ORNL/SPR-2023/3077

Supply Chain Management in the Cyber Grid Guard Framework

Raymond Borges Hink
Aaron Werth
Gary Hahn
Emilio Piesciorovsky
Annabelle Lee

September 2023

OAK RIDGE National Laboratory

ORNL IS MANAGED BY UT-BATTELLE LLC FOR THE US DEPARTMENT OF ENERGY

ORNL/SPR-2023/3077

Electrification and Energy Infrastructures Division

SUPPLY CHAIN MANAGEMENT IN THE CYBER GRID GUARD FRAMEWORK

Raymond Borges
Aaron Werth
Gary Hahn
Emilio Piesciorovsky
Annabelle Lee

September 2023

Prepared by
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, TN 37831
managed by
UT-BATTELLE LLC
for the
US DEPARTMENT OF ENERGY
under contract DE-AC05-00OR22725

CONTENTS

ABSTRACT

Grid modernization has given impetus to innovative power grid applications and energy resources that are increasingly distributed. Blockchain/distributed ledger technology has the potential to enhance the resilience of the electric infrastructure, particularly in a decentralized and distributed environment. The benefits of blockchain are that it can ensure asset information and life cycle events are secure and traceable and identify potential malicious modifications of data. Oak Ridge National Laboratory has developed a framework, Cyber Grid Guard, incorporating blockchain. The system implements a low-energy, fast, and robust enhancement to system trustworthiness within and across electric grid systems, including substations, control centers, and metering infrastructures. Currently, supply chain attacks are a major concern. Recently, several attacks have occurred that significantly affected critical infrastructures and organizations around the world. This document focuses on how Cyber Grid Guard can address the supply chain issue.

1. BACKGROUND

The modernization of the US power grid weaves together traditional legacy infrastructures and next-generation technologies. These advanced technologies bring intelligent components into the electric grid, enabling sophisticated two-way communication, dynamic optimization, and wired and wireless connections. As renewable energy sources like solar and wind are deployed, the interconnectivity between varied organizations and systems becomes more pronounced, heralding a new set of demands for contemporary power systems. Central to these demands is the assurance that sensitive grid information remains protected, preventing unauthorized access. It's equally crucial to maintain the accuracy and trustworthiness of data, as this underpins the safe and efficient operation of the grid. Despite potential disruptions, the systems must also ensure an unwavering power supply, delivering energy consistently to all endpoints.

The supply chain presents its complexities, from design and manufacturing to operations and maintenance [11]. This chain, vulnerable at every juncture, faces a spectrum of growing and sophisticated cyber threats. By leveraging digital supply chains, malicious entities can circumvent traditional defenses, compromising components that were considered trustworthy. Thus, the task of protecting the supply chain becomes as critical as the overarching goal of securing the entire grid [2, 3, 10].

Supply chain attacks can be organized into the following three categories:

- **Software attacks:** These attacks focus on the source code of a vendor's software. The attacker injects malicious code into an application, including library code.
- **Hardware attacks:** These attacks target physical devices such as routers. Typical forms of hardware attack involve inserting backdoors into the hardware or installing and deploying counterfeit devices. Counterfeit devices may not meet the safety requirements necessary in the energy sector.
- **Firmware attacks:** This type involves injecting malware into the boot code. The malware runs after the computer boots up.

2. CASE STUDY: SOLARWINDS SUPPLY CHAIN ATTACK

One of the most significant recent supply chain attacks was against SolarWinds [9] Orion software. Advanced persistent threat actors infiltrated the supply chain of SolarWinds, inserting a backdoor into the SolarWinds Orion product (Oladimeji and Kerner, 2023). Because customers downloaded the Trojan horse installation packages from SolarWinds, attackers could access the systems running the SolarWinds product(s). The SolarWinds supply chain attack involved deploying a malicious software or malware

called "Sunburst." This malware was discreetly embedded within legitimate SolarWinds' Orion product updates, allowing the threat actors to gain undetected access and control over affected systems.

While the SolarWinds incident was primarily an information technology (IT) system breach, its implications for power grid supply chain security are profound. The modern electric grid's digital evolution has intertwined IT and operational technology (OT), making them more interdependent. As a result, vulnerabilities in IT systems can provide pathways into OT environments. The SolarWinds breach underscores the critical need for comprehensive security strategies that address threats in both domains, ensuring the protection of our interconnected and evolving critical infrastructures.

A detailed examination of this sophisticated attack revealed the following:

- **Attack vector:** The attackers targeted the source code, injecting malicious code into the application. More specifically, attackers targeted the SolarWinds Orion network management system, injecting malicious code known as Sunburst.
    - **Method:** The attackers compromised the build system, inserting malicious code into a legitimate update file. The method was a supply chain attack where the malicious code was inserted into updates distributed by SolarWinds.
    - **Disguise:** The malicious code was carefully disguised as benign, evading detection by standard security tools.
    - **Distribution:** When customers downloaded and installed the Trojanized update, the backdoor was activated, allowing the attackers to access the systems running the SolarWinds Orion product(s).

- **Impact:** Numerous organizations were compromised, leading to potential data exfiltration and system disruption. Over 18,000 SolarWinds customers installed the malicious updates, giving the attackers broad access to customer information technology (IT) systems. More than 30,000 organizations were using the affected Orion system, leading to extensive compromise of data, networks, and systems, which are still being studied to understand the full extent of the impact.

- **Mitigation and the Cyber Grid Guard (CGG) framework:** The SolarWinds attack underscores the need for advanced solutions such as the CGG framework to enhance supply chain security. This includes:
    - **Detection:** CGG Hyperledger Fabric (HLF)–based blockchain technology provides traceability and nonrepudiation, enabling the detection of unauthorized changes to the software.
    - **Prevention:** Using distributed ledger technology (DLT), the CGG framework ensures the integrity of the source code, making it more resistant to unauthorized modifications.
    - **Response:** The framework’s ability to securely manage configurations and patches enables a more rapid and coordinated response to the intrusion. Also, having the data in the blockchain ledger enables a more trustworthy postmortem analysis of events and changes in data and configurations.

This real-world example underscores the need for robust supply chain security solutions like the CGG framework. The SolarWinds attack is a stark reminder of the complexities and vulnerabilities inherent in modern supply chains. Some supply chain attack techniques [6, 7] that may be used are misconfiguration, masquerading, denial of service, unauthorized access, easily obtained credentials, and rogue devices. Once inside, an attacker can deploy malware, exfiltrate sensitive data, or disrupt operations. Protecting the supply chain associated with manufacturing and maintaining technology is of utmost concern, particularly for critical infrastructures such as the energy sector. This case study emphasizes the crucial role of

innovative technologies such as blockchain in building resilience against increasingly sophisticated cyber threats [4].

3. OVERVIEW OF BLOCKCHAIN

Blockchain enables distributed access, validation, and record-updating of a distributed ledger in an immutable manner across a network of multiple stakeholders, entities, and locations. Information is stored securely and accurately using keys and cryptographic signatures. The decentralized, distributed nature of the ledger makes it resilient to various cyberattacks because all copies stored across the network must be compromised simultaneously for the adversary to succeed [5, 6, 8]. This distributed nature precludes the single-point-of-failure attack.

The following list identifies the key characteristics of a blockchain:

- **Nonrepudiation:** This ensures that the individual or device that digitally signs the data with their private key cannot deny that they have signed it. The private key is known only by the owner and is not shared. The receiver uses the associated public key to verify that the transmitted data have not been altered in transmission.
- **Immutability:** Once a transaction is recorded, it is challenging to delete or rollback. This ensures the provenance of the transaction.
- **Anonymity:** Each transaction is digitally signed with a private key known only by the owner. Therefore, the real identity of the owner is not revealed.
- **Traceability:** Every transaction added to the ledger is digitally signed and time stamped. This provides a link to the previous block. Therefore, an entire history can be reconstructed. This characteristic supports a complete, auditable record of transactions.
- **Data integrity:** in blockchain is ensured through two key features tamper evidence and tamper resistance. Tamper evidence allows for identifying any data modifications, while tamper resistance makes it difficult to alter past transaction records.

There are two general classes of blockchain: private (permissioned) and public (permissionless). For the energy sector, private blockchains are recommended because of the sensitivity of the power grid application data, particularly in the OT environment. A private blockchain requires identification and authentication security controls for participating devices and individuals. Smart contracts, one of the key features of blockchain, are programs that execute when specific conditions are met. A “smart contract” reads or writes transactions, orders transaction proposals, and queries transactions in the ledger. Smart contracts do not operate on data external to the ledger. They operate on the data received as arguments for their functions and the data in the ledger. Any data required by a smart contract must be included in the ledger. Because of the sensitivity of the power grid application data and to conserve energy, only private permission-based blockchains, such as the HLF-based blockchain, are recommended within the CGG framework so that additional identification and authentication security controls are required for participating devices and individuals.

3.1 APPLICATION OF BLOCKCHAIN TO SUPPLY CHAIN SECURITY

Blockchain can support the following to advance supply chain security for hardware, software, and firmware: [1]

- Attestation/provenance tracking of components (e.g., ordered asset and received asset)
- Configuration management, including baseline configurations
- Patch management, including patches for identified vulnerabilities

- Complete system life cycle management
- Ongoing monitoring

An effective blockchain solution for the electric sector will include many organizations (e.g., utilities, suppliers, vendors, integrators, and third-party service providers). A given supplier may develop physical components and distribute them to another entity, who in turn supplies an integrated and complete product. Another example is computerized relays for power systems in utilities. The relay company would acquire computer chips and electrical components to create the frame for the relay. Various suppliers would make each of these components. The software for the relays could be produced in-house by the relay company. An adequate supply chain solution will ensure that sensitive information such as vendor product specifications or a utility's OT architecture will be shared only with contractual organizations.

Firmware updates typically have digital signatures that can be used to confirm whether the firmware is authentic. This can be helpful to manage the software aspect of the supply chain. There is commonly an IT network and an OT network for critical infrastructure. To ensure security, a given operator may download the firmware to an IT network rather than the OT network. The operator can scan and examine the firmware from the IT network before allowing it to be used in the OT network.

3.2 DARKNET CGG AND SUPPLY CHAIN MANAGEMENT

Under the US Department of Energy's Oak Ridge National Laboratory's DarkNet initiative, a team has been developing a unique set of approaches to handle the challenges of the supply chain. The system is called Cyber Grid Guard and has a DLT-based remote attestation framework that uses blockchain-based methods for verifying device and data trustworthiness for the electric grid, including device attestation and data integrity within and between grid systems, subsystems, and appliances. CGG's attestation framework is intended to strengthen the resilience and security of the US grid by increasing the trustworthiness of devices and data. Also, when a given substation is commissioned initially or other parts of the grid are commissioned or set up, it is important to inventory all the devices. The power grid data and device configuration settings (artifacts) are used to diagnose and respond to cyber events and electrical faults, whether malicious or not. The inventory is stored in the CGG system. Specifically, the approach of CGG is to detect anomalies and discrepancies in the data being shared between devices compared with the last-known correct baselines.

The CGG system also records other information about the devices relevant to networking and communications, such as their IP addresses, media access control (MAC) addresses, and serial numbers. The CGG system stores the data from the network and preserves the data immutably and redundantly across the DLT nodes. The data captured include voltage and current as time-series data in a raw but summarized form as time-sampled alternating current (AC) signals and root mean square (RMS) values.

Remote attestation is necessary because the DLT CGG system is intended to be implemented in a distributed environment. Remote attestation includes a verifier that validates data from a prover. There are three types of attestation: hardware-based, software-based, and hybrid. Hardware-based remote attestation leverages physical devices/chips and modules to achieve remote attestation. Software-based remote attestation does not rely on any hardware to perform remote attestation. Hybrid remote attestation includes both hardware and software components. Because many electric grid devices have limited processing and storage capacities, CGG implements software-based remote attestation.

Figure 1 illustrates how the CGG blockchain framework can be expanded to include all life cycle phases of the supply chain as addressed by utilities. The focus is on the OT environment, where availability is critical. Latency of commands could adversely affect the operation of facilities such as transmission and distribution substations. Therefore, a blockchain solution must ensure data collection and processing will

not affect availability. This consideration is absent in the IT environment, where processing capacity and data storage are typically almost unlimited. CGG was designed considering these constraints while also ensuring that compromises are detected. The following techniques employed in CGG ensure this consideration of not interfering with ongoing system operations.:

- **Time-Windowed Data Processing**: The CGG system efficiently processes data in one-minute windows. Focusing on these short timeframes, the most relevant data dynamics are captured without overburdening the system with high-frequency fluctuations.

- **Statistical and Summary Data**: Instead of storing voluminous raw data, which can strain storage resources and slow retrieval times, the CGG framework emphasizes storing statistics and summary data in the off-chain ledger. This approach ensures that the most critical insights are preserved and readily accessible while significantly reducing the data footprint.

- **SHA-256 Hashes on the Ledger**: The integrity and authenticity of the data is paramount. To maintain this while ensuring efficient storage, we save only SHA-256 hashes of the one-minute data windows to the blockchain ledger. This cryptographic hashing ensures data security, offers a quick verification mechanism, and keeps the on-chain storage lean and fast.

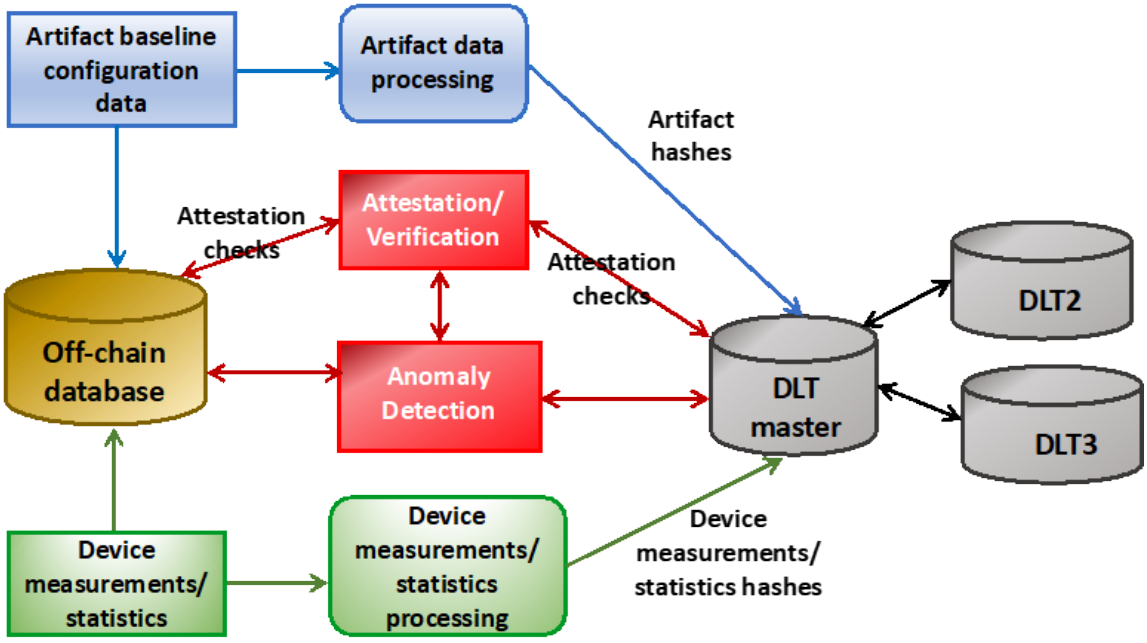

Figure 1. Generalized CGG supply chain framework.

The following subsections describe how blockchain can be used by a utility to support the supply chain life cycle phases. The approach is based on CGG research.

3.2.1 Phase 1: Product Receipt

This phase focuses on ensuring that the ordered asset matches the received asset. The CGG team coordinated with the BLOSEM project (Blockchain for Optimized Security and Energy Management), which used schemas for tracking items. Each item has information that can be stored in a database, such as the product name, product serial number, product version, vendor, country of origin, hardware bill of materials (BOM), and software BOM. The objective is to ensure traceability of the various components.

Typically, this information is stored off-chain with a hash in the blockchain. This process of storing only hashes significantly reduces the storage and speed required to support many devices on a network.

3.2.2 Phase 2: Baseline Configurations and Configuration Updates

In phase 2, a baseline is created for each selected component. This includes hardware, software, and firmware. This creation occurs on initial system setup or when a user manually establishes a new baseline. The baseline configuration data is stored off-chain, and a hash of the configuration data stored in the blockchain ledger. In CGG, two categories of data are collected: measurement data and configuration (artifact) data. The CGG attestation framework triggers the baseline collection process at startup using software to manage the configuration data for each device. Measurement data are collected from sensors, meters, intelligent electronic devices, network devices, and other sources. For grid data, the objective is to ensure that the data are within certain bounds and/or are sent at a standard frequency. These statistics are useful to establish a profile of the system's behavior. Examples of configuration data include the following:

- Protection schemes (group settings)
- Device configurations
- Network settings (port, frequency, data sent/received)
- Tags for IEC 61850 and similar items for other protocols (e.g., registers for Modbus and identifiers in DNP3)
- Firmware, program settings, and status (reclose enabled/ground enabled, breaker status, long-term settings, GOOSE [Generic Object-Oriented Substation Event] messages)

The collected data are stored in an off-chain database for statistical and anomaly analysis. After an abnormality is detected, the system addresses issues with storing increasing amounts of data. Configuration data and statuses are stored off-chain for historical data retention, long-term analysis, and forensics. The continuous transmission of measurement data at various frequencies, especially as the number of network devices grows, presents potential performance and storage challenges. To mitigate these challenges, CGG aggregates or filters the packet data and then hashes the data using static window periods. (It's worth noting that measurement data collection is not typically a part of supply chain cybersecurity. However, with the rise in malware deployment, documenting and validating configuration settings have become crucial.) The measurement and configuration data can be cross-verified using both off-chain and on-chain (hashed) data. The frequency of such verification is anticipated to align well with the system's availability.

When configurations are updated, a new baseline is developed. This may include updating the configuration artifact data and revising the measurement data. The hashed values are stored on-chain, and the summarized raw data is stored in the off-chain database.

3.2.3 Phase 3: Anomaly Detection

This phase is typically not part of supply chain cybersecurity. As in phase 2, regular validation of the system architecture is essential, including the software, firmware, hardware configurations, and measurement baselines. The objective is to detect unauthorized configuration modifications, including identifying unauthorized devices and potentially out-of-band measurement data. The anomalous data must be confirmed to prevent false positives from being reported.

The CGG anomaly detection software stores only a hash of the statistical baseline patterns in the blockchain ledger for comparison. When measurement data or configurations, settings, or parameters do not match the baseline, an alert is triggered for that device, indicating the new and last-known-good

configuration hash. The source of anomalous data is identified by the IP address and/or MAC address. For measurement data, determining whether an anomaly has occurred is based mainly on threshold checking. When an attestation check event is triggered, the attestation scheme repeats the data verification step to compare the newly acquired data window with the stored configuration/measurement hashed baselines in the DLT. Anomalous data does not automatically imply that a cybersecurity event has occurred; anomalous data can result from a device failure or misconfiguration.

3.3 CGG FRAMEWORK CRYPTOGRAPHIC TECHNIQUES

The CGG framework incorporates advanced cryptographic techniques to enhance the security and resilience of the electric grid. Regarding supply chain management, the framework leverages several cryptographic methods to ensure data and devices' integrity, trustworthiness, and security within the grid. The critical aspects of CGG cryptographic techniques are listed in the following subsections.

3.3.1 Hash Functions

Creating unique identifiers: The SHA-256 hash function creates unique identifiers for data blocks and components within the grid. This ensures traceability and detects unauthorized changes. This technique to hash the off-chain data is known in the literature as trust anchoring.

Tamper resistance and immutability: By chaining blocks and creating unique hash values, any unauthorized alteration to the content can be detected, contributing to the immutability of the data within the CGG framework.

3.3.2 Digital Signatures

Enhancing traceability: Time-stamped and digitally signed transactions within the CGG framework allow for a complete auditable history of transactions, supporting traceability and accountability.

3.3.3 Consensus Algorithms

Verifying transactions: CGG, which employs HLF-based blockchain, uses the Raft consensus algorithm to verify transactions within the network, adding a decentralized verification mechanism.

Enhancing network security: Consensus algorithms play a vital role in maintaining the decentralized integrity of the grid, ensuring no single entity can control or compromise the network.

3.3.4 Application of Cryptographic Techniques in CGG

Detection and prevention of supply chain attacks: The CGG framework uses cryptographic techniques to detect unauthorized changes to the software, such as in the SolarWinds attack, and to prevent unauthorized modifications.

Configuration management and response: The ability to securely manage configurations, patches, and trustworthy postmortem analyses is enhanced through cryptographic principles within the CGG framework.

4. CONCLUSION

The overall architecture of the electric grid is changing from centralized control and management to distributed and decentralized control. This change has resulted in an increased attack surface and requires new approaches to address potential cybersecurity attacks. One technology that has been proposed is blockchain, which is inherently decentralized and distributed. This paper describes the Oak Ridge National Laboratory (ORNL) CGG framework and how it can be used to address supply chain issues. The ORNL CGG framework enhances security through several distinct mechanisms:

- **Traceability and Nonrepudiation**: By embedding every transaction with a unique identifier, the CGG framework ensures every action can be traced back to its origin, ensuring accountability and deterring malicious modifications.

- **Integrity and Tamper Detection**: The application of cryptographic hashes, such as SHA-256, facilitates the immediate detection of any unauthorized changes, guaranteeing the immutability and trustworthiness of data.

- **Configuration Management**: The CGG framework supports dynamic updates, ensuring configurations remain current and secure.

- **Consensus Mechanisms**: Utilizing algorithms like the Raft consensus in its HLF-based blockchain, the CGG framework ensures that all transactions are validated in a decentralized manner, adding an extra layer of trust, and reducing vulnerabilities.

- **Anomaly Detection**: The framework is adept at identifying discrepancies from known baselines, swiftly detecting potential threats, and ensuring prompt remediation.

5. REFERENCES

1. Asante, M., G. Epiphaniou, C. Maple, H. Al-Khateeb, M. Bottarelli, and K. Z. Ghafoor. 2023. "Distributed Ledger Technologies in Supply Chain Security Management: A Comprehensive Survey." *IEEE Transactions on Engineering Management*, vol. 70, no. 2, pp. 713–739. doi: 10.1109/TEM.2021.3053655.
2. Boyens, J. et al. 2021. *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry*. NISTIR 8276. National Institute of Standards and Technology, US Department of Commerce.
3. Boyens, J. et al. 2022. *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*. NIST Special Publication (NIST SP) 800-161r1. National Institute of Standards and Technology, US Department of Commerce.
4. Chang, S. E., and Y. Chen. 2020. "When Blockchain Meets Supply Chain: A Systematic Literature Review on Current Development and Potential Applications." *IEEE Access* vol. 8, 62478–62494.
5. Gourisetti, S. et al. 2021. "Standardization of the Distributed Ledger Technology Cybersecurity Stack for Power and Energy Application." *Sustainable Energy, Grids and Networks*, vol. 28, 100553. doi: 10.1016/j.segan.2021.100553.
6. Lee, A. et al. 2023. "Assessment of the Distributed Ledger Technology for Energy Sector Industrial and Operational Applications Using the MITRE ATT&CK® ICS Matrix." *IEEE Access*, vol. 11, 69854–69883. doi: 10.1109/ACCESS.2023.3288428.
7. Miller, J. F. 2013. *Supply Chain Attack Framework and Attack Patterns*. McLean, VA: MITRE Corporation.
8. MITRE Corporation. n.d. "ICS Matrix." MITRE ATT&CK. https://attack.mitre.org/matrices/ics/.
9. Oladimeji, S., and S. M. Kerner. 2023. "SolarWinds Hack Explained: Everything You Need to Know." TechTarget. https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know#:~:text=How%20did%20the%20SolarWinds%20hack,to%20hack%20the%20networks%20directly
10. Papaphilippou, M., K. Moulinos, and M. Theocharidou. 2023. *Good Practices for Supply Chain Cybersecurity*. European Union Agency for Cybersecurity (ENISA).
11. Shen, L., R. Fan, and Y. Wang. 2021. "Integration and Optimization of Green Supply Chain Networks under the Epidemic Environment." *Mathematical Problems in Engineering*, vol. 1, no. 2, 3.