Revisiting user registration and authentication

The boring stuff that bite you as you grow

Vassilis Poursalidis

Principal Software Engineer

@ Epignosis

The company behind TalentLMS

@poursal

Summary

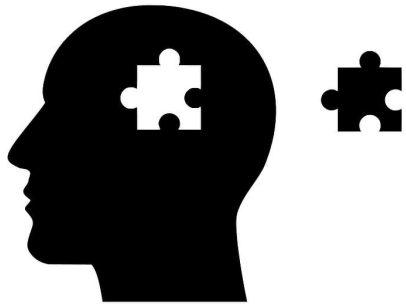
We will dig deeper into the following:

- Proof of Work
- Zero-Knowledge Password Proof

That can help us with:

- User registration (and rate limiting in general)
- User authentication

And enhance the robustness of our solutions.



How it starts

You have a **great idea** and you want to cut corners on the boring stuff. So you **choose an approach** on how users register and authenticate on your portal.

➔ **Rate limiting**
Count and limit the total number of registration.

➔ **CAPTCHA**
To prevent automated bots from registering.

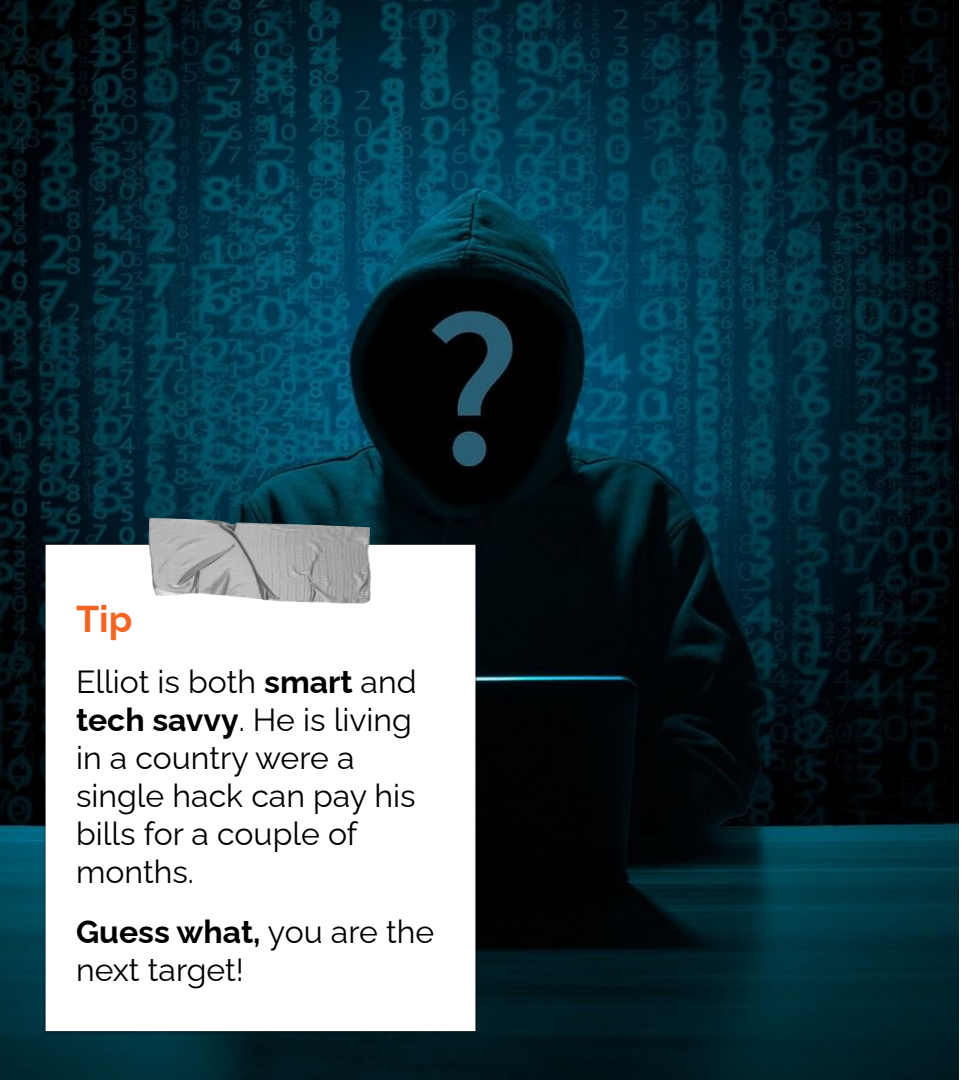
➔ **Nothing (!)**
Too early; I can get away with it for now.

But you have done your homework and you know that you must store hashed and salted passwords in your DB!

Warning !!!

You have done well, but not your **best.**

Your customers must still **send their passwords** to your application in order to authenticate.



Tip

Elliot is both **smart** and **tech savvy**. He is living in a country were a single hack can pay his bills for a couple of months.

Guess what, you are the next target!

Meet Elliot.

On the hunt for quick wins:

- register multiple accounts,
- hack into legitimate accounts,
- active attacks on the infrastructure.

Now meet our defences

Proof of Work

- Require work to fend off attackers
- Increase/decrease work based on risk

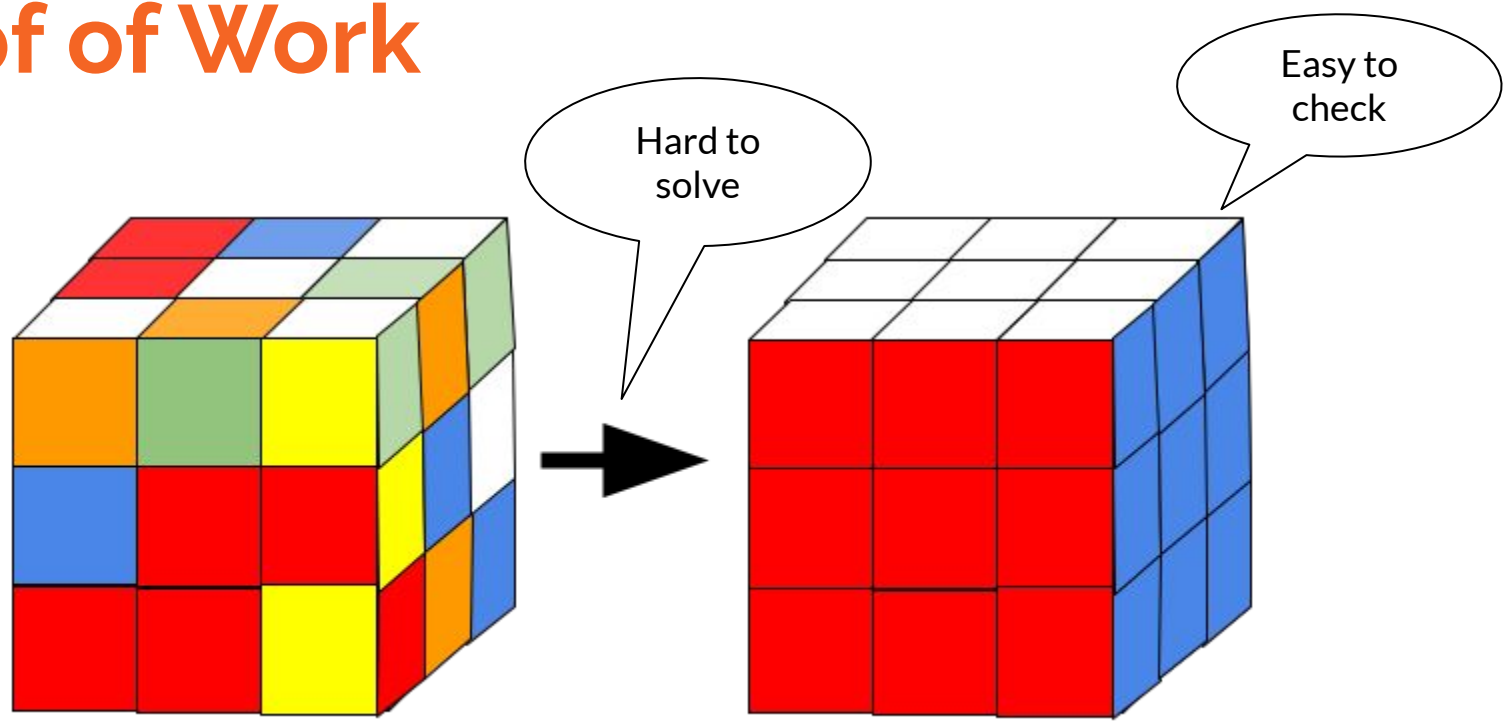
ZKPP

- Never see the user password
- Establish session keys as a bi-product

Transforming rate limiting

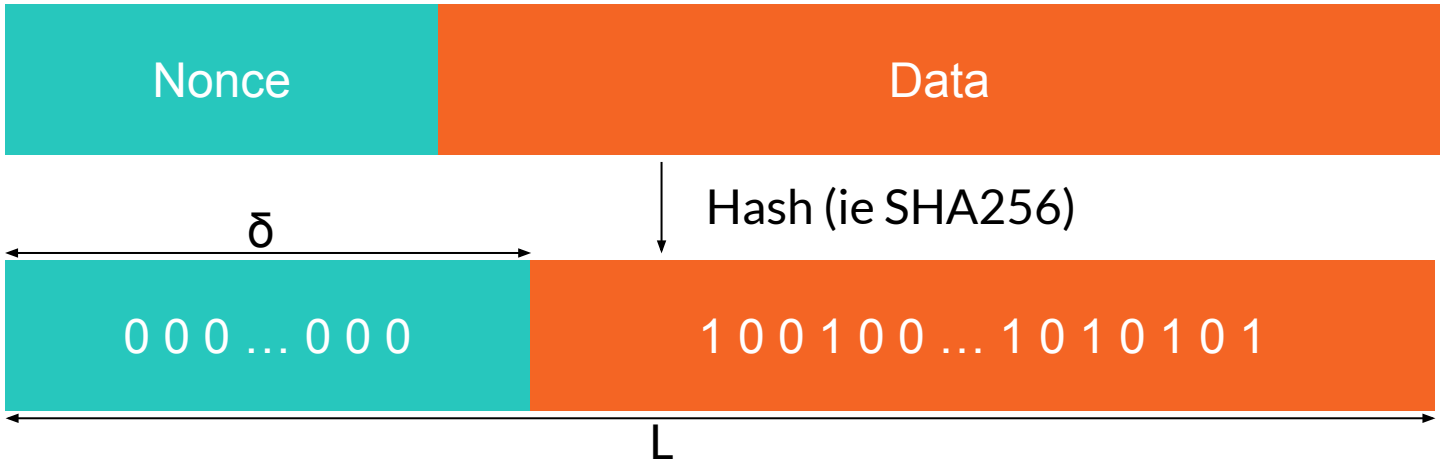
Using Proof of Work for user registration (and beyond)

Proof of Work

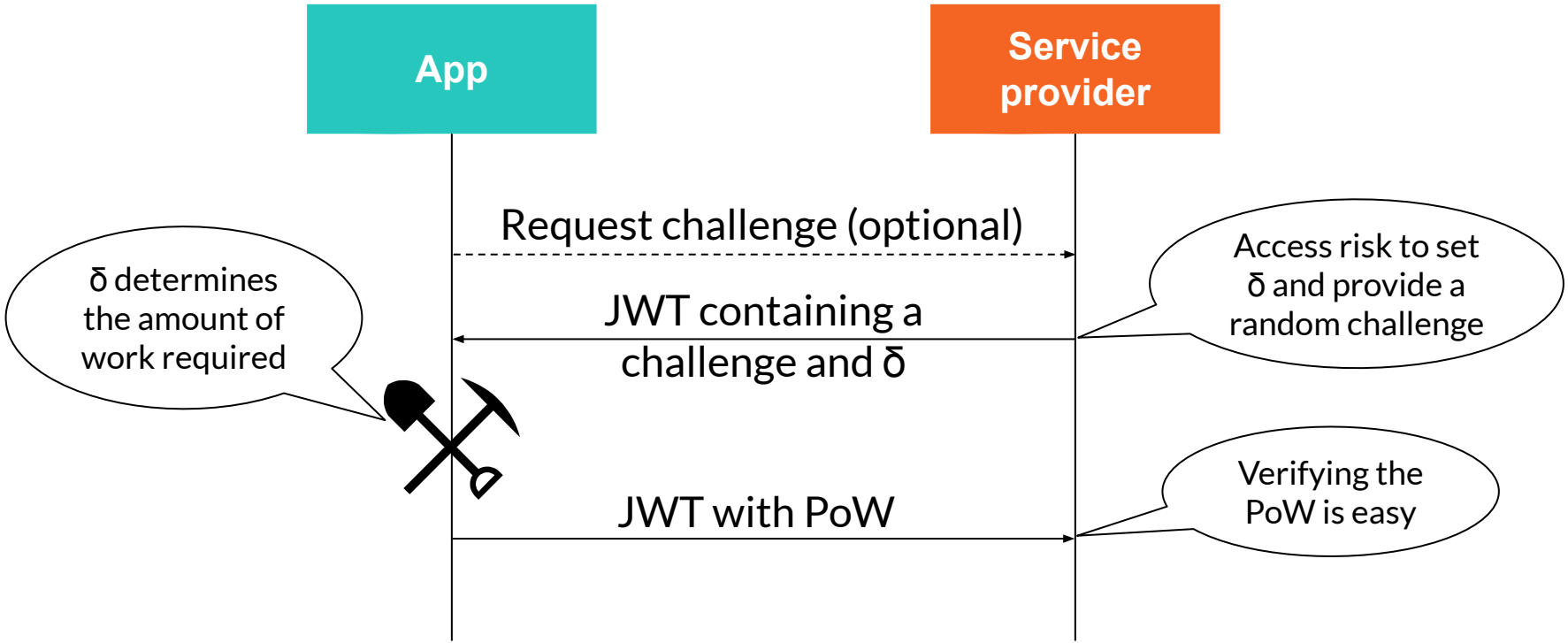


Hashcash

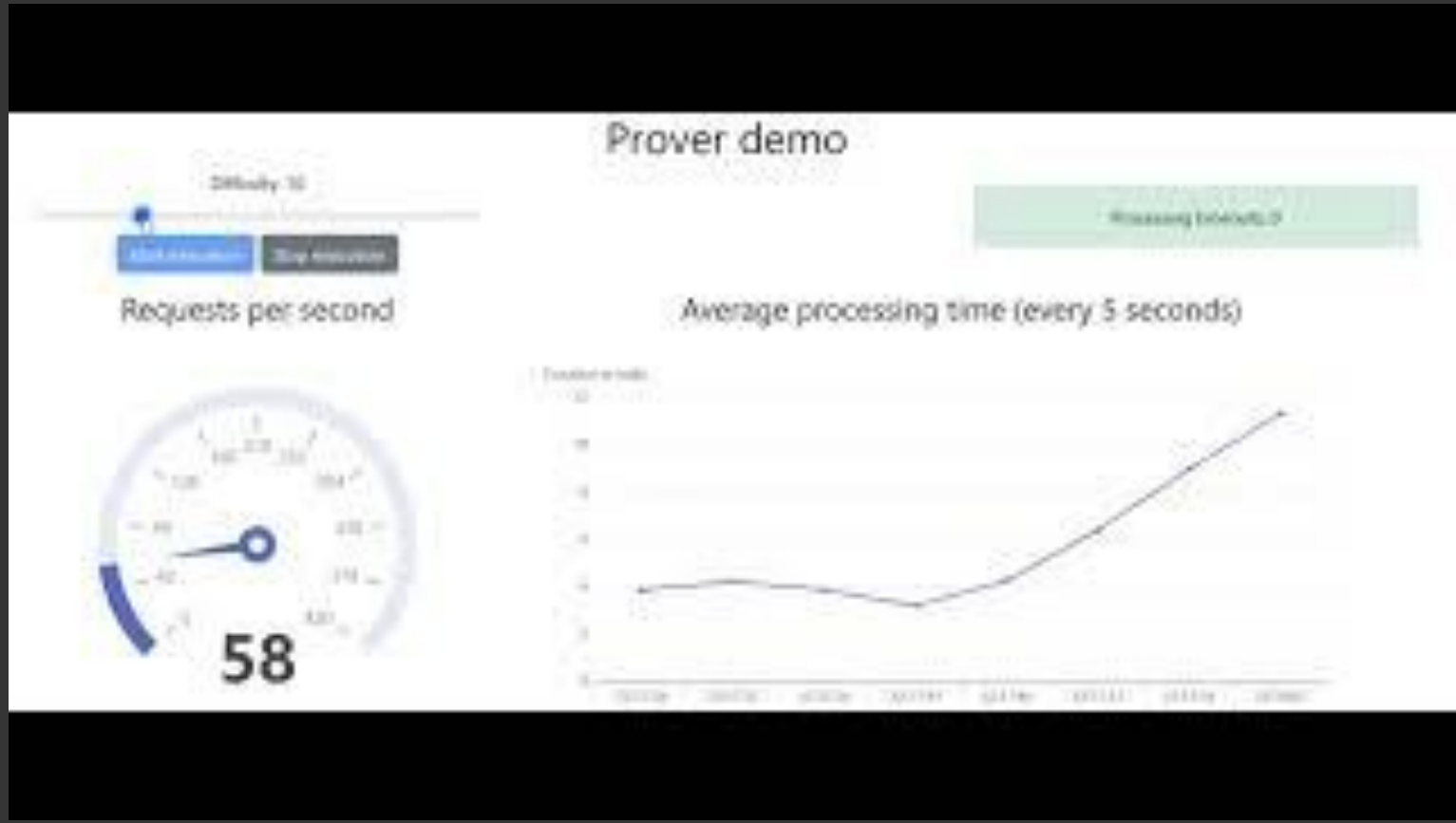
- A version of PoW introduced in 2002
- Used extensively in cryptocurrencies, but being phased out due to environmental concerns



Prover protocol



Time for a demo

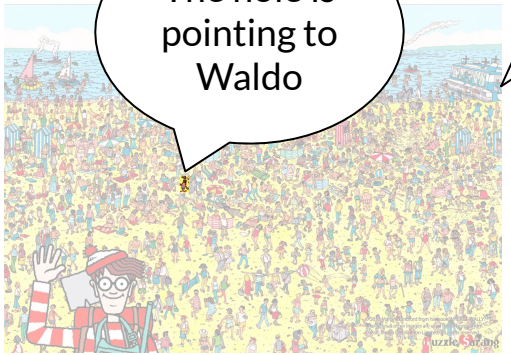


Transforming credentials

Using ZKPP for user authentication (and beyond)

Zero-Knowledge Password Proof

Large board with a small hole

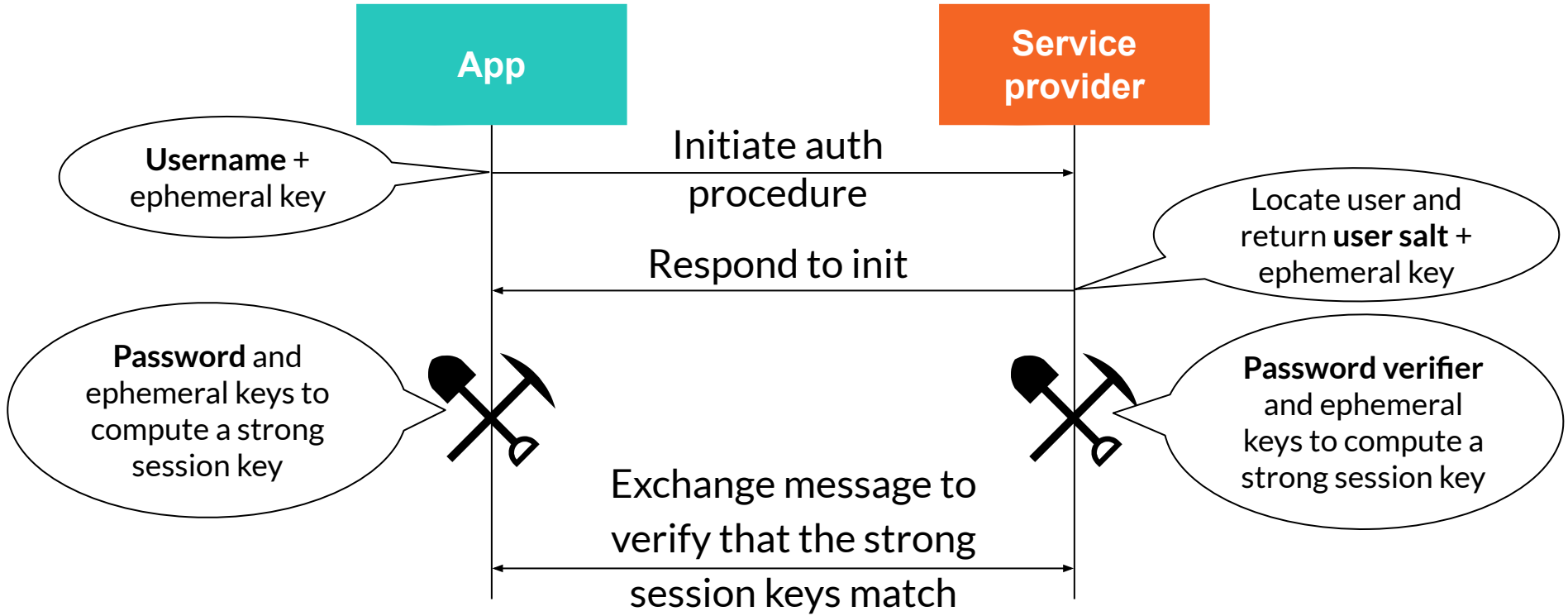


The hole is pointing to Waldo

The poster is randomly positioned behind the board

SRP6a

During user registration the SP stores the **user's salt** and **password verifier**



Thank you!

Questions anyone?