

September 15, 2003

## GrammaTech Awarded Air Force Research Grant to Develop Source-Code Analyzer that Detects Buffer-Overrun Vulnerabilities

Ithaca, NY -- GrammaTech, Inc. announced today that it has been awarded a \$749,979 Small Business Innovative Research (SBIR) Program Phase II grant by the United States Air Force. Under the terms of the agreement, GrammaTech is developing a source-code analyzer that statically detects buffer-overrun security vulnerabilities.

Popular languages like C and C++ are particularly prone to programming errors that expose systems to attack. The most commonly exploited vulnerability is inadequate bounds checking on C/C++ buffers. By overrunning a stack buffer, an attacker can overwrite critical system bookkeeping information and take control of a system.

The seriousness of the problem has led to the development of tools targeted at preventing buffer overruns. Some of these tools do run-time monitoring-but such tools require significant computational overhead and/or miss classes of vulnerabilities. Furthermore, run-time tools do not completely eliminate the vulnerability, so it can still be exploited through a denial-of-service attack. In contrast, source code scanning tools have the potential to completely eliminate buffer overrun vulnerabilities, without run-time overhead.

GrammaTech's approach uses advanced constraint analysis techniques. The technology greatly increase the accuracy of automatic vulnerability detection, drastically reducing the amount of manual source code analysis required. Furthermore, the remaining manual investigation can be simplified by GrammaTech's program understanding tool, CodeSurfer. The technology has the potential to help programmers rapidly identify and fix buffer overflow vulnerabilities before applications are deployed.

**ABOUT GRAMMATECH** GrammaTech was founded in 1988 to design, develop, and market language-based productivity tools for software engineers. The company has an active research agenda sponsored by the Defense Advanced Research Projects Agency (DARPA), the National Science Foundation (NSF), the Air Force Research Laboratory (AFRL), the Missile Defense Agency (MDA), the National Institute of Standards and Technology(NIST) and the National Aeronautics and Space Administration (NASA). The company has conducted previous research on dependence graphs, formal methods, and language-based programming, and has successfully transitioned its research into commercial software tools. GrammaTech currently markets CodeSurfer, a software-understanding tool, Ada-ASSURED, a language-sensitive editor, Ada-Utilities, a language-sensitive toolset for project-wide quality and standards auditing, and the Synthesizer Generator, a tool for developing language-sensitive program-development environments. These products are available directly from GrammaTech. Additional information is available on the Internet at [www.grammatech.com](http://www.grammatech.com).

For more information contact Mark Zarins at GrammaTech, 317 N. Aurora St., Ithaca, NY 14850. Phone: 607-273-7340 EXT:22. Fax: 607-273-8752. E-mail: [mzarins@grammatech.com](mailto:mzarins@grammatech.com)