PC Security Depends on Configuration Control

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

Reader Tracy Southworth has very kindly allowed me to quote an interesting message she wrote to me last year:

>The articles on security are very interesting and have offered many ideas over the months about how to enlist people in the organization to participate in security.

The problem is that this advice is constantly contradicted by the advertising one sees on the Internet. It's take a look at this, try this, click this all day and no matter how well intentioned people are, they are only human and will eventually click on a link that installs something on their PC. It seems to me that the problem is not with the staff, but rather that the operating systems (Windows) are tied so strongly with the Internet access that there is really no such thing as a secure system anymore.

I would like to see a series of articles that addresses this problem and how we can build bullet-proof systems. Specifically, technologies other than strong passwords to identify users, systems that do not allow software to be installed and other ways to lock down platforms to enforce security. I remember a program we used to use called pcRdist that would check all the files on the PC against an image on the network and download or erase files until everything matched. It was a good way to maintain PCs in a University library setting where you wanted to ensure conformity.

The point is that we have built insecure systems (with all this Internet access) and having to rely on users to make them secure for us just doesn't make sense to me. <

I think you have identified a major practical problem for decentralized, PC-based working environments. Although data centers had disadvantages too, centralized control did at least help to limit unauthorized and poorly-conceived mixtures of software, installation of untrusted products, and misconfiguration of software and hardware parameters.

Configuration management (CM) can be broken into two major areas: software CM (SCM) and network CM (NCM).

Some useful Web resources dealing with SCM:

* The USENET group < newsgroup comp.software.config-mgmt > focuses on software development configuration control (making sure that the right versions of software are being compiled and installed) and has a FAQ list at < http://www.iac.honeywell.com/Pub/Tech/CM/ >.

* The Institute of Configuration Management has extensive links to a wide variety of

information in the software CM and is available at < http://www.icmhq.com/ >.

For NCM, see for example

* White papers on NCM from ON Command, makers of the CCM (Comprehensive Client Manager) product that allows centralized deployment of authorized software to PCs on a network; see < http://www.on.com/dlctr.htm#whitepapers > for more information.

* Program Security Guard (PSG) from Reflex Magnetics < http://www.reflex-magnetics.co.uk/products/dn_5.htm >, which is described as follows: ". . . PSG allows you to set file and folder protection that the user cannot bypass. PSG will prevent modification or deletion of existing files, and any changes to applications. PSG will also prevent any executable files from being installed, giving the Administrator full control of all software running on the network."

* A little 228 Kb shareware program called PC Security Guard "will look through all the places where an unwanted intruder (trojan or some kind of logger) can be run from and shows you suspicious entries. It can automatically recognize most common trojans. The program will check registry, .ini files, autoexec, startup folder, VxD. . . ." See < http://www.geocities.com/SiliconValley/Hills/8839/pcguar.html > for information and downloads.

* FolderGuard v4.14 from WinAbility < http://www.winability.com/folderguard/ > is described as allowing an administrator to curtail configuration changes of many kinds by PC users. Some of the features described:
– Actually hide files and folders
– Make files and folders read-only for real
– Protect files and folders with passwords
– Prevent users from installing unauthorized programs
– Prevent users from running programs from the floppy disks
– Prevent users from reformatting local drives
– Restrict access to the Dial-Up Networking settings
– Prevent access to the Date/Time settings
– Monitor the logon and disable the CANCEL button on the password window
– Restrict access to Control Panel and other resources
– Restrict software downloads from the Internet
– Restrict the Save As Wallpaper command

* * *

Neither the author nor AtomicTangerine have any financial interest in the companies named. Any products named are mentioned solely as examples and inclusion in this article does not constitute or imply endorsement by the author, his employer, or the publisher of this newsletter.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience.

For information about AtomicTangerine, visit < http://www.atomictangerine.com >.