Blockchain Based OT Monitoring Solution (BBOTMS)
Who are we?

Asif Hameed Khan (@stix2taxii)
- OT/ICS Cybersecurity
- Cyber Threat Intelligence (CTI)
- Digital Forensics and Incident Response (DFIR)
- Platform - OTISP (OT Threat Information Sharing Platform)

Gagandeep Singh Jattana (@gaganjattana)
- IoT Penetration Testing
- Hardware Security Testing
- Firmware Analysis
Introduction to Operational Technology (OT)

- Industrial Control Systems (ICS) is a general term for hardware and software working together to achieve Industrial objectives.
- Supervisory Control and Data Acquisition (SCADA) is a monitoring of the functioning of ICS. Operations are controlled offsite/remotely.
- While DCS are functionally very similar, DCS is generally employed at large, continuous processing facilities. Operations are controlled onsite rather than remotely.
- Operation Technology (OT) refers to the computing systems used to manage the whole Industrial operations.

Source: https://www.securicon.com/whats-the-difference-between-ot-ics-scada-and-dcs/
Introduction to Operational Technology (OT)

- Purdue Enterprise Reference Architecture (PERA)
- Developed by Purdue University
- Conceptual architecture
- Good source to start
- Basis of all well known ICS Architectures available

Source: [https://www.sans.org/reading-room/whitepapers/ICS/paper/36327](https://www.sans.org/reading-room/whitepapers/ICS/paper/36327)
Why OT Security?

• Industry 4.0 and Industry 5.0
• Commercial Off The Shelf (COTS) Products
• Integration of IoT in OT → IIoT
• Enterprise and Process Control Network Connectivity
• Cyber breach in OT environment may have permanent impact (i.e Environmental, Human loss etc)

Source- https://twitter.com/zaidlearn/status/981083540631699461
Common Myths

• We have a Firewall and IDS Deployed
• We are Air-Gapped
• We have SIS and Safety Devices Deployed
• Why Hacker will Target Us?
• We are not connected to business network
• IT Security vs OT Security (IT>OT)

Note: OT Security > IT Security

Source- https://media.kaspersky.com/pdf/DataSheet_KESB_5Myths-ICSS_Eng_WEB.pdf
OT Monitoring Solutions

• Referred as OT SOC (Security Operation Centre)
• Passive and Active Mode of Monitoring
• 24x7 Continuous Monitoring of OT Assets
• OT SOC → Enterprise SIEM → SOAR
• Many Vendors in the Market

Source: https://www.gartner.com/reviews/market/operational-technology-security
OT Monitoring Solutions

Source: https://www.nozominetworks.com/blog/nozomi-networks-scales-globally-to-deliver-advanced-ics-cybersecurity/
Challenges in OT Monitoring Solution Deployment

Challenges:

• Separate/Parallel Network Deployment for OT <-> IT Connectivity.

• Increase in Connectivity between Process Control Network and Business Network → Threat Vector

• Third Party Vendor Connectivity to OT SOC and Enterprise SOC.

• Access Control/Accountability and Authorization → IAM, PIM and PAM

Source- https://www.nozominetworks.com/blog/overcoming-it-ot-cybersecurity-convergence-roadblocks/
What is Blockchain?

- Database of blocks with hash linking between the nodes
- Similar to chain of link list except of pointers we have Hash connectivity
- First blocks contains the configuration for the whole database known as Genesis Block

Source: https://www.tutorialspoint.com/blockchain/blockchain_proof_of_work.htm
Blockchain Concepts

• Decentralization → No Single Point of Failure and High Availability
• Transparency → No Man in The Middle (MiTM)
• Immutability → Database can not be tampered and deleted once created

Source- https://blockgeeks.com/guides/what-is-blockchain-technology/
Blockchain Use Cases

- Bitcoin and Decentralized Currency
- Governance
- Identity and Access Management (IAM)
- Asset Tracking
- Data Management
- Internet of Things (IoT)
- Digital Forensics
- Cyber Threat Intelligence (CTI)
- Decentralized Applications

Applicability of Blockchain in OT Monitoring

- Decentralized Network and Applications
- Immutable Database
- No Tampering
- Consensus
- Privacy
- Act as an Intermediate network between IT and OT.

Proposed Work - BBOTMS

Benefits

• Decentralized OT SOC
• Access Control/Accountability and Authorization
• Robust Cyber Threat Intelligence (CTI) Database
• Secure Connectivity to the Enterprise/Business Networks
• Robust Network Forensics

Challenges

• All Challenges associated with the Blockchain Technology
Why Not Hashgraph?

Benefits over Blockchain
- 50,000 Times Faster Speed
- Equal level field
- Provable or Verifiable
- Secure by Byzantine
- Cheap and 100% Efficient

Limitations
- Patented Technology
- Not Easily Available
- Integration Issues

Source: [https://www.hedera.com/](https://www.hedera.com/)

<table>
<thead>
<tr>
<th>Generation</th>
<th>Transactions per Second</th>
<th>Average Fee</th>
<th>Transaction Confirmation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st</td>
<td>3+ TPS</td>
<td>$0.20 USD²</td>
<td>10-60 minutes</td>
</tr>
<tr>
<td>2nd</td>
<td>12+ TPS</td>
<td>$0.13 USD³</td>
<td>10-20 seconds</td>
</tr>
<tr>
<td>3rd</td>
<td>10,000+ TPS¹</td>
<td>$0.00001 USD</td>
<td>3-5 seconds (w/ finality)</td>
</tr>
</tbody>
</table>
Thank You!