Application Software and Security
by Gary C. Kessler

Mich Kabay writes: My friend and colleague Prof. Gary Kessler is the Program Director of the Computer Networking major at Champlain College in Vermont <http://neworking.champlain.edu/> and chair of the Vermont InfraGard chapter <http://www.vtinfragard.org>. He always has interesting thoughts about practically everything, and today I am offering you his thoughtful and thought-provoking essay on the long-term security implications of the software we choose.

* * *

I [Gary Kessler] was in a discussion recently with a colleague in my college's Web Design major. I was venting frustration with Web designers who build their pages using features only supported by one browser (invariably Internet Explorer). "When I was a baby programmer," I snorted, "we designed code for the ease of the user not the ease of the developer.” His retort was that IE got market share and Navigator lost market share because the folks at Netscape didn't add support of all of the fancy bells and whistles that Microsoft did.

This conversation and countless similar ones have been simmering in my overheated brain for a while and it dawned on me that the problem is as much application as it is operating system. And the bottom-line is this question: We all talk a good security story, but do we practice what we preach and do we put our money where our mouths are?

Let me focus for now on Microsoft network applications. All companies that use these application make a specious argument about "productivity” versus security. But if you really care about information security, how can you justify using products that seem to have a never-ending stream of security vulnerabilities, are subject to frequent attacks by Bad Guys, and are common attack vectors for viruses, worms, and other exploits – all this trouble to enhance user productivity? There are other products to enhance user productivity that don’t have this lamentable history of security failures.

As an example, why do so many sites use Outlook when it is known to be hard to secure, rarely used in a secure fashion anyway, and is a major target of attacks? When one considers the features needed by most users, there are many other clients that provide equivalent functionality (including a shared calendar function).

The same can be said about the Internet Information Service software. IIS is not the best nor most feature-rich Web server -- nor is it the only free one. It is, however, susceptible to the most HTTP attacks and recent advisories warn us about vulnerabilities with... the Microsoft extensions to HTTP. So tell me again, why are we using IIS?

I am not bashing Microsoft; I am merely reporting the headlines. In fact, there are probably a number of good reasons to use Outlook and/or IIS. All too often, however, these applications are used for no other reason than because they are there or because they were recommended by a consultant – usually one who also sells and/or supports this software.

What I am suggesting is that we take the precepts of defense-in-depth seriously and seriously
consider the equivalent of biodiversity, as well. Microsoft has long claimed that the computer world and cyberspace would be safer with monolithic software; i.e., operating system, browser, and application suites all from the same source. But I would suggest that the exact opposite provides the best possible defense. Ecosystems with a diverse set of organisms are more stable than monocultures.

I have been fortunate to date in that I have never had a virus problem on one of my own personal systems. Or, put another way, I have been careful and vigilant. Although I usually use a Microsoft Windows operating system, I employ network applications, anti-virus software, and personal firewall software all from different vendors -- even though this sometimes costs money. And just as biodiversity protects forests and farm crops from the devastating effects of a species-specific disease, I avoided getting smacked by Code Red, Nimda, Klez, and BugBear. A large number of my all-Microsoft colleagues have not been as lucky.

So I really do have a point. Security takes time and money -- but not as much as some would make you think. It makes no sense to use software just because it is “free” if it comes with a very high hidden cost and is, in fact, inferior to alternatives. And if we always take the path of least resistance, using software merely because it shipped with the operating system rather than choosing the best software for our given tasks, we will eventually end up with no software choice at all.

* * *

Gary C. Kessler can be reached at <mailto:kumquat@sover.net>. More information about Gary can be found at <http://www.garykessler.net>.

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www.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 <mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2002 Gary C. Kessler. 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.