Assured Cyber Supply Chain Provenance Using Permissioned Blockchain

Website: http://cred-c.org/researchactivity/blockchainprovenance

Researchers (ODU/Illinois): Sachin Shetty (ODU), Xueping Liang (ODU) and Andrew Miller (Illinois)

Industry Collaboration: We are collaborating with the following to develop a blockchain based cyber supply chain provenance tool for the power utility sector:

- Electric Power Research Institute (EPRI)
- ReliabilityFirst (RF)
- National Rural Electric Cooperative Association (NRECA)

Description of research activity: The approach proposed in this activity focuses on customized consensus engine for cyber supply chain provenance and security mechanisms in permissioned blockchain platforms. We will develop a customized consensus engine which will not require participants in the cyber supply chain to make significant investment on computation and will balance the tradeoff between number of transactions processed, transaction validation time, incentives and security rules set by participators in the cyber supply chain. We will develop a capability for encoding the electronic component's firmware/software design into transactions while balancing tradeoff between validation accuracy and latency. We will develop strategies to encode the firmware/software design and their computed hash values will be encoded in the blockchain. The hash values and the firmware/software designs will be delivered through the cyber supply chain and participators at every stage can ensure authenticity of the design by verifying the hash values. However, allocation of appropriate incentives for the participants is another emerging challenge where the trade-off between the incentive and cost of participation in consensus needs to be resolved. We will develop game theoretic based incentive mechanism to self-motivate participators in order to participate in the consensus. We will develop a layer for security assurance within the blockchain architecture to protect the business critical data. Data and transactions will be encrypted using threshold cryptography, such that multiple validating nodes must interact in order to decrypt and compute over this data. This will ensure that business critical data is not revealed even in the event that some number of the validating nodes are compromised.

How does this research activity address the Roadmap to Achieve Energy Delivery Systems Cybersecurity?
The proposed research supports the Roadmap strategy "Assess and Monitor Risk" and supports the strategy "Develop and Implement New Protective measures to Reduce Risk". Additionally, with the requirement from FERC to establish a cyber supply chain for the electric grid; there is a need for technologies to ensure provenance and guarantee that the processes in the supply chain are functioning according the intended purpose.

Summary of EDS gap analysis: There is a lack of tools or technologies that can protect the entire cyber supply chain and ensure that all software and firmware verified for their trustworthiness before they are integrated into EDS OT. We will develop permissioned blockchain based data provenance techniques to certify the software and firmware at all stages of an cyber supply chain in EDS so that the end-users can easily verify whether the purchased electronic component's software or firmware is tampered with or not. We will develop integrity mechanisms for permissioned blockchain platforms so that critical data remains secure even in the presence of data breach attacks.

Full EDS gap analysis: Developing techniques and tools to provide assured cyber supply chain provenance are top priority for addressing cyber supply chain risks such as, counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware, as well as poor manufacturing and development practices [1-3]. The globalization of cyber supply chain has resulted in software and firmware developed by offshore enterprises and has resulted in tremendous savings for the EDS sector. However, the dependency on third-party services has resulted in increase in threats across several stages in the cyber supply chain. Specifically, there is a need for tools or technologies that can adequately address risks involved in processes, sourcing, third party vendor management (every actor that has

physical or virtual access to software code and/or systems), acquisition of compromised software or hardware purchases from suppliers, embedded malware in hardware or counterfeit hardware and third party data storage or data aggregators [1,2]. Solutions such as, side-channel fingerprinting, reverse engineering, and formal methods are mostly deployed at the chip level to detect presence of counterfeit chips. However, these methods cannot be scaled to protect the whole cyber supply chain. There is a need for a top-down methodology to scale the process of protecting the cyber supply chain.

Blockchains are a new technology which uses a distributed public ledger to record transactions and facilitate trusted delivery of transactions across a distributed network without involvement of centralized authority or intermediaries. Blockchains have the following advantage over centralized databases: (1) Ability to directly share databases across diverse boundaries of trust in situations where it is difficult to identify a trusted centralized arbitrator to enforce constraints of proof of authorization and validity. In a blockchain, transactions leverage self-contained proofs of validity and authorization based on a verification process enforced by multiple validating nodes and a consensus mechanism that ensures synchronization. (2) Ability to provide robustness in an economical fashion without the need for expensive infrastructure for replication and disaster recovery. Blockchains provide built-in technical mechanisms to handle tasks which would otherwise require complex institutional processes. Nodes in a blockchain automatically self-configure and connect and sync with each other in a peer-to-peer fashion, feature built-in redundancy, avoid the need for close monitoring, can tolerate multiple communication link failures, allow external users to broadcast transactions to any node, and ensure that disconnected nodes will be caught up on missed transactions.

In this work, we will develop permissioned blockchain-based data provenance techniques to certify the software and firmware at all stages of a cyber supply chain in EDS so that the end-users can easily verify that the purchased electronic component's software or firmware is not tampered with. Our previous work demonstrated a permissionless blockchain based data provenance system for cloud auditing, but required investment of computation resources [4]. Current blockchain based industry solutions for addressing supply chain threats either use the Ethereum platform based on Proof-of-Work consensus, which requires investment of computational resources and can process fewer than 20 transactions per second and transaction validation time takes several minutes [5-7], or the Hyperledger fabric platform [8] which cannot guarantee safety from data breach on validating nodes. In previous work, we have developed cryptographic methods to ensure security for blockchain applications even when some participants are compromised [9]. Our research efforts will focus on the following: (1) Consensus engine for cyber supply chain provenance – We will develop a customized consensus engine within Hyperledger Fabric which will balance the tradeoff between number of transactions processed, transaction validation time, incentives and security rules set by participators in the cyber supply chain (2) Security in permissioned blockchains – We will develop cryptographic techniques based on secret sharing that we can incorporate into a security layer for Hyperledger Fabric to mitigate against data breach attacks on the validating nodes.

Bibliography:

- Energy Sector Control System Working Group, "Roadmap to achieve Energy Delivery Systems Cybersecurity," September 2011
- Cyber Supply Chain Best Practices, http://csrc.nist.gov/scrm/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf
- Cyber Supply Chain Risk Management, http://csrc.nist.gov/scrm/
- Xueping Liang, Sachin Shetty, Deepak Tosh, Charles Kamhoua, Kevin Kwiat, Laurent Njilla, "ProvChain: A Blockchain-based Data Provenance Architecture in Cloud Environment with Enhanced Security and Availability," The 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), May 14-17 2017.
- Ethereum reaches 50 % Bitcoin transaction volumes, http://www.trustnodes.com/2017/05/17/ethereum-reaches-50-bitcoins-transaction-volumes
- Skuchain, https://skuchain.com/products/

- Microsoft's Project Manifest: Blockchain-Based Product Tracking: https://www.ethnews.com/microsoft-project-manifest-blockchain-product-tracking
- Blockchain for supply chain, https://www.ibm.com/blockchain/supply-chain/
- Hawk: The Blockchain Model of Cryptography and Security-Preserving Smart Contracts. Ahmed Kosba, Andrew Miller, Elaine Shi, Zikai Wen, Charalampos Papamanthou. IEEE Security & Security (Oakland), May 2016.