1 Elevator Pitch

The Innovation

SIREN is a cyber security tool for high performance computing (HPC) systems. It monitors a program's *dynamic signature* and takes pre-determined actions to isolate software that attempts to violate the integrity of the system. SIREN's "killer feature" is its novel low overhead approach for application isolation based on the capabilities of the TAU Performance System® [1]. ParaTools' deep experience in parallel software profiling (over 100 years combined) enables this unique innovation. **Applications protected by SIREN have a similar runtime, program image size, and level of user interaction as unprotected applications, making it suitable for HPC applications where performance is as important as correctness.** Unlike virtualization and virtual machine based security schemes, SIREN protects applications with little or no runtime dilation. Applications protected by SIREN require no additional system libraries or filesystems, whereas container-based solutions like Docker dramatically increase the program's image size, complicate the runtime environment, and create new attack surfaces by introducing user-level filesystems. The SIREN secure execution environment complements existing security measures. It adds an additional layer of protection over all hardware and software firewall approaches currently deployed and is fully compatible with container-based and virtualization-based security measures. System administrators may safely deploy SIREN without changes to their existing security infrastructure.

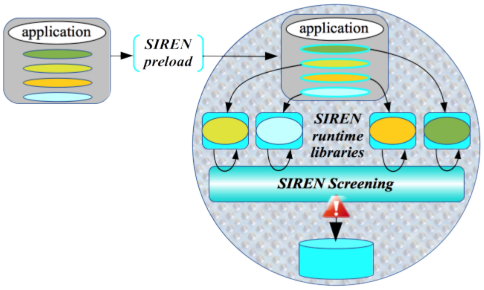

Figure 1: The SIREN Secure Intellegent Runtime Environment.

The Value Proposition

SIREN protects mission critical operations co-located with compromised or malicious software by automatically isolating infected software from healthy applications. It does this with little or no performance impact, making it a viable solution for HPC centers. HPC is not only widely regarded as a fundamental technology for future science and engineering discovery, but is now a matter of competitive survival for the overwhelming majority of small and medium-sized U.S. enterprises (SMEs). Over two-thirds of U.S. industry representatives assert that HPC is critical to the future direction of their businesses [2]. Small US manufacturers in particular desperately need to deploy HPC solutions to keep pace with industry demands. The potential for a security breach is increasing as more users host critical operations in the same HPC center. A security breach, while damaging to a large organization, is cataclysmic for a small or mid-sized company working with sensitive data. Hence this burgeoning market is eager to employ protection solutions that isolate their operations from their neighbors without performance loss.

The Customer

Industry, government agencies, national labs, universities, and research centers in the USA and abroad operate HPC centers ("supercomputers") to provide mission critical operations. HPC centers account for over 36% of the global HPC economy, which generated over $22 billion in 2015 and is predicted to reach $36.1 billion by 2019 [3, 4]. We will sell SIREN and related consulting services and products to the national laboratories and HPC supercomputing centers through our existing channels. ParaTools will also use its unique relationship with Northrop Grumman Corporation via the Northrop Grumman Cync program to provide SIREN to Northrop Grumman and other prime contractors. Based on the customer feedback we will receive in Phase II, we will commercialize this technology to target a broad audience and ultimately release a version of SIREN targeting desktops and laptops to complement SIREN installations at HPC centers.