Sandia National Laboratories

# CHIRP

## Cloud Hypervisor Forensics and Incident Response Platform

SCR# 2278

MULTI-PLATFORM

### A VMI-based cloud forensics platform that enables analysts and defenders to collect evidence and incident response materials in real time, without disturbing the user environment or alerting the intruder

The shift to Infrastructure-as-a-Service (IaaS) has brought challenges to cyber Incident Response (IR) and forensics teams investigating not only breaches and leaks, but also cyber-crime. Due to the ephemerality, location, and ownership of the data, disks, and technology provided by Cloud Service Providers (CSPs), cloud-based entities and cloud customers have yet to establish foundational forensic capabilities that can help reduce security risks. Even further, IaaS platforms rely on hypervisors to virtualize computer systems, but most do not offer a useful Application Programming Interface (API) to support customizable, contextual introspection which is what an analyst needs to conduct investigations.

Sandia's **Cloud Hypervisor Forensics and Incident Response Platform (CHIRP)** introduces a novel Virtual Machine Introspection (VMI) based approach to provide intelligence and forensic artifacts from active VMs in cloud systems. Using CHIRP, analysts can pinpoint suspicious activities, track and record attacker actions for forensic analysis and retrieve materials transparently from the targeted machines automatically or on-demand. These extractions occur in real-time without affecting the guest, averting guest detection. The features of CHIRP may also be leveraged to disrupt malicious copying, deleting, obfuscating, encrypting, and relocating of data in a coud environment. It is a first of its kind advancement that provides new opportunities to meet challenges in the cloud through innovative VMI, including correlation with network data and active state collection.

**Operating System/Version:**

For host (hypervisor) machines: Modern versions of Linux-based distributions (CentOS, Red Hat Enterprise, Ubuntu, Debian) and ESX 5.0-6.5; Intel x64-based architecture.

For virtual machines: supports x64-based architectures of Linux 3.0 Kernels, Windows 7 to current version, Windows Server 2008 to current version.

## TECHNICAL BENEFITS

- Windows, Linux, and OSX guest compatible
- Collects artifacts and intelligence to discern potential threats in real-time without disturbing the user environment
- Scalable, in-depth out-of-band VM instrumentation for fast-handling of events
- Direct access to VM state or memory in a safe, stable fashion

## APPLICATIONS & INDUSTRIES

- Ideal for cyber defense and security requirements and applications
- Deployable to Infrastructure-as-a-Service (IaaS) or any VM-based service
- For IR and digital forensic teams, as well as cloud service providers (CSPs)

🏠 ip.sandia.gov
✉ ip@sandia.gov

*Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525. SAND2020-2780 M*