
Security Myths

Jesper M. Johansson

Steve Riley

Information

This article is an excerpt from Jesper and Steve's new book "Protect Your Windows Network." The book is available from Addison-Wesley. For more information, see:

<http://www.awprofessional.com/title/0321336437>.

Security configuration changes and guides have been around for about 10 years in the Windows world, longer in other areas. The original Windows NT 4.0 guides published by the US National Security Agency and SANS were basically just lists of changes, with a little bit of rationale behind each setting, but no overall cohesiveness. They were a response to a demand for what we call the “big blue ‘secure-me-now’ button.” The problem is that such a button does not exist. If it did, the vendor would ship it.

There is a lot at stake in security configuration guidance. First, it is easy to understand why people are clamoring for it. Everyone can see the benefit in turning on some setting and blocking an attack. In some environments, doing so is not even an option. A system must be configured in accordance with some security configuration or hardening guide to be compliant with security policy. In other environments security configuration guidance is strongly encouraged. We feel that it is very important before you start making security tweaks, however, that you understand some of the fundamental problems with security tweaks. These are what we call the myths.

Before we start sounding like we hate security guides (which we do not) let us point something out: the authors have taken part in authoring, co-authoring, or editing almost all the commonly available guides for Windows in the past 10 years. Guides are valuable, done right. To do them right you must understand what they cannot do though. That is why the myths are important.

Warning

This section is somewhat (ok, very) cynical. Take it with a grain of salt and laugh at some of the examples we give. Do not lose sight, however, of the message we are trying to get across. These are myths, and you need to be careful of falling into the trap of believing them. If you can avoid that you can focus your efforts on the things that make a real difference instead of being lured into staring at a single tree and failing to see the security forest, like so many others.

Myth 1: Security Guides Make Your System Secure

Hang on, why is this a myth? Isn't the basic purpose of a security guide to make you secure? Yes. That is the general idea. However, the term “secure” connotes an end-state. We will never actually get there. Security is a process, to be evaluated on a constant basis. There is nothing that will put you into a “state of security”. Unfortunately many people (surely none of you readers though) seem to believe that if you simply apply some hardening guide your system will now be secure. This is a fallacy for several reasons.

First, consider any of the recent worms, sasser, slammer blaster, nimda, code red, ILOVEYOU and friends, etc, etc, ad infinitum ad nauseum. Not a single one of them would have been stopped by any security settings. That is because these worms all exploited unpatched vulnerabilities. While most of the guides tell you that you need the patches applied, we have seen many systems that had the guides installed and whose owners therefore felt the patch was not important. If you are unsure of which patches to install the proper answer is “all of them.” Ideally, you should have more of a process around patch management though. Few settings can prevent your network from getting attacked through unpatched vulnerabilities.

Second, settings rarely stop real attacks. There are a few things that are harder to do, but in general, networks do not get attacked through settings that can be turned off. There are a few exceptions. For instance, a security guide might turn off storage of LM Hashes, which would have made cracking passwords much harder. However, as we pointed out in an earlier article (<http://www.microsoft.com/technet/community/columns/secmgmt/sm1004.msp>) cracking passwords is strictly speaking unnecessary. A guide might also make anonymous enumeration harder, but attackers almost always have access to some account that can be used instead of anonymous connections.

This is largely because security guides are meant to be simplistic, while sophisticated attacks are complex. Security guides provide a great starting point, but to really improve your security you need to do a lot more. Generally, you would need to resort to complex measures to stop complex attacks and complex measures do not package well in the form of a security template.

A security guide does not make your system secure. At best it provides an additional bit of security over the other things you have already done, or will already do, to the system, as explained in other chapters. At worst it will compromise your security. For instance, a guide may very well compromise the availability portion of the Confidentiality-Integrity-Availability triad by destabilizing the system.

Myth 2: If We Hide It the Bad Guys Won't Find It

If we had a dime for every time we had seen someone try to hide their system. Hiding the system so rarely helps. Some examples are in order. For instance, some people advocate turning off SSID broadcast in wireless networks. Not only does this mean you now have a network that is not compliant with the standard, your clients will also prefer a rogue network with the same name over the legitimate one. Oh, and it takes a few minutes to actually find the network anyway, given the proper tools. Another example is changing the banners on your web site so the bad guys will not know it is running IIS. First, it is relatively simple to figure out what the web site is running anyway. Second, most of the bad guys are not smart enough to do that so they just try all the exploits, including the IIS ones. Yet another one is renaming the administrator account. It is a matter of a couple of API calls to find the real name. Our favorite is when administrators use group policy to rename the administrator account. They now have an account called “Janitor3;” with a comment of “Built in account for administering the computer/domain.” This is not really likely to fool anyone.

Renaming or hiding things is generally speaking much more likely to break applications than it is to actually stop an attack. Attackers know that administrators rename things, and go look for the real name first. Poorly written applications assume the Program Files directory is in a particular place, that the Administrator account has a particular name depending on region, and so on. Those applications will now break. Arguably, they were already broken, but the result is that they no longer function.

Myth 3: The More Tweaks the Better

Security guides contain a lot of settings, and why not, there are a lot to choose from. Windows Server 2003 contains 140 security settings in the group policy interface, and that does not count access control lists (ACL), service configuration, encrypting file system (EFS) policies, IPsec policies and so on. The “best” configuration for these for every environment is nebulous at best. Therefore, a number of people take the approach that if you only make more changes you will be more secure. We distinctly remember a very memorable headline from late summer 2003 (in the northern hemisphere). It read “Dell Will Sell Systems that Are Secure by Default.” Dell had just announced they would start selling Windows 2000 systems configured with the CIS Level 1 benchmark direct from the factory. The article went on to point out that this guide applies “over 50 security changes...significantly improving the default security of Windows 2000.”

Well, there were a couple of problems with that statement. First, the benchmark only made 33 changes, not “over 50.” Second, only three of them had any impact on security at all. Lastly, while Dell may have configured some security settings on the system, it was being sold without the latest service pack slipstreamed, which would seem at least to us to be a basic requirement for security. Don’t get us wrong, it is encouraging to see vendors that step back and look at older operating systems and evaluate whether they can be made more secure than what was considered prudent several years ago when they were first released. The problem, though, is that first this was presented as a way to get a “secure” system, when there is obviously no such thing. Second, the vendor had missed many of the basic requirements for a protected system.

Many settings people make have no real impact on security. Consider, for instance, the “Restrict floppy access to locally logged on user only” setting. It ensures that remote users cannot access any floppy disks via the network; if and only if (IFF) a user is currently logged on to the system hosting the floppy, otherwise the setting does not take effect; AND a share has been created for the floppy disk (not done by default); AND the ACL on the share specifies that the remote user can get to it; AND the system has a floppy drive in the first place AND there is a disk in it. Most systems sold today do not even have a floppy disk, not to mention how unlikely the other requirements are to occur together. We would be inclined to say that this setting has no impact on security whatsoever.

We are also very fond of the “NetworkHideSharePasswords” and “NetworkNoDialIn” settings that several of the guides advocated for years. The former is designed to ensure that when you set a share password it is obscured in the user interface dialog; if you are running Windows 95. The setting has not worked since then (Windows NT, including 2000, XP, and Server 2003, has never supported share passwords). Of course, even on Windows 95 the setting had been much more effective had it been spelled correctly (network\hidsharepasswords). The latter setting, also misspelled, controlled modem dial-in permissions, also on Windows 95. In spite of the fact that these settings have never worked on any Windows NT-based operating system there are still “security auditors” running around explaining to management that the security guys are not doing their job unless these two settings are configured - on Windows 2000 and even XP. Far too often the guides we see are taken directly from obsolete and technically inaccurate documents for other, obsolete, operating systems. Then they are made a requirement by people who do not understand security OR the operating system they are trying to protect.

Actually designing security to a threat model seems to be a luxury when it is so much easier to just charge exorbitant consulting fees for parroting back what someone else, who also did not understand the product, claimed was correct.

There are some basic ground rules.

- ? Requiring settings that are already set by default do not improve security
- ? Settings that only modify behavior already blocked elsewhere do not improve

security (although in some cases defense in depth is appropriate as long as you do not break required functionality in the process)

- ? Settings that destabilize the system do not improve security
- ? Misspelled settings do not improve security
- ? Settings that do not work on the relevant product do not improve security

If you are one of the unfortunate people who get evaluated based on the number of settings you make then go ahead and make a bunch of these meaningless changes. Heck, invent a few of your own (everyone else seems to). Here are a few you could use without breaking anything

- ? HKLM\Software\Microsoft\Windows NT\CurrentVersion\DisableHackers=1 (REG_DWORD)
- ? HKLM\Software\Users\SocialEngineering\Enabled=no (REG_SZ)
- ? HKCU\Software\Users\CurrentUser\PickGoodPassword=1 (REG_BINARY)
- ? HKLM\Hardware\CurrentSystem\FullyPatched=yes (REG_SZ)
- ? HKLM\Software\AllowBufferOverflows=no (REG_SZ)

Make sure you set proper ACLs on them too. This way you can show that you are actually doing much more than anyone else. If you also create a pie chart showing how much you are improving return on investment (ROI) with your careful management of security your promotion into Useless Management Overhead (UMO) is a virtual certainty!

Meanwhile, the rest of us will focus on actually improving security through designing security measures to a threat model.

Myth 4: Tweaks Are Necessary

Some people consider tweaks a necessity; claiming that you cannot have a secure (read “protected”) system without making a bunch of tweaks. This is an oversimplification. Tweaks block things you cannot block elsewhere. For instance, if you have two systems on a home network behind a firewall, or a corporate system that has IPsec policies that only allow it to request and receive information from a few well-managed servers, then tweaks are mostly not necessary to improve security. Those systems will be perfectly fine without making any tweaks.

Even on highly exposed systems most of the tweaks are not necessary. In eWeek’s Open Hack IV competition in 2002 (see <http://msdn.microsoft.com/library/en-us/dnnetsec/html/openhack.asp>) we built what was probably the most protected network we have ever built. In all we made only four registry tweaks, a couple of ACL changes, and set a password policy. The rest of the protection for those systems was based on proper network segmentation, a solid understanding of the threats, turning off unneeded services, hardening web apps (see *Writing Secure Code*, 2nd Ed, by Howard and LeBlanc, MS Press, 2003), and properly protecting the SQL and web servers. Of course, this was a specialized system with very limited functionality, but it still shows that less is often more.

Proper understanding of the threats and realistic mitigation of those threats through a solid network architecture is much more important than most of the security tweaks we turn on in the name of security.

Myth 5: All Environments Should At Least Use <Insert Favorite Guide Here>

One size does not fit all. Every environment has unique requirements and unique threats. If there truly was a guide for how to secure every single system out there, the settings in it would be

the default. The problem is that when people start making these statements they fail to take into account the complexity of security and system administration. As we mentioned in the first article (<http://www.microsoft.com/technet/community/columns/secmgmt/sm0104.msp>), administrators usually do not get calls when things break. Security breaks things; that is why some security-related settings are turned off by default. To be able to protect an environment, you have to understand what that environment looks like, who is using it and for what, and what the threats are that they have decided need mitigated. *Security is about risk management, and risk management is about understanding and managing risks, not about making a bunch of changes in the name of making changes solely to justify ones own existence and paycheck.*

At the very least, an advanced system administrator should evaluate the security guide or policy that will be used and ensure that it is appropriate for the environment. Certain tailoring to the environment is almost always necessary. These are not things that an entry-level administrator can do, however. Care is of the essence when authoring or tailoring security policies.

Myth 6: “High Security” Is an End-Goal for All Environments

High security, in the sense of the most restrictive security possible, is not for everyone. As we have said many times by now, security will break things. In some environments you are willing to break things in the name of protection that you are not willing to break in others. Had someone told you on September 10, 2001 that you needed to arrive three hours ahead of your flight at the airport to basically be strip searched and have your knitting needles confiscated, you would have told them they are insane. High security (to the extent that airport security is truly any security at all and not just security theater) is not for everyone and in the world we lived in until about 08:00 EDT on September 11, 2001, it was not for us. Once planes took to the skies again, few people questioned the need for more stringent airport security.

The same holds true of information security. Some systems are subjected to incredibly serious threats. If they get compromised people will die, nations and large firms will go bankrupt, and society as we know it will collapse. Other systems are protecting my credit card numbers, for which I am liable up to \$50 if they get compromised. The protective measures that are used on the former are entirely inappropriate for the latter; yet we keep hearing that “high security” is some sort of end-goal toward which all environments should strive. These types of statements are an oversimplification that contributes to the general distrust and disarray in the field of information security today.

Myth 7: Start Securing Your Environment by Applying a Security Guide

You cannot start securing anything by making changes to it. Once you start changing things, the environment changes and the assumptions you started with are no longer valid. We have said this many times, but to reiterate, security is about risk management; it is about understanding the risks and concrete threats to your environment and mitigating those. If the mitigation steps involve taking a security guide and applying it, so be it, but you do not know that until you analyze the threats and risks.

Myth 8: Security Tweaks Can Fix Physical Security Problems

There is a fundamental concept in information security that states that if bad guys have physical access to your computer, it is not your computer any longer! Physical access will *always* trump software security – eventually. We have to qualify the statement though because there are valid software security steps that will prolong the time until physical access breaches all security. Encryption of data, for instance, falls into that category. However, many other software security

tweaks are meaningless. Our current favorite is the debate over USB thumb drives. In a nutshell, after the movie “The Recruit” everyone woke up to the fact that someone can easily steal data on a USB thumb drive. Curiously, this only seems to apply to thumb drives. We have walked into military facilities where they confiscated our USB thumb drives, but let us in with 80 GB i1394 hard drives. Those are apparently not as bad.

One memorable late evening one author’s boss called him frantically asking what to do about this problem. The response: head on down to your local hardware store, pick up a tube of epoxy, and fill the USB ports with it. While you are at it, fill the i1394 (FireWire), serial, parallel, SD, MMC, Memory Stick, CD/DVD-burner, floppy drive, and Ethernet jack with it too. You’ll also need to make sure nobody could carry the monitor off and make a photocopy of it. You can steal data using all of those interfaces

The crux of the issue is that as long as there are these types of interfaces on the system, and bad guys have access to them, all bets are off. There is nothing about USB that makes it any different. Sure, the OS manufacturer could put a switch in that prevents someone from writing to a USB thumb drive. That does not, however, prevent the bad guy from booting to a bootable USB thumb drive, loading an NTFS driver, and then stealing the data.

In short, any software security solution that purports to be a meaningful defense against physical breach must persist even if the bad guy has full access to the system and can boot into an arbitrary operating system. Registry tweaks and file system ACLs do not provide that protection. Encryption does. Combined with proper physical security, all these measures are useful. As a substitute for physical security, they are usually not.

Myth 9: Security Tweaks Will Stop Worms/Viruses

Worms and viruses (hereinafter collectively referred to as “malware”) are designed to cause the maximum amount of destruction possible. Therefore, they try to hit the largest numbers of vulnerable systems and hence, they tend to spread through one of two mechanisms: unpatched/unmitigated vulnerabilities and ~~stupid~~ unsophisticated users. While there are some security tweaks that will stop malware (Code Red, for instance, could have been stopped by removing the indexing services extensions mappings in IIS), the vast majority of them cannot be stopped that way because they spread through the latter vector. Given the choice of dancing pigs and security, users will chose dancing pigs, every single time. Given the choice between pictures of naked people frolicking on the beach and security, roughly half the population will chose naked people frolicking on the beach. Couple that with the fact that users do not understand our security dialogs and we have a disaster. *If a dialog asking the user to make a security decision is the only thing standing between the user and the naked people frolicking on the beach, security does not stand a chance.*

Myth 10: An Expert Recommended this Tweak as Defense in Depth

This myth has two parts. Let us deal with the second half first. Defense in depth is a reasoned security strategy applying protective measures in multiple places to prevent unacceptable threats. Unfortunately, far too many people today use the term “defense in depth” to justify security measures that have no other realistic justification. Typically, this happens because of the general belief in myth 3 (more tweaks are better). By making more changes we show the auditors that we are doing our job and therefore they chalk us up as having done due diligence.

This shows an incredible immaturity in the field, much like what we saw in western “medicine” in the middle ages. Medics would apply cow dung, ash, honey, beer, and any number of other things, usually in rapid succession, to wounds to show that they were trying everything.

Today doctors (more typically nurses actually) clean the wound, apply a bandage and potentially an antibiotic of some kind and then let it heal. Less is very often more and using defense in depth as a way to justify unnecessary and potentially harmful actions is inappropriate.

The first part of this statement is one of our favorites. As a society we love deferring judgment to experts, because, after all, they are experts and know more than we do. The problem is that the qualification process to becoming an expert is somewhat, shall we say, lacking? We usually point out that the working definition of a security expert is “someone who is quoted in the press.” Based on the people we often see quoted, and our interaction with those people, that belief seems justified. It is no longer actions that define an expert, just reputation; and reputation can be assigned. Our friend Mark Minasi has a great statement that we have stolen for use in our own presentations. To be a security consultant all you have to know is four words: “the sky is falling.” Having been security consultants and seen what has happened to the general competence level in the field, this statement certainly rings true. There are many, many good security consultants, but there are also many that do not know what they need, and in some cases, fail to recognize that and then charge exorbitant amounts of money to impart their lack of knowledge and skills on unsuspecting customers.

Learning more

This article has dealt with the things that you should avoid when managing security. In the book "Protect Your Windows Network" Jesper and Steve cover the things you should do, and you may be surprised at some of the conclusions.

As always, this column is for you. Let us know if there is something you want to discuss, or if there is a better way we can help you secure your systems. Just click the “Comments” button below, and send us a note.