# Global Information Assurance Certification Paper

# Nanotechnology:
# Technological and Security Implications

Joel A. Rivers

27 April 2004

Practical Paper for the SANS GIAC Security Essentials Certification (GSEC)
Version 1.4b

## Table of Contents

**Abstract**

The evolution of nanotechnology has been described as the next "Industrial Revolution" ushering in radical new innovations in science, technology, and lifestyle. It has the potential to impact every aspect of our lives. The National Intelligence Council (NIC) published a report in 2001 entitled *Global Trends 2015*. Utilizing private industry and U.S. Government experts, this report indicated that by 2015, "We anticipate that the world will almost certainly experience quantum leaps in information technology and in other areas of science and technology." (Gershwin, 2001).

This paper will limit its scope to describe some recent and projected innovations in nanotechnology that will have an impact on computer technology and security. This paper will look at seven different areas; The Law and Politics associated with this new technology, its impact on computer chips and memory, encryption standards, user authentication, backups and archiving, and networks.

## Nanotechnology: What is it?

Nanotechnology is a broadly defined term that entails many scientific, engineering, technological, and medical disciplines. The common denominator in all cases is the use of nano-sized devices. The dimensions of these devices can be measured in billionths of a meter, or nanometer. These dimensions are 10,000 times smaller that that of a human hair (Nanotechnology's Homeland, 2003). Because of the size of the devices involved much of the work involved with nanotechnology requires working at the atomic level, changing and manipulating atoms and molecules. Because nanotechnology works at this level it has become a source for much controversy. Most of the controversy relates to nanotechnology's impact on the medical sciences and the environment. The debate has the potential to impact all areas of nanotechnology development. The next section of this paper will explore the law, politics, and public perception surrounding the development of nanotechnology and ultimately how this could impact computer technology and security.

## Law and Politics

Science fiction and early articles published on the subject have done a lot to shape perceptions concerning nanotechnology. In 2000, Bill Joy, co-founder of Sun Microsystems wrote an article describing self-replicating nano-bots that over time destroyed the human race reducing the world to a mass called "gray goo". Also, Michael Crichton wrote a novel entitled, "Prey", which has nanoparticles causing mass hysteria. Most experts today reject this "doomsday" notion but

serious concerns about the development of nanotechnology persist (Weis, Rick, 2004).

Similar to the activist that spoke out against biotechnology (genetically engineered foods); groups are organizing and protesting against the advancement of nanotechnology. Many fear that nanotechnology will develop too rapidly and proper safeguards will not be in place to protect the public. Some would like nanotechnology production stopped so it can be properly studied and from this develop safety regulations and guidelines (Weis, Rick, 2004).

The government and industry realize the importance of public acceptance and are taking steps to change the negative perceptions. Experts are being hired to study why nanotechnology is viewed in such a negative light and hope this will help not only turn public perception, but also help the industry develop responsibly (Weis, Rick, 2004).

Many experts expect the nanotechnology industry to be worth close to one trillion dollars within the next decade. A positive step towards this occurred in December 2003 when President Bush signed a $3.7 billion bill that is intended to spark research and development in nanotechnology. This high profile attention and commitment on the part of the government should help shed some of the negative press (Weis, Rick, 2004).

The outcome of public opinion will drive the commitment of government and industries toward nanotechnology. It will also frame the amount of regulation that will be imposed on this developing area. All of this together will have a direct impact of how rapidly nanotechnology can be applied to computer technology and this will impact the rate at which computer technology and security standards will change.

**Chips / Memory**

The area of computer technology that has seen the most impact from nanotechnology is the arena of chips and memory. The primary reason for this is the immediate impact this will have on consumer electronics.

Moore's Law has been the standard by which chip development has been based. Moore's 1st Law states that chip speed doubles approximately every 18 months while doubling the number of transistors on a given chip every two years. Moore's 2nd Law indicates that the cost of chip manufacturing plants double every three years. Nanotechnology developments will be able to extend Moore's 1st law beyond what was thought possible and virtually eliminate Moore's 2nd Law (Hendrich, Lucas, 2002).

One of the main reasons Moore's 1st Law works is the ability of chip manufactures to make smaller and smaller transistors. Recent advancements in

nanotechnology will be able to extend Moore's Law but the end is in sight based on current manufacturing techniques. Researchers at IBM estimate that after 2021 chipmakers will no longer be able to shrink the size of the transistors that fit on the chips (Kanellos, 2003).

The primary issue has to do with how electrons flow through transistors. In order for a transistor to work effectively they must be able to act as an on/off switch (the familiar "1"s and "0"s of binary computer operations). Experts indicate that when a transistor reaches the 5 nanometer (nm) size an effect called "tunneling" occurs. The space isn't large enough to effectively stop the flow of electrons so the net effect is the switch always being on, or at best unpredictable. With a failure rate around 50 percent, this makes for a very unreliable chip (Kanellos, 2003).

In February 2004, Intel introduced a chip that is 90nm wide. Currently chips are typically from 130nm to 180nm wide (Sheils, 2002). The new Intel chip, which is used in Intel's NOR flash memory device, named Crystal, fits 2 ½ times more transistors onto the chip. This chip is also 2 ½ times faster in read performance and 4 times faster in write performance. While this chip isn't down to the atomic level in size it is considered a major milestone in this development (Keenan, 2004).

The restrictions and limitations mentioned above assume the same manufacturing techniques currently used. Researchers from around the world are working on other methods for reducing the size and cost of chips while increasing their performance. Three such proposed innovations are, Nano Dot (MND) Memory, photonic microchips, and quantum bits.

Nano Dot (MND) Memory is a potential new type of non-volatile memory that is based on "synergy ceramic technologies" currently being developed by the Asahi Glass Co., Ltd. This differs from the current manufacturing technique of using silicon. The MND film on this chip is made of metal nano dots about 2 nm in diameter. Ashahi's researchers claim that this technique offers higher densities, which provides for better charge retention. See Figure 1 (Asahi Glass Co, 2003).

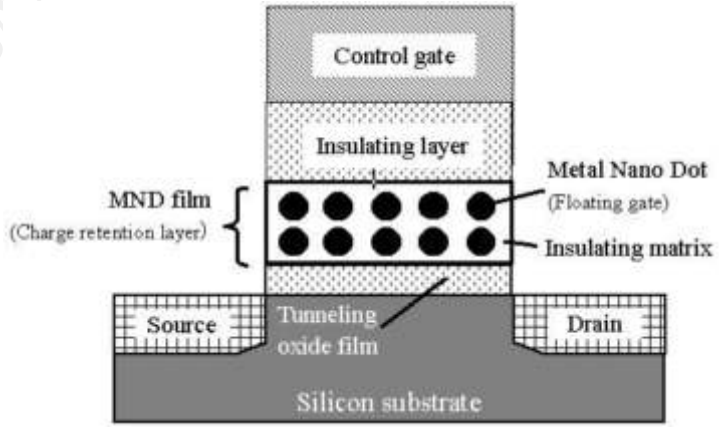

Figure 1

Another technique being developed is nanophotonic microchips. This uses beams of light in place of streams of electrons. Wires are replaced by waveguides. Waveguides, simply put, bend or guide the light along its path. The hope is this technology will lead to the practical application of fiber optic lines to home users (Steele, 2004).

Quantum bit technology is probably the most far reaching of the three discussed here. If quantum bit technology becomes a practical reality the development of a quantum computer will be closer to a reality. The basic idea has to do with the production of quantum bits (qubit). Dr. Yokoyama states, "Unlike classical computers, in a quantum computer, the quantum bit can exist in coherent superposition of 0 and 1 states." While current computing requires switching between two electrical states, quantum bit allows both states to exist at the same time. Because of this a quantum computer would be able to do in days what a traditional computer would take millions of years to do. This is a long-term goal because it is estimated that a quantum computer is expected to take 20 or more years to develop (Japan Nanonet bulletin, 2003).

Regardless of which technology is utilized, the size of computing devices will be drastically reduced in size and price while become more powerful. This has numerous implications for security. Computing will expand even more rapidly beyond the "safe" perimeter of current LANs. We already see remote access to corporate networks moving from laptops to PDA's and cell phones. Nanotechnology will enable these devices and others with more computational power and memory. This opens up obvious concerns not only with securing data but also the physical security associated with these smaller devices.

**Encryption**

Another area that will be impacted by nanotechnology development is in the arena of encryption. Current encryption standards Double DES, Triple DES, and AES are considered secure, with AES being the current government standard providing 128-bit, 192-bit, and 256-bit key sizes (Cole, 2003). Nanotechnology not only provides a way to improve on these encryption standards but also the potential to render current standards ineffective.

Quantum cryptography promises to provide encryption that is practically impossibly to decode. The development of Quantum encryption technology has been in development for over twenty years. This encryption method utilizes the behavior of photons. Photons are encoded in one of four positions, two diagonal, one horizontal, and one vertical. Due to the sensitive nature of photons, anyone attempting to "listen in" or intercept the transmission will not only tip off the intrusion attempt but will also invalidate the code (Mason, 2004).

Another advantage has to do with keys. Current encryption systems rely heavily on keys. Even if a perfect algorithm encrypts the data, if the key is compromised then the data is compromised as well. Quantum encryption keys are transmitted using the method described above and they also can be changed numerous times in transit making them nearly impossible to compromise (Varghese, 2003).

MagiQ Technologies introduced the first commercially available quantum encryption system in November of 2003. Their system, called Navajo, utilized two 48cm boxes between nodes on a fiber optic network. There is a distance limitation of 112km between these devices. The cost for this system ranges from $50,000 to $100,000 (Varghese, 2003).

Taking MagiQ's system one step further, two professors at Northwestern University have discovered a way to encrypt the actual data at speeds of 250 Mbits/second. Their hope is to be able to apply this technique to Internet backbone speeds of 2.5 Gbits/second. The two professors argue that their encryption technique has broader application than MagiQs (Johnson, 2002).

Some experts don't see this type of cryptography as being commercially successful in the short term due to the fact that many of the current encryption standards are considered unbreakable. Also, many security experts would argue that having an unbreakable encryption standard is only one part of the security chain and there are many other weaker links that need to be addressed first (Varghese, 2003). The need for this type of encryption will become more of a necessity if the above-mentioned Quantum computer becomes a reality. Quantum computers have the potential to render current encryption algorithms ineffective. DES is a prime example of how computing power has rendered a once standard encryption method insecure.

**Authentication**

Authentication is a key component in the network security cycle and will be impacted by nanotechnology developments. Nanotechnology will enable authentication to be scaled down and also improve the accuracy associated with authentication. While there are many aspects to authentication, this paper will be discussing the impact of nanotechnology on fingerprint authentication as an example. A combination of small microchips and advancement in fingerprint sensing devices have enabled this form of authentication to be applied to mobile phones, PDAs, and other small mobile devices.

A single touch and a rapid swipe sensing device are being introduced that will make this application possible. The pixels that make up the sensor are about 45um with a resolution of around 500 dots per inch (dpi). The sensor pad material is composed of material that make up the sensor pads are composed of microscopic hard metal electrodes with a coating that resists wear allowing for years of use (McArthur, 2003).

The basic technology relies on analyzing the ridges and valleys that compose a fingerprint. How the ridges and valleys interact with the sensor determine a pattern for each fingerprint. Figure 2 (McArthur, 2003) illustrates how this works.

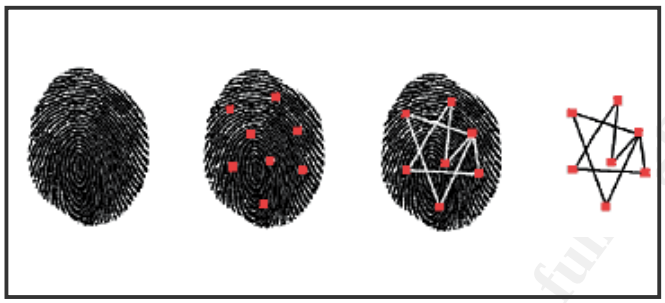

Figure 2

The software creates a template for each fingerprint and then uses this to create a match. Using this system false rejection rates (good fingerprints seen as bad) is no more than 1 percent and false acceptance rates (bad fingerprints seen as good) is .01 percent (McArthur, 2003).

The big difference between single touch and rapid swipe is size and speed. Rapid swipe enables quick identification by capturing 2000 frames per second. The size for a rapid swipe sensor is approximately 3.6 x 13.3mm while the single touch sensors usually measure 15 x 15mm (McArthur, 2003).

This technology has the potential to provide for more secure mobile computing. For instance, mobile phone users will be able to authenticate to their phones via fingerprint identification. PIN numbers will become obsolete. This technology can also be configured to automatically erase important data on the phone if repeated attempts are made to break into the phone (McArthur, 2003).

**Backups / Archiving**

Nanotechnology will reduce the size of computer microchips and will also change how data is backed up and archived. Nanotechnology will enable large amounts of data to be stored on smaller media at increasingly faster speeds. This is important because there is every indication that the need for more storage on a global basis will increase dramatically. For example, experts at Oracle Corporation predict data storage will reach a critical state in the near future. Also, many research organizations, as well as universities, are seeing an increase in the demand for more storage. It is predicted that current storage techniques will not be able to keep up with the demand. Backups are also a critical component to not only recovering from a disaster but to the recovery of

data that might be useful in an investigation. This will become even more important as the above-mentioned demands become reality. Current formats can only transfer data at a rate of 320 megabits per second and use power very inefficiently. The current methods of data storage are also reaching their physical limits because of the material used in the production process (Newton, 2004).

One such innovation has been developed by engineers at Princeton and Hewlett-Packard. Unlike current CDs or digital tapes the device they have developed contains no moving parts and would plug directly into a circuit. This device uses PEDOT, which is a clear polymer material that is highly conductive, and is currently used as a coating on photographic film as well as in video display development. This technology would be able to store more that a gigabyte of information in a one cubic centimeter area. While the device is "write-once", it can be produced inexpensively, which will make it a practical solution for archiving data (Schultz, 2003).

Another innovation, being developed by Colossal Storage Corporation, is in the area of atomic holographic optical storage. Current two dimension storage devices range from 60 gigabits to 300 gigabits per square inch. The 3D optical drive proposed by Colossal would have a capacity up to 40,000 Terabits per cubic centimeter and a data transfer rate over 100 Terabits per second. The technique is a complex process that uses laser diodes to affect ferroelectric molecules. The specifics are beyond the scope of this paper. This method of storage can be maintained for well over 100 years (Thomas, 2003).

**Networks**

Networks, WANs, LANS, and MANS also will benefit from advancements in nanotechnologies. Most of today's networks rely on the transmission of data over wire via electrical signals. As nanotechnology improves the speed and capacity of computers, current network standards will need to be improved.

Similar to the way the Internet was originally developed as a communication tool for research, Oak Ridge National Laboratory has been given a grant to develop a high-speed network that will operate 200,000 to 800,000 faster than the current dial-up speed of 56K. The purpose of this network will be to link research facilities across the country to facilitate the advancement of their studies (Associated Press, 2003). While this network is very specific in scope the technologies used in its development have the potential to be used in the public sector (Associated Press, 2003).

Another innovation that has the potential to improve networks is through the use of nanoptical switches. These devices transmit data using lasers that are only 8 nanometers wide. These switches will enable data to be transferred in nanoseconds and will greatly increase the speed of networks (Egan, 2003).

Currently, wireless network technology is one of the fastest growing segments in the world of information technologies. Another solution for addressing wireless networks that utilizes nanotechnology advancements is "free-space optics" (FSO). While FSO has been in existence for some time the latest enhancement utilizes quantum lasers to transmit data at high speeds. There are advantages to this method. The lasers are mobile, easy to set up, and rather inexpensive when compared to current landlines. The wavelengths on these lasers are only 8-12 microns making them highly resistant to environmental changes like rain and fog (Thompson, 2003).

While nothing is perfect, FSO is more secure than standard wireless technologies for the following reasons. Since FSO utilizes laser beams to transmit data, the wavelengths on which the data travels are extremely focused and not easily intercepted. Any attempts to "tap" into this transmission are more easily detected than with tradition wireless technology because the detecting device must be intentionally placed in the beam. This makes tapping very difficult to achieve. There also needs to be specific knowledge of a FSO network before data stream is attempted. These networks are also more difficult to randomly detect since the signal is so narrowly focused and not broadcast. To further enhance the security, the data transmission can also be encrypted (Steege, 2002).

**Conclusion**

As nanotechnology changes the face of computing and brings innovation that will improve so many aspects of the IT industry, it will also bring about many challenges. The world's economy is becoming more and more networked and nanotechnology will help facilitate the flow of this information. However, like dynamite more than a century ago, there will be bad that comes with the good. Hackers and other "adversaries" will also utilize this technology because of its low cost and high availability. It will be more important than ever that that security professional are prepared to meet this challenge. In order to meet these challenges rethinking current paradigms of networks and network security will be necessary.

Current system development is typically done in a way that maximizes the developer's bottom line. This may or may not be good for the overall security of the Internet. Too many systems are unable to communicate with others or are restricted from doing so. Also, most networks are fire walled and isolated from the rest of the Internet. Network security becomes a constant battle between network administrators and hackers.

While this battle continues, one idea is to rethink network security in terms of biology. Currently, the Internet can be seen as a connection of multiple intranets across various media links. While these separate networks share data

necessary for business transactions there is little sharing of critical data necessary to prevent the spread of infections. A growing number of security experts believe that more openness is necessary in order to meet the security needs of the future. One idea to accomplish this has been coined, “Biological Network Security” (BNS). The basic idea is to think of the Internet and all the devices that make it up as one entity, or body. Similar to human body’s defenses that rely on quick detection and eradication of harmful germs / viruses, BNS requires quick detection and removal of infection by developing an open standard that allowing infected devices on the Internet to be detected and cleaned immediately. BNS proposes an Internet wide central monitoring and detection system to facilitate this. The basics for BNS are already in place. Current IDS systems model this concept but on a smaller scale so the idea is to expand this to the entire Internet (Gillespie, 2002).

This is just one example that illustrates “out of the box” thinking that will be necessary and computer and security professional address the changes that are, and will result from, nanotechnology innovation in the area of computer technology and security.

## Bibliography


Asahi Glass Co., LTD, "Successful Development of New Next Generation Non-Volatile Memory." December 24, 2003. URL: http://www.agc.co.jp/english/news/1224.html (15 March 2004).

Associated Press, "Oak Ridge Grant Gives Lab Green Light For a Really Fast Connection." Smalltimes.com, November 25, 2003. URL: http://www.smalltimes.com/print_doc.cfm?doc_id=7004 (15 March 2004).

Cole, Eric, Fossen, Jason, Northcut, and Stephen, Pomeranz, Hal, "SANS Security Essentials with CISSP CBK", February, 2003. Version 2.1 Book 2: p. 950-953.

Gershwin, Lawrence K., "Cyber Threat Trends and US Network Security." National Intelligence Council, June 21, 2001. URL: http://www.cia.gov/nic/congress_cyberthreat.html (15 March 2004).

Gillespie, Brandon, "Biological Network Security." Securityfocus.com, January 25, 2002. URL: http://www.securityfocus.com/guest/10094 (15 March 2004).

Hendrich, Lucas, "Beating Moore's 2nd Law: Advances in Nanoengineering and New Approaches to Computing at the 2002 Annual Meeting of the AAAS." KurzweilAI.net, February 21, 2002. URL: http://www.kurzweilai.net/articles/art0407.html?printable=1 (14 March 2004).

Japan Nanonet bulletin, "Fusion Will give Birth to a New Industry – Focusing on the Three Fields of Nanotechnology." Nanonet, November 27, 2003. URL: http://www.nanonet.go.jp/english/mailmag/2003/006a.html (16 March 2004).

Johnson, Colin R., "Quantum Encryption Secures High-speed Data Stream." EEtimes.com, November 8, 2002. URL: http://www.eetimes.com/article/showArticle.jhtml?articleId=16506177 (17 March 2004).

Kanellos, Michael, "Intel Scientists Find Wall for Moore's Law." CNET News.com, December 1, 2003. URL: http://news.com.com/2100-7337-5112061.html (15 March 2004).

Keenan, Robert, "Intel Details First 90-nm Flash Device." Commsdesign.com, February 19, 2004. URL:

http://www.commsdesign.com/showArticle.jhtml?article=17700219 (15 March 2004).

Mason, Jack, “Quantum Cryptography Companies Tap into Nanoscale’s Quirky Core.” Small Times.com, February 19, 2004. URL: http://www.smalltimes.com/print_doc.cfm?doc_id=7448 (16 March 2004).

McArthur, Douglas, “Fingerprint Identification and Authentication.” Sensormag.com, January 2003. URL: http://www.sensormag.com/articles/0102/14/pf_main.shtml (16 March 2004).

“Nanotechnology’s Homeland Security Potential to be Explored.” SpaceDaily.com, December 11, 2003. URL: http://www.spacedaily.com/news/nanotech-03zzr.html (15 March 2004).

Newton, Jon, “Every File You Ever Owned On 1 Disc.” P2Pnet.net, February 25, 2004. URL: http://p2pnet.net/story/842 (14 April 2004).

Egan, Dennis, M. and Petersen, John, L., “Small Security: Nanotechnology and Future Defense.” Defense Horizons, March 2003. URL: http://www.ndu.edu/inss/DefHor/DH8/DH08.htm (15 March 2004).

Schultz, Steven, “New Memory Device Could Offer Smaller, Simpler Way to Archive Data.” www.princeton.edu, November 12, 2003. URL: http://princeton.edu/pr/news/03/q4/1112-forrest.htm (15 March 2004).

Sheils, Maggie, “Thinner Chips with Everything.” BBC News, November 6, 2002. URL: http://news.bbc.co.uk/2/hi/technology/2404599.stm (15 March 2004).

Steege, Mark, “Free-Space Optics: A Viable, Secure Last-Mile Solution?” FreeSpaceOptic.com, January 23, 2002. URL: http://www.freespaceoptic.com/WhitePapers/FSOSecurity.doc (15 April 2004).

Steele, Bill, “Cornell-developed Tools to Guide and Switch Light Could Lead to Photonic Microchips and Practical Home Fiber-optic Lines.” Cornell News, February 15, 2004. URL: http://www.news,cornell.edu/releases/Feb04/AAAS.Lipson.ws.html (15 March 2004).

Thomas, Michael E., “Atomic Holographic Optical Storage Nanotechnology.” Colossal Storage.net, September 15, 2003. URL: http://www.colossalstorage.net/3d_volume.pdf (14 April 2004).

Thompson, Valerie, “U.S., Swiss Quantum Connection Has Potential for High Payoff.” Smalltimes.com, February 27, 2003. URL: http://www.smalltimes.com/print_doc.cfm?doc_id=5576 (16 March 2004).

Varghese, Sam, “Encryption Promises ‘Unbreakable’ Codes.” Theage.com, November 28, 2003. URL: http://www.theage.com.au/articles/2003/11/28/1069825960663.html?from=storyrhs (17 March 2004).

Weis, Rick, “For Science, Nanotech Poses Big Unknowns.” Washington Post.com, February 1, 2004; Page A01. URL: www.washingtonpost.com/ac2/wp-dyn/A1487-2004Jan31?language=printer (3 March 2004).

Yokoyama, Naoki, “Fujitsu Research Labs Help Shape the Nanotech Revolution.” Fujitsu’s Interaction magazine, October 10, 2003. URL: www.fujitsu.com/au/interaction/archives/2003/2003 10-02.print.html (17 March 2004).