Risks of Monoculture

The W32/Blaster worm burst onto the Internet scene in August of 2003. By exploiting a buffer overflow in Windows, the worm was able to infect more than 1.4 million systems worldwide in less than a month. More diversity in the OS market would have limited the number of susceptible systems, thereby reducing the level of infection. An analogy with biological systems is irresistible.

When a disease strikes a biological system, a significant percentage of the affected population will survive, largely due to its genetic diversity. This holds true even for previously unknown diseases. By analogy, diverse computing systems should weather cyber attacks better than systems that tend toward monoculture. But how valid is the analogy? It could be argued that the case for computing diversity is even stronger than the case for biological diversity. In biological systems, attackers find their targets at random, while in computing systems, monoculture creates more incentive for attack because the results will be all the more spectacular. On the other hand, it might be argued that cyber-monoculture has arisen via natural selection—providers with the best security products have survived to dominate the market. Given the dismal state of computer security today, this argument is not particularly persuasive.

Although cyber-diversity evidently provides security benefits, why do we live in an era of relative computing monoculture? The first-to-market advantage and the ready availability of support for popular products are examples of incentives that work against diversity. The net result is a "tragedy of the (security) commons" phenomenon—the security of the Internet as a whole could benefit from increased diversity, but individuals have incentives for monoculture.

It is unclear how proposals aimed at improving computing security might affect cyber-diversity. For example, increased liability for software providers is often suggested as a market-oriented approach to improved security. However, such an approach might favor those with the deepest pockets, leading to less diversity.

Although some cyber-diversity is good, is more diversity better? Virus writers in particular have used diversity to their advantage; polymorphic viruses are currently in vogue. Such viruses are generally encrypted with a weak cipher, using a new key each time the virus propagates, thus confounding signature-based detection. However, because the decryption routine cannot be encrypted, detection is still possible. Virus writers are on the verge of unleashing so-called metamorphic viruses, where the body of the virus itself changes each time it propagates. This results in viruses that are functionally equivalent, with each instance of the virus containing distinct software. Detection of metamorphic viruses will be extremely challenging.

PAUL WATSON

Is there defensive value in software diversity of the metamorphic type? Suppose we produce a piece of software that contains a common vulnerability, say, a buffer overflow. If we simply clone the software—as is standard practice—each copy will contain an identical vulnerability, and hence an identical attack will succeed against each clone. Instead, suppose we create metamorphic instances, where all instances are functionally equivalent, but each contains significantly different code. Even if each instance still contains the buffer overflow, an attacker will probably need to craft multiple attacks for multiple instances. The damage inflicted by any individual attack would thereby be reduced and the complexity of a large-scale attack would be correspondingly increased. Furthermore, a targeted attack on any one instance would be at least as difficult as in the cloning case.

Common protocols and standards are necessary in order for networked communication to succeed and, clearly, diversity cannot be applied to such areas of commonality. For example, diversity cannot help prevent a protocol-level attack such as TCP SYN flooding. But diversity can help mitigate implementation-level attacks, such as exploiting buffer overflows. As with many security-related issues, quantifying the potential benefits of diversity is challenging. In addition, metamorphic diversity raises significant questions regarding software development, performance, and maintenance. In spite of these limitations and concerns, there is considerable interest in cyber-diversity, both within the research community and in industry; for an example of the former, see www.newswise.com/articles/view/502136/ and for examples of the latter, see the Cloakware.com Web site or Microsoft's discussion of individualization in the Windows Media Rights Manager. C

Mark Stamp (stamp@cs.sjsu.edu), an assistant professor of computer science at San Jose State University, recently spent two years working on diverse software for MediaSnap, Inc.