Detecting threats in multi-party computation systems

You work for an organization that uses multi-party computation systems. Blockchain infrastructure incorporates a diverse set of technologies, across a distributed network, which means it faces some unique challenges. Some of the most significant infrastructure threats include denial-of-service (DoS), key theft, network partitioning, consensus manipulation, and blockchain integrity attacks. You need to be able to consistently detect and handle these threats.

Required data

You can analyze Hyperledger Fabric’s data with the following tools:

- Splunk Connect for Hyperledger Fabric. This add-on ingests ledger and metric data from a Hyperledger Fabric deployment. The Splunk Docker logging driver can be used to send container logs to Splunk.
- Splunk App for Hyperledger Fabric. This app facilitates the analysis of this data in Splunk.

How to use Splunk software for this use case

Your organization can use Hyperledger Fabric as a way to collaborate without compromising on safety and integrity. The Security Monitoring dashboard in the app provides access to a high level view of several threat indicators:

- Indicators of DoS include trends in transaction latency and throughput, unique senders, and open gRPC connections.
- Orphaned blocks may indicate attacks on blockchain integrity.
- Indicators of consensus manipulation include configuration updates and consensus leader changes.

You can expand on the searches in any of these dashboards yourself, using events captured from data utilized by blockchain environments, including node logs or ledger data, and Prometheus/StatsD Hyperledger Fabric metrics. This data can be separated into on-chain and off-chain data.

- On-chain data consists of the ledger data, which is persistent and resistant to tampering from network-wide replication.
- Off-chain data is often ephemeral and may not be widely distributed. Examples of off-chain data include the state database, network traffic, as well as node metrics and logs.

<table>
<thead>
<tr>
<th>Threat</th>
<th>Indicators</th>
<th>Data Sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denial-of-service</td>
<td>Tx throughput &amp; latency</td>
<td>Block headers</td>
</tr>
<tr>
<td></td>
<td>Block latency</td>
<td>Node metrics</td>
</tr>
<tr>
<td>Threat</td>
<td>Indicators</td>
<td>Data Sources</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Consensus manipulation</td>
<td>Number of Senders</td>
<td>Blocks</td>
</tr>
<tr>
<td></td>
<td>Number of Open connections</td>
<td>Node logs</td>
</tr>
<tr>
<td>Ledger manipulation</td>
<td>Changes in chain configuration</td>
<td>Block headers</td>
</tr>
<tr>
<td></td>
<td>Leadership Elections</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Orphaned blocks</td>
<td></td>
</tr>
</tbody>
</table>

**Example: Denial-of-service attack**

In this scenario, an authorized user has their keys compromised and begins spamming the network with transactions.

In a normal situation where a single client sends 10 transactions per second, your dashboard might look like the following image. Note the transaction latency, throughput, and number of open connections.

![Image of normal situation dashboard](image1.png)

In this example DoS attack, a single client opens persistent 1000 connections, each performing 1 query per minute. The transaction latency starts to increase, transactions per second decreases, and the number of open connections increases. At this point, it may be difficult to determine if this change is because of a high period of load, misconfiguration, or a denial of service attack.

![Image of DoS attack dashboard](image2.png)

You can investigate further in the Infrastructure Health and Monitoring Dashboard, where you can see connection and I/
O timeout errors.

Because you have noticed a large number of open connections, you should query Splunk to see the distribution of gRPC message subjects and addresses.

```
index=hyperledger_logs "line.grpc.method"!=" |
| stats count BY line.grpc.peer_subject |
| rename line.grpc.peer_subject AS Subject, count AS Count
```

When you perform this search you may see a large discrepancy in message count. In this example, the screenshot below shows that "User1@buttercup.example.com,L=San Francisco,ST=California,C=US" is likely compromised or misconfigured and should be investigated further.

---

**Next steps**

The content in this guide comes from a previously published blog, one of the thousands of Splunk resources available to help users succeed. In addition, these Splunk resources might help you understand and implement this use case:

- Blog: [Introducing Splunk App for Hyperledger Fabric](#)
- GitHub: [Splunk Connect for Hyperledger Fabric](#)