CHIRP

CLOUD HYPERVISOR FORENSICS AND INCIDENT RESPONSE PLATFORM

Sandia National Laboratories

CHIRP is a cloud forensics platform that empowers analysts and defenders to collect evidence and incident response materials in real-time without disturbing the user environment or alerting the intruder.

Business Problem

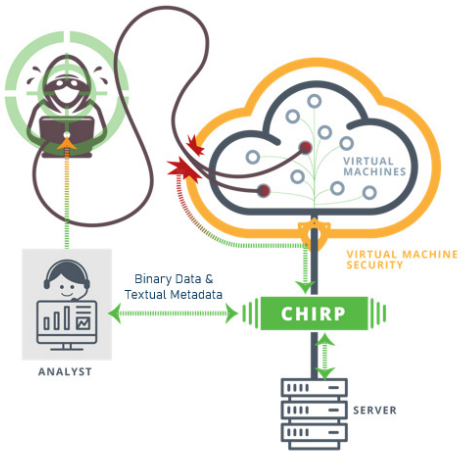
With more than 92% of enterprises now having a cloud presence and the frequency of large-scale data breaches rising over 273% year-over-year, does your organization have the tools to know whether and how it has been breached?

Customer Need

The widespread adoption of enterprise cloud computing and Infrastructure-as-a-Service (IaaS) poses challenges for cyber incident response and forensics teams investigating not only breaches and leaks, but also cyber-crime in cloud environments. As cloud computing and IaaS become more ubiquitous, so does the need for tools that can conduct effective cloud forensics and incident response.

Due to the ephemerality, location, and issues with ownership of the data, disks, and technology provided by Cloud Service Providers (CSPs), cloud-based entities and cloud customers have struggled to establish foundational forensic capabilities to 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.

A more global cloud forensics solution is needed that can provide instrumentation with minimal overhead, common data models, and collection of broad data sets. A virtual machine (VM), hypervisor, and operating system agnostic solution would offer needed versatility for varied enterprise infrastructures. A solution that encompasses these features could enable analysts to better address current issues in enterprise cybersecurity.



Our Approach: CHIRP

Sandia's Cloud Hypervisor Forensics and Incident Response Platform (CHIRP) introduces a custom Virtual Machine Introspection (VMI) based approach to provide intelligence and forensic artifacts from active VMs in cloud systems. This platform agnostic solution involves significantly lower overhead than comparable solutions. Its ability to collect text and binary data allows correlation with other sources.

Typically, hypervisor-based solutions abstract underlying computer hardware from operating

U.S. DEPARTMENT OF ENERGY | NNSA National Nuclear Security Administration

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. SAND2021-12253 M

CHIRP

CLOUD HYPERVISOR FORENSICS AND INCIDENT RESPONSE PLATFORM

Sandia National Laboratories

systems running on virtual machines. Instrument virtual machine solutions (VMs) place an extra load that attackers can detect or even influence. Instrument hypervisors such as CHIRP provide an advantageous solution where the attacker cannot detect monitoring.

Using CHIRP, analysts can pinpoint suspicious activities, track and record attacker actions for forensic analysis, and may retrieve materials transparently from the targeted machines automatically or on-demand. These extractions occur in real-time without affecting or alerting the intruder to the detection.

Benefits

CHIRP offers a broader set of features compared with current commercial offerings. Designed for IaaS applications from the start, CHIRP provides a platform and OS agnostic solution with much lower overhead. Compared with other existing solutions, CHIRP is lightweight and can provide a real-time dynamic response. Its configurable logging delivers insights for meaningful incident response or forensics.

Competitive Advantage

Compared to existing commercial offerings, CHIRP has a broader set of features, including fewer installation dependencies and better portability. *See Figure 1.*

Large or complex organizations such as government agencies, providers of cloud service or managed services as well as cybersecurity forensics and enterprise security operations teams may benefit from the versatile features and capabilities of Sandia's CHIRP solution.

Next Steps

Sandia is seeking partners ready to test CHIRP in their environments as part of a pilot program. The pilot includes a simple sign-up process with easy setup and deployment. Varied licensing models are available for different sectors, including providers of government services, commercial services, or cybersecurity tools.

Interested in participating in the CHIRP Pilot Program? Contact:

Sandia National Laboratories
Licensing & Technology Transfer

ip@sandia.gov
ip.sandia.gov

U.S. DEPARTMENT OF ENERGY | NNSA National Nuclear Security Administration

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. SAND2021-12253 M

CHIRP

CLOUD HYPERVISOR FORENSICS AND INCIDENT RESPONSE PLATFORM

Sandia National Laboratories

Figure 1: CHIRP Feature Comparison

Feature	CHIRP	Azure Security Center	Fortinet FortiAnalyzer-VM	VMware Guest Introspection	Magnet Axiom Cloud	LibVMI-Volatility
Installation Dependencies	Make	Proprietary	Proprietary VM	Proprietary *(vCenter)*	N/A *(third party)*	Cmake, libtool, yacc/bison, lex/flex, glib, libvirt, libjson-c
Portability	Any system running supported hypervisors	Microsoft Azure Cloud	Service-based *(e.g., AWS Market Place)*	VDI, vSphere	Service-based	Off-line system
Hypervisor Support	KVM, Xen, ESXi	Hyper-V	Xen	ESXi	N/A	Xen, KVM
VM Support	Windows, Linux, OSX	Windows, Linux	N/A	Windows, Linux	N/A	Windows, Linux, OSX
Visibility	User, VM, Network	VM	VM	VM	User	VM
Requires User Credentials for Cloud	No	Yes	Yes	Yes	Yes *(Username, Password)*	VMI Only
Service	Deep introspection *(VM, IaaS)*	Log data *(IaaS, PaaS, SaaS)*	Log data *(IaaS, PaaS, SaaS)*	Agent-based introspection *(VM)*	Log data SaaS *(Apple, Google, FB, Microsoft, Dropbox, Twitter)*	Introspection/ Memory analysis *(VM)*
Guest Agent	No	Yes	Yes	Yes	N/A	No

U.S. DEPARTMENT OF ENERGY NNSA National Nuclear Security Administration

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. SAND2021-12253 M