Global Information Assurance Certification Paper

Virgil L. Hovar

"Personal Area Networks How personal are they?"

SANS Security Essentials
GSEC Practical Assignment
Version 1.2e
Current as of December, 2000 (amended May 22, 2001)

Introduction:

On the surface, the concept of a Personal Area Network (PAN) seems pretty benign. What could be so wrong with being able to connect to my printer without a cable or beam my email to my PDA without having to park it in the docking station? As we consider the developments in connectivity options and the proliferation of devices that may be able to connect to such a network we suddenly realize that our PAN may not be so personal.

History:

One of the first PAN concepts, however, was very much personal. Even to the point that it used the wearer's own body to generate enough electrical conductivity to make a data exchange during a simple handshake. [1]In 1996 T.G. Zimmerman from the IBM Almaden Research Center published a paper and demonstrated a prototype that detailed such a network. Even at that early stage it was well understood that "Clearly, privacy is a big issue". At the same time the great potential that "autonomous yet interconnected devices may transform the notion of ubiquitous computing to the concept of ubiquitous I/O" was also realized. Although there have been few years pass between then and now this concept of "ubiquitous I/O" seems to be coming closer to a reality.

In March of 1999 the IEEE 802.15 Working Group was formed to develop Personal Area Network standards for short distance wireless networks. Since then several Task Groups have been formed to look at the various aspects of the Wireless PAN (WPAN™). [2]The IEEE 802.15 Publicity Committee for WPANs™ provides the following definition to help position PAN with the other types of networks we might be familiar with:

> WAN (Wide Area Network) - interconnect facilities in different parts of a country or of the world
>
> MAN (Metropolitan Area Network) - shall be capable of operating over an area up to 50 Km in diameter
>
> LAN (Local Area Network) - shall be capable of supporting segments at least 100 meters in length. If composed of segments connected by physical layer inter-networking devices, shall be capable of operating over a physical medium that is at least 2 Km in length.
>
> **PAN (Personal Area Network) - shall be capable of supporting segments at least 10 meters in length.**

In today's offices and homes we are very familiar with the concept of LANs, both wired and wireless. These ever present LANs provide us access to the global reaching Internet and corporate Intranets that we all use. Much has been written and continues to be written about these points of access and the need for secure connections and appropriate authentication and authorization for their use. Many security products are currently in the market place and the environment is well understood. Not so with the PAN. As standards are yet being developed and access technologies debated much is yet to be learned about the security issues involved with these new points of access to the global network.

In my own "bubble":

A person's Personal Operating Space (POS) is the space that typically extends up to 10 meters in all directions around a person and envelops the person. This POS "bubble" is present whether stationary or in motion. As you go throughout your daily activities there are many opportunities for information to be exchanged between you and others or between your POS "bubble" and currently existing applications or devices. The concept of a PAN targets connectivity to this POS "bubble" and the various points of contact one may encounter. On the inside of this "bubble" may be an array of devices including phones, PDAs, pagers, watches, headphones. All poised ready to make an invisible "handshake" with an awaiting device either standalone like a printer or connected to a much larger network with access to services and data.

Imagine if you would the ability for your automobile to sense that you were approaching and automatically adjust the seat and stereo setting to your likings. Or as you enter your office and approach your desk your email is automatically downloaded to your PDA. Practical uses are only limited by your own imagination once the technologies are in place to make and break these wireless connections automatically as you move in and out of these point of contact. As Albert Proust states: [3]"the full picture includes a whole new level of automation where devices and appliances are programmed to communicate important information to each other, with or without human intervention." It is the development of these wireless connections that are making the PAN closer to reality.

Connection Options:

While it is obvious from the press and latest technical news that [7]"Much of the hopes for personal area networks have been pinned on Bluetooth" it is not the only technology being considered for PAN connectivity. Many devices currently have implemented line-of-sight infrared that is backed by the Infrared Data Association (IrDA). According to IrDA, there are more than 300 million IR-enabled products to date with 180 million products shipped last year. Additionally, m-commerce standards are being promoted that will enable payments from these various devices at many retail outlets. Infrared has been around for several years and it is not expected to disappear anytime soon.

Another wireless LAN technology is 802.11b. While this is not in direct competition for the PAN environment there will be PDA products on the market this year using the 802.11b Wi-Fi standards and more products released in the next year.

In spite of the decision by [4]Microsoft not to support Bluetooth in it's initial version of Windows XP it is clear that sufficient momentum has been gained in connectivity technologies to make the PAN a reality.

Is my PAN personal?

With the proliferation of home networks, some [5]2.1 million homes and home offices today with an anticipated [6]10 million homes by 2002, [7]"households are turning into pervasive Internet environments." These ever increasing networks, both home and office, are the actual target of the PAN. [7]While first "wave" of these WPAN™ technologies is simple wire replacements for

peripherals undoubtedly the real power is in the ability to transparently and conveniently connect to the broader networks and exchange important data and information. It is this exchange and storage of data that must be safeguarded. Access to personal and corporate data through any PAN must be the focus of continued scrutiny by security professionals. Simply because we can now access our data easier does not diminish the importance of keeping that data secure. We can already see a dangerous trend in the PDA space as more professionals increasingly store potentially sensitive data on their hand-held devices. How much more of a problem may this become as we have the ability to connect and disconnect our POS "bubble" to networks as we go through our daily routines. How much of this "personally" stored data now becomes accessible to the ever-waiting PAN connections and potentially fall into undesirable hands?

Another aspect of the personal nature of this environment is a person's identity. In today's environment a user deliberately identifies themselves to whatever network they log into by use of one of many ways, userid, token card, smartcard or some other means that uniquely identifies the person logging in. With a PAN one would expect the POS "bubble" to be able to provide the identity of the user to the network transparently. As we see more devices being PAN aware and more points of access this could become an increasing problem. A single person may have several identities that change as they go throughout the day. Someone shopping at the market would not necessarily want a PAN enabled kiosk to identify them as an employee of a specific organization nor would the employer necessarily want that person identified as one of their employees. Likewise one would not want to be mistaken as an employee of an organization that they have just visited to provide some consulting services. This could provide a very real risk in sharing of confidential information. The ability to adjust and protect our personal identities as we interact with various PANs we may come in contact with is critical as this space develops.

Security policies must be modified to include this developing PAN environment and the various pieces of technology it will bring to the workplace or home office. Policies must be written to make it very clear what data will be allowed to be shared and what data will be allowed to be stored "personally". Simply because I have the ability to connect and exchange data transparently doesn't mean that I have the authorization to exchange that data. [8]"The theft of data is costing organizations and government entities billions of dollars on an annual basis." according to a PricewaterhouseCoopers report published last year, [8]"breaches of systems were causing about $1.6 trillion in damages worldwide". This number can only rise as there are more and easier access points into organization's networks.

Secure vs Convenience:

Security has been considered as part of the various connection technologies at the physical layer but do very little in addressing the security of the data being exchanged. Bluetooth, for example, addresses the auto-configuring of devices as they connect to the network but once the connection is established it is up to higher level protocols or the applications to provide the data security. While there is still some debate on who's responsibility it is to provide the end-to-end security with a PAN connection it is well stated that security [8]"will become of utmost importance as Bluetooth and other wireless technologies are operated more regularly in predominantly wired businesses."

There is a direct contention between ease of use and security when we are looking at these ubiquitous connections. In discussing service discovery for wireless connections Robert Pascoe states [9]"such networks must be self-configuring, rendering them virtually transparent to consumers. Connection must work out of the box, without setup wizards, online settings or manuals." One of the major promises of the PAN is that transparent connection to our data sources and information. It is in this ease of setup and configuring we will find that we are much lacking in the area of security. We know from today's experiences that many existing wireless connections are woefully lacking in their security. Most of the time it is not for lack of ability or lack of available technology but rather for the sake of convenience. [10]How many wireless networks have been setup in the rush to provide connectivity that the attention to proper security configuration was lost in that rush? Or how many networks have been setup in an "temporary" status only to be found still running months later without any additional thought to how secure they are? Convenience is the Achilles heal to proper security in our wireless networks as [10]"security is inversely proportional to convenience: Anything convenient is inherently insecure. And wireless LANs are very, very convenient."

When we consider our PAN environments we can only see that this problem of insecure connections is going to be compounded exponentially. As we move on to the 2nd wave of our PAN and get beyond the simply wire replacement we will start to see the growth of applications that are eager to exchange data with our POS "bubble". This exchange of data being made too difficult with overburdening security requirements could stunt the adoption of PAN. More likely, however, will be the continued growth of PAN without sufficient security included.

What to do:

We are still very early in the adoption of firm PAN standards that will sufficiently address the security needs of today's information exchange. However, manufactures continue to produce PAN devices and we continue to purchase them and connect them to our existing networks. Much like the mobile and home-office workforce of today, we will see a continued move to make more of our data accessible in a convenient form that is easily accessed.

It is not to soon, however, to begin to address some of these issues with existing security policies. Now would be the time to seriously consider adding appropriate sections to policies to address the use of PAN devices in your organization.

Security Policy considerations:

As you begin to consider updating existing policies to include PAN access it is imperative that the proper level of control is maintained. [11]Michele Crabb-Guel outlines these very important points in her SANS course on "Building An Effective Security Infrastructure":

- Security needs and culture play major role.
- Security policies MUST balance level of control with level of productivity.
- If policies are too restrictive, people will find ways to circumvent controls.
- Technical controls are not always possible.
- Must have management commitment on level of control.

Without keeping this proper level of control in mind when updating our policies we run the risk of making the policies so restrictive or unworkable for this new environment that we force people into non-compliance.

One of the first steps in updating your security policies is to identify potential risks from PAN connected devices in your specific organization. There are several areas of risk that immediately come to mind:

- new connections into the networks -
  We are already familiar with and have worked at securing workstation, pc, portable access into our networks but what about these new devices that will connect without human intervention. What do we understand about the authentication that will be required to access the network and how can it be enforced?
- new devices that may be accessed from these personal devices -
  As we see new devices developed that will allow connectivity we need to be aware of their abilities and functionality. Is there risk from allowing multiple users access these devices at will? Will there be some potential for information to be inadvertently shared without the user's knowledge through use of these devices?
- data being stored on these devices -
  What data can be stored in our "personal devices"? How secure is this data if the device is connected to another PAN?
- users identity -
  Now that the PAN can identify who is connected how do we control and maintain true identity? Is the person's identity the same "on the job" as it is "off the job"? What type of authentication is provided in this transparent connection?

These personal devices and associated PANs will continue to proliferate in our environment and they will become increasingly easier to use at the same time greatly improving our productivity. Just as we have seen the influx of PDAs in the workplace over the past year we will see even more wireless personal devices in the upcoming months. With these devices comes the increase threat to our secure data and networks. Our security policies can either accept this and adapt or they are in danger of forcing people into non-compliance and provide little to increase security. We cannot afford to wait until standards are set and products fully accepted in the market place to address these issues.

Existing security policies must be continually reviewed and updated to reflect these new devices and their use is our organizations.

Conclusion:

Having a device that connects to a Personal Area Network may in fact not be so personal. Sufficient security products and experience are not available to ensure the security of such connections. The misconception that your POS is a strictly "personal space" aides in the deception that issues dealing with corporate security are somewhat insignificant in the PAN arena. As we see an ever increasing blending of the workplace and ever present global network it becomes more critical that we continue to evaluate every connection point into our networks and to be aware of the data that is exchanged.

References:

[1] Zimmerman , T. G. "Personal Area Networks: Near-field intrabody communication". IBM SYSTEMS JOURNAL, VOL 35, NOS 3&4, 1996. URL. http://www.research.ibm.com/journal/sj/mit/sectione/zimmerman.html (19 July 2001).

[2] Kraemer, Bruce. "IEEE 802.15 Publicity Committee". Rev. 0.4(Modified: 25-April-2001). URL: http://ieee802.org/15/pub/PC.html (17 July 2001)

[3] Proust, Albert. "Personal Area Network: A Bluetooth Primer" O'Reilly Network. 11/03/2000. URL: http://www.oreillynet.com/pub/a/wireless/2000/11/03/bluetooth.html (17 July 2001)

[4] Neel, Dan. " Microsoft to wait on Bluetooth backing in Windows XP" Network World Fusion. 04/05/01. URL: http://www.nwfusion.com/news/2001/0405msblue.html (17 July 2001)

[5] Ruber, Peter. "Building a Home-Office Network." InternetWorld. June 15, 2001. URL: http://www.internetworld.com/magazine.php?inc=061501/06.15.01feature5.html (17 July 2001)

[6] Baran, Suzanne. "Networking Begins at Home." InternetWorld. June 15, 2001. URL: http://www.internetworld.com/magazine.php?inc=061501/06.15.01feature6.html(17 July 2001)

[7] Cohn, Michael. "Personal Networks." InternetWorld. June 15, 2001. URL: http://www.internetworld.com/magazine.php?inc=061501/06.15.01feature1_p1.html (17 July 2001)

[8] Armstrong, Illena. "Plugging the Holes in Bluetooth" SC Magazine, February 2001. URL: http://www.scmagazine.com/scmagazine/2001_02/cover/cover.html (17 July 2001)

[9] Pascoe, Robert A. " Service discovery spans platforms" Network World Fusion 05/29/2000 URL: http://www.nwfusion.com/archive/2000/93009_05-29-2000.html (17 July 2001)

[10] Malloy, Rich. "What You Can't See Can Hurt You" Mobile Computing & Communications Magazine. August 2001: 48

[11] Crabb-Guel, Michele. "Model Security Policies, Determining Level of Control" SANS Institute Resources. URL: http://www.sans.org/newlook/resources/policies/bssi3/sld012.htm (18 July 2001)