Title:
Why Easy To Use Software Is Putting You At Risk

Word Count:
1117

Summary:
Article about how complex systems, software, and operating systems may be putting you at risk for infection and security breaches. Computer code has become way to complex in the name of ease of use and functionality.

Keywords:
Insecure software, security holes, software attacking viruses, application backdoors, poorly developed software, application failures, complex applications

Article Body:
Can Easy To Use Software Also Be Secure

Anyone who has been working with computers for a long time will have noticed that mainstream operating systems and applications have become easier to use over the years (supposedly). Tasks that use to be complex procedures and required experienced professional to do can now be done at the push of a button. For instance, setting up an Active Directory domain in Windows 2000 or higher can now be done by a wizard leading even the most novice technical person to believe they can "securely" setup the operating environment. This is actually quite far from the truth. Half the time this procedure fails because DNS does not configure properly or security permissions are relaxed because the end user cannot perform a specific function.

If It's Easy To Develop, Is It Also Secure

One of the reasons why operating systems and applications "appear" to be easier to work with then they use to is developers have created procedures and reusable objects to take care of all the complex tasks for you. For instance, back in the old days when I started as a developer using assembly language and c/c++, I had to write pretty much all the code myself. Now everything is visually driven, with millions of lines of code already written for you. All you have to do is create the framework for your application and the development environment and compiler adds all the other complex stuff for you. Who wrote this other code? How can you be sure it is secure. Basically, you have no idea and there is no easy way to answer this question.

Secure Environments Don't Exist Well With Complexity

The reality is it may look easier on the surface but the complexity of the backend software can be incredible. And guess what, secure environments do not coexist well with complexity. This is one of the reasons there are so many opportunities for hackers, viruses, and malware to attack your computers. How many bugs are in the Microsoft Operating System? I can almost guarantee that no one really knows for sure, not even Microsoft developers. However, I can tell you that there are thousands, if not hundreds of thousands of bugs, holes, and security weaknesses in mainstream systems and applications just waiting to be uncovered and maliciously exploited.

How Reliable and Secure are Complex Systems?

Let's draw a comparison between the world of software and security with that of the space program. Scientists at NASA have know for years that the space shuttle is one of the most complex systems in the world. With miles of wiring, incredible mechanical functions, millions of lines of operating system and application code, and failsafe systems to protect failsafe systems, and even more failsafe systems to protect other systems. Systems like the space shuttle need to perform consistently, cost effectively, and have high Mean-Time-Between-Failure(MTBF).

All in all the space shuttle has a good record. One thing it is not though is cost effective and consistent. Every time there is a launch different issues crop up that cause delays. In a few circumstances, even the most basic components of this complex system, like "O" rings, have sadly resulted in a fatal outcome. Why are things like this missed? Are they just not on the radar screen because all the other complexities of the system demand so much attention? There are million different variables I'm sure. The fact is, NASA scientists know they need to work on developing less complex systems to achieve their objectives.

This same principal of reducing complexity to increase security, performance, and decrease failures really does apply to the world of computers and networking. Ever time I here associates of mine talk about incredibly complex systems they design for clients and how hard they were to implement I cringe. How in the world are people suppose to cost effectively and reliably manage such things. In some cases it's almost impossible. Just ask any organization how many versions or different brands of intrusion detection systems they have been through. As them how many times the have had infections by virus and malware because of poorly developed software or applications. Or, if they have ever had

a breach in security because the developer of a specific system was driven by ease of use and inadvertently put in place a piece of helpful code that was also helpful to a hacker.

Can I Write A Document Without A Potential Security Problem Please
---

Just a few days ago I was thinking about something as simple as Microsoft Word. I use MS-Word all the time, every day in fact. Do you know how powerful this application really is? Microsoft Word can do all kinds of complex tasks like math, algorithms, graphing, trend analysis, crazy font and graphic effects, link to external data including databases, and execute web based functions.

Do you know what I use it for, to write documents. nothing crazy or complex, at least most of the time. Wouldn't it be interesting that when you first installed or configured Microsoft Word, there was an option for installing only a bare bones version of the core product. I mean, really stripped down so there was not much to it. You can do this to a degree, but all the shared application components are still there. Almost every computer I have compromised during security assessments has had MS-Word installed on it. I can't tell you how many times I have used this applications ability to do all kinds of complex tasks to compromise the system and other systems further. We'll leave the details of this for another article though.

Conclusion

Here's the bottom line. The more complex systems get, typically in the name of ease of use for end users, the more opportunity for failure, compromise, and infection increases. There are ways of making things easy to use, perform well, and provide a wide variety of function and still decrease complexity and maintain security. It just takes a little longer to develop and more thought of security. You might think that a large part of the blame for complex insecure software should fall on the shoulders of the developers. But the reality is it is us, the end users and consumers that are partially to blame. We want software that is bigger, faster, can do just about everything, and we want it fast. We don't have time to wait for it to be developed in a secure manner, do we?

Original URL (The Web version of the article)
---

http://www.defendingthenet.com/NewsLetters/WhyEasyToUseSoftwareIsPuttingYouAtRisk.htm