BBX Fights the Unknown

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

After the first articles in my little series on intrusion detection appeared, several firms in the active intrusion-response arena contacted me with breathless enthusiasm about their products. I recently had an enjoyable chat with two enthusiastic computer security executives who filled me in on their progress towards another weapon for the constant war against The Bad Guys. [Note that I have no financial interest or any other relationship with BBX other than finding my two interlocutors very friendly, likeable and intelligent folks.]

***

James G. Kollegger [JK] is President and CEO of BBX Technologies <http://www.bbxtechnologies.com>. A former Operations and Command Information Officer in the U.S. Army Strategic Communications Command, Mr. Kollegger went on to a varied career in the information technology industry with special emphasis on managing high-technology startups.

John R. Michener, PhD [JM] is Chief Scientist and VP for Business Development at BBX. Dr. Michener has patents in cryptography and network security and has worked with security for Siemens and Novell. He is a widely published author (see pointers at the end of this article) who has a long career in security and e-commerce.

[MK] So how did you get involved in this project?

[JK] We got involved about 18 months ago. We always look for revolutionary or disruptive technologies. Our sense was that the computer security industry was ripe for this kind of change because three elements were fast coming together, literally like a “Perfect Storm”:

1. Increased use of the Internet, despite the security risks. Businesses, the military, and civilian agencies are not just using the Internet, they’re building business models on it. Browsing the web is inherently not secure. People just don’t understand how vulnerable they are to subversion of their systems by malicious and clever software. I asked the CTO of a Fortune 100 company what his biggest security headache was—he said it was PC’s exposed to the Internet.

2. New technology emerges constantly creating further weaknesses in this fabric-- e.g., new cell phones that upload data to computers, flash drives that slip into your pocket. These are real security problems. For example in Washington, a federal CIO told us that Blackberries are a major problem because they’re not secure and also the servers are in Canada. A second problem he faces is USB flash drives that can easily be plugged into a computer to upload malware. Even automated email verification updates can be dangerous – they can download probes you can’t even see.

3. The new breed of hackers are more sophisticated, more technologically expert and more
politically motivated. We have discovered hackers in China and Eastern Europe who are…

[JM] … they’re not really just hackers: they’re more like tool developers. For example, one of them developed a screen-scraping tool for collecting user IDs and passwords from Web logins that is as good as a keystroke logger for breaking identification and authentication controls.

[JK] Last summer, some Chinese hackers tried to seize control of a Navy ship (they failed). So this breed of arms merchants to the digital wars produces a scenario that isn’t very pretty. You look at the current defenses—firewalls, anti-virus, IDS, intrusion prevention – a good part of the new attacks will get through. These old methods are signature based and they’re always playing catch-up. So we developed an entirely new approach. Our system doesn’t try to find out what the malware looks like; it addresses keeping the integrity of the computer intact. And that’s why EDS and other big integrators are taking our products into the market as the final shield—the last line of defense.

[MK] Much like the heuristic systems of antivirus products.

[JM] We’re really looking at an integrity lockdown. Applications should deal with data but not modify executables. In general, your software should change only when an authorized individual is installing or updating software. Thus, we can start from the approximation that the executable environment should be invariant. So we started off looking for modifications of about 13 types of files. If the software sees a new or changed executable on the system, it queries a policy layer that we have implemented. First we ask if the changed software is storing data (Some applications store data in DLL’s. We allow the administrator to enter such files into a “ignore changes” list.) ; or maybe it’s part of a directory tree where changes are allowed. If it’s allowed, it goes in. If it’s not, our software deletes the executable and issues a management report. We focus on the system and operating system directories where we detect all changes to the executable environment; but unlike other products, we detect and deal with the addition of unauthorized executables anywhere in the protected system; we have instrumented the kernel and the file system and this allows us to monitor all the changes. A direct benefit of this approach is it allows us to deal with any attack that carries an executable payload without requiring a signature.

We assume that what’s in your computer when we install is the baseline; anything else gets knocked out. For example, we’ve installed with BackOrifice already in place; when the malware goes active, we detect its attempts to modify code and we delete it. If an administrator tries to kill our process, the command is rejected. We provide a dual key system that can be configured to permit such inactivation. First you need to authorize the removal and then you can remove the protective process. In the newest version, we’re adding the capability for real-time filtering of new installs.

Our current product allows authorized updates such as antivirus products or software upgrades into administrator settable directory subtrees. Supporting trusted updates of arbitrary files and locations across the system will have to involve digital certificates if you expect to protect the system against Trojans.

* * *

I would like to congratulate these gentlemen: in the entire discussion, they did not discuss the
names of their products a single time. You’ll just have to explore their Web site (http://www.bbxtechnologies.com) to find out what they’re selling. My thanks to Jim and John for their time.

* * *

Some papers by Dr Michener:


* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www3.norwich.edu/msia> for full details.


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2003 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.