HARDENED VAULT

EFFECTIVELY SECURING CLOUDS

Protecting Valuable Digital Assets with Firmware Security, cryptography engineering and Linux Hardening

Data Protection | DoS Protection | SIEM | IDS/IPS | Operational Security Secure Software Development | IAM

Ring0 Exploit Detection | Encryption Storage | CnBT | SMM Rootkit Detection | TPM/TXT/DRTM

DAC/MAC/RBAC | SPI Flash Write Protection | Kernel Mitigation | Hardware Fault Injection Defense

ME Manufacturing Mode | Metadata Protection | RTL Audit | VISA/IOSF | PCB Analysis

UCODE | Reproducible Semiconductor Fabrication Process | PCB Golden Image

www.hardenedvault.net • info@hardenedvault.net • Suite C, Level 7, World Trust Tower, 50 Stanley Street Central, Hong Kong

Table of Contents

0. Overview

An “ideal” security for your business should be something like 1) The root of trust anchored in multiple hardware components, then the chains of trust extending from firmware, operating systems to application. 2) The crucial parts of each component follow compliance/regulation while are still able to defend against the known and unknown vulnerablity and exploit vectors by integrating the modern mitigation and access control. 3) The communication between each nodes must guarantees the confidentiality, integrity and more importantly, metadata protection by introducing the strong and secure communication protocol. 4) No individual or organization is able to audit every component which is why the user (System administrator, IT security manager, CISO, etc) must have the leap of faith in someone else’s components (hardware, firmware, software).

Cloud adds attack surface (hypervisor, management plane, etc), creates a single, centralized massive treasure to attack and it breaks one's ability to manage security below the OS level as well as communication security between services. Some measures can be trade-off between cost and effectiveness. Hardened Vault propose a strengthened security architecture under zero trust model where the root of trust (the most fundamental building block of security) is fully hardened from hardware, firmware to OS kernel. And then a communication protocol which then can be used to extend the trust from the root to all services running in the cloud or elsewhere.

1. Background: The Rise (and Rise) of the Cloud

When it comes to disruptive technology innovations from the past few decades, the *cloud* is usually at the top of every list. While new-age technologies like AI, machine learning, computer vision, Blockchain, and quantum computing do deserve the attention they get, what's truly changing business for the better is cloud computing. The cloud and its ever-growing ecosystem of platforms, providers (aka Cloud Service Providers or CSPs), processes, products and systems empower all kinds of organizations to improve operations, increase efficiencies, enhance customer service, meet mission-critical goals, and improve their financial position.

Simply put, the cloud is already one of the most influential technologies in today's hyper-connected digital economy. And its influence is only going to increase in the coming years.

And that's why the proportion of enterprise IT spends on cloud computing – particularly on the "Big 3" public clouds like AWS, Microsoft Azure and Google Cloud Platform - continues to increase. IDC reported that in 2020Q2, spending on public cloud IT infrastructure exceeded spends on non-cloud infrastructure, to reach an unprecedented value of $14.1 billion. IDC also expects this spending to grow at a five-year CAGR of 10.4%, reaching $109.3 billion in 2024 and accounting for a massive 63.6% of total IT infrastructure spend.

"Cloud in all its permutations – hardware/software/services/as a service as well as public/private/hybrid/multi/edge – will play ever greater, and even dominant, roles across the IT industry for the foreseeable future."
-- Richard L. Villars, Worldwide Research at IDC

The good news: cloud technology is world-changing.

Although cloud services bring many benefits, they are also accompanied by some bad news –- the security concerns.

2. Cloud Security is a Rising Concern

In many ways, the cloud is the “influencer” of the technology world, but by no means it’s perfect. Organizations are looking to migrate to a robust cloud-native architecture and take advantage of all its elements like microservices, containers, and orchestration platforms must also increase their awareness of the downsides. They should know that as they transition from on-premise to the cloud, they may face serious challenges relating to: i) Security, and ii) Trust.

2.1 SECURITY Concerns in the Cloud

In a 2020 report, the Cloud Security Alliance (CSA) identified these egregious security threats to cloud computing:

i Data breaches
ii Misconfiguration and inadequate change control
iii Insufficient identity, credential, access and key management
iv Account hijacking
v Insider threats
vi Insecure interfaces and APIs
vii Weak control plane
viii Metastructure and applistructure failures in management plane
ix Limited cloud usage visibility

Importantly, the CSA also cited “lack of cloud security architecture and strategy” as a huge threat to businesses migrating to, or operating on, the cloud. Research supports this statement, with 93% of businesses saying that they are worried about public cloud security.

The transition to the could introduces security vulnerabilities like malware, ransomware and Server Side Request Forgery (SSRF) into the organization’s environment. Many vulnerabilities are relatively easy to exploit and, when successful, can lead to data thefts and losses which are hard to predict and harder still to handle. In fact, 69% of organizations say that data losses and leakages are their biggest cloud security concern.

Another security worry stems from the *shared security responsibility model* of public clouds like AWS. In this setup, there’s no real “security perimeter”. Service providers supply only a minimal set of security protections, leaving organizations responsible for the security of their applications. In a multi-cloud environment, these variations introduce complexity and risk. Further, a security gap in one system makes the entire stack, and therefore the organization, vulnerable to bad actors.

2.2 TRUST Concerns in the Cloud

As public cloud adoption increases, the trust issue is becoming more important. Despite their benefits, research shows that organizations don't completely trust public clouds. One reason is that they're concerned about the security of their data. Furthermore, 63% of SMBs (U.S., U.K and France) believe that CSPs should do more to protect their data.

Another reason for lack of trust is a bit more prosaic, but no less important. When organizations store their data and applications on-premise, they have some assurance that these assets are *relatively* secure from unauthorized use, because access requires that the user be physically present at that location. But with the cloud, another organization (i.e. the cloud service provider) is handling their data, which is stored in different data centers in remote places. This situation raises worries like:

Could our credentials, and thus our assets fall into the wrong hands?

Can the provider detect such unauthorized access, and ensure minimal impact on our data or applications?

And finally,

Can the cloud vendor prove that they don't (and won't) misuse, misappropriate or steal our assets?

These questions have been around for over a decade, but CSPs are yet to provide credible answers.

2.3 Current Solutions to Data Security and Trust Concerns

Two solutions attempt to address these worries, although they do it in totally opposite ways.

The first proposed solution is called **enclave** implemented via different ways. Intel's Software Guard Extensions (Intel® SGX) is the most complicated enclave implementation by developing the whole new features in multiple levels of the system: hardware, ucode, firmware, Operating system and SDK for apps. It's aimed at guaranteeing integrity and confidentiality to security-sensitive computations performed on systems where privileged software like the kernel and hypervisor are potentially malicious. SGX is a "hardware enclave", i.e. a protected environment that can run secure computations.

In SGX, code runs in a way that's secured from other processes – even root-level processes – thanks to *isolation* and *attestation*. Isolation allows all computations to run isolated from untrusted software outside the enclave, while attestation lets remote parties authenticate the code that's currently running, and cryptographically trust the computation's output. SGX could give data owners cryptographic control over their data and computations in the cloud, even though the cloud's hardware is not in *their* control, but the CSP's. In effect, SGX puts the cloud vendor and administrator into the threat model, and says, "Don't trust them. Take control of your own data and computations.". There are other implementations of enclave, e.g: Nitro enclave, Sanctum, etc.

At the other end of the spectrum is Intel's Trust Domain Extensions (Intel® TDX). This solution proposes that the user should implicitly trust the cloud vendor administrator. It aims to enhance data security control and IP protection for the org, and help the provider manage resources and maintain cloud-platform integrity. TDX helps deploy hardware-isolated virtual machines called trust domains (TDs). TDX adds a secure-arbitration mode, and is built with Intel Virtual Machine Extensions (VMX) Instruction-set-architecture (ISA) extensions, MKTME technology, and a CPU-attested, software module.TDX technology protects TDs from a range of software by isolating VMs from the virtual machine manager (VMM)/hypervisor, and any other non-TD software on the platform. It implements the isolation, attestation and Dynamic Root of Trust Measurement (DRTM) integration by utilizing current x86 technology,e.g., VMX, TXT and SGX. TDX can also protect the VMs from some forms of hardware attacks.

But here's the kicker: neither SDX nor TDX actually solves the original problem that every cloud tenant organization faces at one point or another: *How can we still trust the providers with our data and applications in the cloud?*

2.4 Server (or Workstation) Architecture: Then vs Now

2.4.1 THEN

In older computing architecture, the central part of an operating system (OS) aka the *kernel* controlled *everything*. It allowed access to system resources by controlling programs run by users in a restricted, “permission only” environment known as *Userland*. It also prevented applications from modifying their own or other applications’ memory stacks.

The CPU provided hardware support to separate the kernel from the user environment, so programs couldn’t take over the kernel, and threaten its security. Its hardware relied on *protection rings* or *privilege levels*, usually ranked from 0 to 3:

- Ring 0: Kernel:: Most privileged
- Ring 1: Device Drivers:: Less privileged
- Ring 2: Device Drivers:: Less privileged
- Ring 3: User applications:: Least privileged

In a fully-secure world, Ring 0, would be able to control processes running in the other rings, but the reverse would not be true. The processor would block the least privileged Ring 3 applications from accessing kernel memory in Ring 0. Userland applications would also not be allowed to see any details about the memory, allocations, address space, etc. since this could lead to leaks that may compromise the system’s security.

2.4.2 NOW

In the modern computing architecture, the OS sits in Ring 0, but there is another higher level of privilege called Ring -1 which is “virtualized”. With virtualization, the kernel/hypervisor allows various isolated user-space instances (also known as VMX-based containers or virtual machines) to exist. The process allows multiple OS to be installed on one workstation (or server). It separates the physical infrastructure into multiple fragments of “virtual” devices or environments that can be used more effectively, efficiently and securely (if it compare to a system without isolation) in a cloud environment.

In the modern cloud computing environments, there can be even more levels of privilege such as Ring -2, Ring -3 and Ring -4 that are higher than the OS kernel in Ring 0. Thus, one of the biggest differences between legacy and modern architectures is that ***Ring 0 is no longer at the core***.

Here’s what these conceptual negative rings look like:[1]

- Ring -1: Virtualization
- Ring -2: Firmware/Payloads
  * Device drivers
  * Hardware initialization
  * Reset vector
- Ring -3: CSME code modules, other independent IPs and peripheral firmware
  * MINIX OS
  * Customized SOC
  * Hardware
- Ring -4: Instructions
  * u-code engine
  * Integrated circuits/PCB
  * Logic gate
  * Transistor
  * Physical phenomena

These additional negative rings represent more levels of processor vulnerabilities that are susceptible to exploitation. For instance, Ring -2, typically called SMM (System Management Mode) holds a lot of proprietary designed code. But limited visibility into this code is a huge security red flag for cloud administrators. For instance, it can be used with multiple exploits for rootkits to reside in without the OS being able to interfere.

The situation becomes even worse in Ring -3 due to a serious lack of transparency and audit. For instance, unknown to the general public, until 2017, MINIX was one of most popular operating systems running on computers worldwide. This open-source, highly modular, UNIX-like OS was designed to work on microkernel architectures. It is at the heart of Intel's Management Engine (ME), a “secret” processor embedded in all Intel CPUs sold since 2007. Intel has always maintained that MINIX helps system administrators monitor, maintain, update, upgrade, and repair Intel-based computers from a remote, central location. In other words, MINIX is all about simplifying the management of workstations on internal networks. But most people familiar with the OS call it a “backdoor” into the computers of unsuspecting users. This is because MINIX’s ME component runs independently from the main OS, and had separate processes, threads, memory manager, hardware bus driver, file system, etc. Even a tech giant like Google has expressed worries about MINIX’s backdoor capabilities, since its code runs on the CPU's deepest access level – Ring -3. Worse, MINIX and its ME also run a web server component that allows *anyone* to remotely connect to

[1]

computers, even when the main OS is turned off. This is a gaping security hole in Ring -3 that most users are not even aware of.

In fact, a vulnerability in this ring was discovered for real in 2017. A bug in Intel's remote management programs that ran on the Management Engine remained undiscovered for seven years. If bad actors had managed to exploit the vulnerability, they would have been able to manipulate not only the vulnerable computer, but also other systems on its network.

Another concept that most organizations are not aware of, although they should be, is Turing-completeness or TC. TC is the property of a system to compute any program, including another computer in some form.

TC is important to system security because it underpins a key issue: why a perfect antivirus program can never exist? Remember the joke about mitigator always raising the bar? Why the defensive side seems always lose in the end? What's the definition of **insanity**? Does "repeating the same mistakes over and over again and expecting different results" sounds familiar to "patching the security fix over and over again"?. The risk of your business is relevant to two types of TCs: Regular TC (Vulnerablity) and Maclious TC (Backdoor). Let's say one big organization spend ton of resources "raising the bar" for the business at one level (RING3 or RING0) but it's far from enough. The reason is that it is possible to create a TC system that's smart enough to run any program on any computer. In fact, it's more likely that systems will tip over into TC. TC lurks everywhere, which is why perfect security is impossible to achieve. Furthermore, a clever bad actor who has even a tiny bit of control over input, can easily leverage that control into full-blown TC. They also get an escape hatch from a small, predictable, controllable, and secure system, to a system that could in theory, do anything. Such dangerous hidden programs can do everything from extracting information about the surrounding program, to take the host system into strange and untested territories. For all these reasons, businesses must be better aware of the odds of a malicious Turing Machine taking over their machines.

The industry starts taking serious about the risks which open source and hacker community have been discussing for years. A Microsoft report (Mar 2021) shows that more than 80% of enterprises have experienced at least one firmware attack in the past two years, but only 29% of security budgets are allocated to protect firmware. DHS CISA announced a campaign VBOS (Vulnerabilities Below the Operating System) to address some well-known COREs issues in May 2021.

To effectively deal with all such security concerns in modern-day virtualized cloud environments, organizations need a more robust solution that provides multiple trust anchor Root of trust, Linux kernel hardening, Firmware security, Trusted computing, cryptography engineering, etc.

3. Hardened Vault: A Modern Solution to a Modern Problem

Founded in late 2017, Hardened Vault was the result of work done by a security research group whose focus area was *infrastructure security*. The group did some great work in the past, particularly in secure communication protocols, firmware security, kernel hardening, and hardware security. But it wasn't until early 2021, when the founder Shawn Chang decided to formalize the solution under a registered company.

Hardened Vault is ideal for users and businesses that:

i Don't trust the public cloud, despite CSPs' claims to provide strong security using a shared responsibility model (e.g. AWS)

ii Operate in industries or sectors with high security demands like:

- FinTechs
- Traditional banking, financial and credit organizations
- Supernodes in P2P networks
- Blockchain applications
- Securities exchange platforms (trading policy engines or dispatch servers)
- Energy and Utilities
- Space industry
- Healthcare and Medical
- Education

Hardened Vault is also suitable for users willing to build their own "cyber bunker" to protect their applications and businesses through a Hardware Root of Trust (RoT). An RoT is a source that provides the foundation a computing system's secure operations depend on. It is the starting point of a "chain of trust" that's needed to ensure computers boot with legitimate code. When the first piece of code (in the BIOS) has been verified as legitimate (by the chip), it is executed, and these credentials are trusted to execute each subsequent piece of code.

ROT (Root of Trust) is the foundation for the secure operation of the computing system, which is the starting point for ensuring that the computer initiates the "chain of trust" required to start the legitimate code, and when the code of the first stage (in the BIOS) is verified as legitimate (the chip), it is executed, and these credentials are trusted to execute each subsequent stage of code.

Because ROT always has inherent trust in cryptography, it must be secure by design. RoTs typically include a hardware module to protect them from malware, and examples of hardware-based RoTs can be found in OpenTitan and Nitro security chips.

In general, every organization that owns valuable digital assets, needs servers to operate, and are unwilling to blindly trust CSPs, will benefit from Hardened Vault.

3.1 Hardened Vault: Product Details

Hardened Vault consists of three key components:

i.i Vault 111 Hardened Server, hardware + firmware

i.ii Vault OS, Linux security baseline + Linux kernel hardening + Fuzzing as a service

i.iii Vault1317, federated secure communication protocol

i. Vault 111 Hardened Server

Hardened Vault provides a *Vault 111 Hardened Server*. Its current version supports x86 processor models. Vault 111 Hardened Server is custom build 1U server which has been custom built with trusted hardware components and fault injection prevention to against some level of physical attacks.

The Vault 111 Hardened Server is shipped with VaultBoot and Vault OS with a critical hardening profile. In the critical profile, The VaultBoot utilizes the security features provided by the chipset, binding the key for full-disk encryption under TPM. It supports both coreboot (for high-security demands) and UEFI (a random machine provided by the customer) on many aspects including trusted computing, security enablement of chipset, and neutralized CSME. VaultOS ships with more security features than simply an exploit detection/prevention system and security baselines, e.g: The professional paranoid’s kernel hardening mode.

Hardware specifications:

- Xeon E-2186G
- 128 GB ECC UDIMMs
- 500G SSD
- 1U server chassis

ii. Vault OS

With hardware and firmware established by Vault. The next level of security must be the OS. Vault OS provides a Debian GNU/Linux based security solution that mainly focuses on exploit detection/prevention system and security baselines with situational hardening policies. The exploit detection system can detect and mitigate the general exploits which are frequently utilized by random attackers. VaultOS ships the exploit detection system by default, e.g: Vault exploit detection system is able to detect and prevent the public PoC/exploits and it provides more detections even in post-exploitation stage. For high-security demands, Hardened Vault is shipped with PaX/Grsecurity which fundamentally prevent whole classes of bugs and exploits by changing the behavior of the OS kernel. It also provides an easy-to-integrate interface with SIEM (Security information and event management) or open source log analysis systems. NixOS and Guix – a package manager, fully-programmable OS inspired by Nix and Guix System – are also available, albeit as optional features.

iii. Vault1317 Decentralized Federated Communication Protocol

Vault1317 is a cutting-edge solution to protect the machine's privacy. It's an authenticated key exchange protocol that specializes in public key concealing and participation deniability. Such a key exchange can help establish a secure communication channel to ensure secure messaging without leaving any cryptographic evidence of the communication. This might be counter-intuitive to many IT security people. Vault1317 is meant to work in such use-case where 1) Metadata have to be protected, which is machine's privacy matters 2) The authentication server can't be trusted.

Some protocols are available today that don't leave any cryptographic evidence, even if there's a betrayal by one or more participants and/or disclosure of long-term key materials. However, this is no longer a big advantage. If metadata can somehow be fetched from pivotal nodes, and other technologies (e.g., Big Data) used to analyze it, it won't be difficult to reveal a user's identity through long-term public keys.

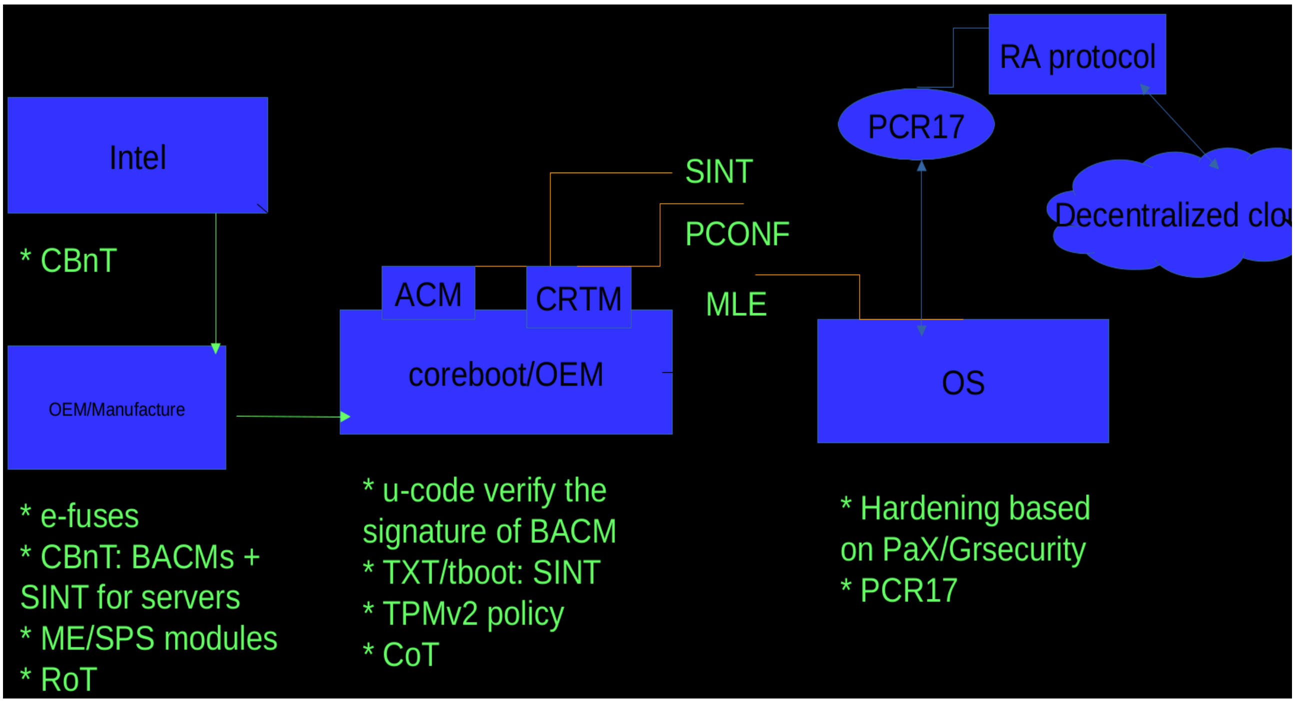
Vault1317 addresses the drawbacks of existing solutions which claim to be deniable to some degree. This protocol can conceal the public keys from the outside of the secure channel. It also provides open source implementation.

Hardened Vault is based on Vault1317 decentralized federated communication protocol to ensure fully secure communication that removes the need to trust centralized servers. Customers can integrate it with their current infrastructure, or just use the attestation node manager provided by Hardened Vault. Furthermore, organizations can take full control of their data and application security in the cloud. Hardened Vault leverages several key technologies to provide world-class security that cannot be matched by any CSP. These include:

- Hardware/Firmware security
- Linux kernel hardening
- Fuzzing as a service
- Supply chain security
- Cryptography engineering

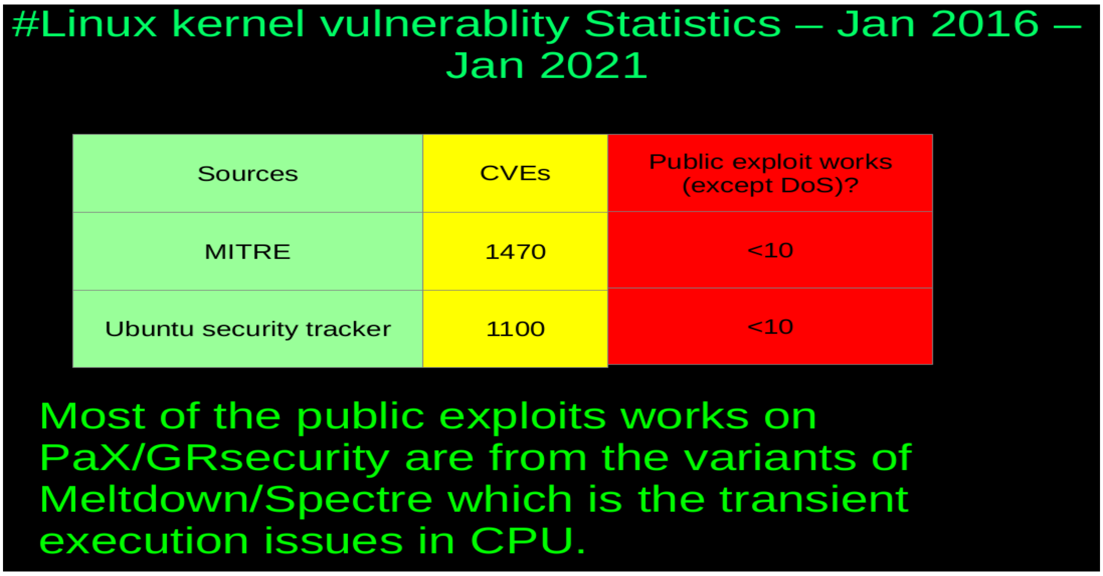
4. Hardened Vault: Key Technologies for Powerful Security in the Cloud

Hardware/Firmware security: Hardened Vault developed a firmware security solution called VaultBoot based on previous HardenedBoot by HardenedLinux which was out-of-date. VaultBoot supports both coreboot (high-security demands) and UEFI (a random machine provided by the customer) on many aspects: trusted computing, security provisioning tooling and enablement of chipset, neutralized CSME, and more. The solution also includes multi-anchor for RoT options due to the physical security assessment and requirements in the customer's data center. The goal of firmware security is to solve the problem from RING -2 and mitigate the threats partially from RING -3.



Linux kernel hardening: The kernel hardening provides an immensely important layer of protection against exploitable bugs conducting remote-code-executions and privilege escalations. Hardened Vault provides multiple solutions for different levels of security demands. The highest security demands will ship with PaX/Grsecurity-based kernel, which incorporates several defense features to ensure that most public exploit techniques can be mitigated. It also achieves better multi-layer defense by providing a role-based access control (RBAC) system to create much stronger sandbox protection, by adding filesystem linking restrictions, by improving auditing capabilities, by restricting chroot operations, etc. A somewhat less secure (but more affordable) solution for the Linux kernel based on some customized hook-based host detection/prevention systems is also available. It can defeat many exploits corresponding to certain code paths.

This work has immense and multiple implications on security. Firstly, the hardened kernel can stop over 99.2% of the most serious public PoC/exploits, such as privilege escalations based on MITRE CVEs and Ubuntu Security Tracker. Next, Hardened Vault’s hardening experts have worked on Linux kernel hardening using PaX/GRsecurity for years. They were also responsible for the backporting of several partially hardening features to Android. The solution was accepted by Google’s Android Open Source Project after a massive exploitation was identified in 2014/2015. The sophisticated hacking attack targeted the owners of Android devices by leveraging a combination of Linux/Android n-days and resolved massive exploitation in the wild for millions of embedded systems. Hardened Vault also developed an exploit detection/prevention system for the normal user’s requirement as well. RING 0 no longer the **CORE** a decade ago but it’s the entry point to the under world. The importance of RING 0 protection is like the original of the **Great Gate of Minas Tirith.**

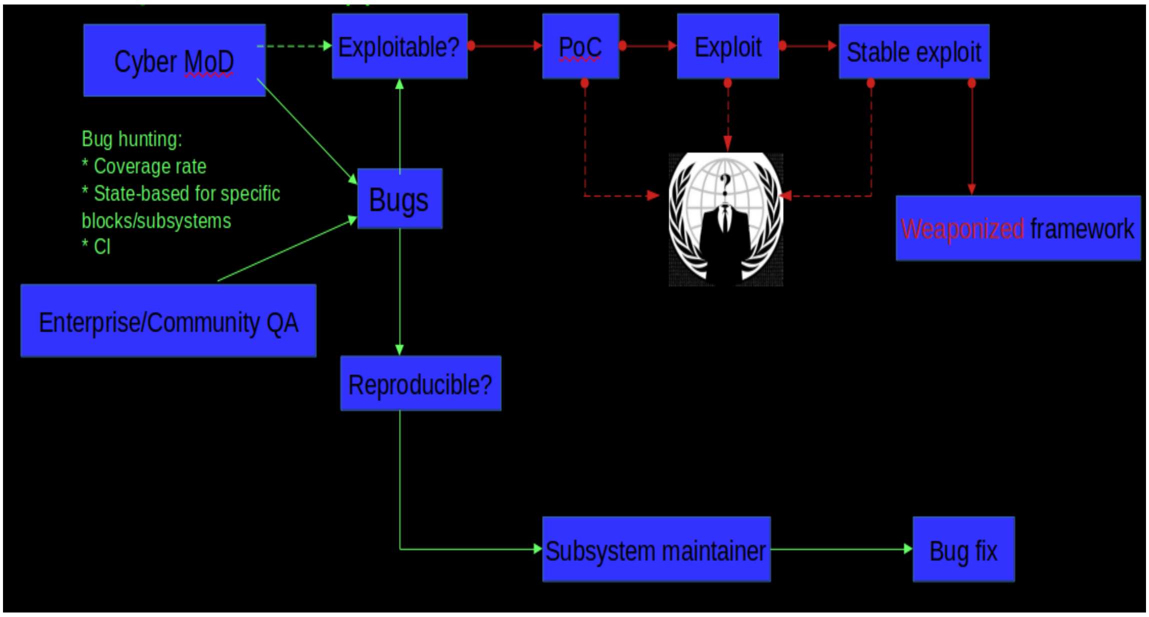


#Linux kernel vulnerablity Statistics – Jan 2016 – Jan 2021

Sources	CVEs	Public exploit works (except DoS)?
MITRE	1470	<10
Ubuntu security tracker	1100	<10

Most of the public exploits works on PaX/GRsecurity are from the variants of Meltdown/Spectre which is the transient execution issues in CPU.

Fuzzing as a service: Every organization must keep in mind that their business is highly reliant on the consequences of complexity of the software/firmware/hardware components Security should be built-in with your business from the outset, not tacked on later as an afterthought. Another way of saying this is that security should be *baked-in*, not *bolted-on*. This is because any breach or hacking event that might halt the business for any amount of time is a serious incident; and the only way to mitigate the impact of such events is to think about security from the start. Hardened Vault improves system stability by utilizing techniques shared by both sides of the security conflict: offense and defense: *Fuzzing*. It increases code coverage with a built-in state-based fuzzer to locate bugs in the early stages of **software development and QA** to proactive improve security, and decrease business risks like potential downtime.



Supply chain security: Supply chain is a long-term problem that cannot be resolved quickly or in a single shot. Hardened Vault provides reproducible builds with cryptography to mitigate supply chain risks for software and firmware. Of course, due to the high complexity of hardware, especially the Hardened Vault server, there is no silver bullet to completely eliminate supply chain security issues. The SolarWinds attack against many U.S. government institutions and Fortune 500 companies that was detected in December 2020, is evidence of this harsh truth. The Hardened Vault team has carefully done a risk assessment of the supply chain from Ring 3 (application), Ring 0 (Kernel), Ring -1 (Virtualization), Ring -2 (Firmware) to Ring -3 (Intel CSME or similar independent IPs on x86 chipset). The kernel hardening experts have also put in more effort on the kernel and firmware to deliver even greater benefits compared to current hardware. They have also demonstrated the complexity of hardware PCB level by CheapPCB.

Cryptography: Cryptography is as crucial as system security hardening, but it only works on a system that's not already compromised by an attacker. This is why the Hardened Vault team went to great strength to strengthen system security *before* stepping into cryptography engineering. They have thoroughly analyzed the crypto component of the product and solution to make sure that all industry-accepted best practices are being followed. These experts have developed a cutting-edge secure communication protocol (Vault1317 Decentralized Federated Communication Protocol) to protect a machine's privacy by public key concealing and participate deniability, and also added federation support for the protocol to avoid the **centralization of the services**.

5. Summary: Why Every Cloud Organization Needs Hardened Vault

In the current business landscape, the cloud is everywhere, with organizations relying on it to streamline their operations, backup their data, and achieve a competitive advantage. But despite its many benefits, the cloud – and cloud providers – cannot perfectly meet the high-security demands of many industries, neither can they adequately address the trust issue. Hardened Vault provides a robust, reliable and powerful solution to these challenges by 1. Providing a true Root of Trust from RING -3 and hardware module via a Vault Server, hardening the core computation infrastructure with hardened Vault OS and then providing a secure communication protocol to connect this core security solution to any existing "node" (cloud environment).

Thanks to several innovative new features that our security experts have developed, Hardened Vault protects organizations from exploitable bugs conducting remote-code-executions and privilege escalations. Keep this in mind: Cryptography engineering only serves you well on a system which isn't compromised (yet!).

Visit our website: https://hardenedvault.net/ for more information or contact us via **contact@hardenedvault.net**

**SUITE C, LEVEL 7, WORLD TRUST TOWER, 50 STANLEY STREET, CENTRAL,
HONG KONG**