lakyara vol.282

On the front lines of blockchain security

Teruhiro Tagomori

10.May.2018

Nomura Research Institute, Ltd.

Executive Summary

Teruhiro Tagomori
Security Engineer
NRI SecureTechnologies

While blockchain-related businesses as exemplified by cryptocurrency exchanges are booming, security vulnerabilities persist. Losses due to security breaches have been increasing. When developing a system that utilizes a blockchain, one must incorporate defense-in-depth into the system and perform risk-based evaluations of the system's architecture and operational design from prospective attackers' standpoint.

While blockchain-related businesses are booming, security vulnerabilities persist. Losses due to security breaches have been increasing. Given how much blockchain security hinges on protection of private keys[1], users are often advised to use a multi-signature (multisig) protocol and/or cold wallet, but it is a mistake to assume that simply using one or even both of these technologies is security enough.

Security precautions when using multisig

Multisig requires multiple private keys to transfer title to cryptoassets, and therefore it generally provides a high level of security. Multisig security levels are expressed in M-of-N terms, where N is the total number of private keys in existence and M is the number required to authorize a given transaction. However, if all M keys are stored on the same server and the server is hacked, they would all be stolen. Additionally, if storage of private keys is distributed across multiple servers within a single network segment and one of the servers is hacked, the hacker could access the other servers also, in which case all M keys would again likely be stolen. It is advisable to assume that any server on which a private key is stored will be hacked and to take precautions accordingly, such as distributing storage of private keys across multiple network segment levels.

Another risk that must be safeguarded against is security breaches by insiders. Even if private keys are stored in an appropriately distributed manner, if a single individual has access to all M of them, their accessibility is a security risk. Operational design is therefore also important. If private keys are stolen by an insider, the anonymity conferred by the blockchain reduces the likelihood of catching the perpetrator. It is best to take nothing for granted with respect to in-house cybercrime.

NOTE

[1] Private keys are used to authenticate title to cryptocurrency. When title is transferred, a transaction specifying the transfer is generated, authorized with one or more private keys and transmitted via a network.

Distributed storage of private keys and controls on employees' access to them are likewise necessary at any backup and/or disaster recovery sites where private keys are stored.

Security precautions when using a cold wallet

A cryptocurrency wallet is like a box in which private keys are kept. A cold wallet is a wallet in an offline environment; a hot wallet is one connected to the Internet. While cold wallet usage makes private keys more secure against external threats, it does not offer much protection against insider theft. Individuals with access to a cold wallet, whether a paper[2] or hardware wallet, can easily make unauthorized cryptocurrency transfers. It is therefore advisable to combine distributed key storage with multisig even when using a cold wallet.

The same applies to hot wallets also. The problem, however, is that not all blockchain platforms are multisig-friendly. One that is not is Ethereum, which enables programs called smart contracts[3] to execute on the blockchain. Although smart contracts essentially possess multisig-equivalent functionality, a bug in smart contracts deployed through a multisig wallet called Parity led to the theft of a large sum of ether, the Ethereum cryptocurrency, in 2017. Ethereum smart contracts are accessible to anyone and therefore always at risk of being hacked. The only channel through which Ethereum is susceptible to attack is its smart contracts. In other words, Ethereum has a single point of attack. As a result, Ethereum smart contracts are, in my opinion, as risky as or even riskier than not using multisig.

Another worthwhile precaution in terms of key management is to use a deterministic wallet. Deterministic wallets can generate multiple private keys from a single seed[4]. The seed takes the form of mnemonic code that is stored as a backup and can restore private keys that have been lost or corrupted. Mnemonic code therefore should be secured in the same manner as a cold wallet.

With hardware wallets, private key leakage risk is extremely low because private keys are never removed from the dedicated hardware in which they are stored, but if that hardware is connected to a computer connected to the Internet, the computer could hacked by malware that, for example, replaces a wallet address copied onto the user's clipboard with the hacker's wallet address. Offline use is consequently recommended.

[2] Paper on which a private key is printed.

[3] For more details on smart contracts and smart contract security, see Tagomori, Teruhiro, *"Kenro na sumato kontorakuto kaihatsu no tame no burokkuchen [gijutsu] nyumon"* (Blockchain [technology] primer for development of robust smart contracts), Gijutsu-Hyohron Co.

[4] Private keys are random alphanumeric strings. The seed generates such alphanumeric strings.

Key management alone is not enough

While key management is indisputably of utmost importance on the blockchain, it is a mistake to assume that robust key management provides failsafe security. Blockchain users must ensure that their overall IT security is robust inclusive of web applications, servers and networks deployed to deliver services. Inadequate security can lead to unauthorized cryptocurrency transfers even in the absence of private key theft.

For example, an HTTP-based service called JSON-RPC (JavaScript Object Notation Remote Procedure Call) is often used to issue commands to interface with blockchains' public client software, enabling the commands to be sent over HTTP. However, use of JSON-RPC should generally be restricted solely to access from local hosts or designated IP addresses, not publicly available applications. In the case of system architecture where JSON-RPC calls are directly issued by a user-facing Web service, or if the service is inadvertently accessible from the public Internet, the service could allow hackers to make unauthorized cryptocurrency transfers with JSON-RPC commands. Searches for blockchains' JSON-RPC ports have already been detected. If a JSON-RPC port is publicly accessible, it is best to assume it will be attacked. Additionally, if a hacker infiltrates a server and replaces public client software with malware that reroutes all cryptocurrency transfers to the hacker's address, the malware would enable unauthorized cryptocurrency transfers even without a private key.

Evaluating security based solely on use of multisig or a cold wallet is perilous. Key management practices should also be instituted and complied with, though such practices will not upgrade the security level unless users understand their essence and the intentions behind them. System architecture and operations will differ depending on the system/business requirements of the services being provided, but the crucial point is that overall security must be evaluated on a risk basis from a prospective attacker's standpoint. In addition to key management, risk analysis and security precautions are as necessary as they are for conventional applications.

about NRI

Founded in 1965, Nomura Research Institute (NRI) is a leading global provider of system solutions and consulting services with annual sales above $3.7 billion. NRI offers clients holistic support of all aspects of operations from back- to front-office, with NRI's research expertise and innovative solutions as well as understanding of operational challenges faced by financial services firms. The clients include broker-dealers, asset managers, banks and insurance providers. NRI has its offices globally including New York, London, Tokyo, Hong Kong and Singapore, and over 12,000 employees.

For more information, visit http://www.nri.com/global/

The report is provided solely for informational purposes for our UK and USA readers and is not to be construed as providing advice, recommendations, endorsements, representations or warranties of any kind whatsoever.

Whilst every effort has been taken to ensure the accuracy of the information, NRI shall have no liability for any loss or damage arising directly or indirectly from the use of the information contained in this report.

Inquiries to : Financial Market & Innovation Research Department
Nomura Research Institute, Ltd.
Otemachi Financial City Grand Cube,
1-9-2 Otemachi, Chiyoda-ku, Tokyo 100-0004, Japan
E-mail : kyara@nri.co.jp

http://www.nri.com/global/opinion/lakyara/index