BLUERiSC

Windows SCOPE
Window into Windows

## BlueRISC Capabilities Brief

BlueRISC is a security solutions and services provider focusing on fulfilling embedded system assurance and cyber security needs.

BlueRISC’s software vulnerability-focused technologies take the form of an automated toolkit (ThreatSCOPE) that is designed to identify, at the binary level (i.e. source-code not required), software vulnerabilities. ThreatSCOPE can be used strictly for static vulnerability characterization, can drive a vulnerability testing infrastructure, and can enable software with implicit exploitation detection and reporting at runtime. Through its interactive visualization interface, users are able to view an application’s potentially exploitable paths via an intuitive graphical representation. Additionally, ThreatSCOPE supports binary-level code insertion, malware characterization, binary-to-source code conversion as well as automated exploitability report generation. ThreatSCOPE is currently being used in both Defense and Automotive applications.

BlueRISC’s system assurance offerings include both software-only and hardware-assisted approaches for establishing Roots-of-Trust (RoT) in otherwise untrustworthy systems as well as a tools and associated technologies for identifying and patching software vulnerabilities in embedded systems. The RoT enabling products and technologies are applicable in embedded systems, endpoint computers and mobile devices. They support secure execution, in-memory protection, data security, and trusted computing specifications providing IP protection, authentication, anti-cloning and many other critical security functions. These solutions contain comprehensive design-time technology insertion tool-suites as well as full post-deployment support.

Additional BlueRISC cyber security and cyber forensics offerings are available through WindowsSCOPE product line. WindowsSCOPE is a cyber-forensics tool that performs deep reverse engineering of an endpoint’s operating system and all components from raw memory for the purpose of discovering cyber threats. When used at the network level, the solution enables a solution capable of tracking malware breaches and intrusions across the network. WindowsSCOPE, as well as its hardware-centric CaptureGUARD accessories, are currently in use in more than 18 countries.

BlueRISC’s team has extensive experience in security-focused software, hardware and tooling design and development and has successfully brought security-centric products to market. To date the team has participated in developing a binary-level vulnerability analysis tool (ThreatSCOPE), a line of security microprocessor (used in anti-tamper and software protection domains), security-focused runtime embedded software, product deployment and post-deployment software support. It has also developed a variety of software and hardware tools for software assurance, cyber security and forensics. BlueRISC has been the prime contractor on several DoD contracts also including 30+ SBIR efforts, some with teaming partners.

More information can be found at www.bluerisc.com and www.windowsscope.com. It should be noted that many system assurance details are purposefully withheld from public views online.

Contact:
Kristopher Carver
Technical Director
kris@bluerisc.com - (413) 359-0599