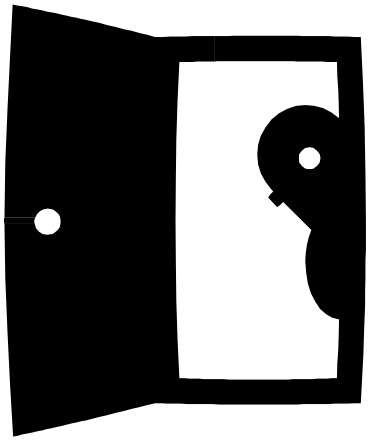
Cyber Security



Before

After

For Your Home Machine

From the Argonne National Laboratory
Cyber-security program office
compsec@anl.gov
Version 1.2

Table of Contents

Introduction

You might be asking yourself why do I need to secure my computer if I don't do anything important on it? Well, hopefully after reading at least this introduction, you are able to get some ideas as to why securing your home machine is important.

I've tried to learn many topics in numerous different ways in the past. However, it seems like the easiest way to learn something that may be dull and boring to you (but exciting to me!) would be to throw a few jokes, pictures, comments, etc throughout this text. I find if you get to know the author, you can understand things better and maybe learn a thing or two. That is what I plan on doing with this document.

Since I am a firm believer that one person can not know everything about everything, I am passing this out and hope to receive some help back. I would like to recognize the Core Networking group because they have been a wealth of knowledge for me. Even in writing this documentation, many people from that group have submitted articles and modified this document in order to expand.

In a nutshell, my name is Mike Wisniewski and you can reach me at wiz@anl.gov. I've been in the cyber-security group now for about 2 years, and have been a computer technician at ANL for 3 years. My supervisor is Michael Skwarek (mskwarek@anl.gov) and he has also helped out a lot in proofing this document and making suggestions. Now that you know a little about us, why is it important that I write this? It's important so you know that even though you may think there is nobody targeting you, there really is. You have to keep in mind that a hacker who is targeting home machines really isn't after you in particular, they may just be after the information on your machine, such as documents that may hold sensitive information (i.e., Credit Card or financial data).

Besides credit fraud, a hacker really likes to have power. The more machines they compromise (break into), the more of a power trip they have. Besides hackers, viruses are now using the same methods a hacker uses to take advantages of open doors in order to infect machines. We will touch upon this a little later on in the presentation.

I hope to make this as simple as possible and if you do not understand anything, please feel free to write an email to me and I will correct this document.

Terminology

I frequently like to explain what things are and throw some terms out so you have a better understanding of what is being talked about. I often don't understand why a glossary is in the back because when you read through the book, the author refers to words and terms that you may have no idea what he or she is talking about! That's why I chose to include a 'terminology' section, so you know what I'm talking about before I write about it!

Internet – When I looked up the definition, it roughly says "a vast collection of inter-connected networks that all use the TCP/IP protocols and that are evolved from the ARPANET of the late 60's and early 70's." Translated to English, this means that there are numerous independent networks that are connected together. To translate this even further, you can think of this as the world and houses. If you take your house and ask yourself, where is your house located? It's located in a city. The city is part of the state, the state is part of a country, and the country is part of the world. The internet is very similar to this, whereas your end computer that's connected to the Internet is your house, and the Internet is the world.

IP Address – Think of it as your house address.

Cable Modem – A high speed internet connection from the cable company to your home. This usually averages about 3 megabits per second (mbps) for you to download files.

DSL – A high speed internet connection. This is usually slower than a cable modem, but you do not share the 'bandwidth' with other people. This usually averages about 500kbps, which is about .5mbps when you download files. This also requires you to live a certain distance from the telephone company's central office (CO). I usually recommend cable modems because of the speed, but they are not offered in all locations. When that is the case, DSL is your next best option.

Analog Modem – This is really the slowest way to connect to the internet. When you don't have cable or DSL access in your area, this is really the only thing you can use. The speeds for this are 56kbps maximum. If you have ever used a modem before, you know it's extremely slow and frustrating! Trust me, if you have a cable modem or DSL access in your area, definitely spend the extra dollars and get that instead! When you add the costs up for an ISP, the phone calls, the equipment, and the frustration, it is well worth the money to get a DSL or cable modem.

Firewall – This is a device that blocks internet traffic. You could think of it as a filter. A rule set is something that tells the network who to let in and who to deny. I like to use the example and make reference to this device as your house. Think

about your house (apartment, dorm, wherever you live). Now, ask yourself the question, why do you have a front door and windows? The reason why you have a front door (at least why I do!) is to keep people out! I do not want any regular Joe walking through my front door and doing whatever they want. I have worked very hard for different items in my house (TV, stove, fridge, food, etc.), and I do not want them missing. That is why I have a front door. If you think of your keys for example, you only give your keys to people you trust, such as family members or close friends. You would never want to give your keys to somebody you don't know.

Now, if you think of a computer network, a firewall is very similar to your front door. You have one to keep people out. A firewall keeps people (hackers) out of the network so that we do not loose important data. Just as you have worked hard for your television, fridge, and other items in your house, Department of Energy (DOE), Argonne, your sponsors, etc have spent a lot of money developing technologies. If we didn't have a firewall, it would be easy for a hacker to steal the documents that we have spent a lot of money developing. But on the other hand, there are certain machines, such as web servers, where you may want to publish your information. In that case, we create "conduits" or holes through our firewall in order to give people the right to access that information. This is sort of like giving people the key to your front door. We trust certain people and we want to give them access to our information.

I hope that explains what a firewall is and how it works. It can be a complicated piece of equipment, but I hope you are able to understand it a little bit.

Vulnerability – Vulnerability is a way to possibly gain access into a computer. There are numerous holes in software that hackers like to find and exploit. Usually, if the exploit is easy enough, a hacker will write script so anybody can break into a machine. This is called 'kiddie-scripts'. Usually, a rather large vulnerability will turn into a virus.

To get a better understanding, I'll try to use an example. Last year, Microsoft had a large vulnerability with Windows 2000 and XP. This was called the "RPC-DCOM Vulnerability". It was pretty well publicized across the news and media. After a few days of this being made public, a hacking group came up with a program. In this program, when you input the IP Address of the machine, it will take you to the command prompt on that machine. Once you are at this prompt, you have full access to the destination machine. The reason this is so scary is because if I take the IP address of your home computer, I can run this program against it and be able to access every file on your computer. You may not care, but some people have sensitive credit card information stored in cookies, they may use quicken, or they might use TurboTax to do their taxes.

Since this vulnerability was so easy to exploit, a few famous viruses came as a result to this. These are Welchia/Nachi, and the infamous MS-Blaster. These viruses would automatically look for machines that it could infect. When it found a machine it could infect, it would run the virus on the machine. Once the virus is run, this machine will look for other machines just like the first one did, and the cycle continues. This is bad because it's a chain reaction. Once a few machines get infected, it can be a disaster.

After this incident, Microsoft came out with a series of patches in order to "fix" the vulnerabilities. But on the downside, the patches are rather large and difficult for dial-up users to apply. Since this is the case, there are still many machines that are vulnerable to this attack.

Viruses – A virus is something that you don't want to get on your computer. If your computer is infected with a virus, you can loose all of the data on your machine. There are many different types of viruses out there. As mentioned above, some will corrupt or delete the data on your computer. Other viruses may infect your machine, and then look for other computers that are vulnerable and infect those machines. Once those machines are infected, they start looking for more computers to infect, and it never ends. How do you stop from being infected? Well, there are really two things you can do; run updated virus protection and make sure you patch your computers.

What if you do receive a virus on your machine? Well, I hope you try to clean it yourself so it saves you a lot of money. If you are not computer literate, I'm sure that you would be able to take your computer to a repair shop in order for them to do it. They may charge you one hundred or more dollars to just re-format and install Windows on your machine! Once they install Windows, they would never even be able to restore your data if you didn't make backups. In this scenario, we are speaking about a virus that could corrupt files on your disk.

Spyware/Adware – Certain web pages will trick you into running programs on your computer. Once a program is run, the machine will track your internet browsing and make "pop-ups" appear on your machine trying to call your attention to items you may be interested in. It seems like after you install something like this once, it's a never ending story and keeps installing more and more programs and pop-ups onto your machine.

Network Address Translation (NAT) – This is a way of taking one IP Address and letting multiple computers use it. Going back to my "House" analogy, it would be as if you live in an apartment building. Everybody has the same street address, but people have different apartment numbers. The NAT would be similar to this.

Virtual Private Network (VPN) – A VPN is a way to allow somebody from offsite to securely access the Argonne internet. All data between your computer and the Argonne computers are encrypted. This means that nobody can sniff (spy) on the data that is being transmitted.

Encryption – This is a way the computer scrambles data so that prying eyes can't see. This is most commonly done on web pages where you would submit your credit card. You will see a little 'lock' at the bottom right corner of your screen, and this means that nobody else except your computer and the computer to which you're sending the information can see it.

Connecting to a Network from Home

You might be asking yourself “OK, I just have a brand new computer, now what!” Well for starters, you might want to think about surfing the web. Why wouldn’t you? Who doesn’t talk about this now? Just about every company has a web site, there’s an infinite amount of free information out there, there is so much to learn and it’s all “just a click away”.

Well, before you get too caught up, you should think about how much money you want to spend and what you want to do. If it’s the money you’re worried about, I’ll try to break this down and justify it for you. I just checked the web page to see how much a dial up account from AOL would cost. According to the page, unlimited dial up access is $23.90 a month. Wow! I never knew that it costs that much for a dial up account! But, putting that aside, you also need to figure in a phone line (if you don’t want to share a line) and phone calls. A phone line (last time I checked) was just $13.00 a month to have the line. You have to pay for taxes and calls in addition to that. So, that brings our price up to $36.90. In this example, we’ll just stop there. Granted, it would be cheaper if you shared the line with your home phone, but if somebody calls you, it will either kick you off the internet or the other person will get a ‘busy’ tone.

On the other hand, if you want to get a DSL line, the latest price from SBC is $29.95 a month. For the extra six or seven dollars, this is well worth the cost. It won’t be the fastest thing in town (or maybe it will, depending whether or not you have cable modem access), but I would highly recommend getting at least a DSL line.

Finally, if you really want the best bang for your buck, you may want to consider a cable modem. I believe these run approximately $35.00 a month. If you do a lot of web surfing and downloading, this is probably the way to go.

Once you get everything installed, what do you do next? Well, the first thing is to patch and update your machine. After you update your machine, you probably want to install some sort of virus protection on the machine. Lastly, you probably want to think about adding a firewall to your computer. I will talk about all of these and how to do them in a later chapter.

If you will be working from home, you may also want to install the VPN client. This software will give you the ability to have your home machine look and work exactly as it would if you were at Argonne. It also allows the encryption of data from your computer across the internet to the Argonne network.

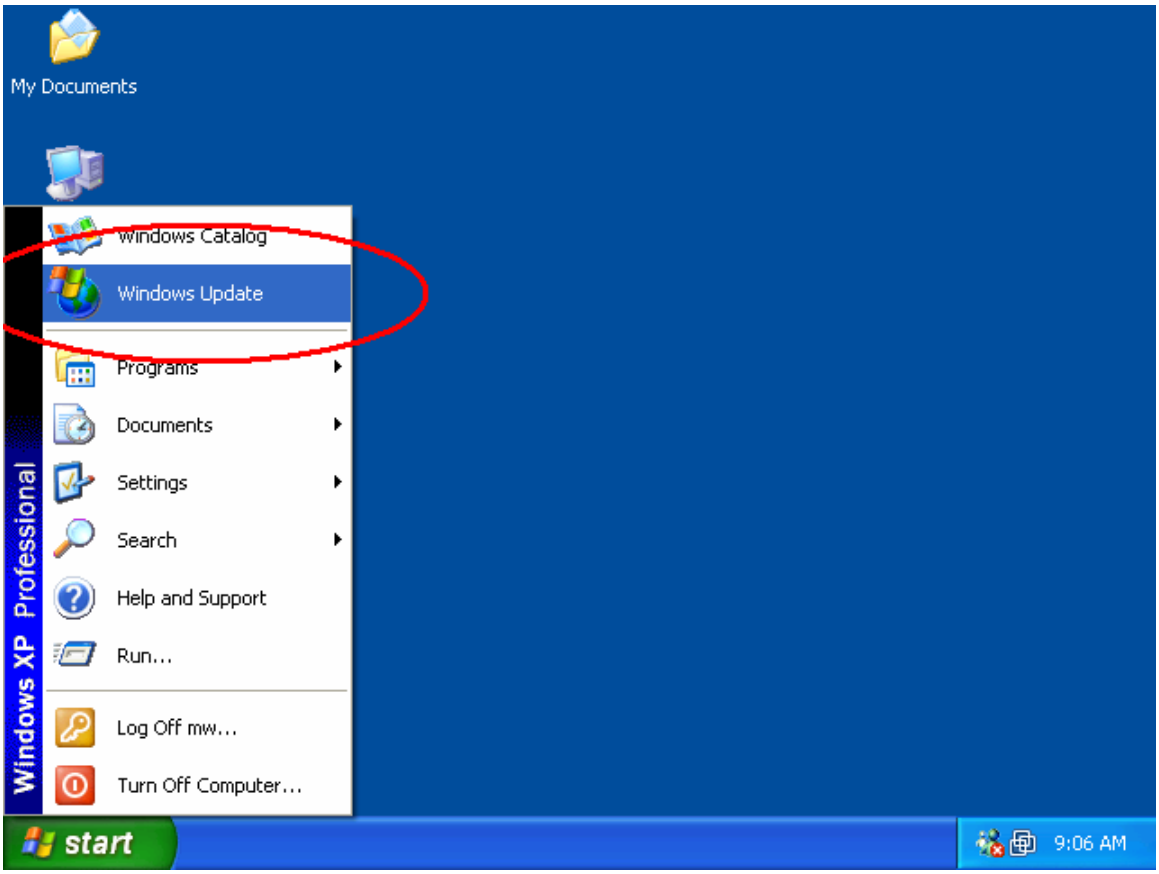
How to Patch

In the introduction, I gave a pretty good idea why you should patch your software. In the old days, we were led to believe that you shouldn't patch and if the software/operating system are working, why mess with it. In today's world, there are so many ways to break into a system; you have to patch the computer in order to prevent this from happening.

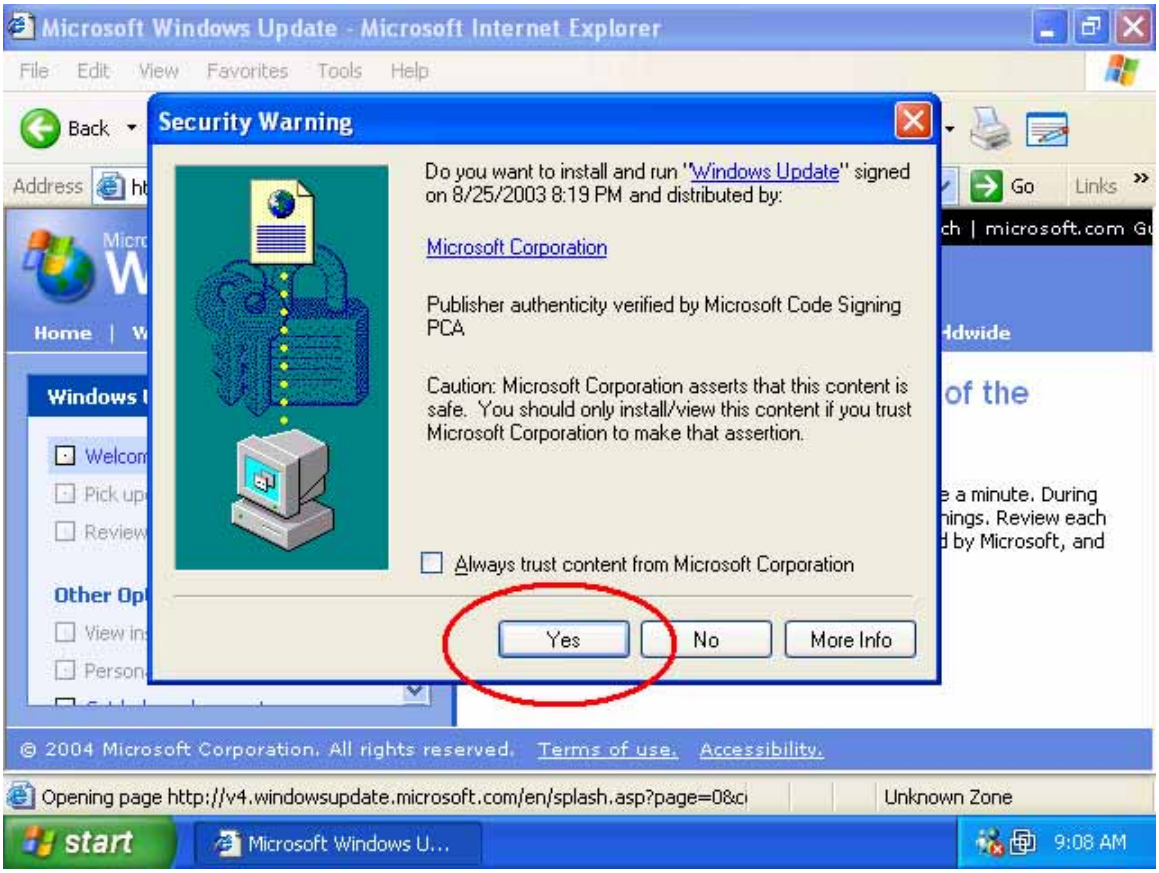
Since the majority of home machines are Windows, I will concentrate on that. In particular, Windows XP will be used in this demonstration, but it will work with Windows 2000 the same way. I will show you how to patch your computer in these steps. There are also a number of ways to skin a cat, but I think this is probably the easiest…

1) Make sure you are connected to the internet and can browse web pages. If you're using dial-up, make sure you do this when you have extra time. This could take several hours so you may want to do it before you go to sleep. However, if you have a DSL or cable modem, this time passes fairly quickly.
2) Boot up your computer and get to the "Start" menu. It should look like the picture below.

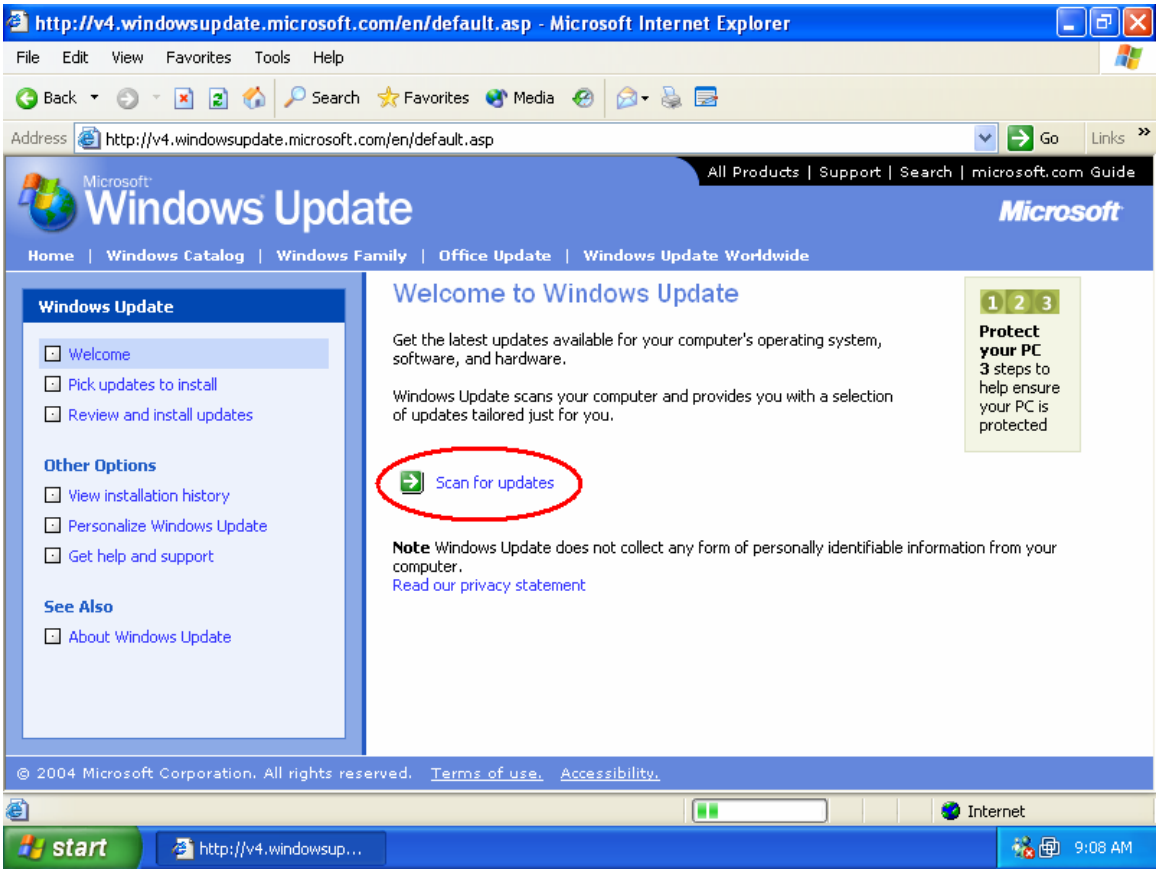
3) Click on “**Start**” and choose “**Windows Update**”.



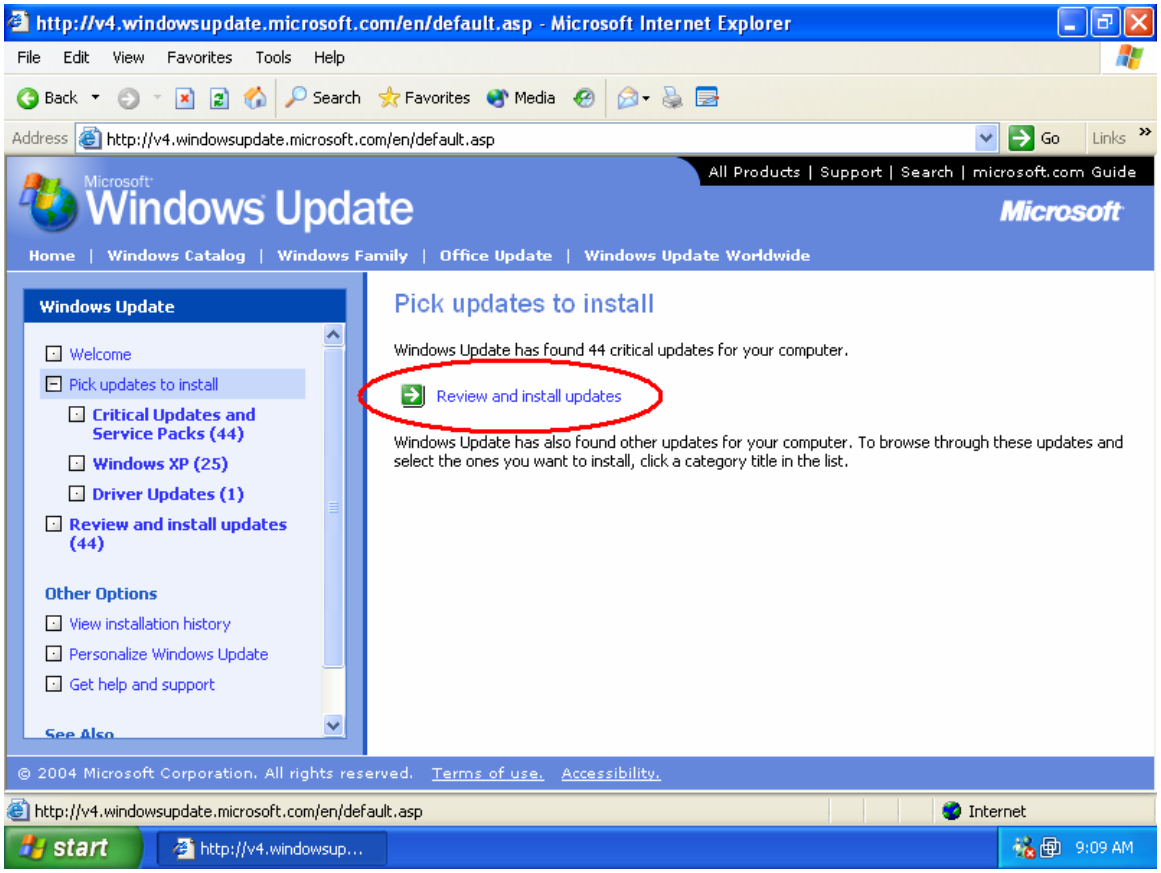
4) From there, you may get a “Security Warning” dialog box. Normally, spyware uses boxes similar to this to trick you to install software. However, this should be digitally signed from Microsoft and it is OK to install this. (Hit “**Yes**”).



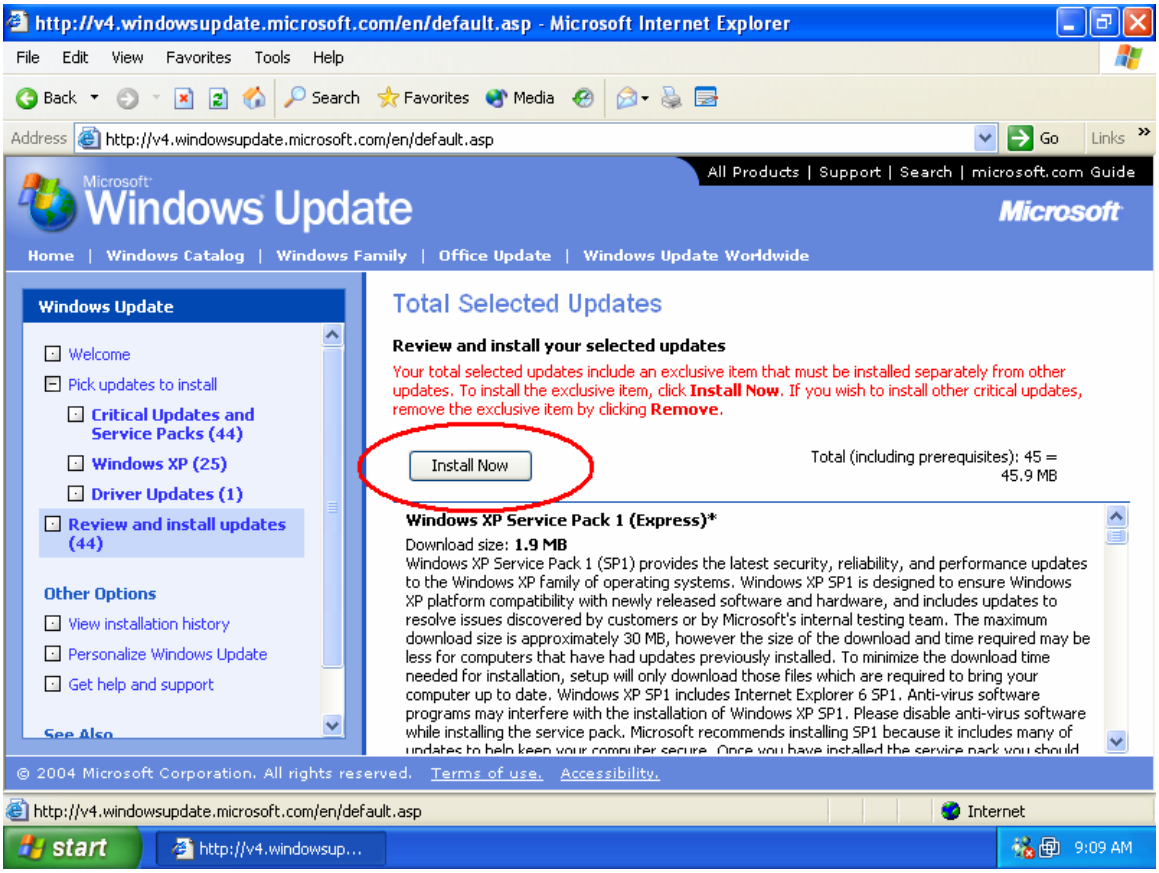
5) The next screen will show a “Welcome to Windows Update” web page. This is the web page where you will scan your computer to see which updates you need. Please hit “**Scan for updates**” when you get to this screen.



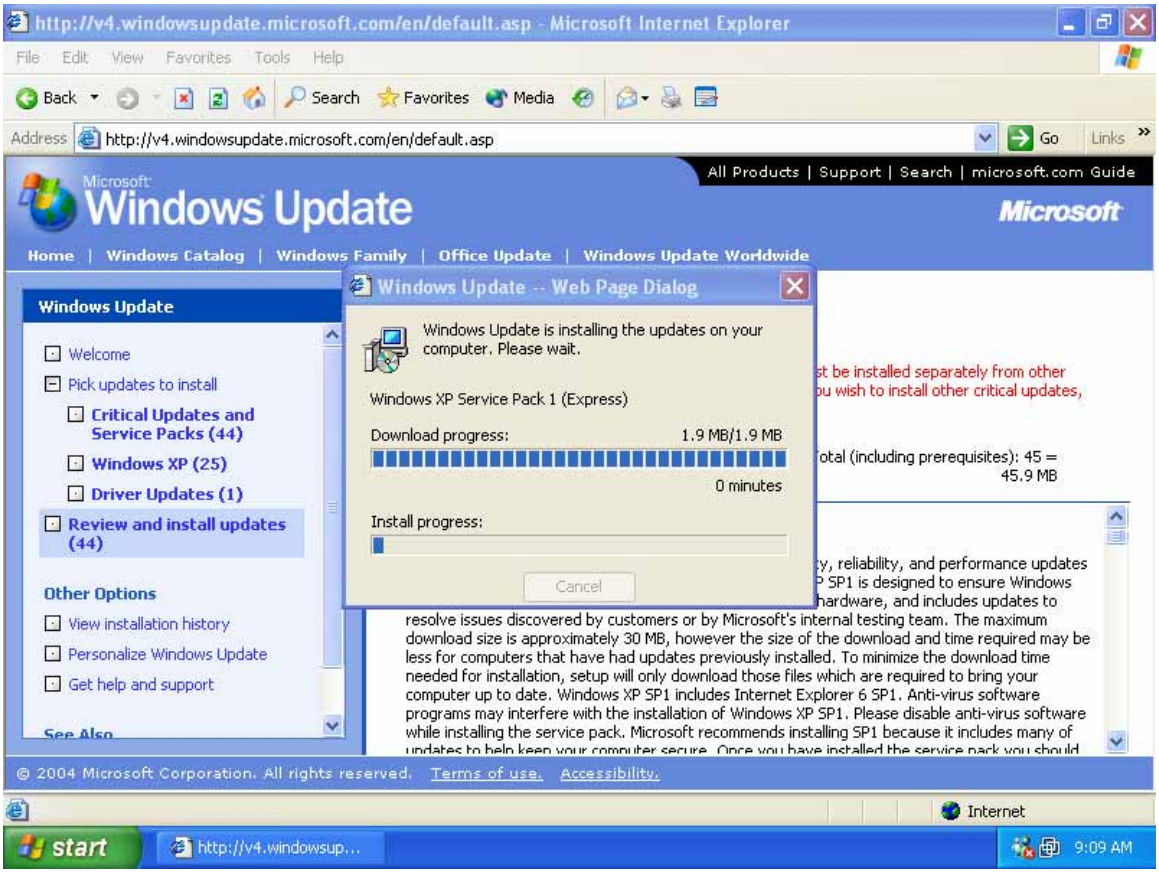
6) After you scan for updates, you will see how many “Critical Updates” you need in parentheses. A new Windows XP install may need 44 or more patches! The choice under “Critical Updates” shows “Windows XP”. These are updates for Windows XP that are not critical, but may make the operating system run better or not crash as much. The last choices (Driver Updates) are updates for device drivers you have on your system. If you’re having problems with a device, it might be a good idea to try to update these as well. Like the “Windows XP” update, these drivers are not selected by default. Generally, it is a good idea to browse the list and choose ones that may apply to you. By default, the “Windows XP” patches are not installed. After this step, please click “**Review and install updates**”.



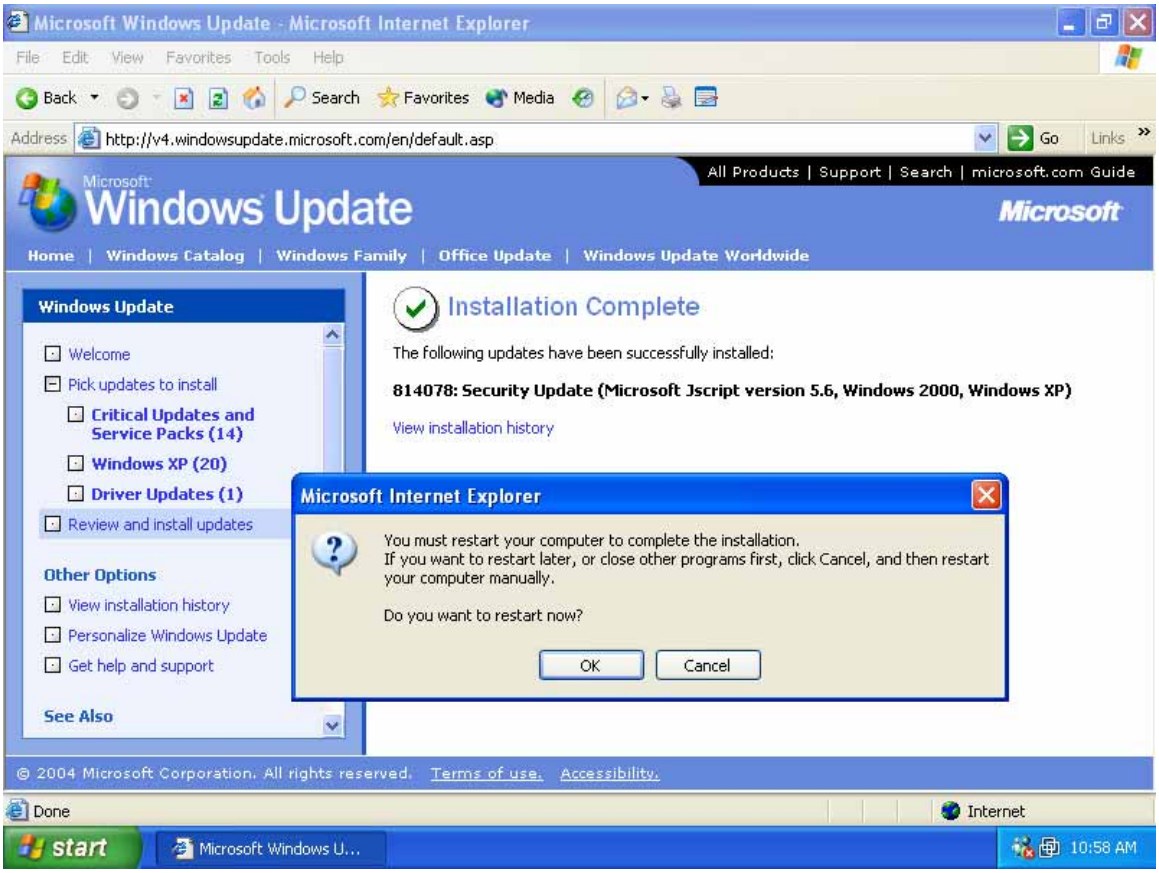
7) After you click “Review and Install Updates”, it will take you to a final web site where you can choose to “**Install**” the updates. When you get here, I would recommend choosing to “Install” them. If you want, you can review them to see which updates you have installed.



8) After you choose to “Install” the updates, you will be taken to a screen that looks similar to the one below. However, if you try to install a rather large and important update, it may tell you that the update needs to be installed by itself. If this is the case, click “**OK**” to continue, wait for the updates to finish, and re-run this update process to ensure all the updates were installed. If not, run through this exercise again until all of the patches have finished.

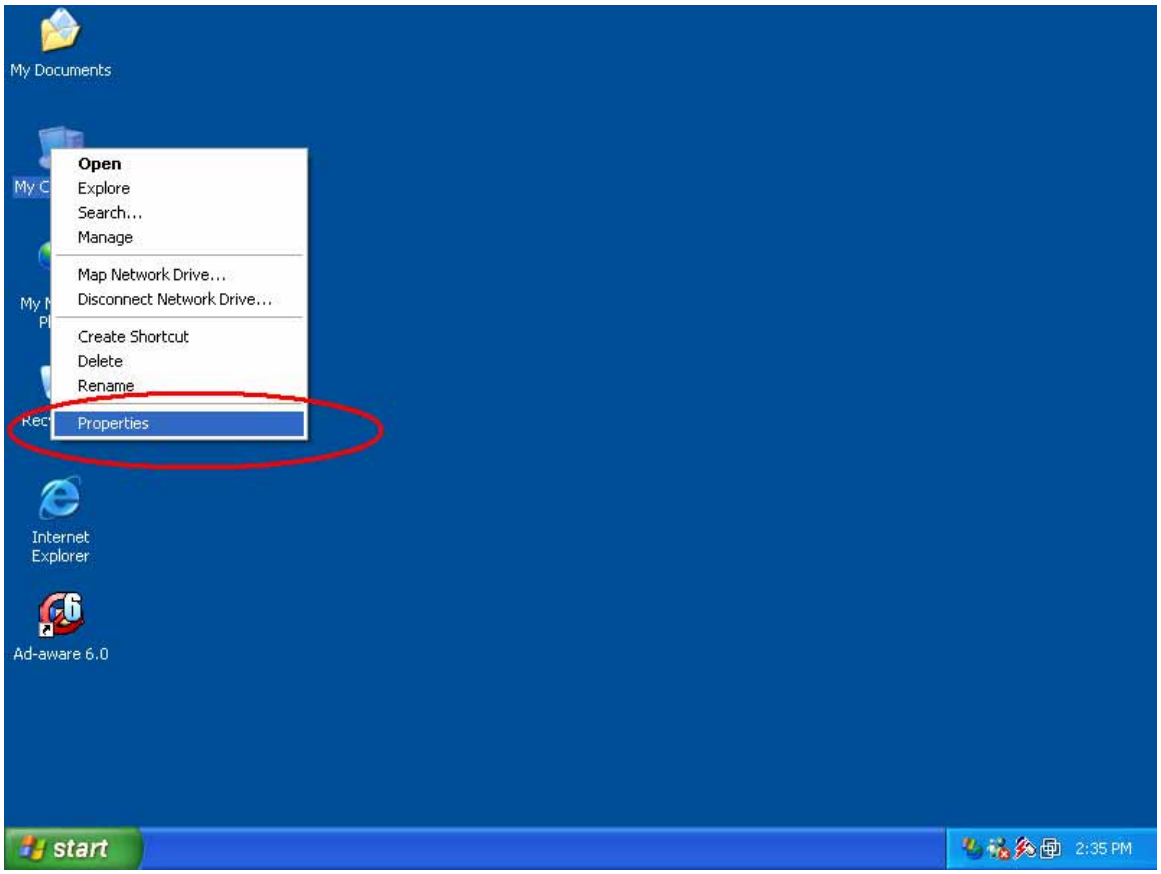


9) After you have installed all the patches, the screen will look like the one below. More than likely, it will probably ask you to reboot the machine. As mentioned in step 8, once you reboot, it's probably not a bad idea to run through this exercise again to ensure all the "Critical Update" patches were installed.

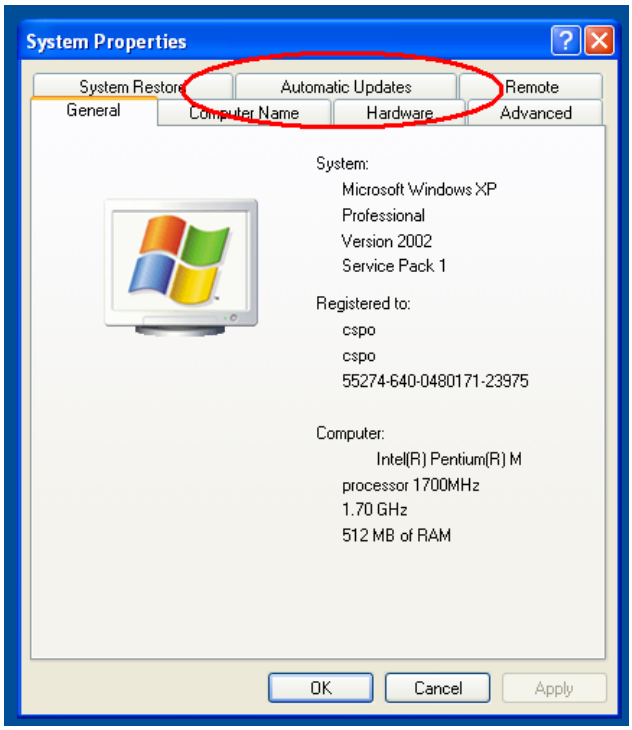


Before we finish our section on patching, there is also a way you can setup so your computer updates automatically. To do this…

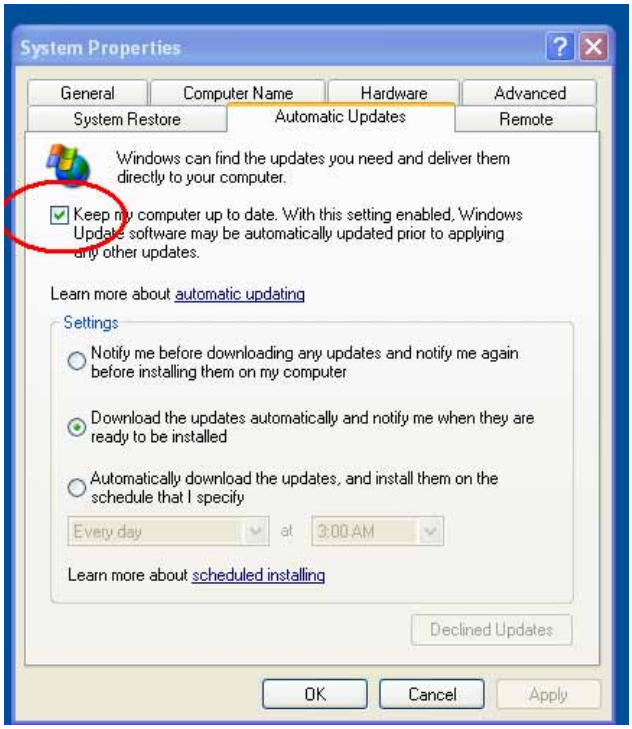
1) Right click on “**My Computer**” on your desktop. Choose “**Properties**”.



2) Choose the “**Automatic Updates**” tab.



3) Once you get to this step, make sure the "**Keep my computer up to date.**" box is checked. This will turn on the auto-update feature.
4) After this is checked, you have three options.
    a. Notify me before downloading any updates and notify me again before installing them on my computer.
        i. This means that when there is a new critical update available, it will cause a little balloon to pop-up in the lower-right hand corner of your screen. It will say "There are new updates to install". Your options will probably be to "Download" the update or "Ignore" it. Once the update is downloaded, you will be prompted again before it will be installed.
    b. Download the updates automatically and notify me when they are ready to be installed.
        i. This is similar to the choice above, but it will download the critical update and let you know when it's finished downloading. From that point, you have the option of installing it or not.
    c. Automatically download the updates, and install them on the schedule that I specify.
        i. Here you can set a day and time when the machine will download the critical updates and install them automatically. Basically, everything is on autopilot and you have nothing to do.



That just about finishes the section on how to patch and update your Windows workstation. It is extremely important that you apply all of the “Critical Updates and Service Pack” patches. It will prevent people from breaking into your machine and will keep everything secure.

How to Install Virus Protection

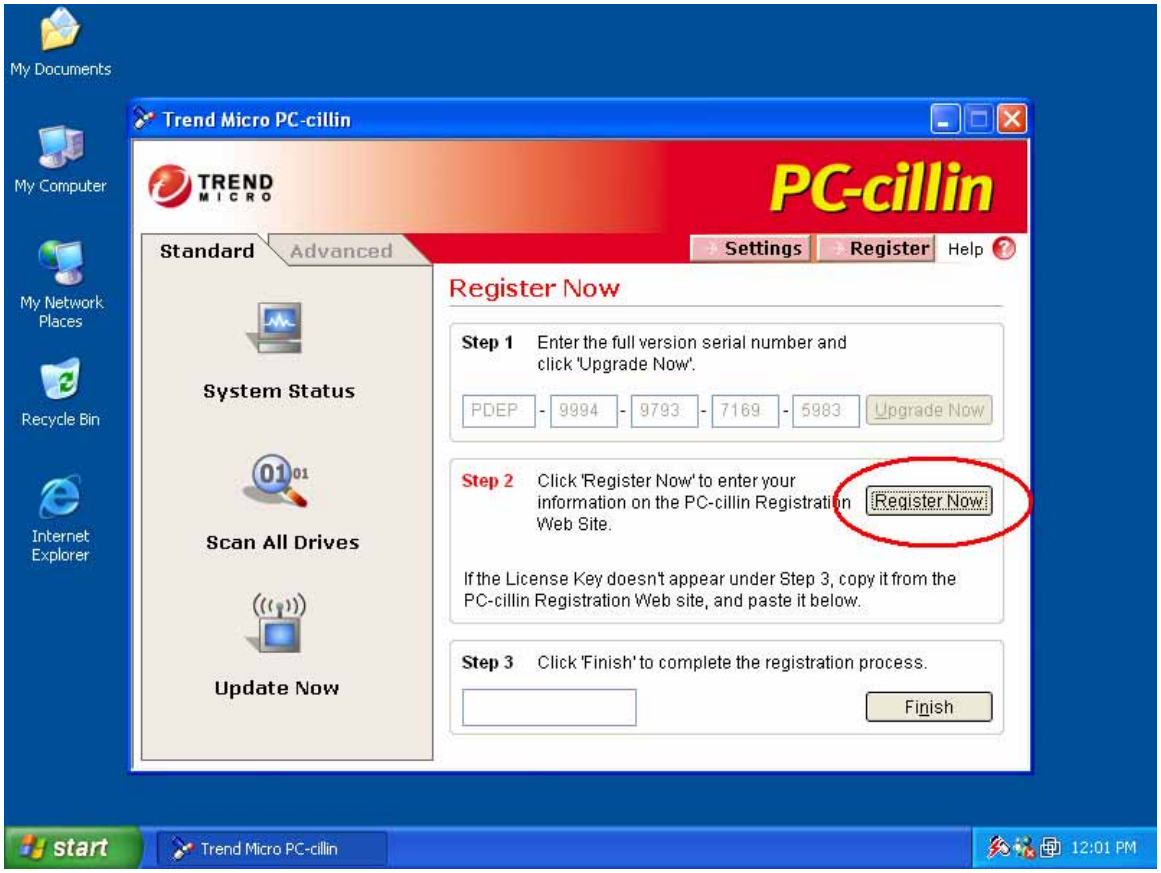
There are dozens of viruses that are written everyday trying to infect your computer. The more time you spend on the internet, the more likely your machine will become infected. Some virus infections are just annoying, others may slow your machine down, and there are even some that will destroy the data on your machine, causing you to loose all your files.

In this section, I will give some insight on how to install virus protection, what is available, how to use and update it. As you may know, Argonne National Laboratory has purchased a site-wide license to use products from Trend Antivirus. In this example, I will use Trend PC-cillin version 2003. At the time of writing this document, there is a new version (PC-cillin 2004), but I find it very confusing to use and hard to configure. There are also other Trend products available, such as Housecall, but I will only focus on using PC-cillin and touch on Housecall.

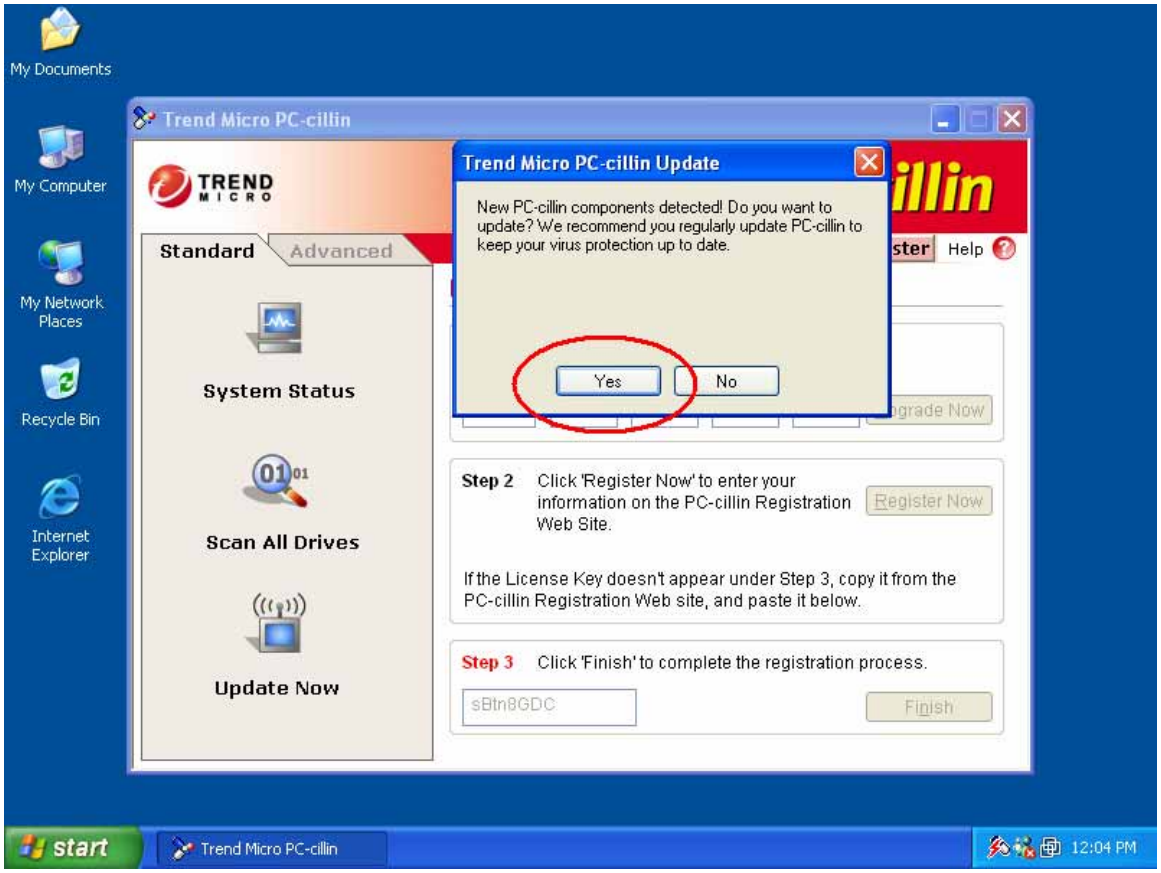
1) The first step in installing the software is somehow obtaining the package to install on your machine. You may be able to download this software from work and burn it to a CD-ROM. You are also able to download the software from home, but it may take some time if you use a dial-up connection.
2) If you would like to use a CD-ROM to install PC-cillin, please contact the Help Desk at 2-9999 and they can arrange to have one sent to you. Open a web browser and visit this page below. However, the page is probably not going to be available to you unless you connect with the VPN client first.
    a. http://www.ccs.anl.gov/trend/default.htm
3) Once there, choose "**PC-cillin 2003**". You will then be taken to a form to fill out. Please fill out the form correctly so that we are able to track the licenses. When you finish completing the form, you are taken to a page that allows you to download the software. In addition to that, please record the "License Number" on this page. You will need to place this in the software when you install it.
4) When you're about to download the file, you are presented with three options. You can either 'open', 'save', 'cancel' or get 'more info'. Please choose "**open**".
5) When you start installing the software, it's best to choose the defaults. You will be prompted to enter your name and the serial number. The serial number is the "Registration Number" that you wrote down in step 3.
6) While going through the installation, it will, if you want to, "**Install the Personal Firewall**". This is really up to you whether or not you would like to do this. I would recommend doing this if you do not have another firewall on your network. However, if you already have a firewall (such as a Linksys cable/DSL router, BlackIce, ZoneAlarm,

etc), it really doesn't make sense to install two firewalls and may only make your machine slower. In this example, I'm going to install it because we will configure it in a little bit. There have also been a few issues with the PC-cillin firewall in the past. Generally, it works well and the way it's supposed to. But there can always be certain circumstances when it may cause you problems.

7) When you finish installing PC-cillin, you will see a box on the screen that says to "Register Now" or "Cancel". You must click "**Register Now**". If you do not register, you will not receive virus pattern updates!
8) You will then be taken to a screen that looks like the one below. Please choose "Register Now"



9) When you register the software, it will ask you for your name and email address. Please fill in this information. When you submit, you will get a "Registration Number". You should write this number down, and then close the window. When you do, you will be taken to the PC-cillin Main screen, which looks like the picture above. However, on this new page, the "Register Now" and "Finish" buttons will be grayed out.
10) After you have completed step 9, you will be asked to "Update PC-cillin". (See screen below). I recommend choosing "**Yes**" to this.



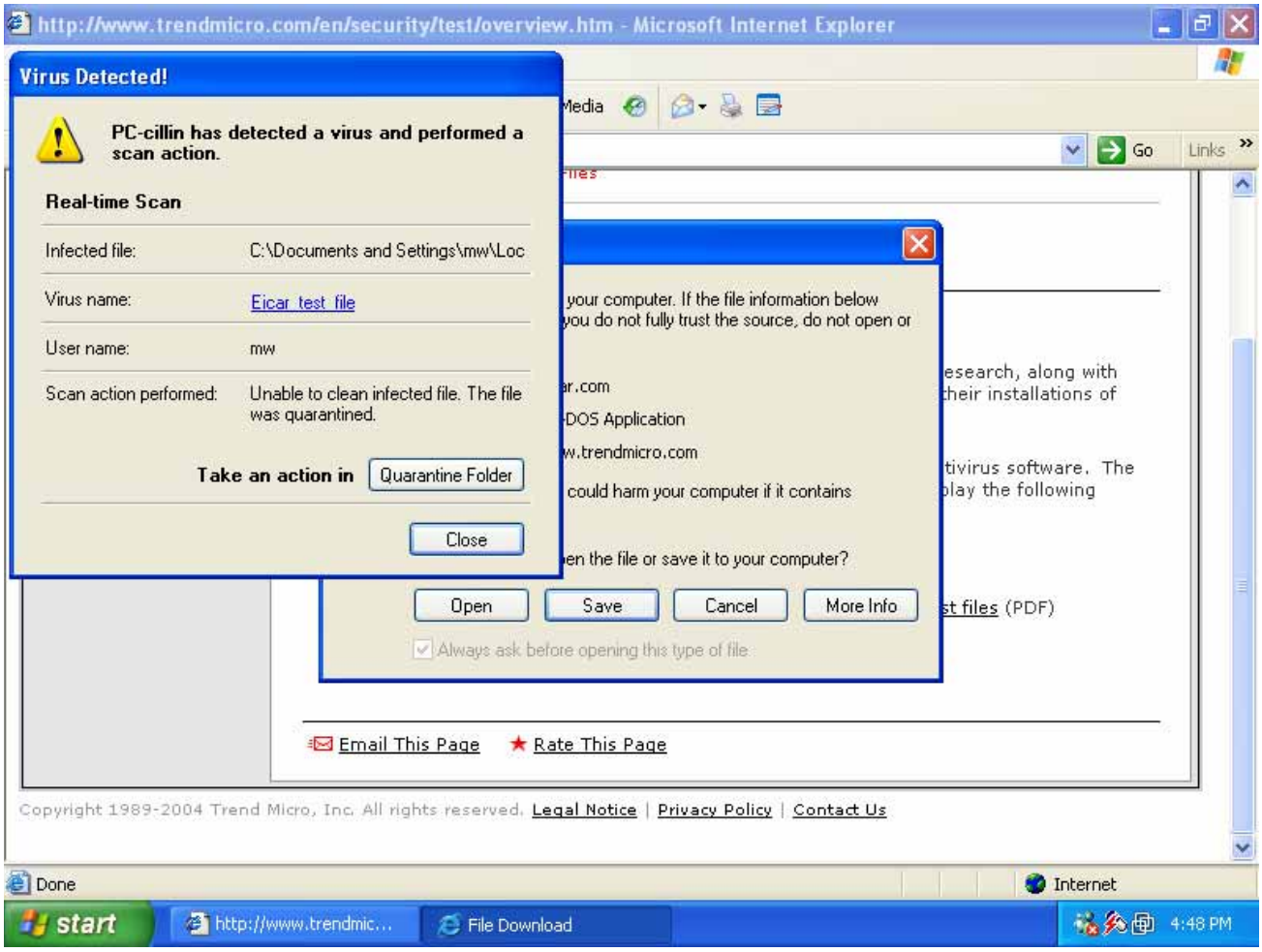
11) Once updated, you may have to reboot your machine in order for the updates to take effect. If reboot is required, it will prompt you to do so.

That should take care of installing your anti-virus software! If you installed the PC-cillin firewall, I will explain how to configure it in the "Firewall" section. There are many other different types of virus scanners out there, but we've had the most luck with Trend Antivirus products. Another good anti-virus program is Symantec Norton Anti-Virus.

Before we get too far ahead, we should probably think about what happens if you do get a virus on your computer. First of all, don't panic! The best thing to do is update your anti-virus software and follow the instructions of how to clean it from the web page. If you go to http://www.antivirus.com, they have a "virus encyclopedia" on the main page. You can either search for a virus in the virus encyclopedia, or click on the virus name to get detailed instructions on how to clean it.

If you don't have virus protection, you may want to check out "House Call" from Trend. (http://housecall.trendmicro.com) This web page will allow you to scan and clean your machine of viruses. If you do have a virus, whatever you do, please **do **NOT** connect to the VPN**! If you do, you may infect machines at Argonne and possibly have your VPN account suspended.

If you are a user of PC-cillin, you might see the message shown in the screen shot below. There is a “test virus” you can download called the “Eicar” test file. This file basically checks to make sure your antivirus real time scanner is working. In the shot below, you can see the infected file (well, part of the directory structure), the virus name, the user, and the scan option that was performed. If you receive this message, it means that somehow, your machine was going to be infected with a virus, but PC-cillin caught it.



Spyware/Adware

In the “Terminology” section, I briefly explained what Adware and Spyware are. Basically, there are some web pages out there that will fool you into installing their software. You may be visiting a web page and a window may pop up asking you if you want to install some software. An example of this was in Step 4 of the “Windows Patching” section. In this section, it was OK to install the software because we were aware of what it was. However, there are some web pages that will trick you to install software that you don’t necessarily want on your computer.

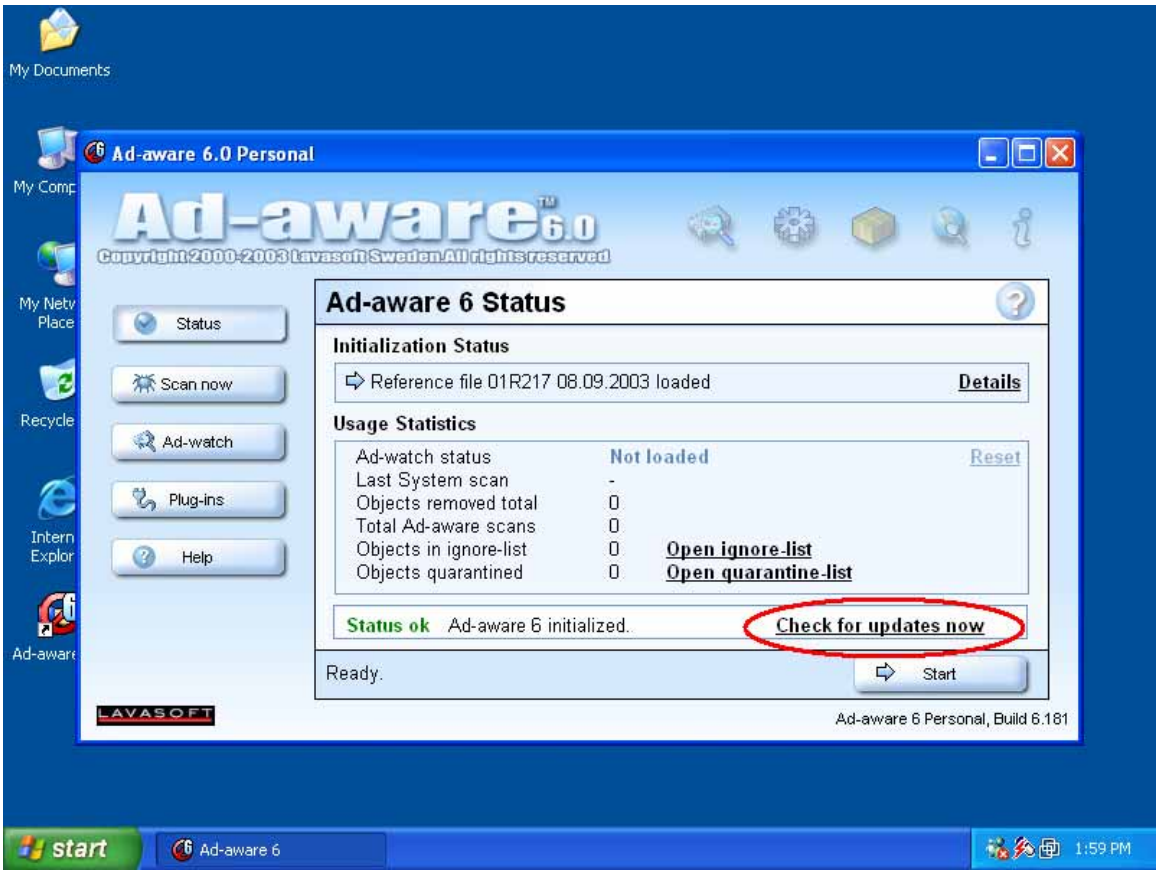
Besides trying to trick the end user into installing the software onto your machine, the spyware/adware may be packaged with certain software installations. For example, if you choose to use a peer to peer file sharing program, such as Kazaa, this company bundles a few spyware/adware programs in it. When you install Kazaa, you also get these additional programs.

After a spyware/adware program is installed on your computer, it will usually track your internet activity. It will record which web pages you may visit. It may also record what keys you press and gather email addresses from this and send it back to the company. After it has gathered this information, you may see ‘pop-up’ advertisements on your computer from time to time. You may open up your web browser and all of a sudden, you will get 5 pop-up windows asking you if you want to buy some sort of product. You may even be doing nothing on your computer and all of a sudden, pop-up’s may start to appear and take control of your computer.

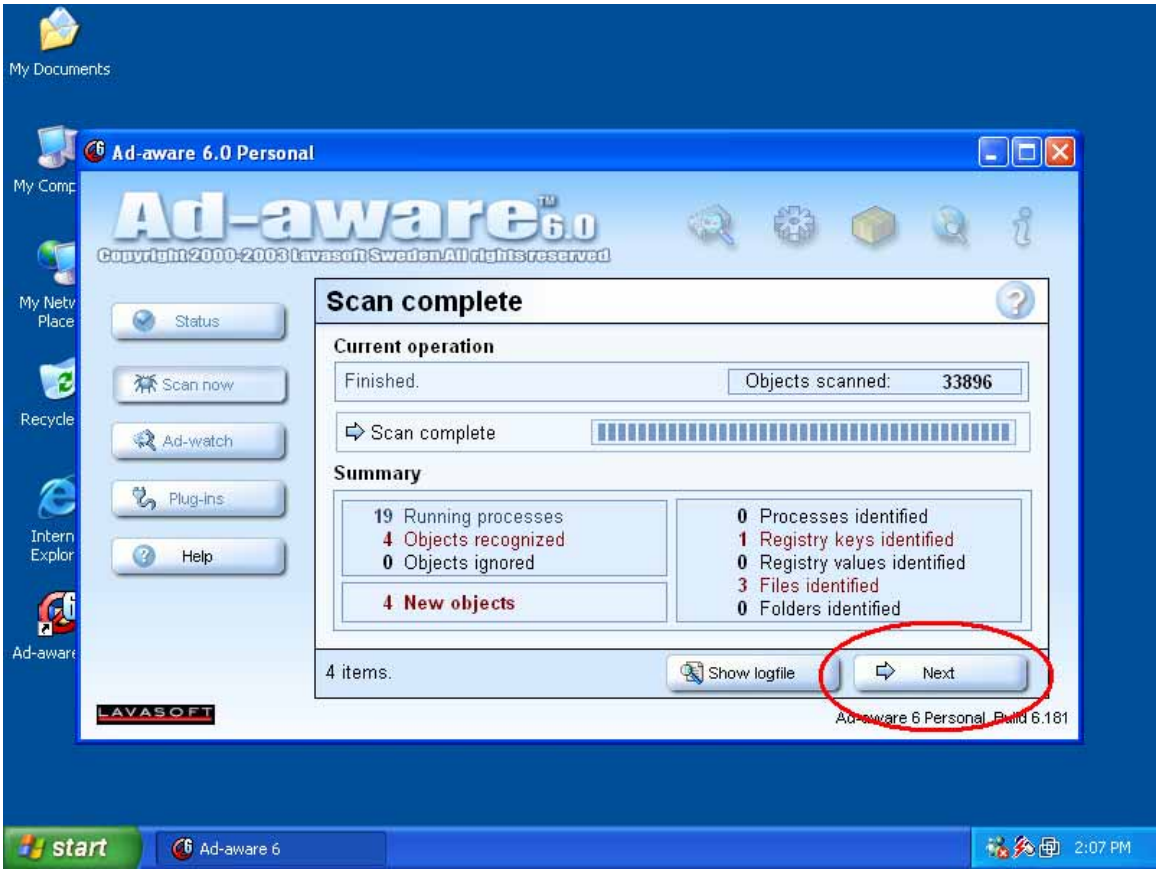
Generally, you usually do not want this software installed on your computer. The most important reason is that it tracks what you do and could possibly send important files to other people. In the very least, you don’t want it on your computer because it may significantly slow your computer (and your connection)!

One way to remove this spyware/adware software is to use a program that is specifically made for this. There are two very good programs you can use. The first is called “Ad-Aware” from Lavasoft. It can be downloaded from http://www.lavasoftusa.com. The other one is called “Spybot: Search and Destroy”. This can be found at http://www.safer-networking.org/index.php?page=download. In this chapter, I will use Ad-Aware and show you how to search and remove spyware. Please be aware that both of these programs are free for personal use!

1) First, you are going to want to install the program. In this example, you would visit www.lavasoftusa.com, and follow the instructions to download and install the software. When you are finished downloading and installing the program, I would recommend choosing the default options, as usual.
2) After you install the software, you're going to want to open the program. Once everything is opened, you are going to update the signature file by pressing the "**Update**" button. After you click update, you will see another box that says "Connect" or "Configure". Choose "**Connect**". Please see the picture below for more information…



3) Once updated, you are taken back to the main Ad-Aware screen. From that screen, you are going to want to click "**Start**". The next screen will look something similar to what you would see when you scan your machine for viruses. You're going to want to choose the defaults and click "**Next**" on this screen. It will now scan your machine for adware/spyware.
4) If it found any spyware on the machine, you will be taken to the screen that looks like the one below. From there, choose "**Next**".



5) The next screen will present you with a list of all the spyware/adware found on your computer. It's usually a safe bet to delete everything. To do this, make sure all the items are checked. If not, right click on an item and say "Select All Objects". From there, click "**Next**".

6) There will then be another screen that will say "*x* amount of objects to remove, "OK"? It's probably safe to say "**OK**" at this box. I've removed spyware/adware from many machines, and so far (knock on wood!) I've had no problems when removing everything.
7) When you are finished with this step, you are brought back to the main screen. From there, I recommend rebooting your computer and running the program again.

Sometimes, certain spyware/adware files are "locked" in memory that can not be removed. If you reboot the machine and run this program again, it should probably clean up all the files that may have been "locked" in memory. In the worst adware cases, you may have to boot the machine up in "safe" mode. I don't recommend doing this if you are not very experienced in using computers. But, to accomplish this, reboot the computer and press the "F8" key numerous times while booting up. You will be presented with a menu of different choices, one of them being "Safe Mode". This means that Windows boots up with the minimum amount of drivers and files necessary to run. After you have reached the desktop, run Ad-Aware and it should remove the files that may have been locked in memory.

Firewalls

In the terminology section, I explained what a firewall is. There are many different kinds of firewalls that are out there. Two of the more common types for the home user are either “Software Based” or “Hardware Based”. Since this is such a great in-depth guide, we will look at both!

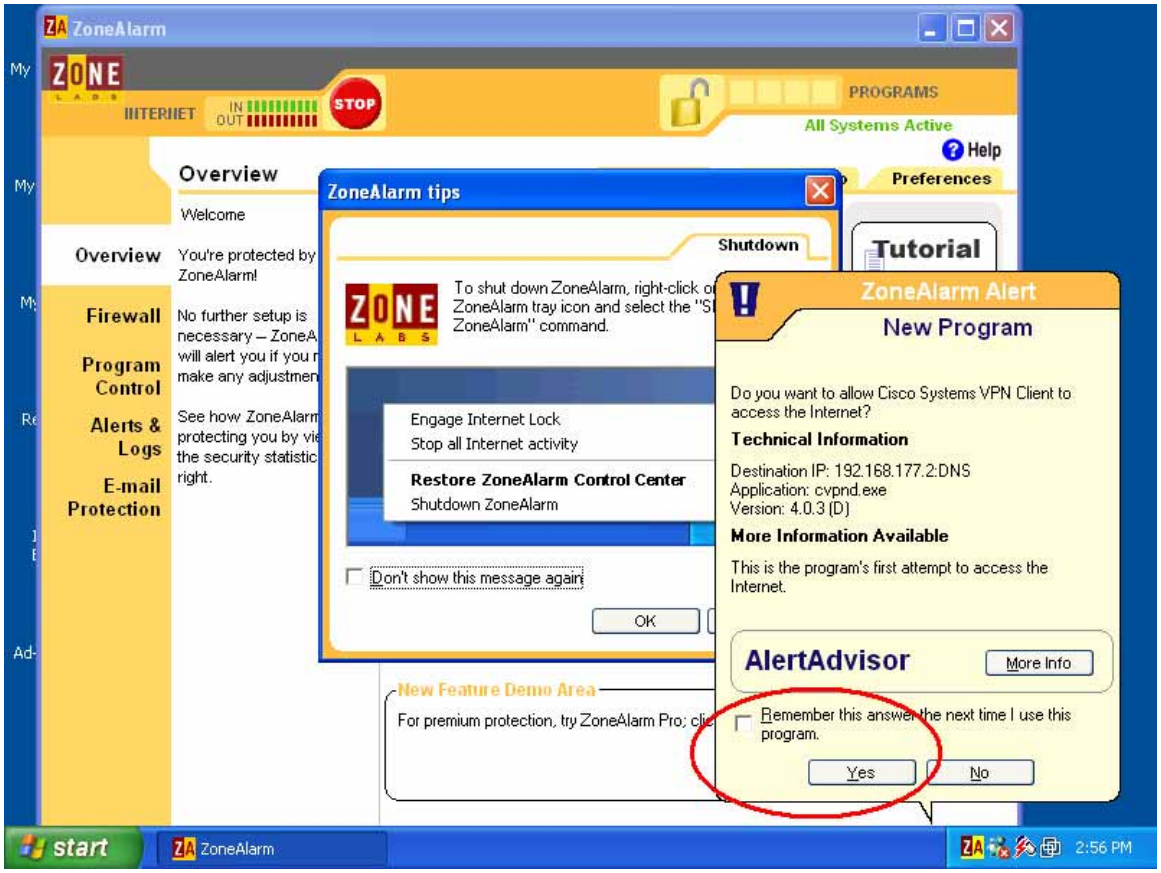
First we’ll compare and contrast each type. The software based firewalls are usually cheaper and easier to configure. On the other spectrum, you may not want to run a software based firewall if you have multiple machines to protect. It’s not very economical to purchase a license (or configure) a firewall on a couple of machines. Also, software-based firewalls have the tendency to corrupt and will prevent them from running on the computer.

On the other hand, hardware based firewalls sit in line with your network. If you have a cable modem or DSL line with multiple machines, I would recommend using one of these. This is better because it’s always on, does an excellent job of blocking traffic, and usually doesn’t cost an arm and a leg. They are not extremely difficult to use and configure, but it does take a little bit of manual reading. No need to worry though, we’ll show you how to configure it in this document. Another plus is that if one of these devices fails, it will just stop the network all together. We hope it never does fail, but when it does, it won’t let anybody in or out!

In terms of recommendations, for a hardware based firewall, I would recommend the Linksys product line. They make good products and have great technical support. Many people around the lab use this product in order to get their broadband up and running. A quick check at CDW shows a 4 port DSL/cable router (the Linksys firewall device) for about $55.00. For a software based firewall solution, I decided to price Zone Alarm, which is one of the more popular solutions. Please remember, they also have a free version that is really a run down version. Granted, it works well, but if you purchase a license, you will have access to a lot more features. According to the ZoneAlarm web site (http://www.zonelabs.com), it is showing a one year update and support license for $49.95. At this price, for about five dollars more, I would recommend the Linksys device because it doesn’t clutter your computer with more software, and it’s yours for life.

In conclusion, the Cyber Security Program Office would recommend using a Linksys DSL/Cable modem router. The model number for the one without wireless is BEFSR41. If you are interested in adding the wireless option, we would recommend model number WRT54G. As for software based firewalls, we feel as if PC-cillin does an efficient job of blocking network traffic. However, if you are interested in additional features or options, such as Intrusion Detection Systems, pop-up blocking, cookie control, cache cleaning, etc., I would recommend looking at ZoneAlarm or BlackIce.

As far as configuration goes, we'll use ZoneAlarm first. After you install the software, it will take you through numerous wizards. The only thing I don't like about ZoneAlarm is that it seems like it keeps asking you a million questions during the first few hours of using your computer. You will have many popups from the lower right corner of your screen, asking you if the program can have access to the Internet. It is a good thing, don't get me wrong. But it just takes awhile to configure the program. You may see a screen similar to the one below.



If you choose to use ZoneAlarm, I would just step through each of these wizards, look at the Application and think to yourself if this program needs to access the internet. If so, choose "Remember this answer the next time I use this program", and choose "Yes". If you also happen to use the VPN with this, you will receive numerous messages like this when you are starting and connecting to the VPN for the first time. Again, I would review the traffic and pop up boxes, but generally, it is probably safe to accept and remember the pop-ups for the VPN client.

If you decide to use PC-cillin for the firewall, there have been a few Connection issues in the past. However, on a recent VPN and PC-cillin install, I experienced no issues with the VPN not working. At the same time, I used the "Default" security policy, which is set to "Medium" in the PC-cillin configuration. If you switch this to "High", the VPN may not work correctly. If you don't know what I'm talking about, it's probably at medium so read on. ☺

Generally, most software-based firewall products are user friendly, so if you try to make a connection, instead of denying it, you might see a pop up with a box asking if you authorize this traffic. The hardware based firewalls are a little bit harder, where they do not have popups. Although, usually with the standard configuration, the typical user does not have to touch this part of hardware-based firewalls.

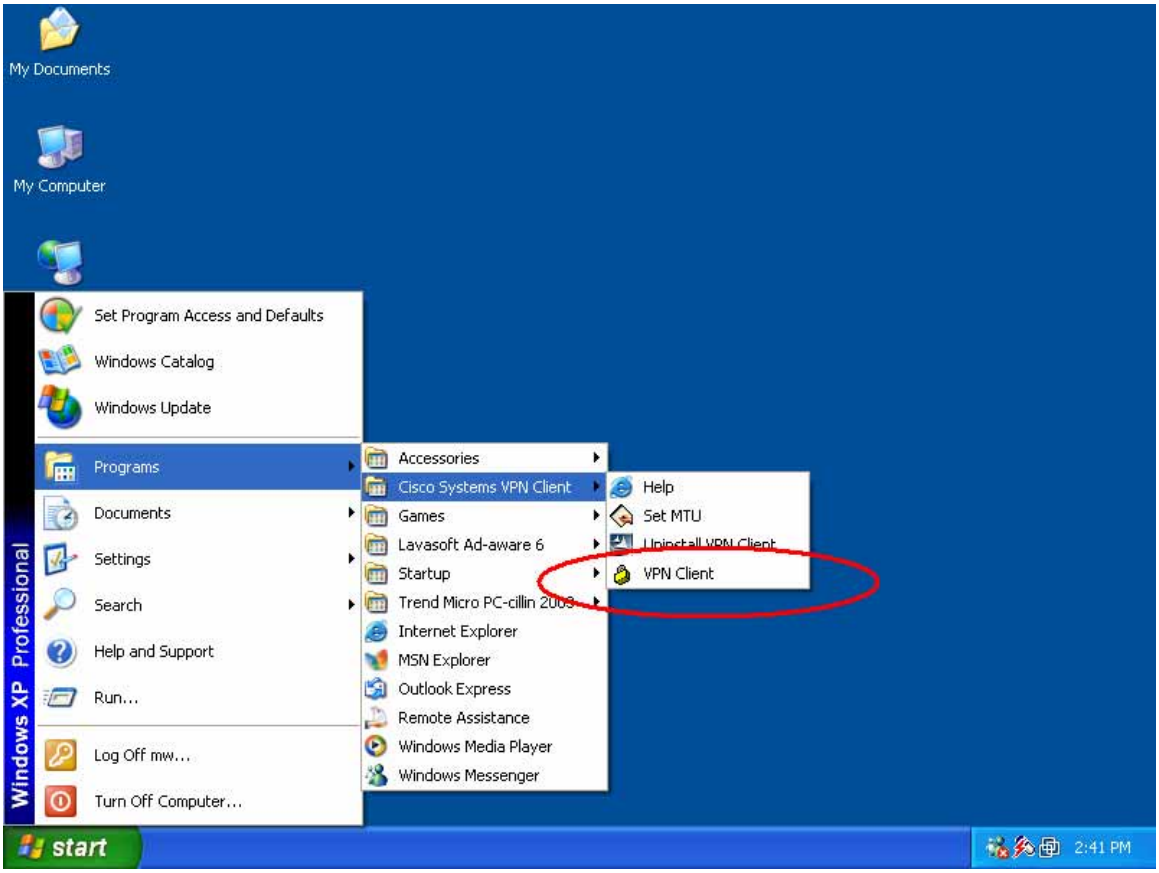
Virtual Private Networks (VPN)

Depending on where you might have worked in the past, you may have used a VPN before. A VPN is a device installed at the destination (Argonne) that will accept connections from your home (hotel, institute, etc.). Once a connection is established, it will encrypt all the data between your computer and Argonne. It is a good idea to use a VPN so other people can not tap into your network connection and see what you're doing at work. In addition to that, it's possible to gather passwords and steal information if you don't use a VPN.

Another good reason to use the Argonne VPN is so your home computer can work almost identical to your machine at work. With a little bit of configuration, you can utilize Microsoft Outlook, map drives, even print things at work all from your home machine!

In order to get cooking with this software, you need to download it from the Argonne web page. It is accessible at https://credentials.anl.gov/VPN/index.htm. When you follow the instructions on the web page to download the software, it should go pretty easy. While you're installing it, I just recommend choosing the defaults and not really messing around with any of the settings if you don't know what you're doing. When it's finished installing, you will probably be asked to reboot.

After you've rebooted, start the VPN by going under "**Start**", "**Programs**", "**Cisco Systems VPN Client**", and then finally "**VPN Client**".



After you start the program, you will see either “ANL-E VPN” or “ANL-W VPN”. Basically, this is self-explanatory. For this example, I will choose “ANL-E”. After this is selected, choose the “Connect” button on the toolbar. You can see this in the picture below.

When you click connect, it will then ask for your “Username” and “Password”. From here, you will type in “ANL\<username>” and password. After that, it will take you to the “Government Banner” that is located on every machine at ANL. Agree to it if you would like to access our network. Going back to the username section. I know that this can get a bit difficult, but I like to tell people that this is the same username and password you use in the morning to boot your computer at work. When you’re at your desk and you login, that is what you would use here. The only difference is that you will put “ANL\” in front of your name. If you are in a different domain other than ANL, you would use the domain name here. Once you are connected, you will see a small padlock by the system clock. The screen shot below shows that.

That should just about get you connected to use the VPN! After this, you are able to configure Microsoft Outlook, connect to network shares, and do whatever you want to. It will work very similar to your machine at Argonne.

Cable/DSL Modem Routers, Firewalls, and NAT's

Since the majority of people are probably going to choose a cable or DSL modem, you are going to want to look into getting one of these network devices. As described in the picture above, it sits between the cable modem and your home computers. It basically acts as a firewall, NAT box, and possibly even a wireless access point. (Don't worry, we'll get into wireless later!). They are pretty easy to setup and they usually work very well.

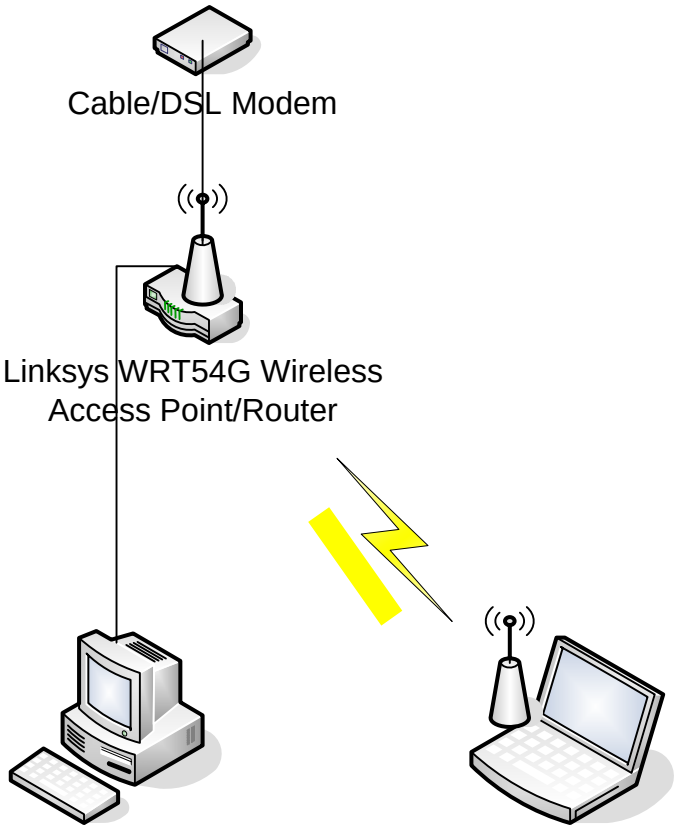
The product line that we recommend is made by Linksys. Granted, there are other products out there from NetGear and other manufactures, but we recommend the Linksys product because we've had the best luck with them.

There are really two different routes to go through when your choosing one of these products. If you have a laptop with a wireless card, you may want to get the Linksys Wireless-G Broadband Router (Part number: WRT54G). At CDW at this time, this product runs approximately $90.00. This device will allow you to connect to the internet and roam wherever you want to, within the range of about 300 feet. It's a great product because you can take your laptop in the front room, kitchen, basement, even outside without worrying if there's a network jack out there! If you are a "gamer" you may also want to think about this option as well. Both the Playstation 2 and XBOX consoles have an 'online connection' option where you can play your games against other people over the Internet. There's a network device that plugs into your PS2 or XBOX and gives you an Internet connection without running a wire for it.

However, if you do not have a use for a wireless connection, you may want to look into the "Linksys Instant Broadband EtherFast Cable/DSL router (Model number: BEFSR41). This product retails at approximately $55.00 from CDW. It's very similar to the product above, but it does not have the wireless option. Instead, it includes a '4-port switch' so you can connect up to 4 computers to this device. If you would like to connect more than 4, you can purchase a switch and expand up to 255 computers.

As I mentioned before, for the cost of $55.00 for the non-wireless model, I would highly recommend a user purchasing this for their cable or DSL modem. It won't protect you from viruses through Email or programs, but it will protect you from network viruses and people trying to hack into your computers.

For configuring these devices, it's good to use the same diagram as in the "wireless network" section. It can also be seen here…



As you can see in the above example, the Linksys DSL/Cable modem router is plugged into your cable modem. Your cable modem (or DSL modem) is then plugged into either a phone line or coax cable, depending on what type of service you have. Moving through the diagram, the computer is then plugged into the Linksys device using a network cable. In this diagram, there is also an optional wireless client that is attached to the Linksys device.

Once you have it all hooked up, the next step is to configure everything. The Linksys device is fairly easy to configure and should be pretty much ready to go. However, if you want to configure it, you must make sure your computer is set to "DHCP". This can be done by doing the following…

1) Clicking on "**Start**" and "**Network Connections**". From there, you can find your network card in the list that is provided. If it is not listed, it probably means that the driver for the device is not loaded or something may be wrong with it. The bottom line is that windows can not see this network card for some reason.

After you are in the “Network Connections” section, you are going to want to right click on the adapter and choose “Properties”. Then, another box will pop up with a bunch of different options. You are going to want to choose “**Internet Protocol (TCP/IP)**”. You may have to scroll through the “This connection uses the following items:” section. When found, click once on this so it highlights the item and click “**Properties**”. When the next box pops up, ensure that “**Obtain an IP Address Automatically**” and “**Obtain DNS server address automatically**” are selected. Click “**OK**”, then ‘**OK**” again to close the “Local Area Connection Properties”.

2) Once you have DHCP Setup, open “**Internet Explorer**” (or your favorite browser) and type in **192.168.1.1** in the address bar. You will then be asked for a password. The password should be included in the directions on how to configure your Linksys router.
3) Once you are inside of the configuration, everything should pretty much be setup and configured correctly. A few options to check are…
    a. Underneath the “**Security**” configuration and “**Firewall**”, ensure that “**Firewall Protection**” is “**Enabled**”. This will prevent people from hacking your machines by blocking the majority of the open ports that are open.
    b. Underneath “**Security**” configuration and “**VPN**”, ensure that IPSec, PPTP, and L2TP Pass-through are all “**Enabled**”. This will make sure that you are allowed the proper access in order to use the Argonne VPN Software.
    c. Underneath “**Administration**” configuration and “**Management**”, you may want to change the “**Router Password**” to something other than the default. Also, ensure that “**Remote Management**” is “**Disabled**”. The password is used to configure the device. By common knowledge, it is usually a good idea to change the default password to something else. This password is used when you first call up the web page in order to do administration. The second choice for Remote Management is used for managing this Linksys device from somewhere else on the Internet. For example, it is setup now for only allowing administration by connecting to the device locally. If you “enable” this, this will let you manage and configure this device from other networks, such as Argonne or anywhere else. Generally, you want this disabled.

Wireless

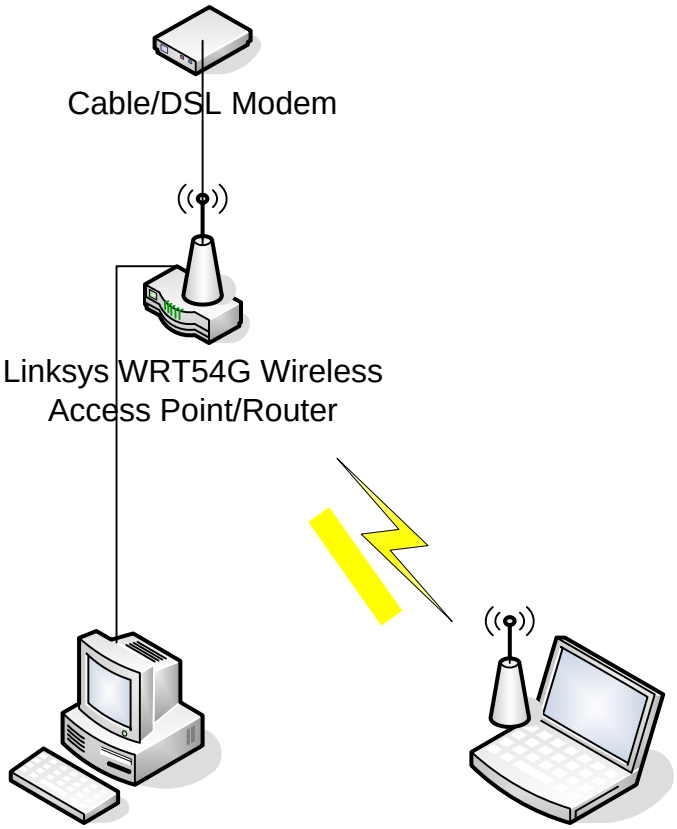
Wireless networking is becoming more and more popular as time progresses. Before wireless, you had to have a network cable (similar to a phone cable) connected to each computer you wanted on the network (Internet). As technology advanced, wireless network evolved into the computer realm.

To understand wireless better, I will compare it to a telephone, since almost everybody is familiar with the phone and how to use it. Back in the 70's and 80's, if you wanted a telephone, you needed to have a wire connected to it and you can only travel the distance the wire would let you. As telephone technology got better, they came out with 'wireless' phones. If you had a phone like this, you knew you could walk around your house and still be able to talk to people. Granted, you couldn't walk down the block because if you did, you would be out of range for the phone.

Wireless technology for computers works basically the same way as the wireless phone does. You have a "base station" (Wireless Access Point) that is the transmitter for the wireless access. You could compare this to the base station for the telephone where you actually plug in the phone cords. You then have a wireless network client, that can either be PCMCIA or PCI cards, or it may even be built into your computer or laptop. This part can be thought of as the "telephone receiver" end. However, you don't need to place the device back in the base station (access point) in order for it to recharge!

As time passes, technology changes and the wireless speeds are getting faster and faster while enabling security inside the device. If you are using a wireless access point, it is an extremely good idea to be able to "lock down" the device and make it secure. In this section, we will talk about how to lock down an access point so other people can't use it. Since the range on these devices are approximately 300 feet, it is easy for your neighbor to steal free internet access from your access point. And, after all, since you are paying good money for it, do you really want you neighbor to use it while you have to pay for it? There are also numerous stories that have been written on hackers that 'war-drive', which is looking for open internet access points. Once they find a wireless connection, they will hack your machine, or possibly other machines. The IP address will be traced back to you (not the hacker), and when the authorities look to see who did it, you will be showing up on their radar screen. Bottom line, make sure you lock down your access points.

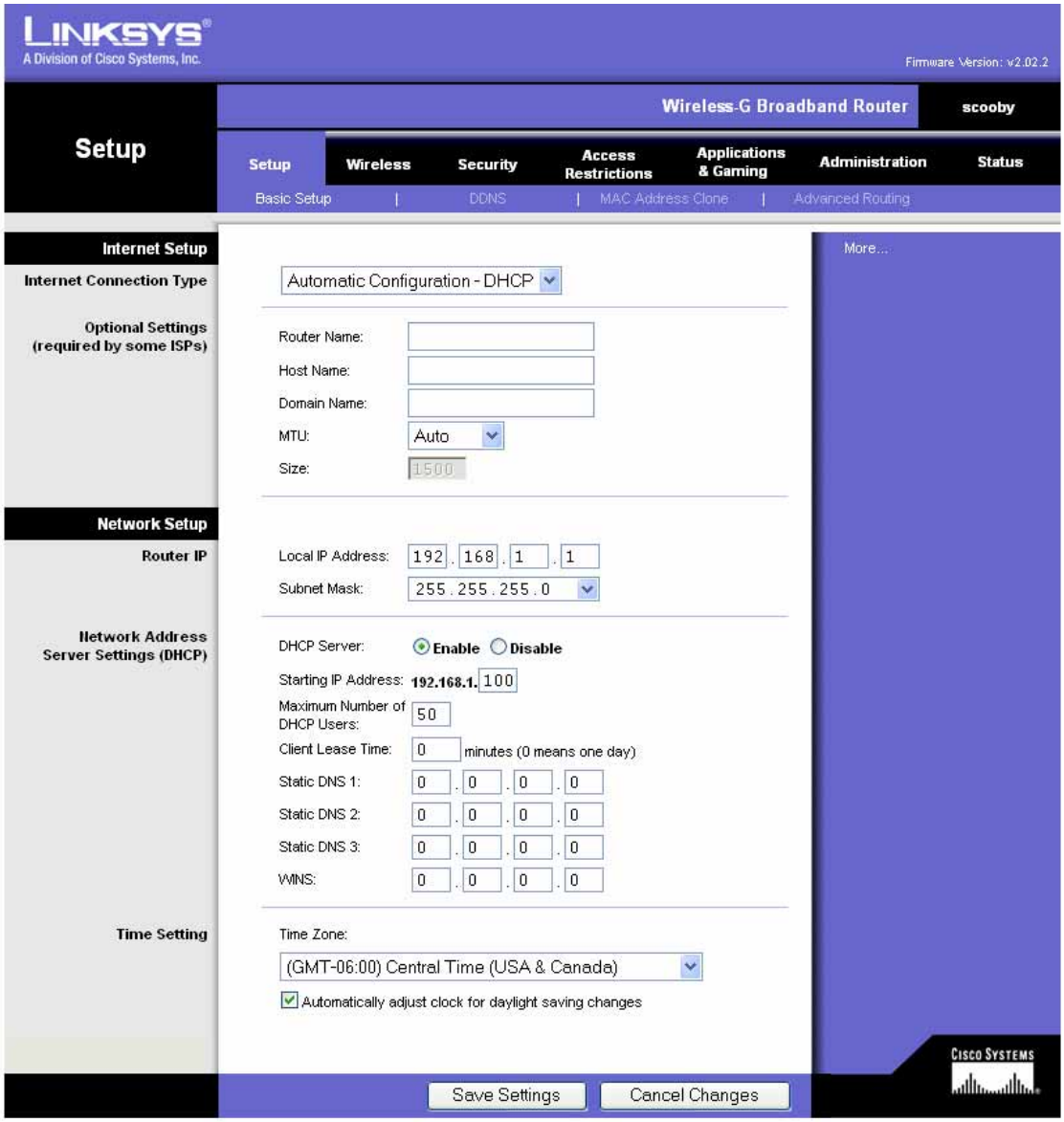
To do this, we will use an example of a Linksys access point. Once you plug in your Linksys Cable/DSL Broadband router/Wireless Access Point, your network might look something like the picture below…



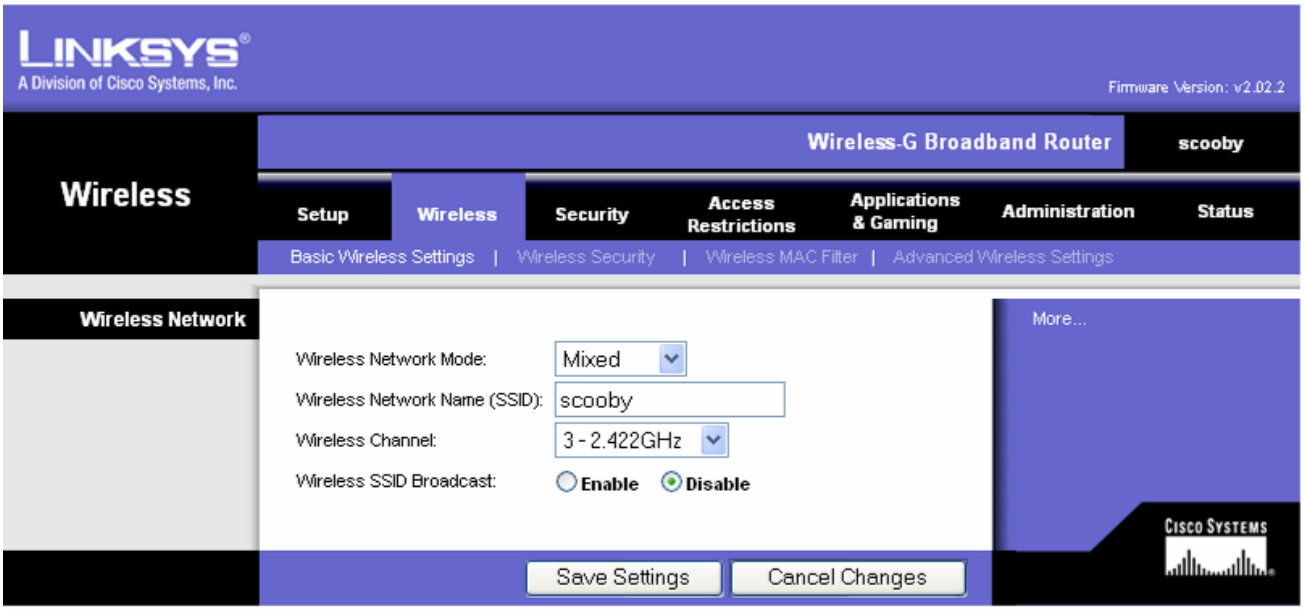
In this example, there is the cable/DSL modem for your high speed internet access. From this device, it plugs into the Linksys Broadband DSL Modem/Router/Wireless Access Point (Model WRT54G). From that point, you can have another network cable plug into your desktop computer, and/or you may have a laptop (or other portable device) that wirelessly connects to the Linksys WRT54G. Granted, there may be some variations in the above picture, but I believe most network setups are going to look like this.

Once you have completed the step above, you need to configure this Linksys device to work with your network. The following are just screenshots and explanations of a general network configuration with a cable modem. Your configuration may look different or it might need some specialized tweaking. In addition to that, below are recommendations to "secure" your wireless access point so nobody can access it but the people you authorize. Finally, the following should be done while you are connected to the access point using a network cable. You can configure it wirelessly, but it is not recommended since some changes will need to be made on the access point and your client computer. One change that comes to mind are WEP keys.

1) Open the configuration of the Linksys router. In order to do this, open a web browser and type in “192.168.1.1” in the URL field. This will take you to the configuration screens after you enter the default password.
2) The picture below is the default page for the device I’m configuring. Your Linksys configuration pages may look different depending on which version of the firmware you are using, but I’ll get into that later.

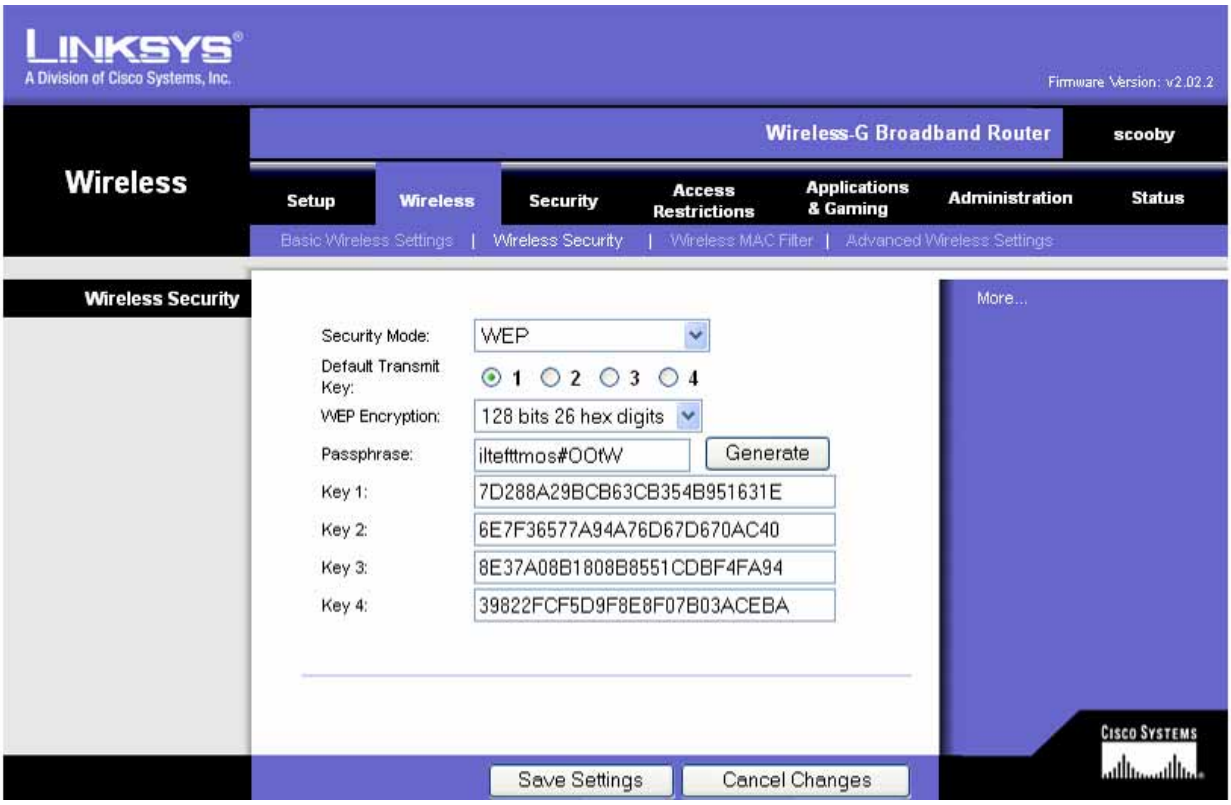


3) As you can see above, you shouldn’t really have to change much on the first page, or really any other pages except the Wireless page. However, if you click on the “Wireless” section, you will be brought to a page that looks like this…



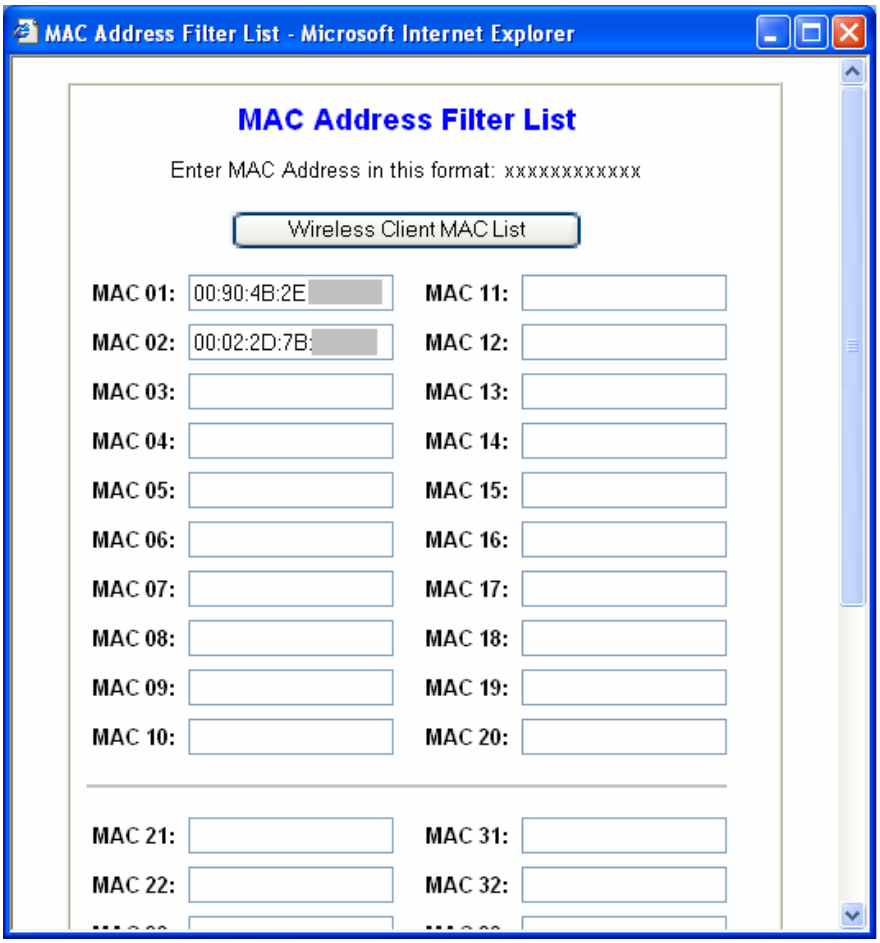
4) From this screen, you will see a few options. The first one is called "**Wireless Mode**". This is used to specify the connection speeds you want. In this model, we either have "B" (11 Mbps) or "G" (54 Mbps) to choose from. In "mixed" mode, it will take either the B or G standard. The second choice is called "**Wireless Network name (SSID)**". In this field you can really type in whatever you want as the name of your access point. On your computer, you will see "Connect to…" and in the example "Scooby" will pop up as a choice. This field just 'names' your access point. The field after that is called "**Wireless Channel**". This is the channel you would want your access point to operate on. The default is 6, but you have 1-11 to choose from. Since I had some interference from other access points and my telephone, I chose Channel 3. (The symptoms would be random disconnections even though you have a strong signal on your laptop). Finally, the "**Wireless SSID Broadcast**" means that you will broadcast your access point name to anybody. You can really disable or enable this if you want to since we will specify who can connect to your machine below. I recommend disabling it because I feel the fewer people who know what's out there, the less chance I have of somebody stealing my internet. However, by disabling this, it will take a little bit of configuration (just remember your SSID, or what you named your wireless network) in order to get this to work.
5) After you configure this, you will have to configure your WEP encryption. The picture below shows what it may look like. It is a good idea to enable WEP (or another method of encryption) from your client machine to the wireless access point. If you do not enable this, it is very easy for somebody to sit in front of your house and capture all the data you are entering over the Internet. By enabling this, it will make it harder for somebody to break into your access point and view the

information getting sent across the network. Going back to the configuration, I would recommend choosing the options I chose below. However, for the "**Passphrase**", create your own and do not use the one I have below. The passphrase is just something that will be used to create your keys. After you choose a passphrase, press the "**Generate**" key and this will generate all of the hex numbers in "Key 1" thru "Key 4".

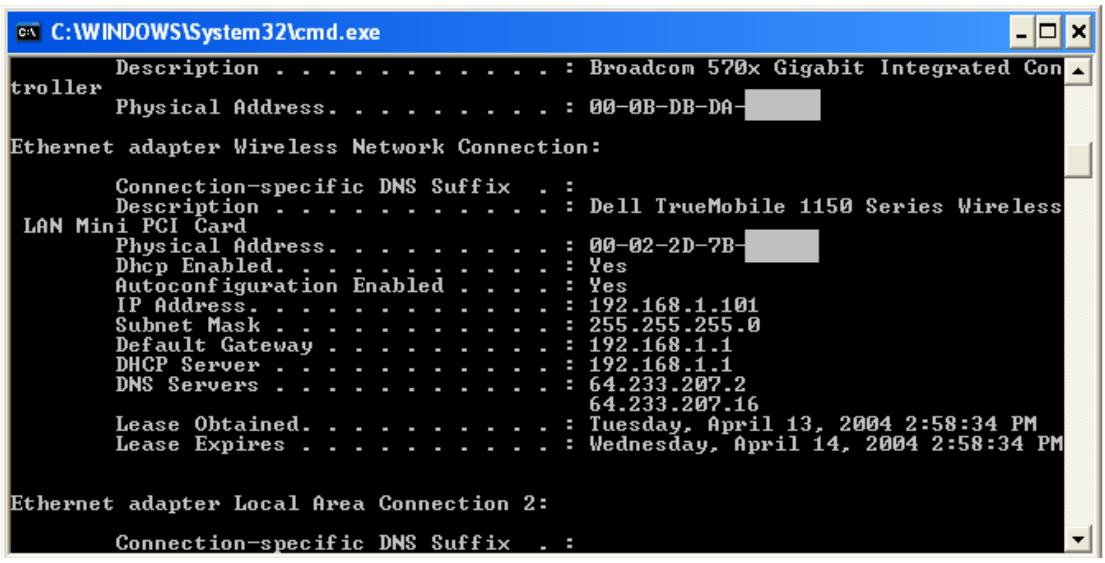


6) After you have completed this step, you will need to write these fields down. Since there are numerous lengthy fields, I would recommend copying and pasting them. You can do this by highlighting each of the key fields and using "CTRL-C" (for Copy). Then, open notepad (click on **Start**, **Programs**, **Accessories**, **Notepad**). I would recommend making a few notes, such as "Key 1 – xxxxxxxx", "Key 2 – xxxxxxx", etc. You can paste the keys that you copied by using "CTRL-V" in Notepad. After that, you can "save the settings" in order to make the changes permanent.
7) In this step, we are going to configure MAC Address Locking. A MAC address is actually a unique, physical address assigned to every networking device in the world. It looks like a series of numbers and letters (Hex). An example would be "00-02-9A-3C-78-06". In the two pictures below, you will see what it looks like to configure "MAC Address Locking". I would highly recommend doing this because it will limit who can connect to your wireless access point. By entering the

MAC address of your laptop, it will only allow that unique MAC address to connect to it. In the example below, you will see that I enabled the "**Wireless MAC Filter**". I also chose to "**Permit Only**" MAC addresses in the MAC Filter List to connect to your access point. In the second box underneath the configuration options is the 'MAC Address Filter List". Here you would put all the MAC addresses of your wireless machines. As you can see, the only MAC addresses that can connect to my access point are listed below. In order to find out what your MAC address is, see the next step.



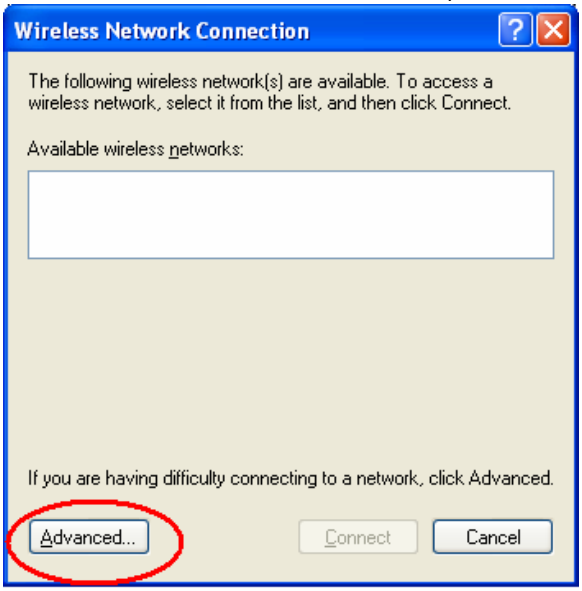
8) Now we will tell you how to populate that MAC Address table! To find out what your MAC Address is, go to "**Start**" and "**Run**". Type in "**cmd**" and hit enter. This will take you to a command prompt, such as C:\ <*directory name*> >. At this prompt, type in "**ipconfig /all**". Listed below is an example of the results. The important line to key in on is "Dell TrueMobile 1150 Series Wireless LAN Mini PCI Card". This is my wireless network card, however, yours may be called something else. More than likely, it will have the name "Wireless" in it. My MAC address is 00-02-2D-7B-xx-xx (I blanked the last 4 digits out). If you scroll up a little to the previous picture, you will see this address entered in the "MAC Address Filter List" for the Linksys router. Do the same for your laptop/desktop (or any other network device) you would like to have on the network.



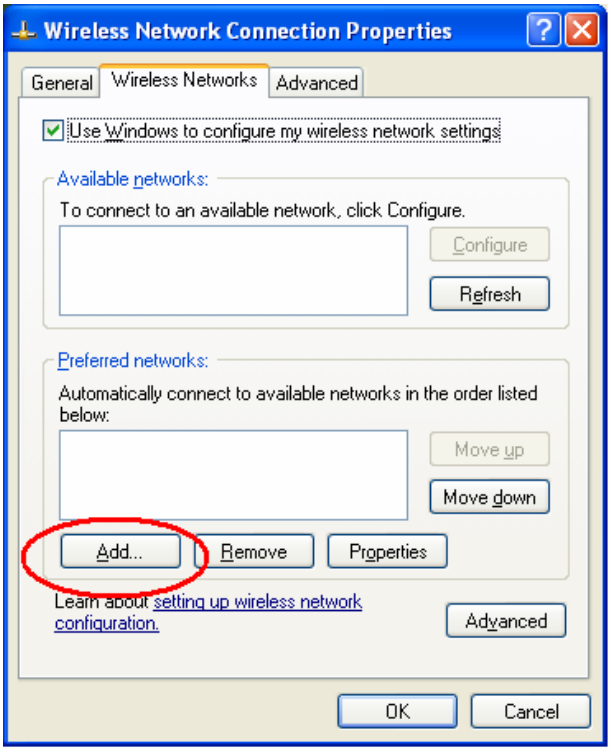
9) The very last command is called "**Advanced Wireless Settings**" in the Linksys Wireless Network configuration. We will completely skip over this since nothing in here would probably need to be changed. I would highly recommend leaving all these options set to default.
10) If you are interested in configuring other options, please see the Cable DSL Router/Modem/NAT section.

To configure the local machine…

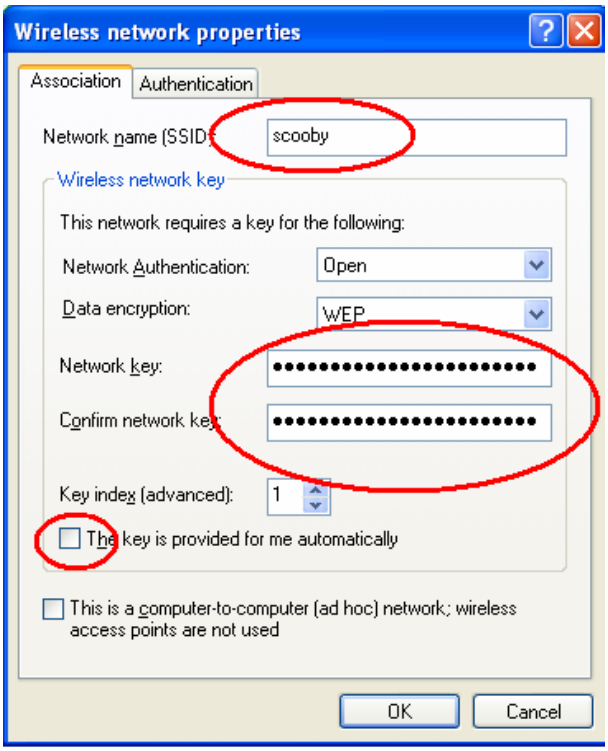
1) Go to "**Start**", click on "**Settings**", then click on "**Network Connections**".
2) Right click on "**Wireless Network Connections**", and choose "**View available wireless networks**". After that, choose "**Advanced**".



3) From there, you will see a box that may have some wireless access points (Available Networks) to choose from. Since we specified not to broadcast the SSID, we will have to "Add" a wireless access point. In this box, choose "**Add**".



4) In the next box, you will have to type the name of the SSID in the space provided. In our example, we will use "Scooby" for this.
5) Make sure the box that says "The key is provided for me automatically" is not checked. Then, you can enter in your WEP key in the "Network Key" space. The "**Network Key**" is actually your "Key #1" in the Linksys Wireless Security section. Please see the picture below step 6 for more information.
6) After you choose "OK", you should be connected within a minute or so. Please see the diagram below for more information.



That should just about finish up the configuration of wireless access points. You have learned how to configure the Linksys Wireless Access Point, setup WEP, make the connection so others can't "listen in" (sniff) our network traffic, to only allow certain people to connect to the access point, and configure the wireless network client.

Encryption

In other sections, you may have heard about Encryption. This is a method that's been used throughout time to hide messages so prying eyes can't see. The simplest encryption method might be taking a message such as monitor, and counting three letters down in the alphabet for each letter. Monitor would turn in to "prqlsxu". Without knowing how to decrypt this, it would just look like junk. This is a simplified form of how computers encrypt data. Naturally, computers can encrypt with much more advanced algorithms because who wants their credit card information transferred across and have somebody see it. I know I don't!

This is really the basic idea behind encryption. There are many ways to know you are transmitting encrypted traffic. One way is through Internet Explorer. You may see https:// on the URL bar. You may also see a little "padlock" at the bottom right corner of Internet Explorer's window.

Another form of encryption is using a VPN. As mentioned in a previous chapter, a VPN encrypts all the data from your home computer to the Argonne network so other people can not see what you're doing. Instead of using the VPN, some divisions may choose to use 'ssh'. SSH stands for Secure Shell. This is a protocol that is used across the internet to encrypt traffic. Before SSH, many used 'telnet' to 'call' other computers on the Internet. The drawback to telnet is that everything is passed across in clear-text. Since it is extremely easy for people to see what you are typing, DOE (Department of Energy) decided to block clear-text passwords (IE: stop people from using telnet) on the network. As an alternative, ssh is used. It works the same as telnet, but just encrypts the data so nobody else can see it.

It is also possible to "tunnel" ports through SSH. I'm not going to get into the details because they are lengthy and boring, but some divisions may choose to do this as an alternative to the VPN. If you are really interested in tunneling protocols through SSH and need assistance doing this, please see your system administrator, or feel free to shoot me an email.

Conclusion

In conclusion, I hope that this document was helpful to you! I tried to cover most of the cyber security topics that are very important for home users to know. If I may have missed something you think is important, please shoot me an email at wiz@anl.gov so I can modify this document appropriately.

You have, no doubt, already learned that technology changes. So this will always be a work-in-progress-type document. I hope this document has provided a lot of useful information, and that you can now better understand technology and how important it is to secure it!

Links

Here are some additional links that will provide excellent information. Please use these for informational purposes only since we are not aware of the content on the sites.

http://www.tom-cat.com/security.html - Securing your Home Computer

- By the time you reach the end of the list you will have acquainted yourself with all of the basics required to take control of and maintain your privacy and security over the Internet. To the novice computer user this may seem like a lot of information to absorb, yet if you are patient and take each item one at a time you will soon realize how uncomplicated this really is. Above all, don't be intimidated. No one learns everything in a single day.