From:
Sent: 20, February, 2023 9:54 PM
To: VATP-consultation
Subject: Feedback on Consulation paper

*** CAUTION: This is an external email. Please validate before further action.***

Dear SFC,

This is Shawn Chang and I'm founder and CEO of HardenedVault. We're a cybersecurity firm highly focus on web2/web3 infrastructure and platform security. I am writing to you to express my excitement about the recent moves you have made in VASP regulation. I have read all cyber security parts in the consultation paper and wanted to provide you with some additional insights that may be helpful in your efforts to regulate the crypto industry.

Firstly, I believe that the use of centralized exchanges without proper regulation, such as FTX, poses high risks. Although KYC/AML procedures can be effective, there are technical solutions that can be implemented as well. FTX fiasco is a trust issue. How can an VA operator gain the trust from their clients? Transparency is the key and it can be utilized by regulator as well. One possible solution is to utilize transparency logs to record all the custodian's server operations on a two-node Merkle-tree service or a side chain that can be accessed by clients or regulators. This is a more effective solution than proof-of-reserve, which is easy being bypassed and nobody believes.

Secondly, I believe that you need to rethink the threat model of the crypto industry. Traditional banking systems rely heavily on physical security measures, such as the management process of tier-4 data centers. However, protecting digital assets from a crypto custodian's perspective requires a different mindset. You should consider put some advisory into the threat model, such as the attacker might have 0day vulnerabilities, internal threats (like Insyde's leaks accident), or where zero-trust authentication server can be compromised by a simple RCE. I believe it would be beneficial to add more cutting-edge cybersecurity solutions to the technical guidelines, such as OS runtime protection and trusted computing with open source firmware.

When it comes to private key storage, I share the view of many security professionals that custodians should only allow HSMs to be used within tier-3 or tier-4 data centers, as it is currently considered the most secure method. However, there are some drawbacks to HSMs. For example, the current custodian framework cannot accommodate users who wish to withdraw funds and use them within 6 hours for DeFi's flashing loan. Additionally, the token could be stolen through OS runtime hijacking or by exploiting vulnerabilities in userspace applications and libraries. While some suggest using Secure Multi-Party Computation (SMPC), I recommend caution and spending more time studying emerging technologies such as MPC. It would be beneficial for regulators to create a technology-based innovation sandbox where new technologies can be tested and studied, and vendors can be given credits if their products pass the test. This can be another Hong Kong's advantage over other region/country.

Another thing that the current regulation does not mention is the risk from the supply chain. As I attended a discussion panel hosted by Mr. Alex Yuen organized by Doctors Think Tank Academy in HKSTP last week, the software supply chain is a risk that we cannot eliminate. For example, if you build a public chain based on open-source implementation, how can you ensure long-term maintenance, and how often do you conduct security backports? If we cannot solve these issues, the risk will increase the longer we use the system. It would be great if you can mention about supply chain risk in the final version.

It's crucial for vendors to provide accurate and non-misleading marketing materials to prevent investors and users from suffering. Unfortunately, some vendors have engaged in misleading marketing practices, causing significant harm to their users. For example, certain vendors have heavily marketed Intel SGX as a silver bullet solution since 2016, leading many to believe it was a foolproof security measure. However, security researchers, including myself, concluded in 2017 that Intel SGX's threat model was flawed and that

it carried many risks. Although it can still be a useful complement to other system security solutions, most people believed the marketing until Intel publicly announced its deprecation for all Intel CPUs (except for high-end servers) in 2021. Another example of misleading marketing is SMPC, with some vendors claiming their solution is fully decentralized when it's not. We've discovered that certain vendors use tricks to "choose" a privileged node for signature verification during the initial setup, making it a centralized solution. It's important for vendors to provide truthful and transparent information to their users to avoid misleading them and compromising their security.

I hope that the information I have provided is helpful to you. Feel free to ping me and I'm happy to help if you have any question about web 3.0 infrastructure and platform security. Thank you for your time.

Reference:

Demystifiying SMPC (Secure multi-party computation) and its threat model
https://hardenedvault.net/blog/2023-02-02-smpc/

Intel confirms leaked Alder Lake BIOS Source Code is authentic
https://www.bleepingcomputer.com/news/security/intel-confirms-leaked-alder-lake-bios-source-code-is-authentic/

Intel SGX deprecation review
https://hardenedvault.net/blog/2022-01-15-sgx-deprecated/

Sigsum:
https://gitlab.glasklarteknik.se/sigsum/project/documentation/-/blob/main/design.md

Next Generation Data Center Security: The Cornerstone of Web3?
https://hardenedvault.net/blog/2022-08-05-next-gen-data-center-web3/

基础架构安全弹性技术指南草案（固件安全篇）
https://raw.githubusercontent.com/hardenedlinux/platform-resiliency-docs/master/%E5%9F%BA%E7%A1%80%E6%9E%B6%E6%9E%84%E5%AE%89%E5%85%A8%E5%BC%B9%E6%80%A7%E6%8A%80%E6%9C%AF%E6%8C%87%E5%8D%97%E8%8D%89%E6%A1%88%EF%BC%88%E5%9B%BA%E4%BB%B6%E5%AE%89%E5%85%A8%E7%AF%87%EF%BC%89alpha%E9%A2%84%E8%A7%88%E7%89%88.pdf

The below-OS for supply chain of critical infrastructure protection
https://hardenedvault.net/blog/2022-11-03-critical-infrastructure-supply-chain-security/

Bootkits samples:
https://github.com/hardenedvault/bootkit-samples

VED (Vault Exploit Defense): Open source implementation
https://hardenedvault.net/blog/2022-06-16-ved-community-version/

regards
Shawn

"Consider the environment - think before printing!"