Advanced cryptographic technique that can render data futile during data breach

Ajith Menon ¹, Zakeer Hussain ²
¹(Director and Head of Innovations & Security Research, ZinnoX Business and Technology Solutions, Bangalore)
²(Founder & CEO, ZinnoX Business and Technology Solutions, Bangalore)

Abstract: One unfortunate outcome of cataclysmic events is that they frequently prompt desperate and malevolent acts that can put valuable information in danger. On the off chance that you are building an application that stores individual data - about the general population affected by a debacle, delicate medical data, budgetary information, and so on - then information security isn't a choice, it's an absolute necessity. This paper demonstrate how to easily infuse security into your application with Hyper Protect Crypto Services and key administration services to render information futile to hackers. The network-addressable Hardware Security Module gives an industry-standard secure PKCS#11 cryptography API interface that is bolstered by various programming languages including Java, Javascript and Swift. It bolsters secure-key tasks and random number generations through IBM Z cryptographic equipment, FIPS-140-2 level 4 technology - the largest level achievable. You can get to Hyper Protect Crypto Services through an Advanced Cryptography Service Provider (ACSP) client, which speaks with the ACSP server to empower you to get to the back-end cryptographic resources. This is the industry’s solitary FIPS 140-2 Level 4 certified technology in public cloud market today. This paper demonstrates the application of the Hyper Protect Crypto Service and how afterwards deliver the cryptographic requests to it. This will also show how to depend on execution under physical assurance of the Hardware Security Module (HSM), rendering Keys — or the real estimation of the keys, to be more exact remain safely covered up inside this unique equipment, while a predefined set of cryptographic activities can be performed referencing the key material. Encrypt and decrypt are the most mainstream tasks, yet PKCS#11- consistent HSMs give access to sign, verify, key generation and significantly more. In addition, it have a decision of different key composes and sizes to best match any prerequisites.

Keywords-CPK (Customer Private Key), HSM (Hardware Security Module), Intel QAT, IBM Hyper Protect Services, Cloud Crypto Services, SWK (Symmetric Wrapping Key)
I. INTRODUCTION

The security of any open key framework lays on keeping private key private. This requires two levels of protection: Right off the bat, private keys must be secured against memory revelation assaults, for example, cold boot attacks and furthermore from different programming vulnerabilities that are equipped for perusing approved information from the memory space of OS piece or client forms, particularly in a hypervisor. Le Guan, likewise did extraordinary work securing private keys against memory revelation assaults utilizing equipment exchange memory. Hardware memory assurance instruments like AMD® SME/SEV and Intel® SGX is equipped for averting physical assaults on memory, and in addition assaults propelled from outside of the owning procedure. Be that as it may, these arrangements are as yet unequipped for shielding private keys from attacks propelled from the procedure’s own location space. A fantastic counterexample in such manner is the acclaimed Heartbleed attack in the OpenSSL stack regardless of whether it were to be kept running under either SME, SEV or SGX.

A second security objective is to keep private key undetectable to the cloud service operator. More than 76% of all associations share no less than one of their private keys with a third party hosting provider and therefore, compromising the most prominent such hosting provider could give access to the private keys for 60% of the domains in the Alexa top-1K. This violates one of the central assumptions underlying end-to-end authentication and security – that all private keys ought to be kept private. The ongoing Keyless SSL solution by CloudFlare is an endeavor toward this path by holding on commence care of clients’ private keys, while sending all SSL private key operations back to the clients’ key server. The undesirable side effects of this are two: it add a performance penalty as the round trek latency between the service provider’s framework and client infrastructure; a second is the requirement for the client to continue to maintain a key/crypto service infrastructure in-house, consequently discrediting the advantage of outsourcing IT services to the cloud.

In the perfect situation, the cloud customer requires two critical attributes for key management: the cloud operator’s native support for BYOK paradigm and a highly scalable performance. This paper proposes a secure, scalable key protection solution based on of IBM® Advanced cryptographic technique that can render data futile for the hackers during a data breach.

II. BACKGROUND AND RELATED WORK

Intel® KPT is another element in Intel® servers in light of the Intel® Xeon® Scalable Processor Family. Intel® KPT works related to Intel® platform feature called Intel® Platform Trust Technology (PTT), which is utilized to store client secrets (keys) at rest. Intel® PTT is an Intel implementation of TPM (Trusted Platform Module) and Intel® QuickAssist Technology (QAT) is hardware cryptography accelerator. There is a secure hardware link between Intel® QAT and Intel® PPT in Intel® C627/C628 Chipset to share keys.
The framework design of this entire solution, which incorporates two major parts, the key management server (KMS) and the cloud platform running applications based on Intel® Architecture. In the Intel® KPT architecture, the private key is securely shared from the KMS to the cloud service node based on Intel® Xeon® Scalable Processor Family. We were able to access many private and personal data including Aadhar details, Medical Records of many refugees from multiple servers during the Kerala flood relief campaigns due to the lack of security. This exposed the serious issues that can result in a catastrophic exposure of personal data to hackers.

III. ANALYSIS ON PREVIOUS ARCHITECTURE

A proof of concept is implemented by integrating Intel® KPT with nginx through OpenSSL. This incorporates two major advances

1. Key Provision/Sharing: Symmetric Wrapping Key (SWK) is provisioned to Intel® PTT on the cloud platform through a key provision application KPTtool, which pursues TPM key export-import protocol as characterized in TPM 2.0 specifications. The client's unique clear private key (CPK) is encrypted using the SWK to yield a wrapped private key (WPK) in a confined environment inside the KMS. WPK, when deployed and shared on compute nodes, is now anchored and secured by SWK. Another private key PEM design following ASN.1 syntax is defined keeping in mind the end goal to specify the process of generation a WPK from its CPK. The new PEM design indicates subtle elements, such as, the algorithms and key size of the SWK, the IV and so forth.

2. Runtime: The prototype depends on a vertical integration of nginx and OpenSSL with Intel® QAT API library, driver and HW engine. WPK is deployed on cloud platform and utilized in memory rather than CPK. Nginx/OpenSSL triggers Intel® PTT to send SWK to Intel® QAT by means of internal secure hardware link. Inside Intel® QAT, WPK is unwrapped to CPK, which is utilized for private key activities. In the entire life, CPK is never uncovered in memory of hypervisor or container.

IV. ANALYSIS AND COMPARISON ON SYSTEM ARCHITECTURE AND PERFORMANCE

A. Security Analysis

We created a Hyper Secure Crypto Environment and analyzed the results with Intel’s Key protection technology, we found that the Intel’s PTT data can be cleared by downloading a BIOS to a USB Drive, plugging it in the powered off NUC and holding the power button for 3 seconds. This will boot to a special boot menu that lets you go to BIOS recovery. This can clear all BIOS stored info.

A user’s unique CPK resource is wrapped in a trusted key management server by key owner. WPK is secured in the form of cipher text in storage and memory of a cloud
platform. WPK is unwrapped only ‘just in time’ within Intel® QAT, utilizing symmetric wrapping key previously imported securely from PTT. On cloud platform, CPK is never uncovered in memory or capacity and never shared to compute nodes.

**B. Versatility**

The private key is conveyed directly to cloud compute nodes rather than all private key operations executed on a central key server as done in keyless solutions. Given that the runtime security of keys is now native to the compute node, this solution can scale out to as many compute nodes as possible, thus keeping up with uprising business demands.

![Fig 1: IBM Hyper Protect Service](image_url)

**C. Execution Evaluation**

The test is executed on IBM Cloud Hyper Protect Crypto Services which is a complete set of encryption and key management services that are backed by IBM Z technology; the same state-of-the-art cryptographic technology that banks and financial services rely on is now available to cloud users. This will enable you to depend on execution under physical protection of the Hardware Security Module (HSM), rendering the real estimation of the keys, to be more exact and to remain safely covered up inside this unique hardware, while a predefined set of cryptographic operations can be performed referencing the key material. Encrypt and decrypt are the most popular operations, yet PKCS#11-compliant HSMs provide access to sign, verify, key generation, and much more. Likewise, you have a choice of different key types and sizes to best match your requirements.
V. CONCLUSION

In this paper, we proposed a solution based on IBM Cloud Hyper Protect Crypto Services and Hardware Security Module (HSM) to protect your own private key in cloud against memory disclosure attacks and share your very own private key to distributed cloud computing nodes without security compromise. As our implementation is integrated with a cryptography accelerator seamlessly, it exhibits huge performance improvement compared with software implementation. The IBM series of Hyper Protect Services are built as application building obstructs that can be utilized to replace standard cloud components with specially solidified variants. These variants provide the most astounding assurance of data protection not only at rest and in flight, but also while processing.

REFERENCES


