**Abstract**

Veracity is a secure virtual coordinate system proposed by Micah Sherr, Matt Blaze, and Boon Thau Loo. The following enhancements were made for better security, modularity, and efficiency before open-sourcing.

**Security**

Nonces - When sending a message that expects a reply, “numbers used once” (nonces) are used. This prevents replay attacks.

What is D’s coordinate?, 0xDEADBEEF

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1, 2, 3)</td>
<td>(9001, 9001, 9001)</td>
</tr>
</tbody>
</table>

Latency = Distance(C, A)

Calculated Locally

(D’s coordinate is at (1, 2, 3), 0xDEADBEEF)

(D’s coordinate is at (9001, 9001, 9001), null)

HMACs - During latency measurement, HMACs are sent along with timestamps. This prevents man-in-the-middle (MITM) attacks.

(9:01 P.M., 0x0001CAFEx)

(9:01 P.M., 0x0001CAFEx, 9:02 P.M.)

0x0001CAFEx = HMAC(9:01 P.M., skey)

(9001 years ago, 0x1337BEEF, 9:02 P.M.)

0x1337BEEF != HMAC(9001 years ago, skey)

**Source Code Enhancements**

Modularity - Most of Veracity was in one file. It is now organized by the sections in the original paper for clarity.

- Event Handler
- RSet Check
- VSet Check

Documentation - All sections of the source code are now commented for readability.

Original Veracity Paper

Original Vivaldi Paper