Shielding applications from an untrusted cloud with Haven

Andrew Baumann Marcus Peinado Galen Hunt

What’s the problem?

Today’s cloud computing infrastructure requires substantial trust. Cloud users rely on both the provider’s staff and its globally-distributed software/hardware platform not to expose any of their private data.

Summary

Introducing a prototype called Haven, which is the first system to achieve shielded execution of unmodified legacy applications on a commodity OS (Windows) and commodity hardware. Haven shields applications using mechanisms such as private scheduling, distrustful virtual memory management, and an encrypted and integrity-protected file system.

Key insights

1. The main challenges in design are protecting from a malicious host OS, and executing existing binaries in an enclave.

Notable Design Details/Strengths

The picoprocess and LibOS enable sandboxing of unmodified Windows applications with comparable security to virtual machines, but substantially lower overheads.

Limitations

SGX limitations such as exception handling, disallowed instruction and thread-local storage.

Haven does not currently prevent rollback of filesystem state beyond the enclave’s lifetime.

Summary of key result

For large, complex, CPU and memory- intensive applications such as SQL Server, and for OS- intensive applications like a modern web stack, Haven’s performance penalty vs. a VM is 31–54%, which significant classes of users will readily accept such overheads, in return for not needing to trust the cloud.

Open questions

The work can be improved by diminishing untrusted time and enable cloud management like VM.