Global Information Assurance Certification Paper

An Intrusion Prevention System (IPS) for the Home PC User: A Look at Prevx Home

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4c

Option 1 - Research on Topics
in Information Security

Submitted by: Eric Baxter
Location: Bloomington, IL

Paper Abstract: Intrusion Prevention Systems (IPS)provide real-time security protection for computer systems. Prevx Home is a free IPS that can be a useful addition to the home PC security tool kit.

Submitted: February 27, 2005

Table of Contents

List of Figures

Abstract/Summary

In addition to the commonly known security tools for home PCs (anti-virus, firewall and anti-spyware), there exists another category of security tools called Intrusion Prevention Systems (IPSes). These tools provide real-time, dynamic monitoring against intrusion events. Rather than relying only upon defined attack vectors, IPSes monitor changes and events that occur in real-time to prevent zero-day and other attacks upon the PC. Prevx Home is a free IPS tool that home PC users may find to be a useful addition to their security tool kit.

Introduction

The Basics of Home PC Protection

Firewall, anti-virus and anti-spyware software should be routinely used by every home PC user. For many users, cost is the overriding reason we buy (or don't buy) a given product. But since there are many low-cost and free tools that the home PC user can use to secure his or her computer, there really is no excuse for neglecting to employ these security tools. There are free anti-virus products, free firewall products, and free anti-spyware tools. Within their respective categories, the free utilities often rate as high—or higher—in effectiveness as their commercial counterparts. These are the basic tools of home computer security.

Additional tools, often used in commercial settings, include Intrusion Detection Systems (IDSes) and a newer class of tools, called Intrusion Prevention Systems (IPSes). It is this latter category that will be covered here, with emphasis on Prevx Home, a non-commercial offering that is available free to the home user.

What They Do

Firewall, anti-virus and spyware software protect against malicious intrusions on computers and networks. Among other duties, firewalls block undesirable network traffic as well as obscure the internal network and devices from outside scrutiny. A free version of the software firewall, ZoneAlarm, can be found at www.zonelabs.com. Anti-virus software has become a jack-of-all-trades, but its basic functionality is to detect, prevent, alert, quarantine and/or fix software viruses, worms and trojans that attack a computer. The company Grisoft, www.grisoft.com, offers a free anti-virus program for Windows or Linux. Free Windows anti-spyware software can be found at Microsoft, Lavasoft (Ad-Aware) and Spybot Search & Destroy.

Another category of software that helps identify malicious activity is the IDS (Intrusion Detection System). While IDSes are often used in commercial applications, they are rare in the home environment. This class of security tool offers event monitoring and often entails a higher degree of user interaction for successful use. They emphasize raising the alarm through alerts rather than directly working against the attack. A free example is the Open Source software called Snort. You can find more information about this product at www.snort.org.

Intrusion Prevention Systems (IPSes) go beyond IDSes by providing a dynamic response to intrusive activity. Unlike IDSes, they don't rely only upon signatures or definitions to respond to attacks. While IDSes have their place, they are not always able to respond well against so-called zero-day attacks. (The same can be said for anti-virus, firewall and anti-spyware solutions.) The term zero-day attack refers to newly identified malware, for which security tools vendors have not yet created alerts and/or responses. It should be noted that while the standard security tools may not be designed with a focus on zero-day attacks, they still provide indispensable value to home computing security.

IPSes monitor for suspicious activities, such as Windows Registry updates, and alert and/or respond to those activities. Because they emphasize monitoring the actions performed rather than malware identification, they can theoretically respond better to zero-day attacks and help the user prevent harmful actions by unidentified malware. To help understand IPSes better, we will dig a bit deeper into IPSes and then take a closer look at Prevx Home. A free version for home use is available at www.prevx.com. The reader should keep in mind that while IPSes may be useful, they complement rather than replace other security tools.

Section One

IDS vs. IPS

Intrusion Detection Systems have been in use for a number of years. They represent a well-understood and widely-deployed security measure. As previously noted, their focus is on monitoring, logging and alerting: they identify suspicious software, traffic and activities and log and/or alert the security professional to their presence. Because IDSes concentrate on known attacks, most use definitions or signatures to help them identify the threat.

Threats for which there is no signature (e.g., Zero-Day attacks) are not recognized by the IDS. To remain effective to new threats, the signatures of the IDS must be regularly updated. Intrusion Detection Systems can be hardware-

based, software-based or some combination of hardware and software. An example of a commercial IDS is the Proventia Intrusion Detection appliance, sold by Internet Security Systems, Incorporated (http://www.iss.net/). The aforementioned Open Source software called Snort is also used in commercial settings, and it can be downloaded for free by those wishing to learn more about Intrusion Detection Systems.

Intrusion Prevention Systems are sometimes thought of as the next step in the evolution of Intrusion Detection Systems. They also can be hardware and software-based, as well as some combination of the two. IPSes proactively monitor and respond to suspicious activity. Thus, once they are installed and configured, they don't require human intervention to protect against threats. IPSes for Windows systems typically monitor the registry, memory and important files for suspicious changes.

IPSes are categorized as Network-based Intrusion Prevention Systems (NIPS) and Host-based Intrusion Prevention Systems (HIPS). This nomenclature is similar to that for firewall systems, to which IPSes bear some resemblance. Indeed, IPSes are sometimes thought of as a melding of IDS and firewall technologies. Prevx Home, the product this review will focus upon, is a HIPS software-based solution.

Because their focus in on potentially damaging actions instead of positive identification of threats, IPSes don't require signatures, as do IDSes. This feature allows more flexibility in responding to Zero-Day attacks than the typical IDS. An IPS can be configured to notify the PC user of a suspicious or unknown activity, so he or she can determine whether to allow the action to complete. Since they can go beyond alerts to actually block certain actions, they provide a more automated response to attacks than IDSes typically provide. Among the attacks Prevx claims to mitigate, where traditional security products may not, are buffer overflows, spyware, adware, Trojans and worms.

Though there are many attack scenarios and new exploits are released daily, diverse threats often have similar goals (e.g., malicious changes to registry or system files). Because of this similarity, the IPS's reliance upon finding and responding to system changes frees them from the need of signature or definitions. This does not mean, however, that the IPS doesn't require periodic updates to allow it to respond to new attacks. Prevx Home, for instance, is regularly updated by the vendor; these updates can be controlled by the PC user.

Now that we have a basic understanding of Intrusion Prevention Systems, let's take a closer look at Prevx Home. This is a free product for home use. There are commercial versions of Prevx that have more functionality suitable for the enterprise, but we will focus on the consumer version, Prevx Home, which can be freely downloaded at www.prevx.com.

Section Two

The Makers of Prevx Home

Prevx Ltd. Is the maker of Prevx Home. The company sells enterprise HIPS software, in addition to the free product. Their website states that Prevx Home is installed on tens of thousands of PCs in 100 countries. They claim that over 3000 downloads of this free product occur daily. They have designed Prevx Home to report threats back to them through their Prevx Advance Warning System (PAWS). PAWS is used to help the company identify and respond to new threats quickly. Thus, the free product helps the company provide value to their commercial customers, too.

Support

Vendor support for Prevx Home can be sought out at the email address previously mentioned. In my own experience, the product has been remarkably trouble-free. The user can visit the vendor website (www.prevx.com) for additional information about the product (FAQs). Internet searches with any of the popular web search engines will also provide useful information. A Prevx user forum can be found at www.castlecops.com. Usenet Groups provide other forums for asking a variety of computing questions. While formal support is restricted, these other avenues should provide plenty of help for the user with any questions or problems using Prevx Home.

Installation

According to Prevx, the minimum system requirements to install and run Prevx Home are:

- Intel Pentium 3 600MHz, 256MB RAM (or compatible system).
- Microsoft Windows XP Professional, XP Home, Windows 2000 Professional and Windows 2000 Server

The Prevx Home Installer file is a self-extracting file, about 7 MB in size. It can be downloaded www.prevx.com. It is recommended that you close all applications before proceeding with the installation. Upon launching the file, the user steps through a series of Windows Installer screens. A web-based, brief tutorial is accessible through the installation screen. Support for the product is limited and email-based (home-support@prevx.com).

The License Agreement is similar to other software installation agreements, but the user may wish to take particular note of the Privacy and Combating Internet Crime section. This section describes the Attack Data which may be sent from your PC when Prevx Home is in use. Prevx states that it is anonymously done, and that neither the user nor his computer is identified. This data sharing is obligatory to using the product, so the product must be inactive or uninstalled to prevent Attack Data sharing.

The installation requires a reboot. I have installed and used Prevx Home on XP Professional systems with SP1 and SP2 without incident. Security tools sometimes interact in unpredictable ways, but I have not had problems with Prevx Home. For instance, I use Prevx Home on systems with Grisoft AVG anti-virus and ZoneLabs' ZoneAlarm firewall without any problems. It also works fine on another PC which has McAfee's anti-virus and firewall software. Both systems also have SpyBot Search & Destroy, Ad-Aware and Microsoft AntiSpyware (Beta) software.

Removal of Prevx Home

If you wish to uninstall Prevx Home, you may do so from the Start Menu or the Control Panel (Add or Remove Programs). You will be prompted to reboot the computer after the removal completes.

Initial View of Prevx Home

After the obligatory reboot, Prevx Home shows with an icon in the System Tray and a message that allows you to optionally update its security settings as well as apply any updates to the product's engine. To receive the most current level of protection, it is recommended you allow this update.

The System Tray icon can be double-clicked to launch the Prevx Home - Management Console. You can also right click to immediately access some functionality. From its menu, you can suspend (and resume) protection; shutdown Prevx Home entirely; perform a trusted installation; check for updates; and show the management console. The trusted installation may be run later, and may be useful in reducing the number of events generated by Prevx Home when installing new software. The System Tray icon also briefly animates to indicate when a new event has been written to the Event History.

In addition to the System Tray icon, the install can optionally place a shortcut on the computer Desktop. The install places shortcuts on the Start Menu to launch the Management Console, Help, a Readme file, and the uninstall. The Readme file contains useful enhancement and troubleshooting information, so should be

read upon installing the product.

The product is quite proactive in letting the user know when it is not actively protecting your PC. When you select Suspend Protection, the System Tray icon for PrevxHome will show an "X" through it; a mouse-over message also informs you that "Prevx Intrusion Prevention Disabled." Finally, to ensure the user notices that the product is in suspended or disabled mode, a pop-up window floats just about the System Tray indicating that "Prevx security has been suspended." There is a Resume button on this pop-up which can be clicked to re-activate Prevx Home.

The installation creates a Prevx Agent service, which is set to start automatically and has no dependencies on system components. Thus, Prevx Home starts automatically when the PC is started. Prevx Home will restart on reboot even after being suspended or shutdown.

Prevx Home – Management Console

The Management Console is the interface through which the user interacts with Prevx Home. It can be launched from the System Tray icon or the Start menu. Closing the console does not stop Prevx Home. We will visit each tab on the console, starting with the default Status tab, to better understand how Prevx Home works.

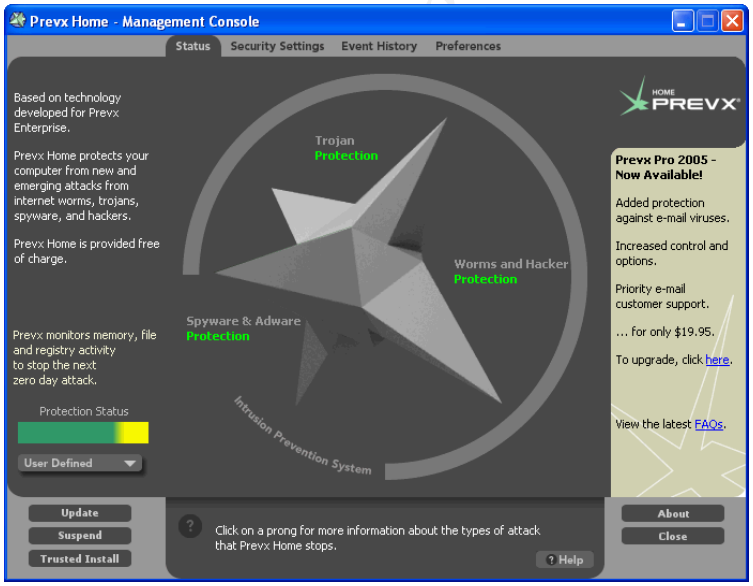

Figure 1. Status tab of Management Console

The Status tab will probably be the most widely used console interface; hence,

its default view. It, along with the System Tray icon, provides a location where the user may check for and install product updates. It is another option for Suspending the product and allowing Trusted Installs, too. All three of the settings can be seen from each tab of the console. The Protection Status (also present by default) allows the user to turn off protection, or use some mix of IPS and IDS modes (Maximum and Detection) by selecting from the User Defined drop-down menu. Clicking on the prongs of the central figure will provide help information about types of protection provided.

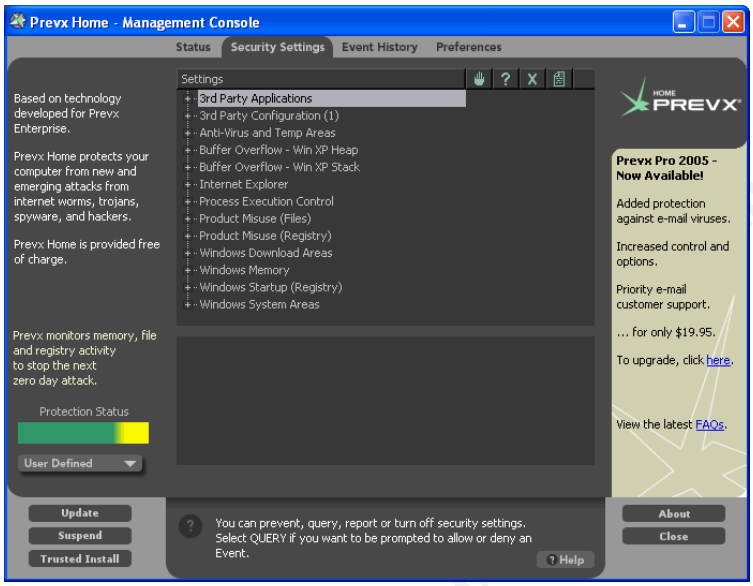

Figure 2. Security Settings tab of Management Console

Figure 2 shows the Security Settings tab of the console. The list of settings has been set with a default action by Prevx, but you can change them if you wish by clicking on the icons to the right of the list. You may automatically stop an activity, prompt the user for action to take, disable a setting, or create a report without prompting.

As noted previously, Prevx Home doesn't use signatures as IDSes do; it monitors for suspicious behavior by watching attack vectors. Although new attacks are constantly appearing, the basic behaviors by which they compromise systems often do not change much. This is how Prevx Home and other IPSes are able to successfully deter attacks by known and unknown—aka Zero-Day—exploits.

The behaviors that Prevx Home monitors include changes to memory (i.e., buffer overflow); unauthorized changes to system files; unauthorized updates to the Windows Registry; uncontrolled program execution (e.g, email worms, Trojans, etc.); and lastly, process hijacking which can used to take control of a system or

stop anti-virus or other security software.

The Update feature not only allows the user to receive product enhancements and fixes: it also can provide newly enhanced security settings. As with many web-based update systems, the user must be logged in as an Adminstrator and have Internet access. If you run a firewall (and you should), configuration of the firewall may be necessary to allow the update process through.

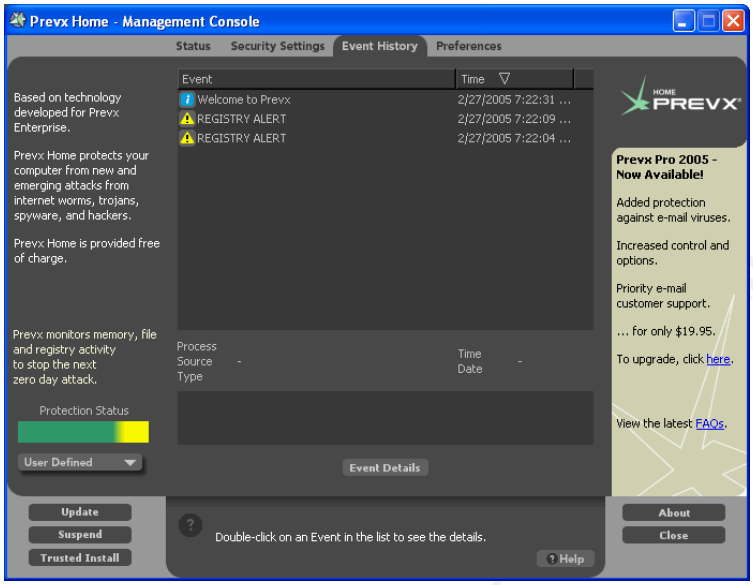

Figure 3. Event History tab of Management Console

Figure 3 shows the Event History tab of the console. Prevx defines an event as a violation of one of the security settings. You can double-click a given event or highlight and click Event Details button to get detailed information about the event. While viewing Event Details, you can click on the Get Advice button, which will take you to the web-based Prevx knowledge base article for the given event.

By perusing the event history, you can gain a better understanding of events and how they relate to actions, whether malicious or benign, unwanted or intended. You can safely rely upon the default security settings provided by Prevx, but it is always better to understand the operation of your system and which actions are acceptable. By knowing these, you will be able to set deny and allow permissions that make using Prevx Home more satisfying. After all, the goal for using the product is intrustion prevention, not intrusive provision.

The last tab of the Management Console, Preferences, is shown in Figure 4. In addition to default configurations seen on other screens, this tab allows you to set configurations for user preferences. You can set (and change) a password

to prevent unauthorized changes to security settings and preferences. Once set, the password must be remembered since there is no way to recover it. A password hint can be set to help the user recall his password.

Also on the Preferences tab are settable options for time of update reminders, and Event History log management by setting the number of events to allow before clearing the history.

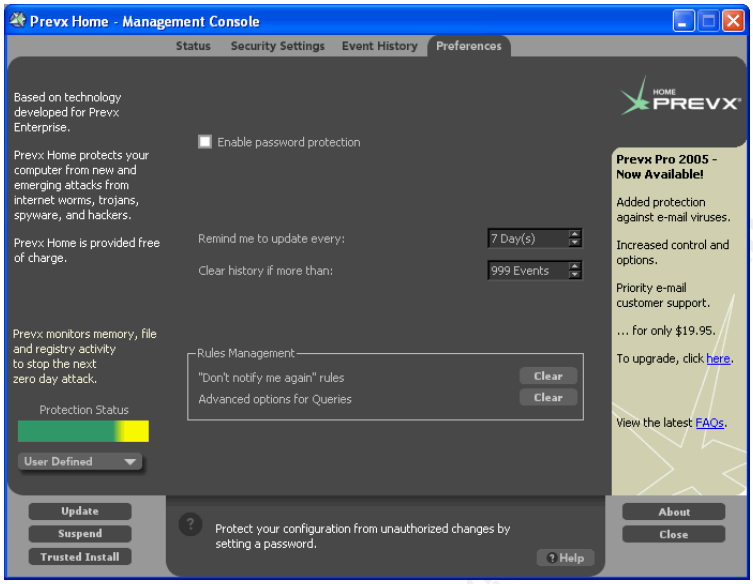

Figure 4. Preferences tab of Management Console

The basic decision facing the user is to decide whether to allow or deny a given action. The Rules Management box has 2 options. Clicking the Clear button for the "Don't notify me again" rules, allows the user to be notified again for events which he had previously set to withhold notification. Clearing the Advanced options for Queries selection will clear the Allow/Deny Events settings.

Section Three

A User Perspective

My experience with Prevx Home has been generally positive. It has a nice, understandable console interface. It has been quite stable. It doesn't appear to conflict with other software, including security tools like anti-virus, firewalls and anti-spyware. It is simple to set up and use. Its different approach to attack

prevention seems to complement the commonly used security tools. On the downside, like a host-based firewall, its messages don't always provide the user with enough information to decide whether the event is malicious or benign. It can be a bit burdensome when installing new software, though the Trusted Installation can help mitigate that distraction. But despite these minor hassles, I find the product quite useful and continue to use it on my home PCs.

Conclusion

In considering security tools for home PC protection, the user should make use of the foundational suite: firewall, anti-virus and anti-spyware. While there are other malware to consider (for example, spam and phishing via both email and Trojan attacks), these 3 tools provide the basics needed by every PC user. Another security tool which has become available recently for home use is the Intrusion Prevention System (IPS).

It differs in some important respects from an Intrusion Detection System (IDS), perhaps the most obvious being that it doesn't make use of signatures. The IPS considers behaviors of attack vectors, rather than their signatures. With this unique perspective, it should be considered as complement to, rather than replacement for, other security tools.

For users who wish to understand how an IPS works and/or use an IPS, a free version is available from Prevx. Prevx Home is a welcome addition for those wishing to take a multi-layered approach to home PC security. This review provided an initial look at this straightforward and useful tool.

References

www.prevx.com – home address of the makers of Prevx Home IPS.

www.zonelabs.com – makers of ZoneAlarm firewall software.

www.grisoft.com – makers of AVG anti-virus software.

www.microsoft.com/athome/security/spyware/software/default.mspx - home of Microsoft AntiSpyware

www.lavasoft.com – maker of Ad-Aware anti-spyware software.

www.safer-networking.org/en/home - home of Spybot Search & Destroy anti-spyware software.

www.snort.org – home of Open Source Intrusion Detection System called Snort.

http://netsecurity.about.com/od/readproductreviews/fr/aapr091904.htm - product review of Prevx Home by Tony Bradley.

www.iss.net – home of Internet Security Systems, Inc.

http://castlecops.com/forum-cat37.html - Prevx Support Forum

www.techsupportalert.com/intrusion-detection.htm - Tech Support Alert review of IDS and IPS.

http://msn-cnet.com.com/Prevx-Home/3000-8022_4-10364927.html - Download.com review of Prevx Home.