BY GEORGE V. HULME

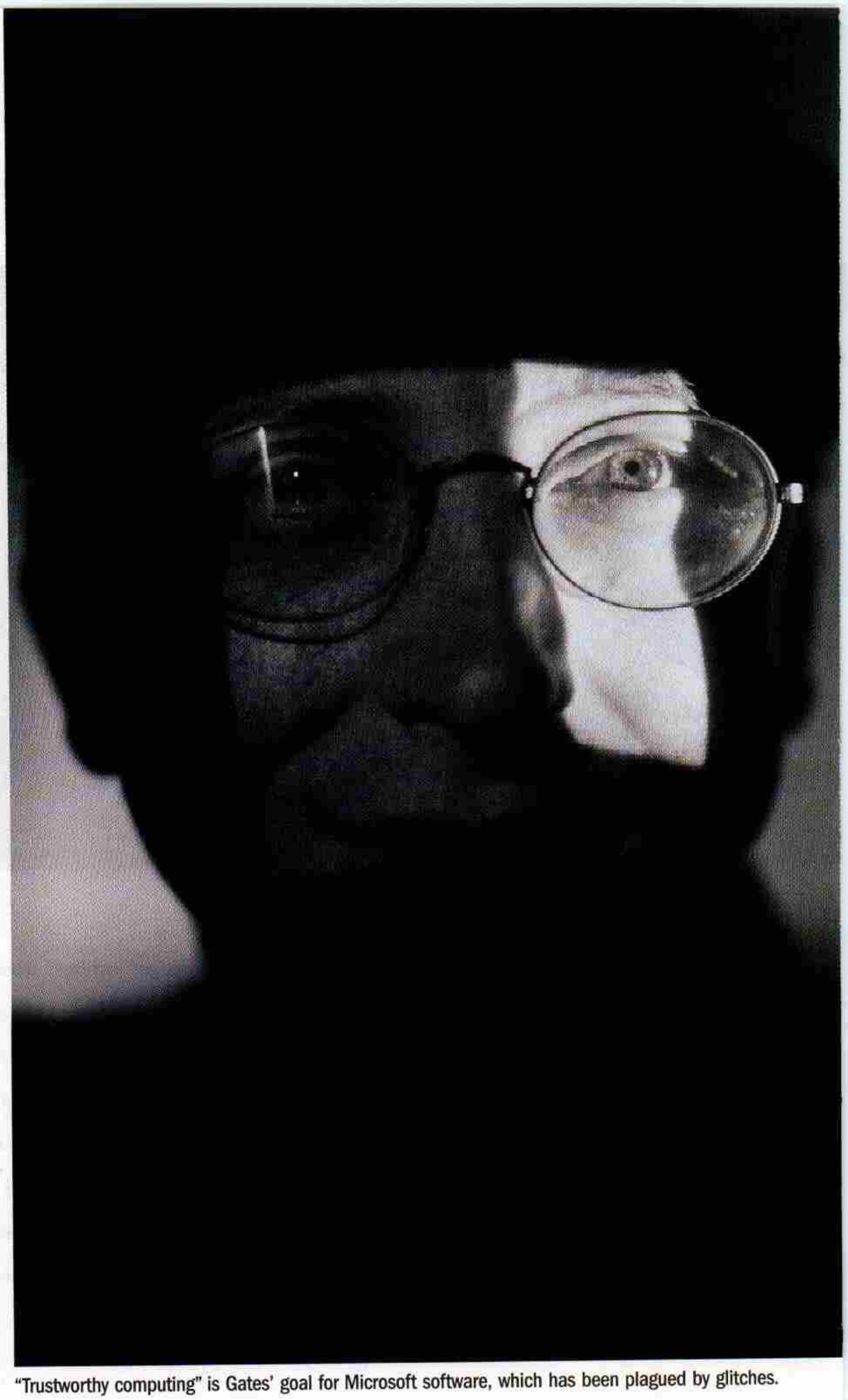
Bill Gates finally got the message, and now he's delivered it to everyone else at Microsoft. In one of his stake-in-the-ground memos to the company's entire workforce, the chief software architect last week said there must be a companywide emphasis on developing high-quality code that's available, reliable, and secure—even if it comes at the expense of adding new features.

Many IT professionals consider the commitment long overdue and not just from Microsoft. Poor software quality and security remain major problems for many businesses as they grapple with a steady flow of applications, upgrades, and fixes. Carnegie Mellon University's CERT Coordination Center, a security watchdog group, says the number of software vulnerabilities reported last year more than doubled to nearly 2,500.

It's an issue that keeps IT departments busy and one that can put business data—including personal and customer information—at risk. "We get CDs of bug fixes every month from our application vendors. We've had to develop our own rigorous suite of tests to stress these apps and make sure we can run our business on them before we deploy them in the production environment," says Jerry Hale, CIO of Eastman Chemical Co. in Kingsport, Tenn. "It's very difficult to recover from some of these bugs, and it's quite costly, too."

In an internal E-mail to employees, Gates coined the term "trustworthy computing" to describe his ambitious goal of software improvement. "As an industry leader, we can and must do better," he wrote. (To read the entire memo, go to *informationweek.com/872/gates.htm.*)

No one would disagree. At stake is customer confidence in Microsoft's Windows XP operating system, emerging .Net infrastructure products, and database and server platforms. "One of the biggest things they hear is, 'You guys get hacked.' Nothing stops a meeting faster than that," says Kerry Gerontianos, president of Incremax Technologies Corp., a New York development shop and president of the New York chapter of the International Association of Microsoft Certified Partners.



"Trustworthy computing" is Gates' goal for Microsoft software, which has been plagued by glitches.

Gates' E-mail was sent the very day the company recovered from a five-day stretch of system glitches that caused Microsoft's Windows update feature to fail intermittently. Users were unable to download software or security-related updates. A month earlier, Microsoft had to fix a potentially serious security hole in Windows XP, which it touts as its most secure operating system yet. And last year, a spate of Internet worms infected Windows computers at thousands of companies.

Microsoft is by no means alone in dealing with reliability shortcomings. The National Infrastructure Protection Center's 2001 summary of software vulnerabilities is 70 pages long, representing companies from Adobe to Zendown. Security expert David Litchfield with Next Generation Security Software Ltd. in Surrey, England, recently identi-

Software's Challenge

It's time for developers to think and act differently

fied several holes in Oracle9i software. In recent weeks, buffer overflow problems have plagued versions of Sun Microsystems' Solaris and IBM's AIX operating systems and America Online's Instant Messaging software. Buffer overflow occurs when the amount of data written to a segment of memory exceeds the memory that's available.

What's wrong? Most security problems are caused by known defects in code, says Watts Humphrey, a fellow at the Software Engineering Institute, a research and development center operated by Carnegie Mellon and a former director of programming quality at IBM. Left unrepaired, the flaws provide hackers with opportunities to break into systems, he says.

If Microsoft is serious about addressing quality problems, Humphrey says, it needs to change an engineering culture that relies too heavily on catching problems during testing, rather than preventing them in development. Even experienced programmers inject about one defect into every 10 lines of code, according to the Software Engineering Institute. If 99% of those are caught, that's still 1,000 bugs in a 1 million-line application. "It doesn't take much for someone on the Internet to bust into a system of that kind of quality," Humphrey says.

Microsoft plans to build tools into Windows that report software problems back to Microsoft and, ultimately, fix them automatically. For many companies, the current process of downloading patches is onerous at best. "We're way too distributed," says John Thomas, CIO at Parsons Corp., a Pasadena, Calif., engineering and construction company with about 10,000 PCs worldwide. Thomas says he'd trade new Windows features for better code, but he's skeptical that Microsoft can deliver. "There's always this promise that the next operating system is going to be more reliable," Thomas says. "But we don't see it."

Skepticism runs high about Microsoft's ability to, in Gates' words, "lead the industry to a whole new level of trustworthiness" in computing. "I don't buy it," says Dan Kesl, information security officer at Newmont Mining Corp. in Denver. "I have no faith in Microsoft when it comes to security." Newmont uses Windows on internal systems, but chose Unix for Internet applications because Kesl considers it more secure.

Other vendors need to be careful in making claims of superiority. At an industry trade show in New York last month, Oracle CEO Larry Ellison bragged that, despite 30,000 attempts a day, hackers have been unsuccessful at breaking into Oracle's Web site since the company launched a marketing campaign touting its software as being "unbreakable." But within a week, software snoop Litchfield published an advisory about a buffer overflow in Oracle9i Application Server, which Oracle has since fixed. Litchfield says he knows of seven other vulnerabilities in Oracle products.

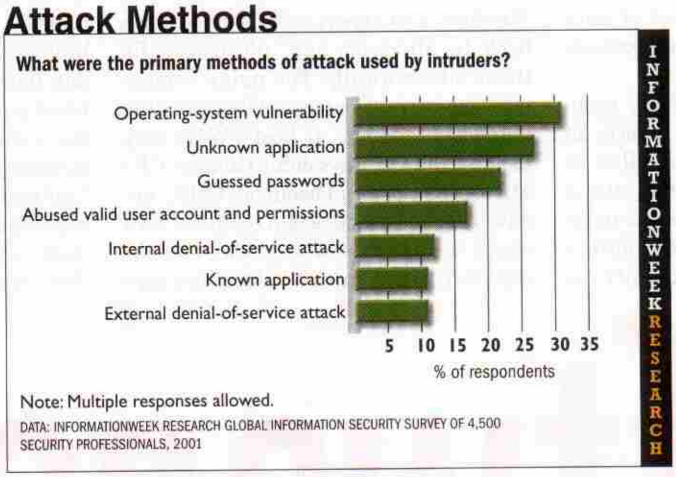
Too often, these types of problems are discovered by customers. Norm Fjeldheim, senior VP and CIO of Qualcomm Inc., a San Diego supplier of digital wireless communications products and services, says his company does regression testing to find performance problems and bugs that vendors should have found themselves. One stress test developed by Qualcomm for Sun Solaris

Gregory Heisler/Corbis Outline

was later included in Sun's own test suite. But all that testing is a drain on Qualcomm's IT resources.

Russ Cooper, editor of NTBugtraq, a security mailing list dedicated to Windows, says secure software development is possible with technology available today. "We've had the tools for years to test buffer overruns and such, and education has been available that teaches programmers how to avoid them," he says. Cooper lays the blame for insecure code on managers who push for quick development cycles and on relatively low pay for quality-assurance workers. "QA people need to be better than the programmers, but programmers make more money," he says.

Attack Methods



Note: Multiple responses allowed.

DATA: INFORMATIONWEEK RESEARCH GLOBAL INFORMATION SECURITY SURVEY OF 4,500 SECURITY PROFESSIONALS, 2001

A fundamental problem with software quality is that programmers make mistakes, says Mark Paulk, a senior member of the technical staff of Carnegie Mellon's SEI. And while there are well-established processes such as the five-step Capability Maturity Model for building quality software, few commercial software vendors strictly adhere to every step.

The irony, says Gerald Cohen, CEO of Information Builders Inc. in New York, is that even when software companies take extra steps to comply with rigorous industry standards, customers may not reward them for it. Information Builders has received the International Organization for Standardization's 9001 certification as testimony to its careful development practices. "For most of our customers, it's a big yawn," he says.

But a growing number of vendors realize they can no longer skirt responsibility. Pierre DeVries, Microsoft's director of advanced product development, says it's going to require a different mind-set at the company, in addition to improved software-development processes. Toward that end, every developer who writes code for Windows.Net and the upcoming Windows.Net Server will be trained in how to write secure software.

At Oracle, the message to developers is "do it right the first time," chief security officer Mary Ann Davidson says. Beyond that, she adds, 90% of what's required is "sheer corporate will."

Garrison Hoffman, a software engineer for technology consulting firm Intrasphere Technologies Inc. in New York, says that, until now, IT managers have had to choose between secure and reliable software or cheap and easy software, an uncomfortable trade-off. "Secure, reliable, cheap, and easy doesn't exist," he says.

Gates aims to change that, but the odds may be against him. "There's an adage in programming that the number of bugs is equal to N+1," Hoffman says. "There's always going to be a bug you haven't found."

Gates, of all people, must know that.
—WITH DAVID M. EWALT, JOHN FOLEY, AARON RICADELA, AND KARYL SCOTT

Write to George V. Hulme at ghulme@cmp.com
Discuss software reliability at our online forum: informationweek.com/LP

After Woes, Oracle Woos Businesses With New Tools

But customers haven't forgotten about buggy first release

Oracle hopes the sixth release of its 11i E-Business applications suite will change customer perceptions that still linger about the bug-ridden first release 19 months ago.

In the months following 11i's initial release in June 2000, 5,000 software patches were issued (see "Apps Made Easy?" March 12, 2001, p. 22; *informationweek.com/828/entapps.htm*). Oracle says it's worked out the bugs, but the company still has work to do when it comes to customer perceptions. In a recent survey of 210 Oracle customers, by Morgan Stanley Dean Witter & Co. and the Oracle Applications User Group, Oracle scored a 5.4, on a scale from 1 to 10, when respondents were asked about the quality of Oracle's applications.

The newest apps, which will begin shipping in March, were unveiled last week at Oracle's AppsWorld conference in Amsterdam, Netherlands. They include: Daily Business Close, which lets companies close their books daily or weekly; CADView-3D, which adds the ability to view computer-aided designs and 3-D models to Oracle's product-development exchange; Enterprise Asset Management, for managing various assets; Partners Online, for managing channel-partner relationships; and Customers Online, a data-management tool to help companies centralize customer records.

The company also rolled out a flat-rate fee schedule based on the workplace roles of each user. It's designed to attract buyers put off by Oracle's practice of charging by the application. Oracle no longer will charge per application module under the new pricing structure but will charge $4,000 for each frequent user who accesses the suite's more-sophisticated features and $400 for each casual user. —STEVE KONICKI *(skonicki @cmp.com)* WITH JENNIFER MASELLI

Visit our Business Applications Center: informationweek.com/techcenters/sw/bizapps