Introducing "Insecure IT"

Rick Kuhn, NIST Hart Rossman, SAIC, Simon Liu, NLM

As its title suggests, this department will be about security in IT systems, ranging from desktops to global e-commerce networks. Our goal, of course, is to offer ideas to improve IT security, by looking at ways it can go wrong, as well as covering good practices. As most security practitioners and researchers have seen, new technology developments nearly always introduce a period in which attackers find relatively easy ways to exploit weaknesses, followed by a gradual closing of vulnerabilities. Wireless networking is a classic example – initially more than half of home users, and a high percentage of business users, installed 802.11 wireless with no security measures. Some spectacular incidents resulted from widespread ignorance of basic wireless security measures. By analyzing vulnerabilities in real systems, we hope to encourage readers to not only avoid similar problems in their own systems, but possibly generalize the lessons to new technologies as they appear. This will be a regular department, and we encourage readers to submit articles and share their lessons with the world.

In keeping with our theme of understanding vulnerabilities to improve enterprise security, we should first take a look at the current state. What are the trends in enterprise security, and where do we stand today? There are two ways to look at these questions: attacks and the vulnerabilities that are targeted by attackers. The latter of these bears directly on the organization's cost to protect assets, because it indicates the effort that is required to patch applications and close security holes as they are discovered. Using NIST's National Vulnerability Database (NVD), we can get a sense of where we are today and what will be important in the near future. The NVD provides fine-grained search capabilities for all known vulnerabilities and is continuously updated, to provide data for automated vulnerability management, security measurement, and compliance. With data going back to 1997, we can also use NVD to see trends in IT vulnerabilities over the years.

The NVD data in Figure 1 gives us some good news and bad news. Clearly, vulnerabilities have increased dramatically in the past few years, and the increase has come from the ones that are most severe. But data for the last two years show a downward trend (2008 figures projected from 10 months of data). While it often seems that software is full of holes and is only getting worse, things really are improving.

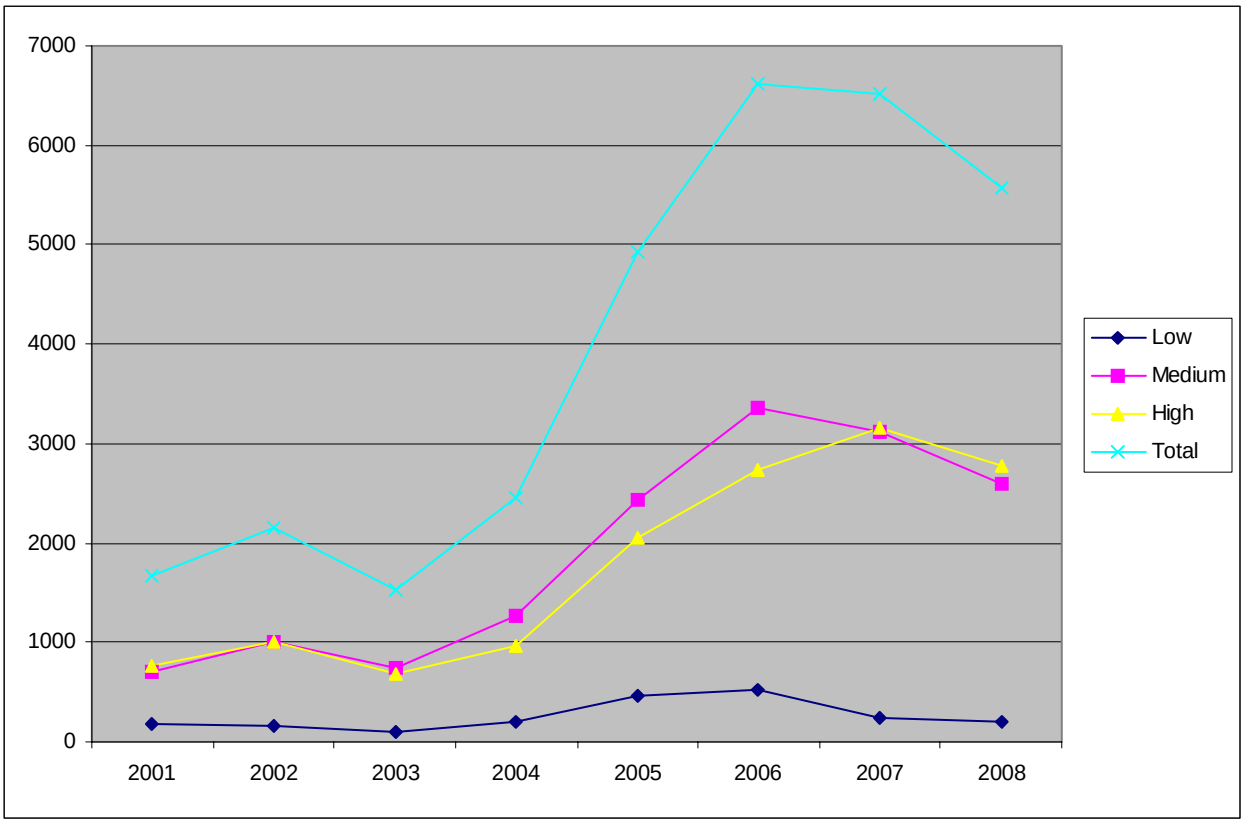

Figure 1. Vulnerabilities by severity

Of course the improvement is relative to the explosion of new vulnerabilities since 2003, and no one responsible for their organization's IT security can be happy with the appearance of over 5,000 new vulnerabilities in a year. Nevertheless, this is the first two-year decline in the data, and the decline from 2007 to 2008 was much more dramatic than the previous year. It's also important to note that this chart covers data from thousands of products. Digging in to the data a bit more, Figure 2 shows the types of vulnerabilities that were discovered in 2008. Vulnerabilities are categorized in Figure 2 using the Common Weakness Enumeration (CWE), which defines a standardized description of software weaknesses designed to provide a common language for describing software security weaknesses. Using CWE, developers and analysts have a standard definition of terms for investigating security problems in architecture, design, and code. CWE also helps in comparing tools that attempt to find security weaknesses.

Buffer overflows, long the most common security bug, are now a distant third, behind two web-based vulnerabilities, SQL injection and cross-site scripting. As can be seen from the left hand side of Figure 2, traditional vulnerabilities affecting operating systems and stand-alone applications have become relatively rare. For example there were only 13 reports of race condition exploits (e.g., changing a file link between the time permission is checked by the OS and the time that the requested operation is performed). Careless applications of cryptography, such as employing a weak encryption scheme, used to be common as well, but only 26 examples were reported for 2008. Some old favorites, however, remain in the middle of the pack, such as poorly configured access control and failure to validate input remain perennial problems. All in all, it appears that software developers are finally beginning to turn a corner in their efforts to

stamp out security-critical bugs, but the data from Figure 2 clearly show that newer technologies, such as web services, bring new bugs to catch.

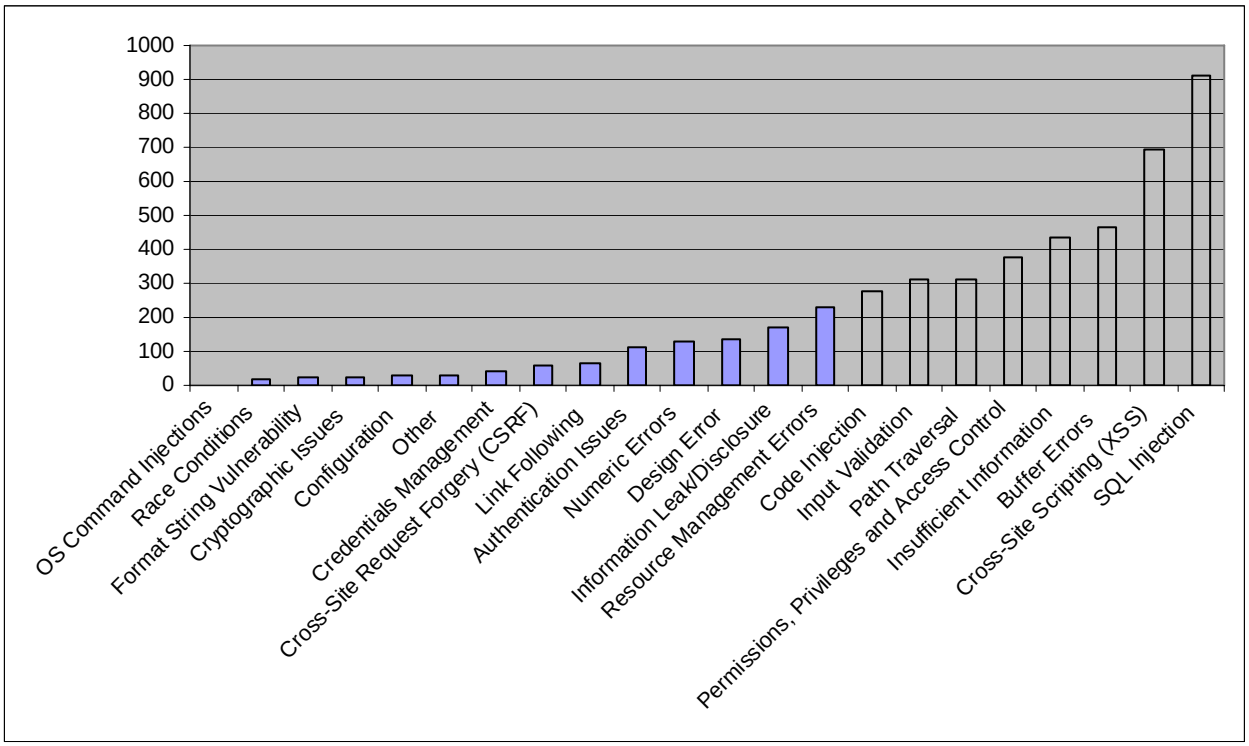

Figure 2. Vulnerabilities by type (Jan – Oct, 2008)

What this means for software developers and system administrators is that their vigilance is paying off across systems with a wide install base and significant time in the field. While this past summer's announcement of a fundamental flaw in DNS by Dan Kaminsky reminds us that core protocols and services still require additional scrutiny and research, it is clear that lessons learned have been adopted across industry and best practices have been proven out. However, emerging technologies and new use cases for established systems are providing fertile ground for new types of vulnerabilities susceptible to an ever creative and persistent adversary. Priorities for attackers and defenders alike have moved to the application space; with an emphasis on anything web oriented or net-centric in nature. This trend can only be expected to accelerate with the proliferation of "always on" robust mobile computing platforms ranging from smart phones to netbooks; and the ever increasing prevalence of net-enabled consumer products in every aspect of our lives. The walls of the enterprise have become blurred and software developers and system administrators will continue to experience an evolving landscape rife with opportunity to actively manage the risk of the systems they develop, deploy, and operate.

Help comes in a variety of forms, from community driven organizations that promulgate best practices and vulnerability watchlists such as the Open Web Application Security Project (www.owasp.org) to you, the reader. We heartily encourage your thoughts and look forward to including your submissions in future columns and as part of our upcoming annual issue focusing on security.

Disclaimer: Certain software products are identified in this document. Such identification does not imply recommendation by NIST or other agencies of the U.S. Government, nor does it imply that the products identified are necessarily the best available for the purpose.