

12 Things You Can Do Now, To Improve Your Security

Ben M. Schorr
ben.schorr@scgab.com

“A journey of 1,000 miles begins but with a single step.”

Securing your systems and your data is a tremendous undertaking and one that grows more complex and more important with each passing hour. Rather than just throw your hands up and surrender, however, there are a few steps you can take right away to significantly improve your security. To keep this list to a manageable number I had to be selective about which tips I'd offer and towards that goal I prioritized steps and ideas that can be done quickly, for little or no cost and without a tremendous amount of technical knowledge. These steps are a good start, from here you can work in conjunction with your Information Technology (IT) staff or consultant to further secure your systems and data.

So let's get started...

Security Is a Process Not a Product

The first thing to understand is that there is no one product out there that can ensure the security of your systems. Actually that's not entirely true; if you would like to defend your systems against intrusion from the outside a pair of wire cutters will accomplish that task – you simply snip the cables of all incoming lines. Of course that's not a very practical solution. Security is a constant balance between keeping your systems secure and being able to use them to accomplish your daily tasks. Generally the more security you add the more difficult the systems are to use.

There Is No Silver Bullet

Security is really about the policies and procedures that you put in place to secure your systems. The products you use: firewalls, anti-virus, Active Directory, heuristic scanners, biometric authentication devices and other such are simply tools to help you implement and enforce those policies and procedures.

There Are Seldom Good Technological Solutions to Behavioral Problems

If you have users who are deliberately trying to circumvent your security policies don't waste time and money trying to find a new piece of software to stop them. Sit them down and make it clear to them that their continued employment depends upon their adhering to company policies with respect to the information systems. Make sure your

policies are agreed to by top management and make sure they are included in your employee handbook.

This last point is absolutely crucial. If you don't get complete buy-in from top management this approach is doomed to failure. For the policies to be effective people need to know that the people who have control over their employment with the firm are serious about these policies.

You can't afford to keep people that you can't trust.

Never Stop Learning and Improving

Every day there are new exploits, new patches, new tricks and new information. Don't rest on your laurels just because you feel that you have defeated yesterday's hack. There are a number of websites such as <http://www.securityfocus.com> which are dedicated to helping you stay up to date on the latest thoughts in information security.

Here are three more:

- <http://www.microsoft.com/security> - Microsoft's dedicated security site
- <http://www.cert.org/> - Carnegie's Mellon's Emergency Response team.
- <http://www.antionline.com/> - From Enterprise IT Planet.

If you have the time and interest there are also two books that I recommend.

- "Secrets and Lies" by Bruce Schneier.
- "Hacking Exposed" by McClure, Scambray, et al.

Either of those books should be available at a decent sized bookstore or thru on-line booksellers like Amazon.com.

Don't Wait

Hackers and malware aren't going to wait until you're ready to deal with them. Confucius said that the superior man strengthens himself constantly. Start today, right now. (okay, you can finish reading this article first)

Document Everything

Documentation is one of those jobs that few people like to do, but it can make a very big difference in the quality of your assessments and in identifying and troubleshooting problems. It can also save you a lot of time and money if you should ever need to bring in an outside consultant to assist you. Your documentation should include the basics such as identifying each of the systems connected to your network, locations and versions of data and applications, as well as model numbers and versions of any hardware you're using. Don't forget to document any changes you make and troubleshooting steps attempted.

If you want to get fancy tools like Microsoft's Visio (<http://www.microsoft.com/visio>) can help you to produce some really useful documentation. What's important is that the information be complete, accessible and understandable.

By the way, keep track of your documentation. If it falls into the wrong hands it makes for a handy roadmap for somebody else to find your vulnerabilities.

Now let's take a look at the steps you can take to start securing your systems.

#1 – No More Passwords

The vast majority of computer systems today use some kind of password in order to authenticate users and a primary goal of hackers is to figure out those passwords in order to gain access to the systems and the data contained therein. The techniques for breaking those passwords vary but one of the simplest is called a Brute Force attack. There is nothing subtle about this method of attack, it simply tries all of the possible combinations of password until it finds the correct one. A modern PC can try tens of thousands of combinations per second and it doesn't matter what kind of encryption or code you use, sooner or later it will find the password. Even if you choose something totally random: 4dAx93 for example that password will be easily cracked in a matter of minutes by a brute force attack. It's not a matter of random; it's a matter of length. That password is only 6 characters long and even with the numbers and mixed case letters there are only 56,800,235,584 possible combinations. A modern PC can try that many combinations in a matter of hours – and it's not likely to have to go through all 56,800,235,584 combinations before it stumbles across the right one.

The key to defeating brute force attacks -- and to some degree their more sophisticated variant the Dictionary Attack – lies in the length of the password. The ideal password is 15 or more characters long, however it can be difficult to remember a password that long. As the password gets longer and harder to remember the user is more likely to totally defeat your security by writing the password on a sticky-note and putting it on their monitor or under their keyboard where no hacker would ever look.

The solution is to get away from using passwords and start using passphrases. "Password" implies that it's a word. "Passphrase" says that it's a phrase which includes spaces and punctuation. Most modern systems support passphrases these days, Microsoft's modern operating systems will allow for a passphrase of up to 255 characters – far more than you need or want.

A good passphrase doesn't have to be complicated to be strong. "My 2 dogs are cute!" is 19 characters, mixed case with punctuation and numbers. It would take centuries for a computer to break a 19 character mixed case passphrase with punctuation and numbers using brute force. Even with that strength it's easy to remember and not hard to type.

Be creative, but use passphrases instead of passwords. The results will be longer and harder to defeat, but easier to remember, passphrases.

Account Lockout

The traditional manner of defeating brute force or dictionary attacks has been to set an account lockout threshold. After 3 or 5 or 10 failed attempts, for example, the account is locked either for some set period of time or until the administrator manually unlocks it. This feature is sometimes a headache for administrators, however, as users mistype their passphrases frequently, get themselves locked out and require administrator attention to get them back in. If you use passphrases long enough to be very difficult to break you can set your account lockout threshold to be quite high – say 100 failed attempts within 5 minutes. No user will type the wrong passphrase that quickly but any automated brute force attack will be defeated.

Check Your Logs

You should have your security auditing configured to log failed authentication attempts in the event logs. Check them for time to time so you can learn two things:

1. Attempted attacks.
2. Users who frequently type their passphrases wrong. They may need some additional training to help them select and use better passphrases and they are also the users who are more likely to write their passphrase on a Post-It and stick it to their monitor.

#2 – Keep Your Passphrases Private

A passphrase shared is compromised. A compromised passphrase has to be changed. That has to be ingrained in all of our people right off the bat. I can't count how many times I've had a lawyer, even a partner, go out of town and give their assistant their passphrase – usually so the assistant could check their e-mail. The problem with that is that once the assistant has the passphrase they have it until the passphrase is changed. If the assistant wants to log into the attorney's account for any reason at any time, they can. They could log in and send e-mail as if it came from the attorney. They could log in and access any accounting or personnel records the attorney has access to. If they leave the firm for any reason they still have the passphrase and could still log in. Do you disable the accounts of assistants who leave the firm? Of course you do. Do you also change the passphrases of their attorneys at that time or at regular intervals? Probably not and that means you may have quite a few former employees that can still access firm systems. Not only can they access the firm systems but they can access it with the permissions and even identity of the attorney or partner!

If a passphrase is compromised it must be changed. Immediately.

Find Alternatives for Temporary Access

There are lots of other ways to handle the situation where an attorney is on vacation.

- You can have their mail forwarded to the assistant

- You can have the attorney's mail forwarded to their home or private account while they're away.
- You can create a temporary passphrase for access to the attorney's account
- The attorney could check their own e-mail, remotely, using a web access client

A word of caution about out-of-office messages

Attorneys going away on trips love to set out-of-office messages (automatic replies that say they're away). There are two concerns I have with those messages.

First an out-of-office message tells people, including unscrupulous people, that you are away. Maybe those people know where you live; maybe they could take advantage of your absence to access your office, or to try and break into your systems knowing you won't be returning for some period of time.

Second, and more commonly, an out-of-office message confirms to spammers that they have found a legitimate e-mail account. Within a very short time you can expect your freshly confirmed e-mail address to be sold to a long list of other spammers.

Don't Write Passphrases Down Unencrypted

Some people will still feel compelled to write their passphrase down no matter how easy you make it for them. To be honest I have to write passphrases down all the time – I'm constantly being told different passphrases for different systems so that I can work on them. The solution to this problem is to write the passphrase down encrypted or to use a reminder.

If the passphrase is "I can't tell you." you could write down a reminder such as "Can you tell me the passphrase?" or "You can tell me, I'm a doctor." Anything that triggers you to remember the phrase but isn't too obvious a clue for hackers makes for a good reminder.

Or you can use a hash to write down the passphrase. By adding one character to each letter "I can't tell you." Becomes "J dbo'u ufmm xpv." Obviously that simple Caesar cipher encryption is not going to fool anybody who is good at cryptography but it's only intended to deter the casual attempts. If I use a simple hash like that it's only for temporary use and I'll shred the paper or change the passphrase shortly.

You can use a more complicated hash or mask if you want to retain the passphrase longer.

#3 – Lock The Doors

Too often we focus so closely on securing our systems with passwords that we forget that we need to physically secure our systems. That means that we need to lock our servers away in their own area where they can't be accessed by unauthorized persons. Are your servers sitting next to a copier? Are they in a public hallway? Damaging your systems could be as simple as a disgruntled working yanking the power cord out of a server

causing a crash. Or maybe the copier repair person turns off the surge protector, not realizing that the copier and the server share the same surge protector. Secure your servers.

Make sure your people are taught to ask questions.

There is a popular adage in the security business that says “If you have a clipboard and look busy you can walk into anywhere.” Just as a test ask a friend who is not familiar at the office to come in one day, carrying a clipboard and looking like a service person, and see how long they can walk around the office before somebody stops them and asks them their business. The results may frighten you. Make sure that you have a policy that visitors to the office must be clearly identified and that your people are expected to challenge any strangers they see in the office unescorted – or that they should immediately notify somebody who can confirm their identity.

Passphrase protect screensavers

A popular hacker trick, if they are able to walk into your office, is to look for an unattended desk and sit down – especially around lunchtime. Next lunchtime walk around your office and see how many people have left their computers on and logged in while they are away. How long could you sit at their desk, access sensitive documents or e-mail messages, even download, alter or print sensitive documents before somebody noticed? If your users don't want to log off, configure their screen saver to require a passphrase before it will turn off. All of the recent Microsoft operating systems already have that feature, you simply need to enable it in the screensaver settings.

#4 – Make Sure Remote Users Have Locks

Broadband access has become ubiquitous and we all support users who log in from home to access e-mail, documents and other office systems. If those systems are not secure then they become a potential entry point for bad things to get into your systems. While you can't always control what people are going to run at home, you can set policies that require firewalls for home users in order to remote access the office. Firewalls don't have to be expensive, at the very minimum users could be sure to have the Windows XP built-in firewall turned on. There are also plenty of hardware devices, like the routers made by LinkSys, NetGear or several other vendors which provide some basic security for well under \$100. These devices are readily available from virtually any computer store or from online vendors like eBay, Amazon.com or Outpost.com just to name a few.

#5 – Count the Doors

How many ways into your network are there? Are you sure? One problem cropping up in corporate networks are users who bring their own wireless access points to the office and set them up so that they can roam wirelessly with their PDAs, laptops and other devices. These rogue access points are often not properly secured and provide a way for the unscrupulous to get into your network without your knowledge.

Check your phone bill for forgotten modems. Another way users can sometimes subvert your security is by setting up PC Anywhere or other such remote access software on their desktop PC and plugging a forgotten phone line into the modem in their PC. Or maybe you have a modem that you used to use for remote access and simply forgot to disconnect when that use ceased. Make sure you know where every modem, wireless access point, network cable drop and other access point for your network is. Set and enforce a policy regarding remote access software on company workstations.

#6 – Change Defaults

Hackers know what the default passwords and settings are on security systems. Don't make it easy for them by retaining those settings – when you set up a firewall, router or other device change the default password. That goes for your voicemail system, copiers, cellphones, PDAs and other devices as well.

Wireless Access Points

Wireless Access Points use a feature called the Service Set Identifier (SSID) to advertise their presence. Make it harder for strangers to locate and connect to your wireless access points by changing the default SSID. Also consider turning off the SSID broadcast which will make your wireless access point invisible to those who don't know it's there.

A word of caution about turning off the SSID

If you are in an area with several wireless access points turning off the SSID broadcast can cause performance and reliability problems with your wireless network.

Additionally, if you frequently bring new devices into and out of your wireless network turning off the SSID broadcast can make it more difficult for those devices to find and connect to your wireless network.

The other default to change on your wireless access point is to enable encryption. All wireless devices support Wireless Encryption Protocol (WEP) but keep in mind that WEP, while better than nothing, is not really very secure. Wireless Protected Access (WPA) is a better solution and it is supported by all recent devices.

If you have a fairly stable collection of devices that will connect to your wireless network, in other words the same few computers with only rare guests or changes, you should enable Media Access Control (MAC) filtering. Every networking device has a MAC address which is, in theory, unique to that device. Most wireless access points will let you specify a list of devices, by MAC address, that are allowed to connect to that wireless access point. The MAC address of a particular device is usually printed on a sticker attached to the device; it's comprised of 12 numbers and letters (A-F) in a format like this: 00 11 22 AA BB CC.

#7 – Backups

If it's worth having it's worth having three copies of. Good backups reduce your exposure to security events because if you do have a problem that results in data

corruption or loss you can restore the data from backup and be back in business with minimal disruption.

Two More Thoughts On Backups

1. Take a copy of your backups off-site. If your server room is destroyed, perhaps by fire or other natural disaster the backups won't help you if they are on the shelf above the server. Off-site doesn't have to mean a fancy storage facility; you can simply had a responsible person take a copy to their home. As long as they are kept in a reasonably safe and climate-controlled environment they should be o.k. One caveat – those backups will likely contain sensitive documents and material so it may be worth getting a safe-deposit box or other locked storage facility to protect them.
2. If you haven't tested your backups then you haven't backed up. Periodically test your backups to make sure that you really could restore files off them if you needed to. If you're using a tape media make sure you're aware of how hold those tapes are – they have a finite lifespan, especially if they're used regularly and need to be replaced periodically with new tapes.

#8 – Are You Current?

As new vulnerabilities are discovered vendors release patches and updates to fix them. It's important to be aware of these updates and to install them on a timely basis. Of course some of these patches cause new problems when fixing other ones so you have the tricky job of trying to figure out which of the patches are safe to deploy to your entire organization and which you want to hold off on. If you have a test lab where you can test the patches in a simulation of your environment that is ideal, otherwise just monitor the patches and the community response to them carefully. Don't wait too long, the time frame between the discovery of a vulnerability and the exploiting of it has gotten extremely short and if you have a patch to close the hole you can't afford to wait until after you've been exploited to fix it.

Operating system patches, from Microsoft most commonly, are probably the most familiar kind of patch but they are far from the only kind. Your application vendors and hardware vendors may issue patches and service packs as well and you'll need to keep track of those updates too.

Pay particular attention to updates for your firewall, anti-spyware and antivirus software – your antivirus software should be checked for updates on a daily basis. Yes, daily.

Software Update Services (SUS)

Microsoft makes several tools available to help you with patch management; one of these is SUS. SUS is a Windows server application that will automatically check Microsoft's

servers on a daily basis for any new patches that can be deployed. You can then review the list of patches, approve the ones you want your users to have and your workstations can automatically obtain and install those patches from your SUS server. SUS is available for download at no cost.

Office Update

If you use Microsoft Office 2003 you can use Help | Check for Updates in any application to access Microsoft's Office Update, which will check for, download and install updates to the Office applications. One notable patch you'll find there are updates for the junk e-mail filters in Outlook.

Don't just be aware of service packs and patches, but of new versions as well. I know it is often expensive to upgrade to the latest version of various pieces of software but often the newer versions close security holes in the older versions and vendors eventually expire their support for older versions and stop developing new fixes for them.

Keeping version-current can be especially important with regards to firewalls, antivirus and anti-spyware software.

#9 – Shut Off Unnecessary Services

Almost every server has at least some services running on it that are unnecessary. Internet Information Server (IIS) is one of the most common examples. File Transfer Protocol (FTP) is another. Review your servers for any services that are obviously unnecessary. Unnecessary services can be holes into your system.

Note: This is a relatively technical operation that is best done by somebody who knows what they are doing.

Unnecessary Protocols

Check your network for unneeded protocols too. A protocol is a set of rules that dictate how systems communicate with each other. Most modern networks rely primarily, if not exclusively, on TCP/IP to communicate. However some devices come with multiple protocols enabled. Find out which protocols you need and disable all of the ones you don't. Not only will this make your network more secure but it will also reduce the amount of traffic on your network and improve your network performance.

Check Workstations Too

Almost every workstation I've seen has had some kind of file and printer sharing enabled on it. In most cases this is unnecessary and exposes your workstations to remote access. This can be of particular concern on notebooks and laptops that are taken out in the field. Connect that laptop to a hotel or coffeehouse network and it is possible that somebody else could connect to your laptop hard drive and access sensitive materials.

#10 – Be Careful With Permissions

Permissions, as the name implies, dictate what a particular user or group of users is allowed to do and access on the network. Be careful what permissions you assign to users and groups – better to give too few permissions than to give too many. As a general rule lock everything down and then open things up as needed.

Chances are good that you or somebody like you is the administrator of your network. Resist the temptation to give your account administrator rights, however. Any malicious code that happens to execute under your account executes with the permissions of your account. If you have administrator permissions and you happen to get infected with a virus or spyware then that virus or spyware has administrator permissions.

Have a user account that gives you just the permissions you need to do your job. Have a separate administrator account that you use for administering your network and don't use that administrator account to casually browse the web, read e-mail or do other user tasks.

#11 – Check the Logs

Today's systems keep a number of log files that document everything from hardware problems to intrusion attempts. It is essential that you check the logs on your systems on a regular basis – at least weekly – in order to detect and anticipate problems. Some of these log files are:

- Event Viewer – Most operating systems have an event log both for servers and for workstations. On Microsoft systems this is called the Event Viewer.
- Antivirus – Your antivirus system will certainly include a log that shows viruses detected as well as the last time your virus detection signatures were updated. These are both important to monitor.
- Intrusion Detection – If you have an intrusion detection system (IDS) or intrusion prevention system (IPS) it will have logs that show intrusion attempts.
- Firewall – Like the IDS/IPS your firewall should have logs that show incidents and events that you need to be aware of.

Logs can often be your first indication of impending problems.

#12 – Educate Your Users

Knowledge is power and your users are important to your defenses. Encourage them to learn the basics of safe computing, talk to them about not opening strange attachments, about being suspicious of strangers walking around the office unescorted (even if they're wearing a uniform and act like they're supposed to be there). Don't be afraid to send them to computer classes.

At one firm I worked at we created these one page tutorials called "Computers in 60 Seconds" which were designed to educate users on one specific topic – such as viruses or backups. We'd leave these pages in the staff lounge where people could read them if

they chose. Also we would leave copies of our computer magazines in the lounge and other reading areas in an effort to encourage more interest and knowledge in the computer systems.

Do It Now!

If you address these 12 things, most of which cost very little other than time or attention, you will be well on your way to securing your information resources from threats. Don't delay.

More Resources

- <http://www.microsoft.com/security>
- <http://www.antonline.com/>
- <http://netsecurity.about.com/od/secureyourcomputer/>
- http://www.infopeople.org/howto/security/basics/threats_vulnerabilities.html
- <http://securityadmin.info/faq.asp>
- Microsoft.public.security newsgroup