



Software Monoculture

A lesson from Irish history

by Aniruddha Chatterjee

By the mid 1800s, the Irish poor had their stock in one plant: the potato. Eschewing other crops, like barley and wheat, they even cut the total number of popular potato varieties to only two. Then, in 1845, the *phytophthora infestans* fungus arrived from North America, decimating this low cost food supply for the next five years. Three million of Ireland's poor, over a third of the population, starved to death. Now, just over 150 years later, the world is facing a similar threat though not from fungus, but rather a digital pest.

Shortly after the year 2000, the world largely chose one operating system: Microsoft Windows. Eschewing other products such as Apple's OS, Linux and Apache, people placed Windows not only on their PCs but on their servers as well. Then, on August 11, 2003, the Blaster worm, a particularly virulent computer virus, struck and proceeded to decimate computer networks for the next few days. Close to 16 million computers were affected and the economic damage is estimated to be hundreds of millions of dollars.

Many critics believe the destructiveness of the Blaster worm's attack is a result of the world's over-reliance on Microsoft Windows. Drawing from evolutionary science, the authors of "CyberInsecurity: The Cost of Monopoly"—Daniel Geer, Charles Pfleeger, Bruce Schneier, John Quarterman, Perry Metzger, Rebecca Bace and Peter Gutmann—argue that Internet security is impaired by the uniformity of the world's operating systems. The key to promoting robustness of the computer ecosystem, the authors cite, is to avoid "monoculture," the abundance of just one crop or animal. The solution is to favor organism diversity. If the Irish planted a greater variety of food crops, they could have survived the blight with other reliable food sources. Similarly, the authors contend, a diversity of operating systems would mitigate the level of harm that could be brought about by a single virus.

The report, authored by a panel of computer

security experts from throughout the industry and available at the Computer and Communications Industry Association website, highlights recent viral attacks against Microsoft-based computer systems. These large attacks are the product of "cascading failures," caused as viruses and worms hop from one similar system to another. The similar computer systems have common weaknesses which viruses can easily exploit, subverting one system and then moving on to the next and repeating the process. Subversions can range from the artificial increase of network traffic which causes a jam that slows the Internet all the way to the deletion of important files from one's hard drive.

The only solution, in the authors' eyes, is system diversification. Like the recommendation that Irish planting numerous crops, instead of just the potato, the authors would like to see the wider variety of operating systems on the world's computers.

The greatest hindrance to diversification, according to the report, is Microsoft. With estimates placing Windows' market share upwards of 97%, the computer world is definitely a Microsoft monoculture. This great market share, "CyberInsecurity's" authors contend, arises from the manner in which Microsoft products are constructed and marketed. Acknowledging that computer security policy is tied to competition, they advocate forcing Microsoft to open its system and allow consumers to mix and match components from Microsoft with other vendors. They also suggest limits on the market share of a single operating system in critical industries and in government.

But the monoculture theory has its detractors. Some in the computer security industry believe that the discussion about monoculture ignores the variety of security threats that are less dependent on which operating system one uses. Computer security expert Mark Ranum, talking to CNN.com, points out that regardless of how many varieties of corn one plants in a plot, if it is not fenced, deer will eat everything.

Microsoft's security chief strategist, Scott Charney, has qualms about monoculture theory's lack of reasonable solutions. Increasing diversity to just two or three operating systems will hardly slow hackers. For diversity to have an impact, Charney contends, will require thousands of different operating systems, rendering interoperability painful, if not impossible.

Microsoft's dominance in computer software has been criticized from many angles. Now, computer security concerns can be added to the litany of issues surrounding Microsoft's monopolistic position. Although monoculture must be weighed against interoperability and other concerns, those scrutinizing Microsoft's market position would do well to have the Irish potato famine in the back of their minds. **S**



The lack of diversity in operating systems is a risk to computer security.