 2006).

Think before you think

Scientists have made rapid progress in recent years studying the human brain in order to understand its working and develop remedies for many brain defects.

Brain-machine interaction is not new. As early as 1950 it was possible to implant single or multiple electrodes into the cortex of humans and animals for recording and stimulation. The field of brain-machine/brain-computer interaction has been steadily advancing since then. A chief influencing factor for this development is the great potential scientists see in finding remedies for brain and

[21] http://www.nhlbi.nih.gov/health/dci/Diseases/pace/pace_whatis.html

[22] http://www.nhlbi.nih.gov/health/dci/Diseases/icd/icd_whatis.html

[23] http://digital-lifestyles.info/2005/03/17/mp3-player-sales-set-to-nearly-%20quadruple-by-2009/

nervous system damage. Another application is in video games and virtual reality[24]. The World Technology Evaluation Center [25] panel report on “International Assessment of Research and Development in Brain-Computer Interfaces” (Theodore W. Berger, John K. Chapin, Greg A. Gerhardt, Dennis J. McFarland, José C. Principe, Walid V. Soussou, Dawn M. Taylor, Patrick A. Tresco 2007), gives complete details of the state of this research. The analysis of brain signals has also come a long way. One report tells of scientists controlling a robot with a monkey’s brain signals[26]. Scientists have tried the opposite of this process as well: They have implanted microelectrodes in a pigeon brain so they can control the flight of the pigeon with signals sent by computer[27]. There are now wearable devices that can watch brain activity in real time and allow the wearer to mentally control other devices through a computer or from the Internet.

We can already see benefits of these technologies today. For example, a quadriplegic man was able to play video games using his brain as a controller[28]. These systems might not be common, but as the technology improves and miniaturization continues we will see these devices impacting our lives. As more and more companies see the commercial benefit from this field, growth will be rapid. This interest is already visible through the demonstrations of devices and participation of companies at trade shows[29][30].

Are you ready for an external device controlling some of your brain’s functions? This sounds like science fiction, but Sony does not think so. The entertainment giant has filed a patent for a noninvasive device that beams pulses of ultrasound at the head and modifies the firing patterns of the brain, which in turn creates sensory experiences of taste and sound[31].

As we can see, computer input has evolved from punching to typing to touching to thinking. MindSet[32], from NeuroSky, is one example of a thinking device. NeuroSky claims MindSet communicates well with game consoles, PCs, and mobile platforms, including cell phones. This suggests that in the future we will use thought-processing devices to control others’ devices.

This thought leads to many complicated and dangerous situations. For one, stealing personal information might become passé; instead we might have incidents of people stealing others’ thoughts. Or imagine future adware, hosted in a public display that displays an ad relating to something you just thought. There could certainly be better uses of such a technology: For instance, you walk into a shop and clothes that match your tastes are displayed in order. Now who wouldn’t

[24] http://www.pinktentacle.com/2007/10/brain-computer-interface-for-second-life/

[25] http://www.wtec.org/

[26] http://www.networkworld.com/news/2008/011508-researchers-control-robot-with-monkeys.html?fsrc=netflash-rss

[27] http://english.people.com.cn/200702/27/eng20070227_352761.html

[28] http://money.cnn.com/2006/07/21/technology/googlebrain0721.biz2/index.htm

[29] http://www.computerworld.com.au/index.php/id;361485560;fp;16;fpid;1

[30] http://www.computerworld.com/action/article.do?command=view ArticleBasic&articleId=9056579&pageNumber=1

[31] http://www.newscientist.com/article/mg18624944.600

[32] http://www.neurosky.biz/menu/main/press_room/press_releases/3/

like that? A human mind can never stop itself from thinking. And therefore humans might need a device that would transmit selected thoughts at specific locations, in other words, an idea-wall.

Walking a fine line

All wearable devices, whether an MP3 player or a pacemaker, have a similar set of constraints that govern their design. The primary constraints are the form factor and power consumption as well as issues such as their influence on the physical, cognitive, and social identity of the user (Dunne et al, 2005). For wearable such as pacemakers, biosensors, and others, these constraints are multiplied because of the application and position of installation.

Any device that is small enough to be wearable as a biosensor or implanted in the body will have a limited functionality. Adding functions will invariably increase both size and power consumption. Wearable devices, particularly those used in healthcare, need to be designed so that they are universally acceptable. They should also be interoperable and configurable so that in an emergency data can be retrieved from these devices. This latter feature is susceptible to attacks because it may be difficult to verify the authenticity of destination devices or the network. The risk is the same as hooking up your laptop to a wireless network in a coffee shop.

Telephones ring a bell

The telephone was born in the 19th century[33], with a single use. Today mobile telephones have turned into PCs. As more and more applications and features have been built into mobile phones, we needed an operating system to handle them[34][35]. This need gave rise to smart phones.

Smart phones have become an essential part of business, and yet they suffer from their own share of problems. Malware authors target all new technologies that offer them a chance to make money, and we have seen a steady increase in mobile malware in the recent past [36](Mikko Hypponen 2006).

There are some similarities between mobile phones and wearable devices in their evolution. As we find more uses for wearable and implanted devices, whether for medical or entertainment reasons, their development grows.

The spread of malware in mobile devices is limited in nature. This is because of the variety of operating systems and also because malware tends to be operating-system specific. The spread is also limited because mobile malware is still in its infancy; but the threat definitely exists. Medical and wearable devices might soon suffer from threats once they achieve interoperability and greater ease to use.

The underground exists

Developing malware to attack implanted and wearable devices may not be too difficult because the technology used in developing such devices should be easily available. This is likely to fuel the

[33] http://www.telephonetribute.com/timeline.html

[34] http://www.microsoft.com/Windowsmobile/default.mspx

[35] http://www.symbian.com/

[36] http://www.mcafee.com/us/local_content/white_papers/threat_center/wp_malware7a_en.pdf

development of malware as long as there’s money to be made. But the development of malware for neuroscience applications is not as likely to be so easy, though it could exist.

Even though the area of the brain-computer interface is not as advanced as for other computing devices, there is already an underground that is developing private experiments in this field. Traditionally malware authors have come from such backgrounds or groups of similar interests.

Neurohacking or neuroengineering is a term for any method used for interfering with the structures or functions of neurons[37], and neurohackers are the people who do this. You might not recognize these terms but they already exist in the advanced research and underground fields. There are many neurohackers already going about their work, which ranges from transferring EEG patterns from one person to another to recording brain waves[38].There are even books that talk about neurohacking, comparing it with computer systems and giving a description of the labs and how to set them up[39][40].

Conclusion

With wearable and implantable electronic devices becoming a common occurrence in the near future because of its use and miniaturization, security issues looms over its use in critical areas. As we have seen there are loop holes found in most of the new inventions. On the other side we have also seen efforts being made by researchers in combating such threats. Keeping in mind the pitfalls we have encountered in the previous systems we will need have a more unified and immediate plan to keep up with the pace of malice. Systems will have to be designed with security as one of the main criteria if these devices have to find a permanent place in critical areas. Laws and standards for this field will have to be made before it gets too late.

[37] http://en.wikipedia.org/wiki/Neurohacking

[38] http://www.eff.org/Net_culture/Cyborg_anthropology/cyber_modification.article

[39] http://home.ramonsky.com/not-for-wimps/index.html#Introduction

[40] http://home.ramonsky.com/stuff/icmm/

References:

Friedrich Gustav Wachter (2006). Integrated Microelectronics for Smart Textiles. Leopold-Franzens-Universität Innsbruck, Ambient Intelligence SE WS2006/07.

Tröster, G. (2004). The Agenda of Wearable HealthCare. IMIA Yearbook of Medical Informatics 2005

Tura, A., Badanai, M., Longo, D., Quareni, L. (2003), A Medical Wearable Device with Wireless Bluetooth-based Data Transmission. Institute of Biomedical Engineering, National Research Council, Padova, Italy.

Guest Editorial Introduction to the Special Section on M-Health (2004): Beyond Seamless Mobility and Global Wireless Health-Care Connectivity, IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE, VOL. 8, NO. 4, DECEMBER 2004

Daniel Halperin, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, William H. Maisel. (2008). Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. IEEE Symposium on Security and Privacy 2008.

T. Scott Saponas, Jonathan Lester, Carl Hartung, Tadayoshi Kohno. (2006). Devices That Tell On You: The Nike+iPod Sport Kit. Department of Computer Science and Engineering University of Washington, Seattle, WA,

Theodore W. Berger, John K. Chapin, Greg A. Gerhardt, Dennis J. McFarland, José C. Principe, Walid V. Soussou, Dawn M. Taylor, Patrick A. Tresco. (2007). International Assessment Of Research And Development In Brain-Computer Interfaces. World Technology Evaluation Center.

L.E. Dunne, B. Smyth, S.P. Ashdown, P. Sengers, J. Kaye. (2005). Configuring the User in Wearable Technology Design. Published in the Proceedings of the 1st Wearable Futures Conference, Newport, Wales, September, 2005