



## SUMMARY

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

- **Reverse Engineering:** The team specializes in extracting intellectual property from a broad spectrum of software. This includes user applications, DLLs, drivers, OS kernels, and firmware. The software can be based on a variety of platforms (Windows/Linux/Mac/Embedded etc).
- **Software Protection:** RRI has extensive experience in evaluating and applying software protections, based on four years of experience performing these functions for the DoD Software Protections Initiative (SPI).
- **Malware/Virus/Rootkit Analysis:** The team can identify and analyze intrusion software to characterize and/or neutralize the threat.
- **Network Penetration Testing:** The team is skilled performing vulnerability analyses and man-in-the-middle attacks to capture and inject network packets on a wide variety of protocols.

## PERSONNEL

The RRI team members hold a variety of security clearances and collectively have over 25 years of relevant software and reverse engineering experience. Their experience includes:

- Wide ranging knowledge of government and commercial protection tools
- Extensive knowledge of specialized tools and attack techniques
- Broad exposure to software and emulation analysis tools on both Windows and Linux operating systems
- Code generation tool development, these include custom compilers, assemblers, disassemblers, linkers, loaders, and debuggers
- Embedded software/firmware development (JTAG, flash, EEPROM, DSP, microcontroller)
- OS Kernel development
- Network software vulnerability assessments
- 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 both classified and unclassified 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. This specialized equipment allows the team to monitor an application's behavior at the hardware level in order to quickly analyze a target system and conduct a detailed analysis of software protection implementations. The team has also developed custom kernel-level debuggers, an auto-unpacker, and stealthy data mining applications that allow them to quickly evaluate software security vulnerabilities on any platform. The team uses these custom tools and leverages COTS analysis products in their assessment efforts. These tools allow the team to simulate a wide variety of attack scenarios from the average game cracker to an adversary with access to advanced hardware and software tools.

## FINDINGS

Proprietary information is held in strict confidence. 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 Jason Raber at (937) 427-7085, [jraber@rri-usa.org](mailto:jraber@rri-usa.org), or visit our website at [www.rri-usa.org](http://www.rri-usa.org).