Adding Network Fuzzing Capabilities to Hyperledger Umbra

<table>
<thead>
<tr>
<th>Title</th>
<th>Adding network fuzzing capabilities to Hyperledger Umbra</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>APPLICATION REVIEW</td>
</tr>
<tr>
<td>Difficulty</td>
<td>HIGH</td>
</tr>
</tbody>
</table>

Description

Hyperledger Umbra is a Hyperledger Lab designed to run unmodified versions of our DLT platforms (e.g. Hyperledger Fabric, Hyperledger Iroha) under a simulated environment with software defined networking for the purposes of running experiments (e.g. scaling experiments, consensus algorithm development, etc) and security audits. Currently Hyperledger Umbra can run unmodified Hyperledger Fabric Docker images and execute a full Fabric network under simulation. Umbra is written in Python and has code for doing virtual network switches and connections. This project is to extend that code to allow for network fuzzing capabilities. The goal is to be able to introduce packet drops, packet delay, packet reordering, as well as unsolicited packets with random/known-bad data. The purpose it be able to test Hyperledger Fabric's resilience to general network "weather" and intentional attacks coming from the network.

Additional Information

This project is going to be fairly difficult and will require somebody with skills in Python programming, networking, and Docker.

Learning Objectives

- First and foremost the mentee will learn how to be a positive collaborator and contributor in an active open source project.
- Learn how to work within the Hyperledger open source ecosystem and culture.
- Apply computer science skills to understand the software architecture and networking fuzzing approach to security scanning.
- Gain a better understanding of distributed network applications and how to test them.

Expected Outcome

- Hyperledger Umbra gains the capability to manipulate packet transit and the injection of packets either as part of the configuration setup or as an external API that 3rd party tools call call into. If an API is to be created an SDK and demonstration application is to be created that shows how to use the API through the SDK.
- A presentation on the use of this new capability to run network fuzzing operations against Fabric.

Relation to Hyperledger

This project directly affects the Hyperledger Umbra lab as well as Hyperledger Fabric and any other Hyperledger DLT that Umbra may support in the future. This will give us a solid network fuzzing capability that can be used in future security audits of our DLT projects.

Education Level

The ideal mentee is a university student or a developer with one or two years of experience with a solid background in Python and computer networking.

Skills

- Python programming
- Computer networking knowledge (e.g. switches, IP addresses, broadcast addresses, routing, etc)
- Experience with Docker

Future plans

This project will further enhance our ability to run effective security audits against Hyperledger Fabric and our other DLT platforms.
Preferred Hours and Length of Internship

Full-time or part-time.

Mentor(s) Names and Contact Info

David Huseby, dhuseby@linuxfoundation.org, dhuseby on chat.hyperledger.org