

Linux security strong as ever

Contributed by Linux
Tuesday, 08 August 2006

Linux security is as strong as ever, despite recent statistics that say otherwise. Perhaps in response to the excessive publicity given to the strong security associated with Linux and open source software, it's no surprise that a number of commentators are making a high-profile argument that Linux, just like every other platform, does indeed have security issues. Members of the open source community have always known that Linux is not immune from security threats, so there is no argument there. What is in question is the final conclusion that these commentators are drawing, which is that Linux is less secure than Microsoft Windows.

Linux security is as strong as ever, despite recent statistics that say otherwise. Perhaps in response to the excessive publicity given to the strong security associated with Linux and open source software, it's no surprise that a number of commentators are making a high-profile argument that Linux, just like every other platform, does indeed have security issues. Members of the open source community have always known that Linux is not immune from security threats, so there is no argument there. What is in question is the final conclusion that these commentators are drawing, which is that Linux is less secure than Microsoft Windows.

Fighting for security for the past 20 years, almost all Linux professionals are also Unix professionals, many of whom have been dealing with online security threats for over 20 years. Remember, the Unix community (and subsequently the Linux community) is the group that first created and still forms the backbone of the Internet. This community was dealing with serious security threats, like the Internet (i.e., Morris) Worm, before Windows NT even existed. Unix users know network and host security inside and out and were the first to implement almost all the intrusion-detection, perimeter-defense, and security-analysis technologies that our industry uses today. Linux/Unix is not invincible from security threats, it's true; but this group has spent the last 20-plus years ensuring that Linux/Unix is more secure than any other system. Yet the pundits who have raised their voices in recent months, including people who should know better, like Paul Thurrott (of WinInformant), are questioning this generally accepted notion among IT professionals that Linux is more inherently secure than Microsoft's professional operating system platforms. For instance, Thurrott has stated: "In Friday's WinInfo Daily Update newsletter, I mentioned a set of statistics from BugTraq, a reputable security/information provider, that shows how various OSs compare security-wise. The statistics show a surprising trend: When you aggregate all the Linux distributions, Linux, not Windows, has had the most security vulnerabilities, year after year."

The Linux way
As I said earlier, there is no shame in conceding that there are no truly secure operating systems. There is only the ongoing process of trying to keep a host or network secure. Security is like a treadmill. If you don't move forward with security patches, security tools, and revamped system security processes, you'll be flung off the end of it. Oh, and by the way, the crackers have access to the treadmill's speed control knob, and they keep increasing the speed. Needless to say, security is a difficult and continuing effort. The open source community has worked diligently to fight the good fight against security vulnerabilities. One of this community's basic security philosophies is, "With enough eyeballs, all bugs are shallow." This Linux axiom points to the fact that when a bug becomes an issue, many people have the source code, and it can be quickly resolved without the help of a vendor.