Software systems are complex, making them hard to understand and prone to errors. Ithaca-based GrammaTech, Inc., creates software development tools that make it easier for programmers to develop robust programs. The company specializes in static program analysis—extracting information about the behavior of a program by analyzing its source code. All of GrammaTech’s tools incorporate leading ideas from academic computer science research. Some tools provide engineers with advanced program-understanding capabilities. Others detect hard-to-find bugs in programs automatically, improving reliability and security while reducing testing costs.

GrammaTech has its roots in the Cornell Department of Computer Science. In the early 1980s, faculty member Tim Teitelbaum and his graduate student, Thomas Reps, were working in the field of programming environments. The research culminated in a revolutionary system for building language-sensitive editors, for which Reps won the ACM Doctoral Dissertation Award. By 1988, hundreds of commercial and academic sites had adopted the system. To provide better support for the users, Teitelbaum and Reps formed GrammaTech and transitioned the system to a commercial product called The Synthesizer Generator.

GrammaTech still sells and supports The Synthesizer Generator, but current R&D focuses on more advanced static analysis for program understanding and automatic bug detection. Over the last several years, the company has built and commercialized a program analysis platform called CodeSurfer, which is now the flagship product. CodeSurfer does a deep analysis of a program’s code, and its built-in graphical user interface enables users to ask very detailed questions about the program’s behavior.

Many organizations have adopted CodeSurfer for its program-understanding capabilities. Some of these organizations—including NASA, Airbus, and Mitre—develop software that must function properly for safety or security reasons. Safety-critical and security-critical software is usually developed methodically, over a long period of time. On these projects, CodeSurfer is used during the verification and inspection phases to examine the software for correctness. Other organizations use CodeSurfer to speed product development. For example, customers that develop software for consumer electronics are often under severe time pressure to get a product to market. Developers may have to work with complex, existing code written by another team. These developers use CodeSurfer to understand code quickly so they can use and modify the code with confidence.

Through millions of R&D dollars over the last few years, GrammaTech has extended CodeSurfer to automatically find bugs in programs. This technology is a new approach to software testing that has the potential to significantly improve the quality of applications. Today, engineers test a software application with dynamic testing, for example, running the application on test cases. The problem with dynamic testing is that even relatively small programs have a huge number of different ways they can run, depending not only on the input but also other factors, like timing. It is usually impossible to construct a set of test cases that adequately test the behavior.

As a rule, less than 10 percent of possible execution paths are checked. This is why deployed software systems often have numerous flaws, despite having been extensively tested before release. With GrammaTech’s bug-finding system, the program is not run on test cases. Instead, the source code is analyzed to extract the structure of the program and build an abstract representation of it. Specialized bug-finding queries are run over this abstract representation. Remarkably, some of the queries are capable of checking most or all of the program’s possible executions. As a result, when the queries are run on a program—even a mature and widely distributed...
expected to receive from an external source. If more data is received than anticipated, the surplus data overflows the allocated buffer, overwriting critical system bookkeeping information. When buffer overflows are accidental, system bookkeeping information is overwritten randomly and the program usually crashes. However, an attacker will overflow a buffer with carefully crafted data; the system bookkeeping information is strategically overwritten so the attacker can take control of the system. GrammaTech's buffer overrun detection technology has been successfully applied to several programs and has found previously undiscovered buffer overrun vulnerabilities in each one.

“We are very excited about our bug-finding technology,” says Mark Zarins, GrammaTech’s sales and marketing director. “The cost of buggy software is huge—to the companies developing the software and the end users. Many studies have concluded that a key to reducing software development cost and improving reliability is finding bugs early in the development process. This is what CodeSurfer's bug-finding technology does.”

The company’s R&D is supported by product revenue and research grants. In 2003, GrammaTech was awarded several major research grants, including $750,000 from the U.S. Air Force, $500,000 from the National Science Foundation, and $200,000 from the Office of Naval Research.

Mark Zarins
Sales and Marketing Director
GrammaTech, Inc.

For more information:
GrammaTech, Inc.
317 N. Aurora Street
Ithaca, NY 14850
(607) 273-7340
Fax: (607) 273-8752
info@grammatech.com
http://www.grammatech.com