Heather Linich

December 1, 2014

Shielding Applications from an Untrusted Cloud with Haven

OSDI 2014

Haven is a new program developed by Microsoft and designed to protect the execution of applications from possible damage and attack on the cloud. The program prototype was introduced at the 2014 USENIX Symposium on Operating Systems Design and Implementation. Haven functions by making use of existing hardware safeguards built into Intel SGX. SGX provides defenses against actual, physical attacks on an application, such as memory probes but also lends resources to solving the challenge of implementing unmodified legacy binaries while in turn keeping them safe from any malicious hosts attempting to attack.

Cloud systems today use a traditional hierarchical security model which only intends to shield the code of the cloud provider. In this case, the user data does not receive any fortification against access from harmful or unauthorized code. The user is put in a precarious position of having to put a large amount of faith in people and systems that they do not intimately know in order to be able to use the cloud service. The user is forced to trust the cloud provider’s software and their staff and administrators.

Currently, best practices for protecting sensitive information or code on the cloud is to use a hardware security module. Haven has set out to provide a level of security to the user that is similar to operating user hardware in a locked cage at a colocation station. The cloud system supplier would then only provide raw resources to the user and could only observe data transmitted over the network. Haven considers this feature to be ‘shielded execution’.

Shielded execution is the opposite of sandboxing. Sandboxing is a way to separate currently running programs in a controlled operating system environment in order to execute untested, untrusted or unverified code, users, etc. (*Wikipedia*) Shielded execution protects the confidentiality of data and code from any untrusted hosts. When executing the program, the user has the same security level as if it were running on hardware that was directly within the user’s control. It also affords safeguards to the provider in the event of a harmful guest by allowing the provider to maintain control of resource allocation.

Not only does Haven set out to protect new programs but also legacy applications that were created without SGX information or functionality. This had presented two significant challenges to Haven: operating legacy binary code within an enclave which greatly taxes the current SGX execution model and the possibility that the host operating system could be malicious.

Haven has employed many features to remedy these challenges. A mutually distrusting interface between the application and host operating system is put in place to guarantee that unmodified programs received shielded execution. In this way, a malicious operating system is not able to deceive the application into operating inaccurately or revealing any secret data or information. On top of this, Haven offers a remote attestation tool that in essence gives users end to end assurances of security for the application.

Another protection is ‘isolated execution’. Isolated execution defends specific code from harm from the system regardless of size or privilege level. The instrument used for isolation still has to allow interaction with untrusted software or hardware components in order to convey results or to gain admittance to system services. These are areas at which the application can be susceptible to harm.

Haven makes use of several important components of SGX. SGX provides functionality to guard the privacy and integrity of pages in an enclave. Data in an enclave is encrypted when it is written to memory and if the data is altered in any way, a fault will be signaled.

Haven also makes use of and enhances SGX’s DrawBridge component. Drawbridge maintains low overhead sandboxing of windows applications and programs. DrawBridge’s two main processes are the picoprocess and their library operating system. A picoprocess is a protected isolation container created from hardware address space but is not able to access any system calls or conventional operating system services. The library OS, or LibOS, is a refactored Windows 8 that runs as a set of libraries inside of the picoprocess. The LibOS and picoprocess allow for sandboxing of unchanged Windows applications with security levels similar to virtual machines but also with considerably fewer overheads. In its original form, DrawBridge only guards the host from untrusted guests but Haven protects both the program and the LibOS from an untrusted host which results in sought after mutual distrust amongst the guest and host.

The creators of Haven set out to measure their application’s performance to determine the real benefit to users. Their approach was to gauge Haven’s sensitivity to a variety of critical SGX performance parameters. Haven’s performance was also measured against a variety of alternative host environments. Their results found that when considering memory and CPU intensive applications or OS intensive applications, Haven’s performance penalty as compared to a virtual machine was 31-54%. The Haven team believes that many users would very willingly accept this penalty in exchange for the cloud security provided.

Haven is a very important product in this day and age due to the increasing prevalence of users accessing the cloud in one form or another. Consumers are increasingly concerned about security issues and Haven attempts to allay security fears for one of the newest technologies available. Presently, cloud computing does not provide much protection for the user as providers have full access to their data. But Haven provides defenses for the user and protections against potential data breaches.

Security issues are at the forefront of most people’s minds today however many people do not trust their cloud vendor to protect them. Most users feel secure storing data on their own systems but once they have to relinquish control of their data to the cloud, a large degree of uncertainty comes into play. Due to the fact that Haven has shielded execution, cloud users can have the same feeling of security as they do on their own hardware through the cloud. Haven and similar products could quickly become the norm as cloud computing and heightened security needs become even more widespread.