1. Introduction

- Disputes between Web service and users:
  (a) Chargeback fraud
  (b) False invoices
  (c) Silent updates of terms and conditions
  (d) Repudiating the execution of malicious programs

- To resolve these disputes, "non-repudiate" proof is vital.

- We propose a logger named LogNEWT, which stores non-repudiable evidence and is transparent to the Web.

3. Related Works

There have been some works to generate non-repudiable evidence, but they have disadvantages, as shown in the table below.

Table 1. Comparison with related works

<table>
<thead>
<tr>
<th></th>
<th>Secure Payment Confirmation API</th>
<th>Signing Extensions</th>
<th>PGP</th>
<th>TTP Website</th>
<th>Sunb et al.</th>
<th>Lib-SEAL</th>
<th>LogNEWT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transparency</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>○</td>
</tr>
<tr>
<td>Anti-logger-bypassing</td>
<td>-</td>
<td>○</td>
<td>-</td>
<td>○</td>
<td>×</td>
<td>△</td>
<td>○</td>
</tr>
<tr>
<td>Secure registration / authentication</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>-</td>
<td>△</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Root of Trust</td>
<td>TTP</td>
<td>TTP</td>
<td>TTP</td>
<td>TTP BC TEE</td>
<td>TEE &amp; TEE</td>
<td>TEE</td>
<td>TEE</td>
</tr>
</tbody>
</table>

TTP: Trusted Third Party, TEE: Trusted Execution Environment, BC: Blockchain

5. Challenges

LogNEWT is based on LibSEAL[6]. However, LibSEAL has disadvantages in security; these are:

1. Vulnerable to logger-bypassing by 3rd-party origin requests
2. Undefined user registration process and non-transparent authentication
3. Attestation of LibSEAL installation is not transparent.

4. Building Block: LibSEAL

LibSEAL[6] is a TLS library that logs requests and responses securely. TEE protects the runtime and generated logs in LibSEAL.

4.1. Users can verify that TSL is terminated by LibSEAL

4.2. LibSEAL provides user registration & authentication API within TEE.

4.3. Users can easily verify the installation of LogNEWT by seeing the service's domain name.

6. Solution

1. Record all requests, including 3rd-party origins, by rewriting their URL.

2. Provide user registration & authentication API within TEE.

3. Users can easily verify the installation of LogNEWT by seeing the service's domain name.

7. Future Work

We will implement LogNEWT and evaluate the security and scalability of LogNEWT.