Workgroup:
Transfer dIGital cREdentialS Securely
Internet-Draft:
draft-lassey-tigress-threat-model-02
Published: 5 June 2023
Intended Status: Informational
Expires: 7 December 2023

Authors: B. Lassey, Google; C. Astiz, Apple; D. Vinokurov, Apple; Y. Karandikar, Apple

TIGRESS Threat Model

Abstract

This document describes a threat model by which the working group can evaluate potential solutions to the problems laid out in the TIGRESS charter.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://bslassey.github.io/tigress-threat-model/draft-lassey-tigress-threat-model.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-lassey-tigress-threat-model/.

Discussion of this document takes place on the Transfer dIGital cREdentialS Securely Working Group mailing list (mailto:tigress@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/tigress/. Subscribe at https://www.ietf.org/mailman/listinfo/tigress/.

Source for this draft and an issue tracker can be found at https://github.com/bslassey/tigress-threat-model.

Status of This Memo

This Internet-Draft will expire on 7 December 2023.

Copyright Notice

Table of Contents

1. Introduction

The TIGRESS Working Group is chartered to deliver a protocol for transferring copies of digital credentials. The charter specifies certain goals:

1.1. Privacy goals:

- The intermediate server should not see sensitive details of the Provisioning Information [Tigress-req-03]

- The intermediate server should not be able to provision the credential itself, acting as an intermediary for the recipient (person-in-the-middle, impersonation attack)

- Aside from network-level metadata, the intermediate server should not learn information about the sender or receiver

1.2. Security goals:

- Allow for ensuring that only the intended recipient is able to provision the credential

- Allow for ensuring that the credential can only be provisioned once (anti-replay)

- Allow for ensuring that the sender has the intent to transfer (proof of the fact that the initiation of the credential transfer is attributed to a valid device and a user)

1.3. Functional goals:

- Allow a sender to initiate a credential transfer and select an intermediary server

- Allow a recipient to view the transfer request with Provisioning Information [Tigress-req-03], and provision the credential information associated with it upon receipt

- Allow a sender and a recipient to perform multiple round trip communications within a limited time frame

- Not require that both the sender and recipient have connectivity to the intermediary server at the same time

- Support opaque message content based on the credential type

- *Support a variety of types of credentials, to include those adhering to public standards (e.g., Car Connectivity Consortium) and proprietary (i.e., non-public or closed community) formats

From these goals we can derive a threat model for the general problem space.

2. Threat Model

2.1. Assets and Data

2.1.1. Credential

A digital credential [Tigress-req-03] is composed of Cryptographic material and other data that enables an user to access a property.

2.1.2. Intermediary data

Data that is exchanged over the course of credential transfer.

2.1.3. Credential transfer invitation

The initial data containing Provisioning Information [Tigress-req-03] sent to the receiver. It represents an invitation to accept the transfer of the credential.

3. Users

3.1. Sender

The user who initiates the credential transfer.

3.2. Receiver

The user who is the intended recipient and accepts the invitation with the transferred credential.

3.3. Credential Authority

The Provisioning Entity [Tigress-req-03] that manages the lifecycle of a credential on a device.

4. Attackers and Motivations

5. Threats and mitigations

Threat Description	Likelihood	Impact	Mitigations
An Attacker with physical access to the victim's phone initiates	MED	HIGH	Section 5.2.1

Threat Description	Likelihood	Impact	Mitigations
the transfer of a Credential to the the Attacker's device			
Attacker intercepts or eavesdrops on sharing message	HIGH	HIGH	Section 5.2.2
Sender mistakenly sends to the wrong Receiver	HIGH	HIGH	Section 5.2.3
Sender device compromised	MED	HIGH	Section 5.2.3
Attacker compromises Credential Authority	LOW	HIGH	None
Credential Authority can recognize and track Sender across shares	HIGH	LOW	None
Credential Authority can recognize and track Receiver across shares	HIGH	LOW	None
Sender can recognize and track Receiver across shares	HIGH	LOW	None
Receiver can recognize and track Sender across shares	HIGH	LOW	None

Table 1

5.1. If an intermediary server is used

Some designs may rely on an intermediary server to facilitate the transfer of material. Below are threats and mitigations assuming that there is an intermediary server hosting encrypted content at an "unguessable" location.

Threat Description	Likelihood	Impact	Mitigations
Attacker brute forces "unguessable" location	LOW	LOW	Section 5.2.4
Attacker intercepts encryption key	MED	MED	Section 5.2.5
Attacker intercepts encryption key and unguessable location	MED	HIGH	Section 5.2.6
Attacker compromises intermediary server	LOW	LOW	Section 5.2.7
Attacker uses intermediary server to store unrelated items (i.e. cat pictures)	HIGH	LOW	Section 5.2.8

Table 2

5.2. Mitigations.

5.2.1. User authentication at the time of transfer initiation

Implementers **SHOULD** take sufficient precautions to ensure that the device owner is in possession of the device when initiating a transfer such as requiring authentication at the time of initiation.

5.2.2. Secret to be sent securely

Solution should require an end-to-end encrypted messaging channel or otherwise specify a way to send a secret out of band.

5.2.3. Transfer control

Implementers should ensure any initiated attempts of credential transfer can be withdrawn or revoked at any time.

5.2.4. Limited time-to-live for mailbox storage

Limited TTL of storage, rate limiting of requests.

5.2.5. Separation of shareURL and secret

Separate transmission of encryption key and unguessable location.

5.2.6. Group transfer warning

Implementor should warn users about transferring credentials to groups.

5.2.7. Encrypted mailbox content

Content on the server is encrypted.

5.2.8. Mailbox size limit and TTL

Intermediary server should have tight size limits and TTLS to discourage misuse

6. Conventions and Definitions

The key words "**MUST**", "**MUST NOT**", "**REQUIRED**", "**SHALL**", "**SHALL NOT**", "**SHOULD**", "**SHOULD NOT**", "**RECOMMENDED**", "**NOT RECOMMENDED**", "**MAY**", and "**OPTIONAL**" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

7. IANA Considerations

This document has no IANA actions.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/

RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

8.2. Informative References

[Tigress-req-03] Vinokurov, D., Pelletier, A., Astiz, C., Lassey, B., and Y. Karandikar, "Tigress requirements", April 2023, <https://github.com/dimmyvi/tigress-requirements/>.

Acknowledgments

This document took as inspiration the threat model that was part of Dmitry Vinokurov's sample implementation document.

Authors' Addresses

Brad Lassey
Google

Email: lassey@google.com

Casey Astiz
Apple

Email: castiz@apple.com

Dmitry Vinokurov
Apple

Email: dvinokurov@apple.com

Yogesh Karandikar
Apple

Email: ykarandikar@apple.com