GIAC Security Essentials Certification (GSEC) Practical Assignment

Version 1.4c (amended August 23, 2004)
Option 1

Brian N Smith

Submitted January 25, 2005

"Un"-securing Ourselves: Common Mis-practices and Missed Practices

Abstract

In the world that we live in today, concerns about security are becoming more and more predominant. Concerns are prevalent not only over information security, but also physical and personal security as well. The September 11th tragedy was a jumpstart for our nation in terms of focus on personal and physical security. Since then, more emphasis has been placed on those types of security than possibly ever before. Fortunately (or unfortunately), we have not had such a tragic event in the field of information security. Even though we recognize the importance of having our information kept private and secure, there has not been such a colossal event leading the charge towards information security. Lacking such an event leads many of us to assume that our information is "generally secure" and promotes poor practices. This paper will address some of those practices and assumptions, detriments, and how one might go about fixing such issues.

Too Much Freedom?

One of the first practices that can lead to information security issues that I wanted to mention is that of making devices "Plug and Play". The Plug and Play concept has been around for a few years in the PC environment and is wonderful for certain circumstances. It's hard to dispute anything that makes our lives easier and makes seemingly complex tasks relatively simple. However, when dealing with devices such as networking peripherals and devices, such a simple solution that anyone can implement can cause several security issues.

It's not the concept of Plug and Play that I take issue; it's the fact that more and more devices are designed and marketed so that they can be installed by casual users instead of professionals. This can easily lead to security holes and a false sense of information protection. A shining example of what I'm referring to lies with the Linksys BEFSR41 Router.

First of all, I should note that it's easy to see why home users were driven to seek such products as a router for the home. Ever since broadband technology has propagated to the masses, multi-PC homes were searching for a way to allow more of their computers access to the Internet. Realizing the need for this, ISP’s stepped in and began offering extra IP addresses for home users. Usually averaging $9.95-$19.95/mo per IP address, home users were quickly dissuaded from allowing the ISP to provide their routing needs. This is where manufacturers such as Linksys and Netgear step in.

One of the most common appliances available now is the Linksys BEFSR41 v3 router. Because of the Plug and Play capability, you can simply unwrap the router from the packaging, plug in the network cable from the modem, the network cables from your other PC’s and the power cord. Voila, instant home routing! All of this can be done without reading as much as the front cover of the instruction manual. As far as a home user is concerned, this is phenomenal. Not only did it take all of 10 minutes to setup, a $50 appliance could save as much as $100/mo in extra IP addresses. In fact, it is so easy, most are convinced that there is no more setup to be done.

I applaud Linksys for their easy-to-use routing setup and Plug and Play efforts. However, there are some very important security issues that come from a default packaged setup. From their user guide, one might notice, “The default password is admin.” (Etherfast Cable, p. 30). This means that for every router of this type setup in this manner by a home user, the password to access their router is the same, simply “admin”. Now, anyone who has access to the router can enable the DMZ for one of the user’s machines, usually “starting at 192.168.1.100” and access the machine as if it were available directly on the Internet (Etherfast Cable, p. 17). It is necessary to note that although the Remote Administration feature is disabled by default (Etherfast Cable, p. 30), there is a current vulnerability in which, “A remote user can access the administration login page even when remote administration has been disabled.” (Gillespie, p. 1) Now, for everyone who simply pulled the router out of the box and plugged in all the cables without reading the manual, their router is accessible over the Internet and has a public (and simple) default password of admin.

Someone might ask a question similar to “Isn’t that setup just as secure as it was before the router was installed?” The answer to that is yes and no. If the machine(s) already had access to the Internet, the answer is yes. If this is a new machine accessing it for the first time, there has been virtually no shield placed between it and the Internet. With many of these personal routers boasting about adding an extra layer of security, these appliances can actually make users’ systems less secure by giving them a false sense of security. From a hacker’s perspective, all they would need to know is if this router is setup at a certain location and its IP address. Knowing this, your systems are easily accessible and compromised.

How might someone go about fixing such a problem if they own this router? First of all, it is always a wise practice to read the manual when installing a piece of hardware you are unfamiliar with. Second, it is generally a good idea to access the website of the hardware that you purchased and make sure the firmware is as up-to-date as possible. Third, ALWAYS change the default password on a device such as this. Even if you pick a poor password, almost any password other than the default will improve your chances of surviving an attack. Another point that I will mention later is that a user needs to realize is that things are not always as they appear to be. In this case, the setup said Remote Administration feature was disabled, but in this case, it was still enabled (Etherfast Cable, p. 30). Finally, if you find your information worth protecting, it is usually best to let a professional do the installation of the equipment, as there are cases when you may be given too much freedom in setup.

The method of reading the manuals, keeping with the latest updates, changing default passwords and even requesting assistance all give you a better chance at keeping your data secure. Even though doing all of these things may still leave your data at some risk, each added level of effort in keeping your data private is a wise defensive choice in a multi-level defense plan.

Everything is not as it seems (or as you left it)

There are many valuable lessons to be learned in the field of Information Technology and Security, but one of those that I was made privy was that of the phrase “Everything is not as it seems”. You may have heard this phrase before in relation to magic tricks or mysterious circumstances. Some malicious software programs seem to perform digital magic in attacking your data and systems.

The first instance of these cases that I’d like to discuss comes with the recent release Windows XP Service Pack 2 ICF (Internet Connection Firewall) or now called the “Windows Firewall” (Understanding Windows Firewall, p. 1). First of all, this is a built-in software firewall that Microsoft has decided to include in the latest service pack for Windows XP. Microsoft states in a knowledgebase article “After you install Microsoft Windows XP Service Pack 2 (SP2), some programs may seem not to work. By default, Windows Firewall is enabled and blocks unsolicited connections to your computer” (Some programs seem, 1). For many users not familiar with firewall concepts, this can cause problems and irritations that may lead to the users turning off the firewall altogether. Although we (as security professionals) are hard pressed to force the user to use certain precautions, sometimes ease-of-use wins over all else for the common user. However, what we can provide for the user is a working product if they choose to use it.

Recently there was a severe bug found in the Windows Firewall that allows access to users’ files in certain circumstances.

“By default, file and printer sharing makes changes to the SP2 firewall to give computers on the "local network" access to shared resources. However, the definition of that local network depends on the Internet service provider. In some cases, especially with dial-up ISPs, it meant the entire Internet, according to Microsoft.“ (Evers, 1)

A patch for this bug was released soon after the bug was discovered (Evers, 1). However, the damage was already done. It's problems like this that lead to users losing confidence in their operating systems, security applications and devices, and about their information security in general. In this example, if the users were not initially convinced to turn the firewall off due to the application issues, they might certainly be convinced that it doesn't matter if their files are open to everyone. This is a case of security-related software giving the user a false sense of information protection, similar to our router example before. As I mentioned, a patch does exist and this makes a great case for the point of patching that I will mention later.

If we continue on our assumption that all is well with our PC's, eventually it is very likely that we will come across a virus or worm. Even the most experienced computer users that keep up to date with the latest patches, are cautious about who they accept files from, where they browse, and only run known applications, cannot be guaranteed to avoid such malicious code. The common practice to circumvent this is typically some sort of antivirus software. The typical antivirus software these days has new updates weekly, if not daily. Even with this protection, the newest viruses have a possibility of slipping by due to the new updates not being installed or not even being produced yet. One such virus I'd like to mention has been named W32/Bagz-mm (Munro, 1).

This virus is particularly malicious in that it possesses multiple thorns in which to attack your system.

“The virus harvests email addresses from the victim's machine, and uses its own SMTP engine to send copies of itself. According to Symantec's analysis, Bagz disables the Windows firewall, and installs its own network driver to bypass third-party firewalls. It also installs a back door and can download files from remote hosts.” (Munro, 1)

This supports my contention that, indeed, everything is not as it seems (or as it may have been left). A system could be protected by a personal router with the latest firmware, all operating system patches installed, Windows Firewall (or other software firewalls) in operation, and the latest antivirus software updates installed and could still be prone to this attack. Let's break down what this virus actually does.

As mentioned in the excerpt, the virus uses its own SMTP engine, which would not have to rely on Outlook Express or some other mail client being installed (Munro, 1). It will disable Windows Firewall without your knowledge and even use its own network driver to circumvent other software firewalls (Munro, 1). Finally, it will leave a back door open on your system allowing file storage (for Warez perhaps) or for further exploitation (Munro, 1). It might be a wise question to ask “How can this be avoided or at least its impact minimized?” In this case, it seems that the virus was mostly transmitted via email in an .exe attachment so email precautions would have most likely avoided an incident altogether (Munro, 1). Also, if the antivirus software was up-to-date and the patch distributed before the mainstream release of the virus, it might have been prevented as well. Barring that, a hardware firewall might have protected your system from the back door file transfers, as might a router with up-to-date firmware and no back doors. A couple of points to note here is the multi-level defense concept that more and more layers of security can mitigate risks that your data can face. A hardware firewall, a router, a software firewall, latest security patches, anti-virus software, and a wise user make a good combination for protecting personal user data. The other point to notice is even though you may have checked to see that your Windows Firewall was turned on yesterday, a malicious program such as this virus could have disabled it in the meantime. Indeed, everything is not as it seems.

The last case in this category that I would like to mention is a true story that I experienced a few years back on the job. This is an incident from which I have certainly learned a lesson or two about situations changing over time. The purpose of this story should be to convince you that you should never let your guard down even if you suspect there is no way that your PC could be compromised.

The request came in one day to setup a PC on the ground floor of our building to display various demonstration videos and/or messages that would be of interest to our customers. We had the perfect location for such a request, it was a storage closet directly past the front doors behind a set of locked double doors and had a display window for the monitor. Needless to say, the management wanted to be able to update the information displaying across the network. Since this PC only had a hardwire NIC in it and there were no network drops in the closet, we needed another solution. My colleagues and I decided a wireless card would allow us to do what we needed. We installed the card and made sure the OS patches were up to date. Upon configuring the PC downstairs in the closet, we found there was no wireless access point that the card could reach. This blew the plan of updating the information across the network. We simply noticed there was no chance of it being accessed over the network or at the console. One major mistake we made was that we set a fairly simple login/password setup for the PC, display/display. This is a very bad idea all the way around, but we figured only a handful of authorized people could ever get to this PC, so there would be no need for a complex password scheme.

Three months or so went by without another thought of this PC on our part. No patches were installed to the machine, as physical access was limited, and there was no wireless access point in the area, and, heck, we were too lazy to carry the patches down there and install them ourselves when we figured there was no reason to. Then I get a phone call one day from our network administrator. He proceeded to tell me some computer linked to a wireless access point in our building had been pumping 8 mbps of data out over the network for the last three days. He had the name of the computer available, display. Imagine my shock, as this computer shouldn't have had any network access. Upon getting the key to the closet and browsing the PC, it seems an FTP server had been setup and serving several pirates with files stored on our display computer. It turns out, wireless access was just rolling out in our building, and a point had made it to the ground floor to cover the lobby area. Our wireless NIC that we installed had been actively searching for available SSID's and had finally found one, linked up, and become available on the Internet. With our simplistic login and password matching the computer name as well as patches three months out of date, it was an easy target.

Now, what could have been done to prevent something like this from happening? First of all, this was in an environment where a router/firewall was not permitted. This is pitfall number one, but sometimes, these devices simply aren't allowed. However, perhaps a software firewall may have been a wiser choice. Secondly, this is a lesson that physical security is certainly not always enough. This machine could've been inside Ft. Knox and a similar event happen. Next, such a foolish login/password should have never been chosen. Patches should have certainly been installed and updated even though the machine seemed secure. Finally, the wireless card should have been disabled to prevent something like this from happening. After this event, the machine was cleaned of all files stored on the PC maliciously as well as any backdoors deleted. All passwords belonging to all accounts have been changed, as well as a patch schedule setup, and antivirus software installed.

The point to all of these cases is one that you should not take lightly as an educated home user or as an administrator. Do not make assumptions that rely on conditions remaining the same, and do not take any precautions for granted. It is difficult to know if a particular software package or hardware device has vulnerability, but, if we practice multi-level defense, we have a better chance of not being a victim to one of these attacks.

Let's Get Physical

The next set of common mis-practices and missed practices that I would like to mention are those involving physical security of the system itself. From a home-user perspective, this topic may not be of much use, as it doesn't make sense to lock your PC away in a secure room. However, there are some practices that a home user may find of interest, especially if the data contained within the PC is of critical importance. With regards to physical security of a computer system, it is of vital importance that this be a top priority in a companies' security plan. Without this component, the system can be subjected to a myriad of other attacks, some more severe than what can be executed over the Internet. Microsoft agrees with this point in saying:

“However, physical security is an extremely important part of keeping your computers and data secure-- if an experienced hacker can just walk up to your machine, it can be compromised in a matter of minutes.” (5-Minute Security Advisor, 1)

There are basically two categories in which attacks involving physical security fall: denial of service and data compromise. The first attack may be fairly obvious, but it’s also perhaps the hardest one to prevent. Denial of Service on a machine over the network may mean to make the system unavailable for transactions, slow to respond, or simply make some data unavailable. Denial of Service for a machine with which one has physical access can be so much more damaging.

A Denial of Service attack for a machine with witch a malicious person has physical access can also fall into several categories: data corruption and/or destruction, theft of hardware, interruption of resources, and various other mischievous acts. Data corruption or destruction is fairly self-explanatory. A deviant person with physical access to a system might simply remove some of the storage devices from the system and give them a good beating. Certainly you would agree that removing a hard disk from a system and smashing it on a concrete floor would constitute a Denial of Service. Although this is a violent incident, it is also a pretty rudimentary attack. Destruction of a storage device should at least give some peace of mind that the data wasn’t compromised by someone else, and the system could be restored by backup later. Theft of hardware might occur if the person might wish to access the data contained within at a later date, but removing the external (or internal) disk(s) would cause that information to become unavailable to legitimate users. Interruption of resources might fall along the lines of unplugging an external storage device, unplugging of network cabling, or simply powering off the system.

These types of problems are usually more a nuisance than an immediate threat to data compromise. Finally, there are hundreds of other ways to damage and disrupt a system than the ones I’ve listed here. Keep in mind that a Denial of Service attack is usually more oriented to disrupting normal operations than information espionage. These attacks may be the hardest to prevent, as there are multiple points that can be attacked and very difficult to find who perpetrated the attack. Imagine one of your servers disappears from the network and it turns out the attacker simply unplugged the cable from the router in your networking closet. An attack like that may be very difficult to prevent if your physical security becomes compromised (and difficult to track down).

The second type of attack that can be committed by someone with physical access to a machine would be one of data compromise. Data compromise attacks can be considered very severe, as once you lose possession of your data, you may have no idea where it goes. This attack applies in the realm of the home user as well as the system administrator of a corporate network. Imagine if you were a home user, having your cookies and local information sifted through to reveal your credit card information. The results of such an attack could be disastrous to your credit rating. Data compromise attacks through physical security are coming to the attention of security professionals as more and more people are encrypting files on their hard disk. Take the example of the EFS (Encrypting File System) found in a few latest flavors of Windows. (The Windows Server 2003, 1) Microsoft says of the EFS, "Overall, EFS makes a reasonable effort at providing file confidentiality". (The Windows Server 2003, 1) In the EFS system, users can encrypt files based on user name at the file-level. As I will mention in a minute, this is a level of security that should be implemented on critical data on systems that support such a device. It should also be noted that this is not a guarantee that your data will be safe from an attacker, but it's yet another level in our multi-level defense system.

Now, how can we prevent breaches such as Denial of Service in our systems with regards to physical security? Implementing a number of safeguards best prevents these attacks. First, keeping your server room locked at all times when no one is present is a good practice. Many cases these days also have intrusion detection mechanisms that alert you when the side panel has been removed. To prevent the entire machine from being stolen, there are cable tie-down systems that secure a case to a rack or some other solid contact point (Bulldog™ Security Kit, 1). Finally, perhaps one of the best deterrents to someone gaining physical access to your computers might be a camera system installed in the server room. Knowing that one has a good chance of getting caught can sometimes be the only measure necessary to dissuade an undetermined attacker.

As I mentioned before, if an attacker has physical access to the system and wishes to read the data on the drive, there are few mechanisms on a simple PC that will prevent him/her from doing so with the correct tools. If the system itself is stolen, the drive can simply be removed and the attack continues. But, let's say that our attacker stole a PC where the user was using the EFS by Microsoft on some critical files. The rest of the unencrypted files will be available to our attacker by simply installing the hard drive in another PC; however, the encrypted files will still be encrypted. By the statement above made by Microsoft, "Overall, EFS makes a reasonable effort at providing file confidentiality" means that they feel this provides reasonable protection; it is not a catch-all (The Windows Server 2003, 1). Their encryption system may not use the latest, greatest, and most secure encryption algorithm. Also, there are ways, depending on how the system was setup to recover the data if the users' account information was not known. The easiest way for an attacker to access these files would be to login with the user id and password, perhaps from a key logger device (Key Ghost, 1), or a brute force attack (@stake LC 5, 1). There are also software packages available that will allow anyone with physical access to the system to reset the administrator's password, but with some tools, "Beware!!! Resetting a user's or administrator's password on some systems (like Windows XP) might cause data loss, especially EFS-encrypted files and saved passwords from within Internet Explorer" (Petri, 1).

How can we, as educated computer users protect our information from getting leaked to the wrong hands? The answer lies in the fact that we have to decide how important our privacy and information is to us. If the information is of almost no consequence, it may not be worth spending thousands of dollars and man-hours to try to protect. However, if it is mission critical to a business, it may very well be worth all that it costs to protect it. From the home user perspective, perhaps the best lesson to be learned is that even though the technology is available to purchase, it may not be the wisest decision to set it up without the required knowledge. Even though there are some hardware issues that exist that allow a system to be vulnerable, an educated security professional will know to update the firmware, install the necessary patches, and know the correct system settings to provide the most security available for the chosen solution.

The next idea we need to keep in mind as educated PC users is that we should never take our security for granted. There are almost daily patches available for the most popular operating systems as vulnerabilities are being discovered at an alarming rate. A system that may be deemed completely secure yesterday may well have a gaping hole open to the world tomorrow. We should always vow to exercise wise practices in avoiding and protecting against viruses, knowing the capabilities of our systems, and using layer upon layer of defense against all the threats that are waiting to strike our computers. As I mentioned in my story above, we assumed there was no way that our PC could be accessed, remotely or physically. In fact, this was the case at the time, but circumstances changed and we were caught with our proverbial pants down.

Finally and perhaps most importantly, physical access to servers and computers should be limited to only authorized personnel. As discussed above, there are a myriad of ways that information on a computer could be compromised from a malicious user with physical access. It is of vital importance that this be a primary concern in your security plan for the reasons listed above.

As we move in to a new age of technology, the focus is coming more and more on information security. To keep your information private, it is vital that everyone, not just security personnel, be educated on best (and worst) practices. It is no longer acceptable to assume that your information is "generally secure" and moreover, the assumption should be changed to "generally insecure" unless measures are taken. Keep in mind; if the data is important to you, chances are it's important to some attacker as well.

Bibliography

@stake LC 5 The Password Auditing & Recovery Application, @stake Inc. 2004 24 Jan 2005.< http://www.atstake.com/products/lc/>

"5-Minute Security Advisor - Basic Physical Security". Microsoft TechNet 7 May 2002. 24 Jan 2005. <http://www.microsoft.com/technet/archive/community/columns/security/5min/5min-203.mspx>

Bulldog™ Security Kit, Belkin Corp. 2004 24 Jan 2005. <http://catalog.belkin.com/IWCatProductPage.process?Merchant_Id=&Section_Id=103&pcount=&Product_Id=22616>

Etherfast Cable/DSL Router with 4-Port Switch User Guide, Linksys Corp. 24 Jan 2005 <ftp://ftp.linksys.com/pdf/befsr41V3_ug.pdf>

Evers, Joris. "Microsoft Fixes 'Critical' XP Firewall Issue" PCWorld.com 16 Dec 2004. 24 Jan 2005. <http://www.pcworld.com/news/article/0,aid,118990,00.asp>

Gillespie, Matthew. "Linksys BEFSR41 EtherFast Router Lets Remote Users Access the Administration Page Even When Remote Administration is Disabled" 1 Jun 2004. 24 Jan 2005. <http://www.securitytracker.com/alerts/2004/Jun/1010357.html>

Key Ghost: The Hardware Key Logger, Key Ghost Ltd. 2000 24 Jan 2005 <http://www.keyghost.com/>

Munro, Jay. "Security Watch: Bagz Will Deep Six Your Windows Firewall" PCMag.com 5 Oct. 2004. 24 Jan 2005. <http://www.pcmag.com/article2/0,1759,1666908,00.asp>

Petri, Daniel. "How can I gain access to a Windows NT/2000/XP/2003 computer if I forgot the administrator's password? How can I reset the administrator's password if I forgot it?" MCSEWorld 1 Jan 2005, 24 Jan 2005. <http://www.petri.co.il/forgot_administrator_password.htm>

"Some programs seem to stop working after you install Windows XP Service Pack 2", Microsoft Corp. 28 Sep. 2004. 24 Jan 2005. <http://support.microsoft.com/kb/842242>

“The Windows Server 2003 Family Encrypting File System”, Network Associates Laboratories. Sep 2002. 24 Jan 2005. <http://www.msdn.microsoft.com/library/default.asp?url=/library/en-us/dnsecure/html/WinNETSrvr-EncryptedFileSystem.asp>

“Understanding Windows Firewall”, Microsoft Corp. 4 Aug 2004. 24 Jan 2005. <http://www.microsoft.com/windowsxp/using/security/internet/sp2_wfintro.mspx
>