

SBIR Topic Number:
OSD04-SP2

SBIR Title:
Next Generation Software
Reverse Engineering Tools

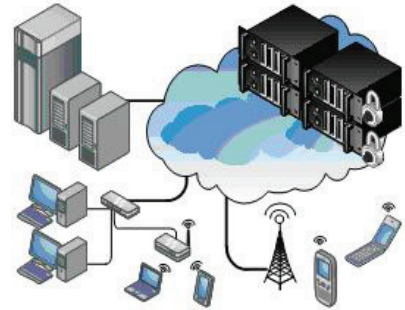
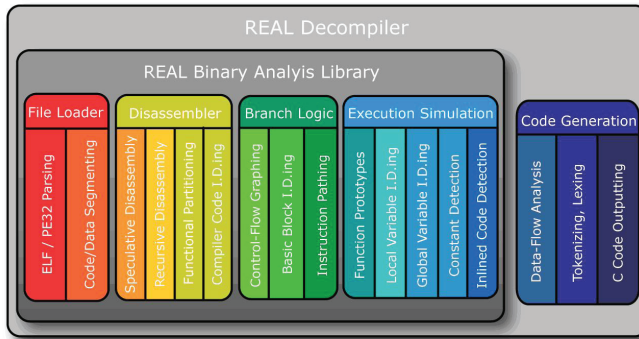
Contract Number:
FA8650-06-C-8049

SBIR Company Name:
Anacapa Sciences, Inc.,
Santa Barbara, CA

Sponsoring Office:
Office of the Secretary of
Defense, Washington, DC

Technical Project Office:
AFRL Sensors Directorate,
Wright-Patterson AFB, OH

This Air Force SBIR/STTR Innovation Story is an example of Air Force supported SBIR/STTR technology that met topic requirements and has outstanding potential for Air Force and DoD.



Left: REAL Decompiler™ and the REAL Analysis Library™. Right: Trust-as-a-Service: Trusted Cloud.

New Generation Software Reverse Engineering

- As part of the Department of Defense (DoD) and Department of Homeland Security's Software Protection Initiative, Anacapa Sciences is developing a set of next-generation reverse engineering tools
- Under the Reverse Engineering Advancement Lab (REAL) project, Anacapa's emerging toolset for accomplishing decompilation automation was named REAL Decompiler™, which streamlines the decompilation process by automating the conversion of compiled binaries back into high-level C language source code
- The heart of the REAL Decompiler is the REAL Analysis Library™ which provides low-level binary analysis capabilities; the Decompiler converts the results of the Analysis Library into a high-level lexicographic representation suitable for generating C source code
- Developers can leverage the REAL Analysis Library through a robust Application Programmer Interface (API) to accomplish a variety of program analysis tasks
- The REAL Decompiler and the REAL Analysis Library have served as enabling technologies for other developments in protected computing

01-15OCT10/OSD04-SP2

A

DISTRIBUTION A:
Approved for public
release; distribution
unlimited.

Air Force Requirement

Government and industry organizations are placed at risk by malicious third parties who seek to co-opt software assets through reverse engineering (RE), making it vulnerable to exploitation. Long a global problem for commerce, the threat of increasingly powerful software RE tools is emerging as a serious threat to U.S. national interests. While software protection schemes are also emerging, the balance between protection and “attack” (RE) favors first one side and then the other in this digital conflict.

RE exploitation includes the use and re-distribution of national-interest software, disruption of the legitimate use of software resources, disruption of the larger software resource environment, and outright destruction of key portions of the national software inventory. Effective software protection technology has become a critical necessity in next-generation computing environments.

SBIR Technology

As part of the Department of Defense (DoD) and Department of Homeland Security’s Software Protection Initiative, Anacapa Sciences is developing a set of next-generation reverse engineering tools. The Reverse Engineering Advancement Lab (REAL) project is an effort to create next-generation RE tools. The DoD Phase I SBIR objective was to make substantive improvements on existing technology to reverse engineer compiled software. As Anacapa made further headway in Phase II, it discovered that it could automate much of the decompilation. The emerging toolset for accomplishing such automation was named REAL Decompiler™.

REAL Decompiler streamlines this process by automating the conversion of compiled binaries back into high-level C language source code. C code can be understood and analyzed much more quickly than assembly language, resulting in faster and more accurate results for RE projects. The heart of the REAL Decompiler is the REAL Analysis Library™ which, as the name suggests, provides low-level binary analysis capabilities. The Decompiler converts the results of the Analysis Library into a high-level lexicographic representation suitable for generating C source code. The division of the REAL software suite into these two components allows other applications that rely on the accurate analysis of compiled binaries, besides the Decompiler, to be easily constructed by incorporating the standalone Analysis Library.

The REAL Analysis Library includes functionality to load, disassemble, parse, and analyze compiled, binary code. This includes state-of-the-art data and control and data flow analysis, as well as strong data typing and logical inference capabilities. Developers can leverage the REAL Analysis Library through a robust Application Programmer Interface (API) to accomplish a variety of program analysis tasks. The Library API gives developers unfettered access to analytical data on the examined binary. The API also allows developers to control which types of analysis are run, in order to better align memory and runtime constraints with the necessities of the project at hand.

Potential Application

With the REAL Decompiler and the REAL Analysis Library, DoD software developers can follow a well-defined process for improving protection. Additionally, the REAL Decompiler and the REAL Analysis Library have served as enabling technologies for other developments in protected computing, as described next.

Company Impact

“This SBIR funding provided Anacapa the opportunity to do advanced software protection research and development that otherwise would not have been possible,” states Dr. Bob Dick, Vice President Technology. “For example, the tools and technology resulting from this effort enabled Anacapa to subsequently develop a unique, software-based, Trust-as-a-Service™ (TaaS) approach to net-centric secure co-processing. TaaS and its component solutions – Trusted Point, Trusted Net, and Trusted Cloud – comprised the Secure Division Toolset, which encompassed the entire application lifecycle for trusted hardware – from developers all the way to end users.”

“Since its formation in 1969, the company has completed more than 800 research and development projects for over 200 different government agencies, academic institutions, and industrial organizations. Anacapa’s vision is to be a leader in the application of cognitive science, information systems, and human factors research to the development of innovative training and technology design.”



SBIR/STTR

Air Force SBIR Program
AFRL/XP
1864 4th Street
Wright-Patterson AFB OH 45433

AF SBIR/STTR Program Manager: Augustine Vu
Website: www.afsbirsttr.com
Comm: (800) 222-0336
Fax: (937) 255-2219
e-mail: afrl.xppn.dl.sbir.hq@wpafb.af.mil

