Non-repudiable Secure Logging System for the Web

Authors: Kosei Akama (B4)*†, Seiki Makino (M1)*†, Masaaki Sato‡, Keisuke Uehara†
Affiliations: †Keio University, ‡Tokai University, Japan
*: Both authors contributed equally to this research.

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.**

2. System & Threat Model

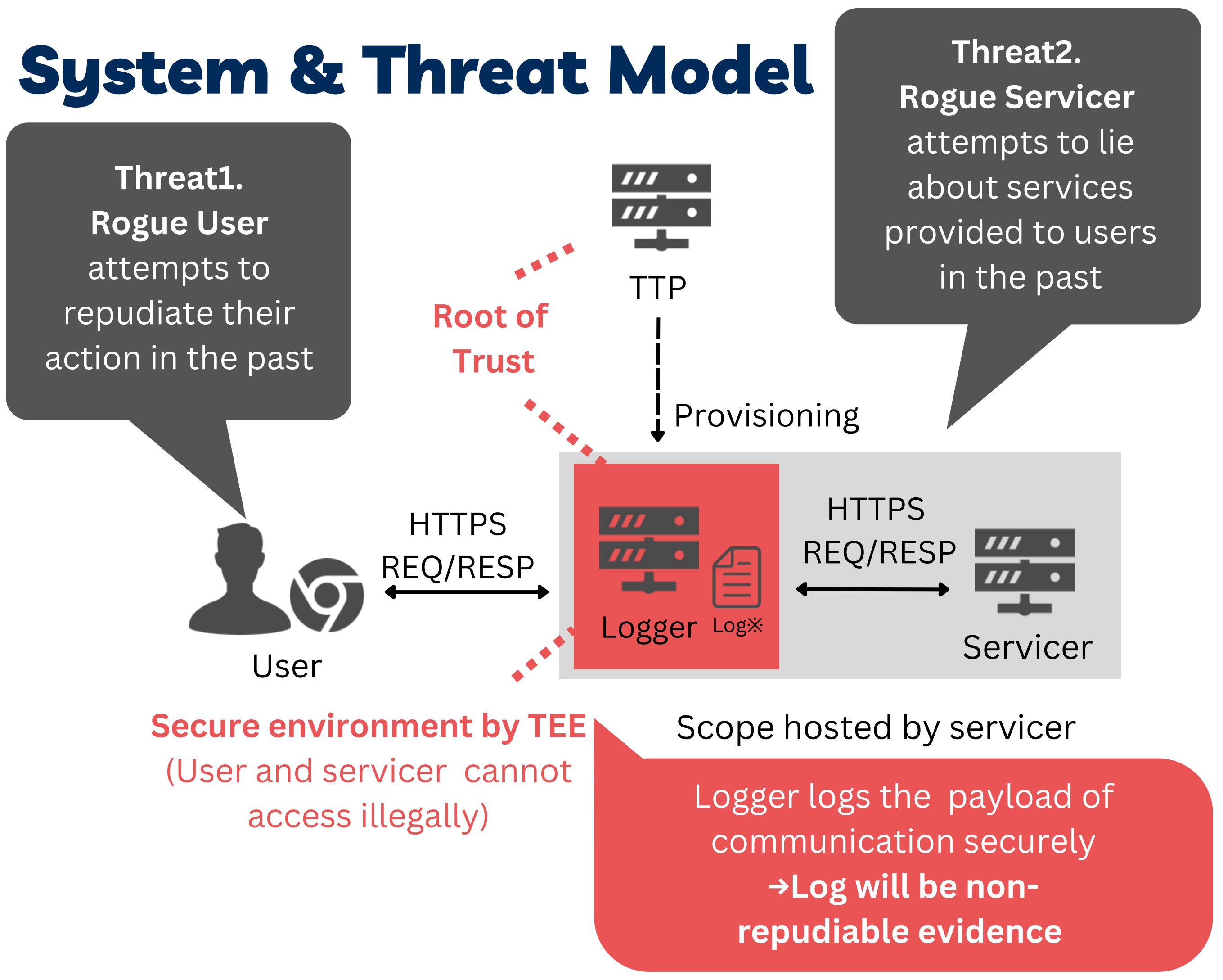

Threat1. Rogue User attempts to repudiate their action in the past
Threat2. Rogue Servicer attempts to lie about services provided to users in the past
TTP
Root of Trust
Provisioning
HTTPS REQ/RESP
User
Logger
Log※
HTTPS REQ/RESP
Servicer
Secure environment by TEE (User and servicer cannot access illegally)
Scope hosted by servicer
Logger logs the payload of communication securely →Log will be non-repudiable evidence

Fig1 . Overview of LogNEWT

Fig1. shows the system and threat of LogNEWT.

Security requirements in LogNEWT are

Non-repudiability and Unforgeability.

Rogue entities can almost not repudiate the honest entity's claims and fake the claims valid.

Otherwise, it can prove which entity caused the fraud.

Non-security goal. Transparency: LogNEWT does not need significant changes in users' and servicers' operations or environments is our non-security goal, and the user's environment is unchanged in particular.
*malware and phishing are out of the scope of this research.

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

	Secure Pay-ment Con-firmation API[1]	Signging Browser Extensions[2]	PGP[3]	TTP Website[4]	Sutton et. al.[5]	Lib-SEAL[6]	LogNEWT
Transparency	○	×	×	×	△	○	○
Anti-logger-bypassing	-	○	-	○	×	△	○
Secure registration / authentication	△	○	○	○	-	△	○
Root of Trust	TTP	TTP	TTP	TTP	BC	TEE	**TEE & TTP**

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

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.

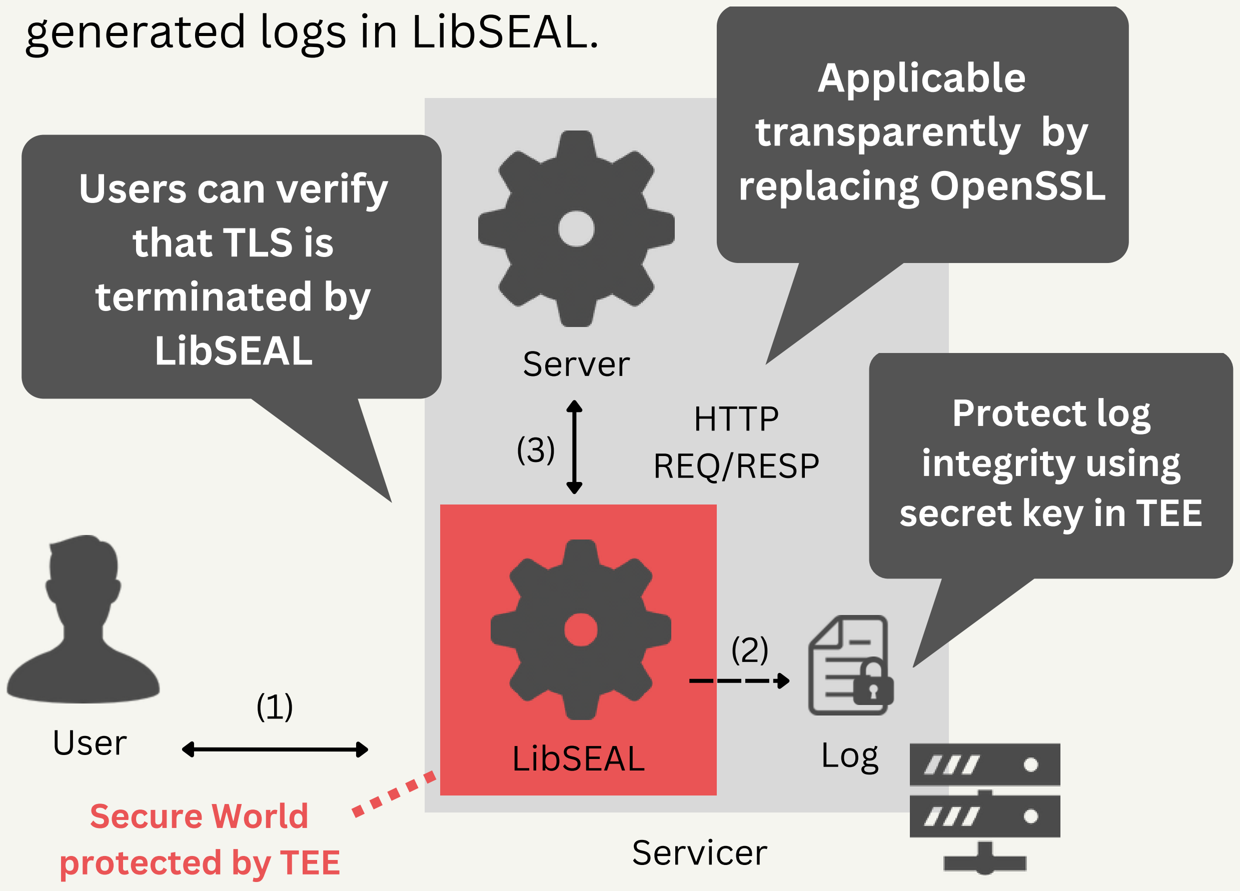

Users can verify that TLS is terminated by LibSEAL
Applicable transparently by replacing OpenSSL
Protect log integrity using secret key in TEE
Server
(3)
HTTP REQ/RESP
User
(1)
LibSEAL
(2)
Log
Secure World protected by TEE
Servicer

Fig2 . Overview of LibSEAL

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.

6. Solution

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

```
<script src="https://cdn.example">
→ "https://service.newt/..."
```

Fig3. Rewriting URL

(2) Provide user registration & authentication API within TEE.

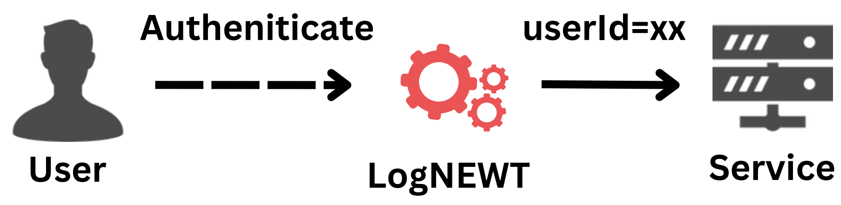
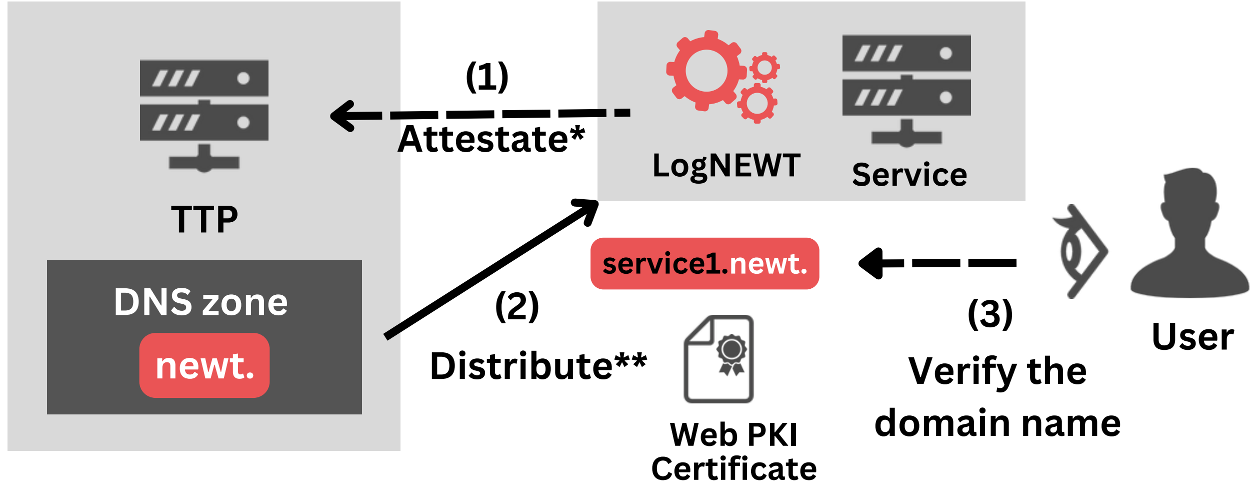


Fig4. Identification and Authencation

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



*: LogNEWT installation can be verified using Remote Attestation feature of TEE.

**: Domain's integrity is guaranteed by DNSSEC, while Certiifcate Transparency forbids rogue CAs.

Fig5. Attestation of LibSEAL

7. Future Work

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

[1] [online] Secure Payment Confirmation. (Accessed on 03/10/2023). https://www.w3.org/TR/secure-payment-confirmation/.
[2] [online] Install and manage extensions - Chrome Web Store Help. https://support.google.com/chrome_webstore/answer/2664769.
[3] P. Wouters, Ed., Aiven,D. Huigens, Proton AG, J. Winter, Sequoia-PGP, Y. Niibe, FSIJ. draft-ietf-openpgp-crypto-refresh-07. https://datatracker.ietf.org/doc/html/draft-ietf-openpgp-crypto-refresh.
[4] [online] DocuSign | #1 in Electronic Signature and Agreement Cloud. (Accessed on 04/08/2023). https://www.docusign.com/.
[5] A. Sutton and R. Samavi. 2017. Blockchain enabled privacy audit logs. In The Semantic Web–ISWC 2017, Proceedings, pp. 645–660.
[6] Pierre-Louis Aublin et al. 2018. Libseal: revealing service integrity violations using trusted execution. In Proceedings of the Thirteenth EuroSys Conference, 1–15.