



Riverside Research Institute

End-to-End Software Security Support

SUMMARY

RRI has established a software security team to provide government and commercial entities with end-to-end software security support. The team focuses on the following areas:

- Secure Development Life-Cycle Integration
- Software Security Analysis
- Binary Security Assessments
- Protection Tool/Technique Analysis
- Protection Planning
- Reverse Engineering
- Software Protection
- Malware/Virus/Rootkit Analysis

PERSONNEL

The RRI team members hold SCI clearances and have extensive software security and reverse engineering expertise based on years of support to the DoD Software Protection Initiative and multiple Red Team operations. Their experience includes:

- Wide-ranging knowledge of government and commercial protection tools
- Broad exposure to software and emulation analysis tools on both Windows and Linux operating systems
- Code generation tool development, including custom compilers, assemblers, disassemblers, linkers, loaders, and debuggers
- Embedded software/firmware development (JTAG, flash, EEPROM, DSP, microcontroller)
- OS Kernel development
- Network interface driver and firmware development, allowing covert remote management and network packet exfiltration

FACILITIES AND EQUIPMENT

RRI has established a state-of-the-art binary analysis lab near Wright Patterson Air Force Base, Ohio capable of supporting classified operations. The lab is equipped with high-end, multi-processor workstations and specialized single processor systems equipped with in-process emulators capable of monitoring all communication to and from the CPU. The team uses custom tools and leverages COTS analysis products in their assessment efforts to simulate a wide variety of attack scenarios from the average game cracker to a sophisticated adversary. Specialized tools include:

- Stealthy Custom debuggers
 - Windows - Ring 3 & Ring 0
 - Linux - Ring 0
- Data/code Miner
 - Control flow analysis
 - Function hooking/rootkit
- Deobfuscator
 - Anti-disassembly
 - Automatically removes obfuscation
- ECM-50 Emulator
 - Monitors activity at the hardware level
 - Captures all instructions into and out of the CPU

FINDINGS

Proprietary information is held in strict confidence, and detailed reports are prepared for the customer. Demonstrations are available upon request.

CONTACT US

For information on how RRI's software security team can help you with your software security needs, contact the Software Security Team at softwaresecurity@rri-usa.org.