New Age Device Security

By Larry Miller (GSEC Practical Resubmission)

The Internet and other networks (cellular, satellite, private wired, wireless) will continue to be increasingly pervasive in society. What were once only protocol definitions is now becoming a reality. Sun's JINI, and Microsoft's Millennium (not to be confused with Microsoft Windows ME) provide protocol definitions, API's, and user communities for the advancement of networking a wide range of devices including microphones, home security systems, refrigerators, and even toaster ovens. New age devices expand on traditional devices in that they are now becoming networked with existing IT systems. Numerous economical and technological benefits arise from networking new age devices. However, these device networks also pose an emerging security threat. Traditional PC's have been the target of viral and worm based attacks for years. Just this year cell phones and Windows CE have been proven to be vulnerable to attack, much like traditional systems. Device networking is growing at an extraordinary rate across multiple verticals and segments including government, military, health care, and home entertainment. Examples include EZPass, Microsoft's Xbox, home security systems, and industrial control systems. Networked devices can be the focus of attack, as well as provide the platform for new attack scenarios on existing systems. The following criteria are critical to securing networked devices:

- Responsibility awareness
- Security policy and procedures
- Information sharing and documentation

Networked devices pose new risks during a time of increased terrorism. The government, military, private industry, and security training facilities must work together towards a common goal of protecting the world's people and assets from internal and external threats.

Device Networking

Device networking is the communication between devices and systems. This is an abstract term, with unlimited implementation possibilities. A web search on common search engines for "device networking" will result in numerous companies marketing this technology. Functional areas include wireless, conventional, and embedded systems. Vertical segments are wide ranging and include government, military, manufacturing, health care, transportation, energy, communications, and entertainment.

Both Microsoft (Millennium, Windows CE, Windows XP Embedded) and Sun (Jini) have invested heavily in research and development of device independent networking. Although the terminology used by these companies may be different, the goal is the same. These companies, along with many others, are providing the protocols and development platforms required to network non-traditional devices.

The benefits of networking devices are numerous. These benefits include remote access and control, a free roaming workforce, real time diagnostic feedback, real time inventory, and automation of existing industries. For example, imagine networking the thermometers in commercial size freezers. Not only would energy distribution be more efficient (and less costly) but an alarm would trigger if the temperature became too warm which would allow management to move expensive meat to another freezer until the problem was resolved. Another example is the integration of scanners and readers with existing networks to track shipped goods. As packages pass from location to location, on the way to the final destination, they are scanned. This allows management to have a real time view into the timeliness of packages, and allows the consumer to have a real time view into where a package may be. Overtime, packages will be moved at a more efficient rate, assuming management makes the correct decisions based on the data provided.

Device networking will decrease costs for products and services across all sectors and verticals. The long-term effects will result in decreased consumer prices, increased productivity, and increased innovation. Although countless benefits arise from the networking of devices, the surface area for security threats also increases. We have seen a dramatic increase in the amount of viruses and worms in recent years. Network devices, including cellular phones, are also prone to these types of attacks. It is a myth to believe that only personal computers and corporate servers are susceptible to viruses and worms.

Recently, the worlds first (known) cellular phone worm was released (Author Unknown 2004). Although this worm, named “Cabir”, was harmless, it proves that networked devices, even cell phones, can be compromised. This particular worm is a telling sign of what is to come. We should assume that any device that can be accessed across a network, is susceptible to attack and exploitation.

Microsoft develops and markets the Windows CE platform. Most Windows operating systems are designed to run on PC based platforms. Unlike traditional Windows platforms, the Windows CE platform is intended to run on networked devices and embedded systems (such as a handheld computer) rather then the traditional desktop PC or server. In July 2004 the world’s first known virus targeted at Windows CE was sent to anti-virus vendors (TechWeb News 2004). Like the “Cabir” worm, described above, this virus does not damage the device, but was intended to show that the Windows CE platform is vulnerable to attack.

Apple’s iPod (Apple 2004), a mobile handheld music device, has been a huge success. It has recently sold its 100 millionth song and is just now beginning to gain global momentum. The iPod can store and playback music on numerous input and output devices including the PC, home entertainment systems, and the car radio. However, it can also be used for illicit activities. Recently, the Ministry of Defense of the U.K. began banning the iPod from sensitive areas because it has the capability to siphon large amounts of data, through USB connections. (Associated New Media 2004). After loading the out-of-the box software, a PC or server can write data to an iPod. With Macintosh systems, the problem is more severe because they automatically discover the iPod without installing any software. If an internal employee or trained janitor gains physical access to a PC, an iPod could be used to transmit large amounts of data directly from the PC, or through a network share. Although the data may be encrypted, it could be broken at a later time, in a location better suited for the task.

The home is our most sacred establishment and our safety zone. It is also one of the leading growth areas for device networking. The report located at http://deviceforge.com/news/NS8970665649.html states “The continued need for broadband sharing and a growing interest in entertainment networking will drive the total value of equipment with a home networking connection of some type from $8.3 billion in 2004 to $17.1 billion by 2008.” (In-Stat/MDR 2004)

Mobile device networking is also a leading growth area. The information provided at http://www.tiqit.com/investors.shtml reports “Current market size estimates from IDC place the mobile & wireless market for handheld devices at $7.8B and notebooks at $47B in 2003. In 2004, the market size is expected to grow $8.7B and $52B, respectively.” (Tiqit 2004)

Devices are becoming networked in all sectors and industries. Whether these devices are hard wired or wireless, makes little difference. If a physical or logical connection exists to a networked device, the possibility for exploitation and attack exists. From the battlefields in Iraq and Afghanistan (iRobot 2004), to the hospitals, energy companies, and schools in the United States, networked devices are all around us. Table 1, below, provides some examples of networked devices across different sectors.

Table 1 Examples of Networked Devices, by Sector

Sector	Examples of Networked Devices
Military	Robots (iRobot 2004), Unmanned airplanes (AeroVironment 2004)
Energy	Automatic Meter Readers, Virtual Power Connect and Disconnect (Echelon 2004)
Manufacturing	Switches, Photoelectric Sensors, Valves, Thermometers (GE Fanuc 2004)
Healthcare	Patient Monitoring Systems, Prescription Management Systems, Electronic Registration Systems (Extreme Networks 2004)
Communications	Cell phones, PDA’s
Transportation	EZPass, Airport Check-in Booths
Security	Retina Scanners (Iridian Technologies 2004), Finger Print Scanners (Bios Crypt 2004)
Entertainment	IPod (Apple 2004)

The Security Risks Posed by Networked Devices

Security risks associated by networked devices can be broken down into the following two categories:

1) Risks associated with using networked devices to compromise traditional systems.
2) Risks associated with compromising networked devices and the systems they control.

According to a recent report by Gartner (The Mac Observer 2004) network devices such as USB based thumb drives, smart media cards, memory sticks, compact flash, keychain drives and portable MP3 players are a security risk to corporations and should either be banned from the workplace or strict security policy must be implemented and maintained. Gartner views these types of devices as being insecure because they bypass traditional security measures. Traditional security measures include firewalls, intrusion detection systems, intrusion prevention systems, honeypots, router and switch access lists, and proxy servers. Gartner argues that privately owned, and uncontrollable networked devices circumvent these traditional security measures and therefore pose an immediate and overwhelming threat to corporate security.

The technical explanation is based on the fact that these devices have network interfaces, which allow them to interact with PC's, servers, and perhaps networking infrastructure devices without being checked against traditional security mechanisms. PC's, servers, and networking devices are now coming standard with USB, FireWire, Bluetooth, and 802.x wireless networking interfaces. It is these components installed out-of-the box in today's computers that are not secured by traditional security devices. Security products should focus on the intersection between traditional systems and networked devices to ensure that all interfaces are secure; not only traditional network interfaces (Ethernet, FDDI).

Risks associated with compromising networked devices are virtually uncountable. Because devices are becoming networked across all sectors and industries, the possibility for increased risk is great. The root of the problem is that these devices control electronics and machinery which typically required physical access. Because these devices are now becoming networked, the reach of an attacker is far greater, and does not require physical access.

Example Threat Scenarios

As you can see, from Table 1 above, networked devices can be found in many forms, and across many sectors. Device networking not only provides new mediums for existing threats, but also increases the surface area for new threats.

The devices are not only the focus of attack, but can also be used to create new attacks, and have the possibility to impact more then just the PC.

An example of an attack in which networked devices can be used for new exploits is a hidden camera, built into eyeglasses, which could communicate via a wide area wireless network to a central server. The server could process this video input via an artificial intelligence program to reveal data, such as the layout of a building or the contents of confidential data. This layout could be used in a 3D modeling program to allow a computer user to "walk" through the environment, from a remote location. A potential use from this type of espionage is real time operational data for an in-progress terrorist attack. Other possible uses include a janitor stealing confidential data from a data center, or a bank robber investigating a bank for planning purposes.

An example of an attack designed for devices is an intelligent worm that secretly records cell phone conversations around the globe, and feeds the sound input to a remote location for further analysis. This recorded communication could be used for numerous illicit activities and could cause a major breakdown in the confidentiality, integrity, and availability of both systems and people.

The ATM (automated teller machine) is a commonly used networked device. Imagine a worm specifically designed to compromise these devices. Automated teller machines are inherently connected to the banking systems around the globe. This type of worm could be used to deduct small amounts of money from each transaction, and deposit that money in multiple foreign accounts.

Securing Networked Devices Through Responsibility and Security Policy

Networked devices exist in many industries. Traditionally IT security experts aimed to secure computer networks. Separate personnel were responsible for the physical security of locations, to prevent theft, espionage, tampering, and to provide safety to employees. It is no longer sufficient to separate the security of the computer network from the security of a physical location. The network is becoming increasingly pervasive and will continue to connect non-traditional devices. The lines between physical security and network security become blurred. Security managers from different parts of the organization must work together to ensure that integration between their controlled domains, and the network that connects them, are secure.

The government is in a unique position in regards to securing our nation and its people, and its assets. It is the only organization that has both the resources and governing authority to enforce a national security policy. Although it is imperative that the government broadens and enforces our national security policy, it is the responsibility of plant managers, CTO's, school principals, and other leaders, to enact security policies within the domains they control.

Although the developer, seller, and user of a networked device is responsible for the security threats posed by that device, they do not have the ultimate responsibility. For example, the iPod can be used to capture wireless data. Perhaps a government employee inadvertently or purposely carries his iPod into a confidential area. The responsibility to protect the data falls on the government and owner of the protected asset, not the manufacturer of the iPod.

The first step in securing our nation, and our world, is to enact laws that clearly define security responsibility, across all sectors and industries; and relate these laws to our national security policy.

Security policy defines the high level policies that an organization will follow in order to protect the confidentiality, integrity, and availability of both systems and people. It does not define the implementation. Based on policy, procedures should be created to implement the said policy. Policy should be broad and should include the protection of people and data. It is also important to include disaster recovery planning and business continuity planning to ensure availability of assets in the event of an emergency.

When developing security policy, three crucial aspects must be considered. They are confidentiality, integrity, and availability. Leaders should drive security policy through analyzing the potential risk to assets based on these three principles. Assets include data, physical resources, and people. Confidentiality is the idea that assets should only be available to those that have the proper authority. Integrity refers to securing assets from corruption. Availability is keeping assets available so that they can be accessed when needed. These aspects sometimes interrelate. All three aspects should be taken into consideration when developing policy. Policy that only considers confidentiality and integrity, and that does not consider availability, for example, should not be written.

Confidentiality protects data and assets from those that should not have access. Examples of confidentiality in every day life are your ATM PIN, and your Internet Service provider username and password. These examples are very basic and do not provide a high level of confidentiality. All one needs to do is steal your PIN or ISP password, and they can gain access as if they were you. Biometric protection, on the other hand, provides a much greater level of confidentiality. To provide a maximum amount of confidentiality, a combination of traditional and biometric protection should be applied.

Integrity protects data and assets from corruption. Data can become completely unusable if corruption occurs. Therefore it is critical to address this when developing policy. For example, multiple layers of defense should be implemented to secure a highly sensitive and private database. A web application firewall can be configured to ensure that improper SQL is not sent to the connected database. An application firewall, in addition to a secure database configuration (strong authentication, encryption, protected schema), can help to ensure that data is protected against corruption.

Availability of data is also a critical aspect that should be considered when developing security policy. As the term suggests, this refers to whether or not data is available for access when required. Multiple layers of protection should be implemented to protect the availability of data. Examples would be a redundant network, system, and application design to ensure that one failed component does not affect the availability of the entire system. Data backup and restoration and disaster recovery are also key aspects that should be addressed when developing policy.

When developing security policy it is important to practice a defense-in-depth strategy. Defense-in-depth is the layering of security mechanisms with the intended goal of greatly minimizing surface area, and increasing the chances to thwart attack. It is not sufficient to provide only one form of security to protect a certain asset. By layering defense, a would be attacker would have to penetrate multiple defense mechanisms to impact the confidentiality, integrity, or availability of assets.

Policy enforcement is also a key element, which should be considered when developing a security policy. If a policy cannot be enforced, or if the effort to enforce the policy requires unattainable resources, then the policy should not be written. Depending on how critical the protected asset is, it may be required to make changes in order to enforce a policy.

Balance is also a key aspect of policy writing. When developing policy it is important to balance intended security goals with continued functionality. If security policy is not strong enough, then assets are vulnerable to attack and compromise. If policy to too strong, the asset may be protected, but could become impossible to function as required. An example of a policy which is too strong would be to force users to have passwords that are longer then 30 characters, and that must change every day. This would force users to keep passwords written in desk drawers, or notepads, which would defeat the purpose of having the password.

Based on the policy, procedures should be written, to enact and enforce the policy. It is important to continually maintain both policy and procedures. Both policy and procedures should be reviewed on a routine basis. The time period should be based on how critical the protected assets are. Policies and procedures should also be reviewed whenever significant changes occur within an organization and its assets. For example, if a fingerprint scanner will be replaced with a retina scanner, it would be imperative to revisit the policy and procedures to ensure compliance.

Other important aspects for developing security policy are

- Research several different sources of information to educate yourself on policy to be sure your understanding is broad.
- Read sample policies.
- Share the policy writing with others to ensure that all aspects of the organization are taken into consideration.
- Document all policies and procedures. If a policy or procedure is not documented consider it non-existent.

Security policy and responsibility are the two most important factors for protecting assets and people. Without policy, an organization does not have any guidelines to follow and security measures will be haphazard at best, and will most likely become out dated.

Terrorism

On September 11, 2001, America was attacked. Prior to this day, war was declared on our way of life. On that infamous day in early September, over 3000 people were murdered, mostly Americans. Some perished in the sky, while others jumped to there death from the twin towers. From a spiritual perspective we can only hope and pray that those murdered are in a better place, and that they will meet there family and friends once again.

We must accept the fact that if our enemy can, they will attack again. Business leaders, security professionals, military leaders, and government officials must be vigilant and proactive against these threats to help ensure that our economy can withstand future attacks, and to save lives if we can. Networked devices should be continually analyzed to determine if they can provide additional security against attack, and more importantly, if terrorists can access networked devices to cause death and destruction.

Recommendations for Government, Military, and Private Industry Sectors

Government

- Continue to develop a national security policy with the understanding that we will most likely be attacked again. Policy should focus on the idea that the network is the world. Networked devices should be the focus of threat analysis, as well as a way of defending against attack.
- Ensure that network devices meet security policy before release into the marketplace.
- Enact laws that force private industry to develop, maintain, and enforce security policy.

- Develop an agency within the government with the sole purpose of ensuring security policy. Much like a tax auditor, security auditors would enforce security policy through vigorous examination.
- Develop an agency within the government to support intelligence, military, and congress in emerging technologies, including device networking. This agency would act as a repository and research facility to ensure that all parts of our government and military understand current and emerging technologies.
- Research networked devices to provide a way to authenticate Americans within our homeland. An example of this would be an embedded chip. This chip would act as a unique identifier. Perhaps the signal would be based on your DNA and other biometric signals to ensure authenticity and integrity of the signal. Networked biometric posts would be installed throughout the nation. If a person came within the perimeter of the post, an alarm would sound if an identification chip were not found. These posts would be installed heavily along our land and sea borders. To get a chip installed a thorough background check would be required.
- Research networked devices to learn if we can protect ourselves against biological, chemical, or nuclear attacks. Perhaps we can install a network of devices throughout the country that would act as a sensory grid and one day a defense mechanism against these types of deadly attacks.
- Enact laws which call for zero tolerance for any physical connection between devices that can cause harm or catastrophe and any public network (such as Internet or POTS). Assume that if a physical connection exists it can be compromised no matter how many software based security mechanisms are in place.

Military

- Research heavily into understanding and implementing networked devices, including the continued use of robots, to help save our troops and innocent civilians.
- Develop an army of network devices with remote control capabilities for espionage and remote attack. These armies, much like traditional armies, would consist of air, land, and water units.
- Develop and maintain a global security policy.
- Ensure no physical connections between public networks and military private networks. This includes the Internet, POTS, and wireless networks.

Private Industry

- Enact business continuity plans and disaster recovery plans to ensure the future of our economy in the event of terrorist attacks or other catastrophes.
- Research networked devices to learn if they can help drive down costs or increase productivity of products and services.
- Enact security policy and procedures to help protect the confidentiality, integrity, and availability of your assets, especially your intellectual property and your people.

<u>SANS and other security training professionals</u>

- Develop a generalized training track focusing on networked devices focusing on securing connection points between networked devices and existing systems. The general idea to convey to students is that networked devices can easily circumvent traditional security systems (such as firewalls and IDS's).
- Develop training tracks that are specific to securing networked devices in specific industries and sectors. For example, a track titled "Biometric Device Networking" would educate business and technical leaders on the advantages and security issues with retina and fingerprint scanning technologies.

Conclusion

The networking of devices is growing at extraordinary rates. Like traditional systems, these devices are also susceptible to attack. This year the first cell phone and Windows CE viruses were discovered. Networked devices are not only the focus of attack, but they can be used for illicit activities such as espionage and terrorism. Risks associated with networked devices can be broken down into two categories. The first category is using networked devices as a platform to attack existing systems. The second category is the risk associated with compromising networked devices and the systems and assets they control. To secure our nation during a time of terrorism and increased networked device connectivity, our nation must work towards asset responsibility and security policy. When developing policy and procedures threat analysis to assets, including people, should be based on three key aspects; confidentiality, integrity, and availability. It is also very important to provide multiple layers of defense, making it increasingly difficult for the would be attacker. We can never forget what happened to our people on September 11, 2001. We must learn from that tragic day, and work proactively and aggressively to ensure the future of our people and our economy. Government, military, and private industry leaders should research networked devices to learn about possible cost and productivity benefits, and to understand how these devices can be used to protect our nation and its people.

August 10, 2004

List of References

AeroVironment. *Unmanned Aerial Vehicles.* AeroVironment July 19, 2004 <http://www.aerovironment.com/area-aircraft/unmanned.html>

Apple. *Home Page*. Apple. July 18, 2004. <www.apple.com>

Associated New Media. *Ipod's are 'Risk to National Security'*. This is London. July 14, 2004 <http://www.thisislondon.co.uk/news/articles/11940768?source=Evening%20Standard>

Author Unknown. *Phone Virus Lurking*. EBCVG. June 29, 2004 <http://www.ebcvg.com/news.php?id=2837>

Bios Crypt. *Home Page*. Bios Crypt. July 6, 2004. <http://www.bioscrypt.com/>

Echelon. *Networked Energy Services*. Echelon. July 20, 2004. <http://www.echelon.com/solutions/utility/default.htm>

Extreme Networks. *Wireless LAN Solutions for Healthcare Providers*. Extreme Networks. July 20, 2004. <http://www.extremenetworks.com/LIBRARIES/whitepapers/technology/WirelessHealth_WP.asp>

GE Fanuc. *Sensor Device Networks*. General Electric. July 12, 2004. <http://www.geindustrial.com/cwc/products?pnlid=2&id=comnet95>

In-Stat/MDR. *Report: Home Networking market to reach $17.1 Billion in 2008.* Deviceforge.com. May 10, 2004 <http://deviceforge.com/news/NS8970665649.html>

Iridian Technologies. *Home Page*. Iridian Technologies. July 10, 2004. <http://www.iridiantech.com>

iRobot. *iRobot Unveils Details of Robot Deployments in Iraq and Afghanistan.* IRobot. June 2, 2004 <http://www.irobot.com/news/press_release_detail.cfm?id=22)>

The Mac Observer. *TMO Reports - Gartner: iPod, Portable Devices a Corporate Security Risk*. The Mac Observer. July 7, 2004.
<http://www.macobserver.com/article/2004/07/07.18.shtml>

TechWeb News. *First Windows CE Virus Emerges*. Information Week. July 19, 2004
<http://www.informationweek.com/story/showArticle.jhtml?articleID=23902136&tid=5978>

Tiqit. *Mobile Wireless Market Opportunity*. Tiqit, Inc. July 19, 2004.
<http://www.tiqit.com/investors.shtml>