BLOCKCHAIN TECHNOLOGY

Annabelle Lee
Chief Cyber Security Specialist
11/28/17
Overview...

- Blockchain is a distributed ledger technology
  - Explicitly distributes control among all peers in the transaction chain
  - Contrast with centrally controlled ledger
- Blockchain networks are *trustless*
  - Assume compromise of the network by both insiders and outsiders.
- Considered *transparent* because
  - Miners confirm and verify each transaction
  - Every participant in the peer-to-peer network
    - Has a copy of the ledger and
    - Can see the contents of every transaction
  - Once recorded, transactions cannot be altered
    - Ensures data integrity
    - Addition of transactions by consensus
Inclusion of digital signature and hashing
- Each block contains a cryptographic hash (typically SHA256)
  - Computed based on all the blocks in the chain, to that point
- Each transaction is digitally signed by the originator
  - Considered “anonymous” -- no personally identifiable information
  - Associated public key distributed

Permissioned vs permissionless blockchain
- Permissioned (private): entity identity must be verified
- Permissionless (public): anyone can participate

Potential use cases
- Currently, most closely associated with enabling cryptocurrencies such as Bitcoin and Ethereum
- Transactive energy to support DER
- eMobility – transact energy charging at stations in multiple service territories
- Customer contracts – removing the middleman from the retail energy market
Implementation Issues

- **Scalability**
  - Significant storage required
  - Technology meeting processing needs

- **Potential attacks**
  - Denial of service (DoS)
  - Widespread distribution of malware
  - Timestamp alteration

- **Key management infrastructure**
  - Key generation, storage, distribution, etc.
Supply Chain Security

- Commercially available Information and Communications Technology (ICT) solutions present significant benefits
  - Low cost
  - Interoperability
  - Meet the needs of a global base of customers
  - Choice among competing vendors
  - Increase the risk of a threat event which can impact the ICT supply chain
    - May include insertion of malicious software, firmware, and/or hardware

Cyber security supply chain issues are of growing concern
Cyber Security Supply Chain

- Blockchain application
  - Potential use case
    - Ensure the integrity of the supply chain
    - *Detect* unauthorized changes to firmware and software
    - Can be applied throughout the supply chain
      - Chips to components to devices
      - What is the provenance?
Blockchain Working Group

- Representatives from the US, the European Commission (EC), and Agency for the Cooperation of European Regulators (ACER)
- Focusing on OT supply chain for the energy sector
- Applicable NESCOR\(^1\) failure scenarios
  - DER.5 Trojan Horse Attack Captures Confidential DER Generation Information
    - Vulnerability: System permits installation of malware in the supply chain for the DER system
  - DER.13 Custom Malware Gives Threat Agent Control of FDEMS\(^2\)
    - Vulnerabilities
      - Physical access may be obtained by unauthorized individuals to embedded equipment in the supply chain, installation organization or maintenance organization,
      - System relies on credentials that are easy to obtain for access to install software on the FDEMS platform

\(^1\)National Electric Sector Cybersecurity Organization Resource
\(^2\)FDEMS: Field Distributed Energy Resources Energy Management System
Applicable NESCOR Failure Scenarios

- DGM.8 Supply Chain Vulnerabilities Used to Compromise DGM Equipment
  - Vulnerability: System permits unauthorized changes to software/firmware at suppliers of equipment, maintenance, and transportation

- Generic.4 Supply Chain Attacks Weaken Trust in Equipment
  - Vulnerability: System permits unauthorized changes in the supply chain.
Discussion

Annabelle Lee
ablee@nevermoresecurity.com
www.NevermoreSecurity.com
240.204.3258