APPLICATIONS

Safe-Secure C/C++ has numerous business applications that can enhance developer's and user's perceptions of C and C++ language programs:

Compiler vendors can significantly improve the security of applications generated by their compiler providing a competitive advantage over other compilers and other programming languages.

Source-analysis tool vendors can add a new dimension of safety and security verification.

Operating system vendors can improve their system security and reliability by verifying drivers to be Safe-Secure before they can be installed.

Large manufacturers can prove that their embedded software is Safe-Secure.

Consulting firms can provide specialized remediation consulting for eliminating vulnerabilities in client code

For further information on how Safe-Secure C/C++ can benefit your organization see www.plumhall.com/sscc.html

PRODUCT FEATURES

Safe-Secure C/C++:

- Automatically infers the requirements on the interface of each callable function
- Supplements the compilation and linking mechanism by producing and using bounds-data files which record requirements and guarantees for the defined and undefined symbols in one or more corresponding object files, as well as checksum information
- Verifies C linkage using type-compatible linkage
- Verifies type-compatible behavior of variadic functions, using a name-mangled string at run-time
- Provides automated remediation of each input source file into a source file which invokes non-deprecated functions in the new C library.

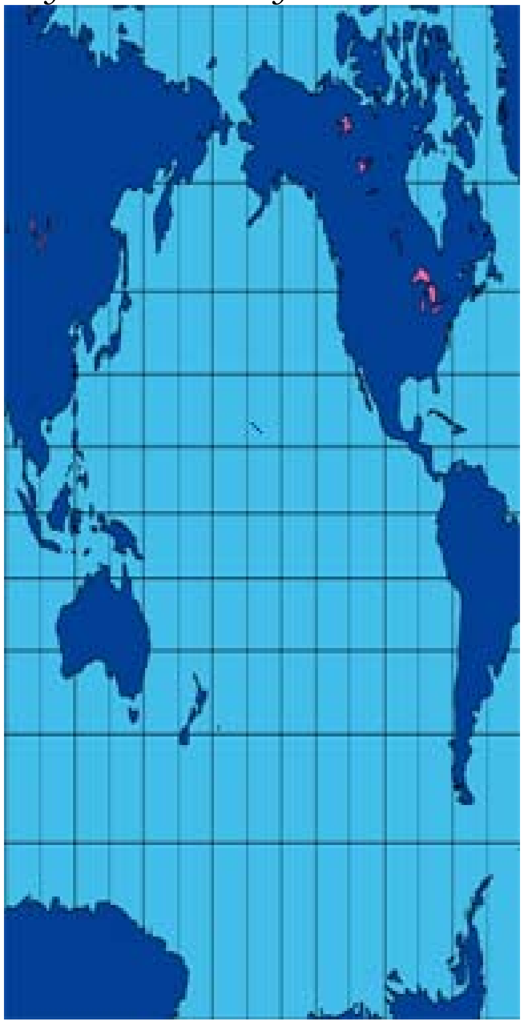
Plum Hall, Inc.

3 Waihona Box 44610
Kamuela HI 96743
Phone 808-882-1255
Fax 808-882-1556
http://www.plumhall.com/
sscc@plumhall.com

Plum Hall, Inc.

SAFE-SECURE^{TM} C/C++

Safe-Secure Software



DEFINITIVE SECURITY FROM PLUM HALL

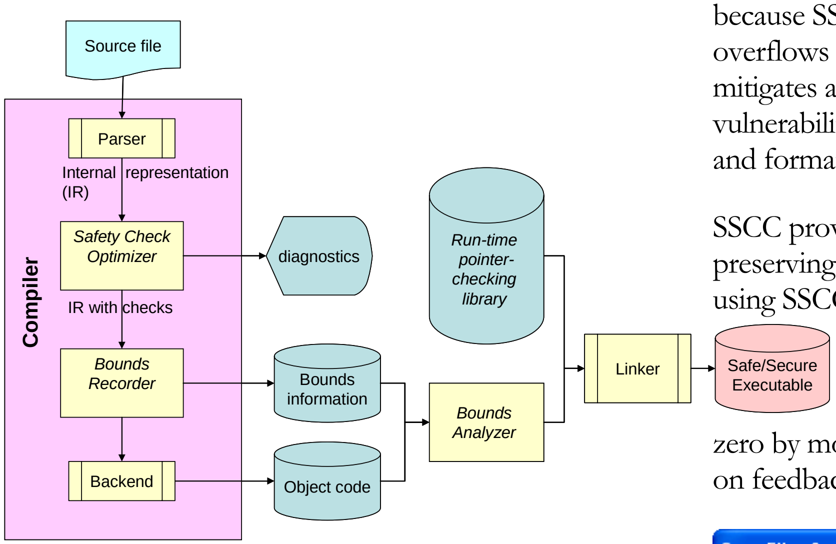
According to CERT Coordination Center statistics, more than 90% of software security incidents are caused by attackers exploiting known software defect types. The most common form of software vulnerability, particularly in C and C++ programs are *buffer overflows*.

The preponderance of buffer overflows in C and C++ has made these languages the bane of the software security community and has caused the redirection of many software projects to other languages that are perceived to be more secure.

By using Plum Hall SSCC™ (Safe-Secure™ C/C++), programs written in C or C++ can be just as safe and secure as programs written in Java or C#, while preserving C/C++ efficiency. This combination of security and performance preserves the viability of C/C++ in a more security-conscious age.

HOW DOES SAFE-SECURE C/C++ WORK?

Safe-Secure C/C++ consists of four major components: *safety check optimizer*, *bounds recorder*, *bounds analyzer*, and *run-time pointer checking library*. These components can be integrated into compilers and software analysis tools to detect and prevent buffer overflows and other common security vulnerabilities in C and C++ programs, as shown in the following diagram:



SSCC combined static and dynamic-analysis methods to create a hybrid solution for eliminating buffer overflows and other common vulnerabilities.

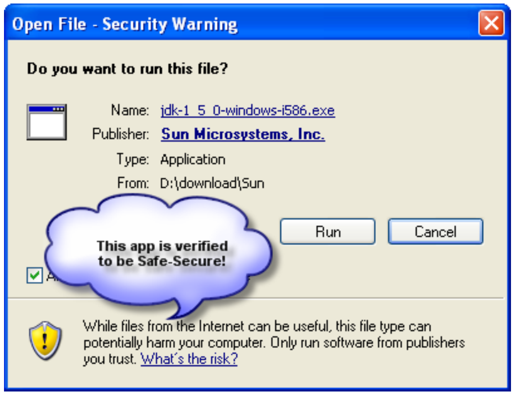
SSCC ensures that 100% of buffer overflows are eliminated.

Compile-time analysis generates safety checks for all possible buffer overflows. Patent-pending static analysis techniques are used to minimize the overhead introduced by the addition of these checks. A highly optimized run-time library is provided for efficient run-time checking of pointer accesses.

BENEFITING FROM SSCC

Programs created using SSCC can be certified "free from buffer overflows" because SSCC ensures that 100% of buffer overflows are eliminated. SSCC also mitigates against other common types of vulnerabilities including integer overflow and format string vulnerabilities.

SSCC provides safety and security while preserving efficiency. Programs compiled using SSCC technology run, on average, less than 5% slower than their insecure counterparts. This over head can be reduced to zero by modifying the source code based on feedback provided by SSCC advisories.


Open File - Security Warning
This app is verified to be Safe-Secure!
Run
Cancel

Do you want to run this file?

Name: jdk-1_5_0-windows-i586.exe
Publisher: **Sun Microsystems, Inc.**
Type: Application
From: D:\download\Sun

☑ A

While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

Certified components can be installed on government, corporate, and home systems with the added assurance that these components are free from buffer overflow vulnerabilities that can be exploited by an attacker to "take over" the system.