NIST Recommendations For Software Supply Chain Security: GBA

Possible applications of blockchain technology

December 8, 2022

Questions & Enquiries: annaaspen@gosh.sh

Executive Order 14028

“The Federal Government must take action to rapidly improve the security and integrity of the software supply chain, with a priority on addressing critical software.”

Among others, the points identified as vulnerabilities in government supply chain security include:

- Build environments
- Auditing
- Dependencies
- Unencrypted Data
- Provenance

NIST Recommendations

The National Institute of Standards and Technology (NIST) recommendations work primarily to educate and train on dealing with cyber threats in the supply chain, with an emphasis on best practices, in 3 Levels:

- Enterprise “strategy, policy, and implementation plan”
- Mission and Business Process “implementation plans assume the context and direction set forth at the enterprise level and tailor it to the specific mission and business process”
- Operational “plans provide the basis for determining whether an information system meets business, functional, and technical requirements and includes appropriately tailored controls”

Blockchain for Access Control

- Blockchain solutions limit access to systems and components that traverse the supply chain. Unauthorized release, modification, or destruction of information are issued mitigated by an immutable ledger
- The separation of the information system and supply chain information flow can be ensured by blockchain encryption and signatures.
- Blockchain consensus protocols ensure that an appropriate separation of duties is established for decisions that require the acquisition of both information system and supply chain components, such as denying developers the privilege to promote code that they wrote from development to production environments.
- Blockchain smart contracts ensure that detailed requirements are properly defined and that access to information regarding the information system and supply chain is protected from unauthorized use and disclosure.

Audit and Accountability

- Blockchain systems can ensure audit records of a supply chain event are handled securely and maintained in a manner that conforms to record retention requirements and preserves the integrity of the findings and the confidentiality of the record information and its sources as appropriate
- Can help enterprises implement non-repudiation techniques to protect the originality and integrity of both information systems and the supply chain network.
- Smart contracts can ensure that monitoring is in place for contractor systems to detect the unauthorized disclosure of any data. Enterprises can be notified immediately in the event of any potential or actual unauthorized disclosure.

Assessment, Authorization, and Monitoring

Enterprises can make use of blockchain-based systems to assist them in activities to assess and authorize an enterprise's information systems, as well as external assessments of suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers, where appropriate.

Activities aided by blockchain include:

- The tracking of chain of custody and system interconnections within and between enterprises
- The verification of suppliers' claims of conformance to security
- Product/component integrity
- Validation tools and techniques for non-invasive approaches to detecting counterfeits or malware (e.g., Trojans)

Configuration Management

Blockchain immutable ledgers allow enterprises to track changes made throughout the SDLC to systems, components, and documentation within the information systems and networks.

It becomes not only possible to know, but also to prove, what changes were made to those systems, components, and documentation; who made the changes; and who authorized the changes.

It also provides evidence for investigations of supply chain cybersecurity compromise when determining which changes were authorized and which were not.

System and Information Integrity

Blockchain guarantees system and information integrity.

The insertion of malicious code and counterfeits are two primary examples of cybersecurity risks throughout the supply chain; these can be combated comprehensively using blockchain technology, formal verifications, and consensus protocols

“The enterprise should ensure that code authentication mechanisms, such as digital signatures, are implemented to ensure the integrity of software, firmware, and information” – these are in-built to any blockchain system

Reference To The Working Group

- The GBA Secure Software Supply Chain Working Group was started on the basis of these NIST recommendations, which highlight issues with potential blockchain-based solutions

- The Working Group is led by GOSH, a blockchain purpose-built for storing git on-chain and securing the software supply chain

- Regular meeting will be held with this presentation as one of the discussion reference points