Method to Better Predict Software Vulnerabilities

June 29 2006

Vulnerability defects in software that can allow hackers to bypass security measures have emerged as a significant threat in a society that increasingly relies on computer systems and the Internet for commerce and other uses.

Researchers at Colorado State University have developed a model to predict with much greater accuracy the number and severity of vulnerabilities that will likely surface in operating systems and in major software applications in the near future. The research is lead by Yashwant K. Malaiya, professor in the Department of Computer Science in Colorado State's College of Natural Sciences. Malaiya is assisted by doctoral student Omar Alhazmi.

In 2005 alone, 5,198 newly discovered vulnerabilities were reported by the U.S. Department of Homeland Security's Computer Emergency Readiness Team, or CERT. Such vulnerabilities can be exploited by hackers if they are discovered and not quickly fixed through patches - updates to fix security problems.

"The hope is that a vulnerability gets patched before it gets exploited," Malaiya said. "Each individual vulnerability discovered can be widely reported to the public, and in some cases, it has caused the value of the stock of the company to drop."

It is impossible to implement an operating system like Windows XP or Linux, Web servers like Apache or Microsoft IIS, or Web browsers that are free from vulnerabilities, Malaiya said. If developers knew when and how many patches will be needed in a certain period of time, they could be better prepared to quickly develop patches and ensure the security of such applications and systems, he said.

Malaiya's group has developed two complementary approaches to predict vulnerabilities: modeling of the vulnerability detection rate with the Alhazmi-Malaiya Logistic model and based on the developer, predicting the number of vulnerabilities per 1,000 lines of code.

The research group at Colorado State is the only university team that is conducting a systematic study of the vulnerability discovery process. Some early results have attracted attention by CERT analysts, and some of their results appear in the book "Secure Coding in C and C++," published in 2005 by CERT.

Applications of such data can be far-ranging, Malaiya said. Companies like Microsoft can project the manpower needed to quickly develop and release patches to minimize the probability of exploitation. An investment company, such as a bank or a brokerage, can better assess the potential risk levels because products containing more projected vulnerabilities tend to be riskier products.

The Alhazmi-Malaiya Logistic model has already seen success in its predictions:

-- In 2005, it predicted the number of vulnerabilities discovered in Windows XP would grow rapidly. It has indeed grown from 88 in January 2005 to 173 by the latest count, making the vulnerability density of XP comparable to that of earlier version of Windows.

-- The model predicted that very few new vulnerabilities will be found in Red Hat Linux 6.2, and the number has stayed unchanged at 117.

-- It predicted that the number of vulnerabilities of Windows 2000 will eventually range from 294 to 410. At that time of the prediction, the number was 172; it now is 250, and vulnerabilities are still being found.

Source: Colorado State University

Citation: Method to Better Predict Software Vulnerabilities (2006, June 29) retrieved 19 April 2024 from https://phys.org/news/2006-06-method-software-vulnerabilities.html