Secure Systems Group, Aalto University

Fajar Malik, Tuomas Aura

Securing User Progression from Short-Lived Stateless to Persistent Stateful Container

(Work in progress)

Introduction

- **Stateless** containers are often short-lived, run for a short time and then destroyed. These containers do not have any side effects, and **no data is lost when they are destroyed**.
- A short-lived stateless container can considered a **function** that has no side effects. The function is given **input**, **processes** it, and then returns a **result**, without a user interface and without any persistent storage.
- In **educational** context, these container can be used to process students' **submission**, to **evaluate** it. An example is Aalto University's **Aplus** platform.

Problem

- Since the containers are short-lived and stateless, they **cannot** have long-lasting features, such as a **user interface** and **persistent storage** to **save user progress**.
- We can have a separate container that is stateful and long-lived, so that it can display a user interface and **save the user's work** to a persistent storage.
- How can we **securely** take the user from the short-lived and stateless container to the persistent and stateful container?
- How can we return the **results**, such as an evaluation, to the original system and **match** them to the **same user**?

Security Properties

- **Authentication**: only users authenticated in Aplus can access the persistent stateful container.
- **Integrity**: the signature ensures integrity of the payload sent from Aplus to the external container.
- **Pseudonymity**: the persistent stateful container does not know user ID in Aplus, since it is given a randomly generated user number. In the event of a data leak, no information can be tied to any user in Aplus.
- **User matching**: the user receiving the result is the same as the user completing the task, since PRG_{Aplus} is deterministic.

Solution

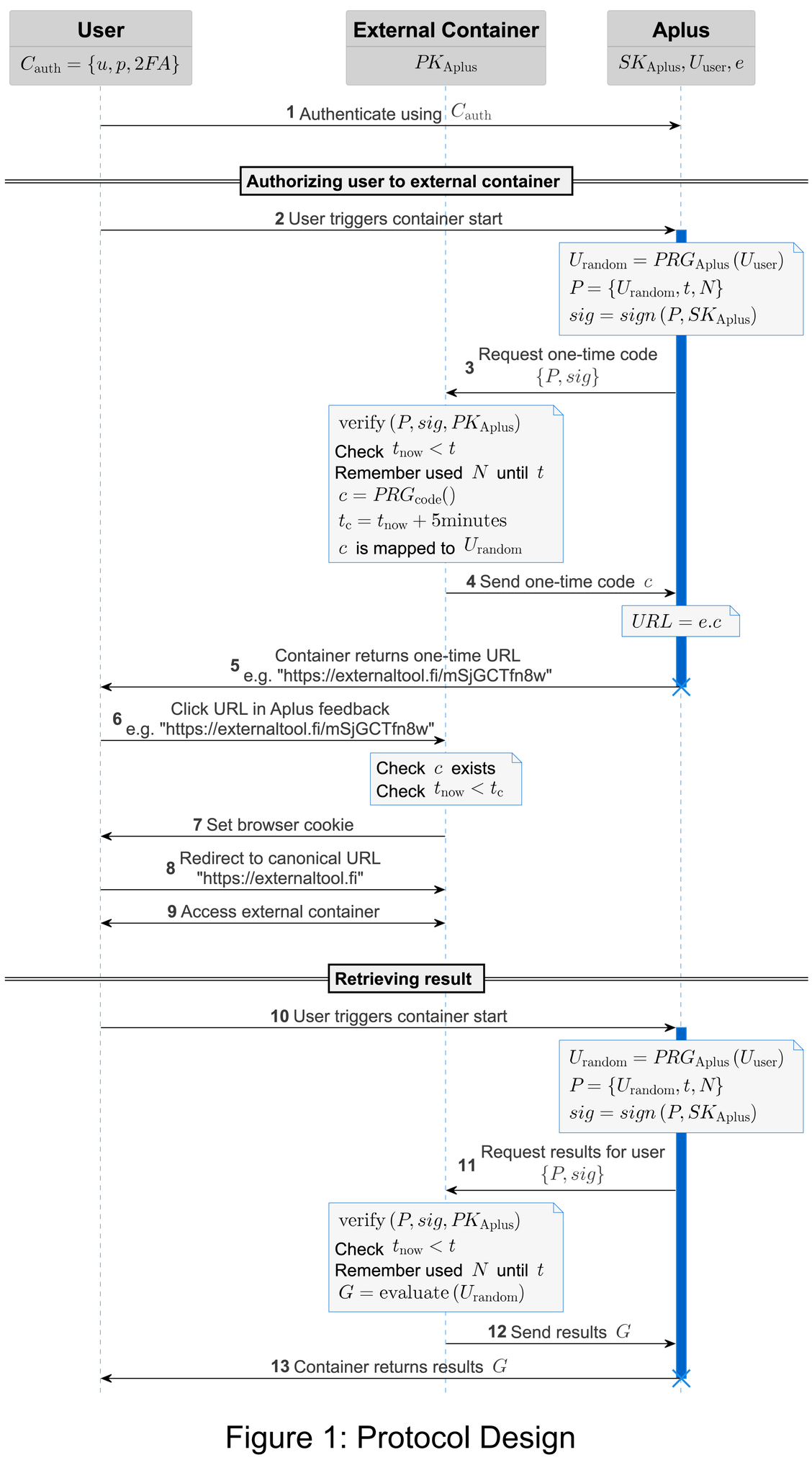

Figure 1: Protocol Design

Security analysis

- Security analysis in **ongoing work** in this thesis project.

Aalto University

Contact: {fajar.malik, tuomas.aura}@aalto.fi