PASSWORDLESS AUTHENTICATION IN A QUANTUM FUTURE

Daniel Gardham
Nick Frymann
Mark Manulis
Franziskus Kiefer
Emil Lundberg
Dain Nilsson

Passwords suffer from a range of human-factor problems, such as:

- password reuse
- password sharing
- low complexity

To mitigate this, more secure techniques that rely on cryptographic keys stored in authenticators are becoming more prolific, based on the WebAuthn standard.

These keys can be generated and stored in many ways:

- Biometrics: Many phones can now be accessed using your thumb print!
- Facial Recognition: FaceID is also a common way of securing your phone or laptop.
- Hardware Tokens: Small devices (e.g. USB drive) that contain secret keying material.

However, these technologies are plagued by challenges, reducing adoption and ultimately leaving users at risk.

GOAL

Secure, easy-to-use and future-proof authentication for the web.

PROBLEM 1: Weak Recovery Methods

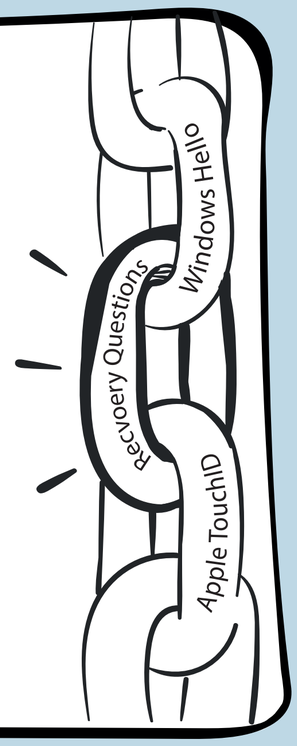
Loss or damage of phones, laptops, or any personal device is a part of every day life, so how do we keep access to our online accounts, such as email, social media or banks?

Online services use recovery methods to reset accounts that are often easily guessable, we say they have low entropy.

A system is only as secure as its weakest link.

This means that attackers can ignore the strong authenticator, and attack the weaker recovery method directly. This removes the security guarantees of the cryptographic authenticator.

Is the name of your first pet really that secret?



SOLUTION 1: Backup Authenticators

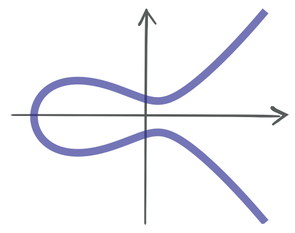
We developed a cryptographic primitive that allows for additional devices to used as back up authenticators. This means that account recovery methods are cryptographically secure; there is no weak link!

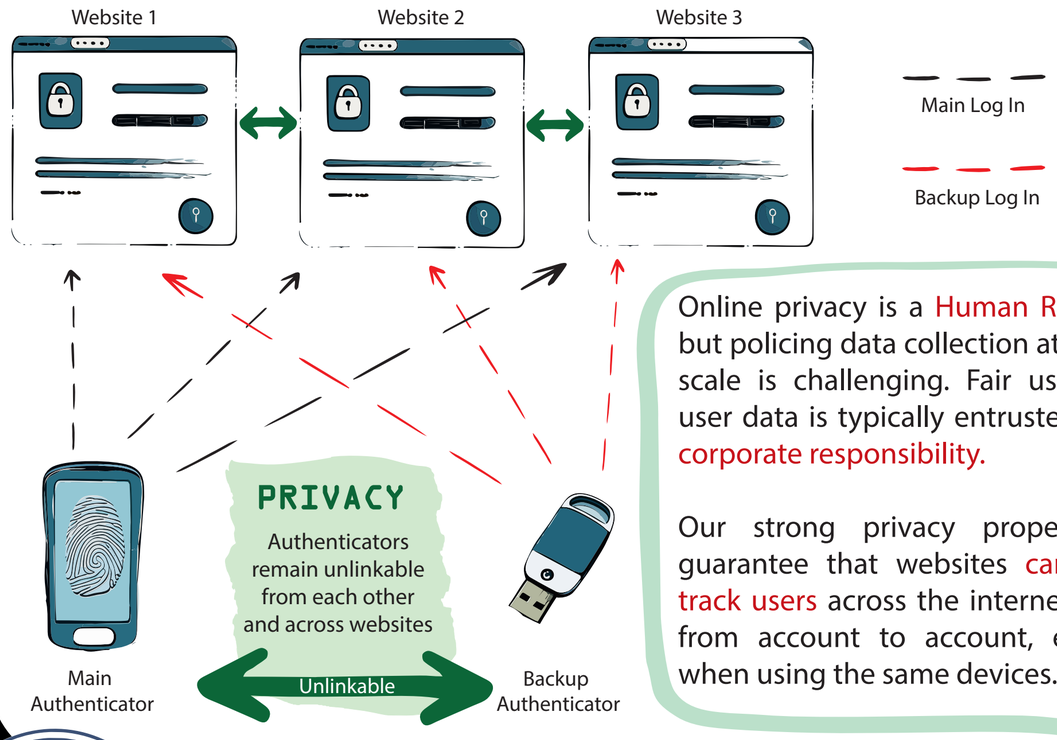
The asynchronous nature of our protocol means that the back up authenticator is not involved with the registration process. This means you can keep it locked away safely, only retrieving it when invoking the account recovery process.

We use elliptic curves to build our primitive, we mathematically prove that it would take 650 million years to break.

Elliptic curves are sets of points that solve the equation:

$$y^2 = x^3 + ax + b$$





Online privacy is a Human Right, but policing data collection at this scale is challenging. Fair use of user data is typically entrusted to corporate responsibility.

Our strong privacy properties guarantee that websites cannot track users across the internet, or from account to account, even when using the same devices.

PROBLEM 2: Password Sharing

Vulnerable people can struggle with technology, and rely on help from others to use online services.

This is typically done by sharing passwords.

This is insecure and cannot be audited, to prevent misuse.

SOLUTION 2: Account Delegation

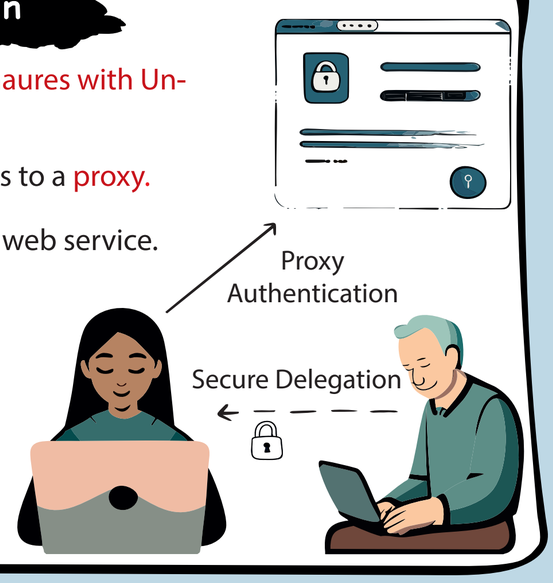
We have created a new protocol called Proxy Signaures with Unlinkable Warrants.

It allows users to securely delegate account access to a proxy.

Proxy does not need to have an account with the web service.

Our design uses cryptographic techniques from our back up authenticator.

Privacy is still a fundemental property. Services cannot trace proxies.



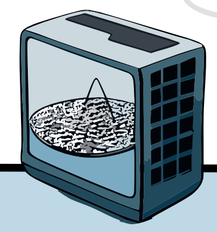
PROBLEM 3: Quantum Computers

Quantum computers bring a new threat to the cryptography that underpins today's technology, using Shor's algorithm discovered in 1994.

They are able to break the underlying mathematics, extracting secrets that were thought to be safe.

Experts cannot say when the first large-scale quantum computer to credibly threaten modern cryptography will exist, but postulate it is likely within the next 5 to 50 years.

Cryptography in use today is susceptible to these attacks.



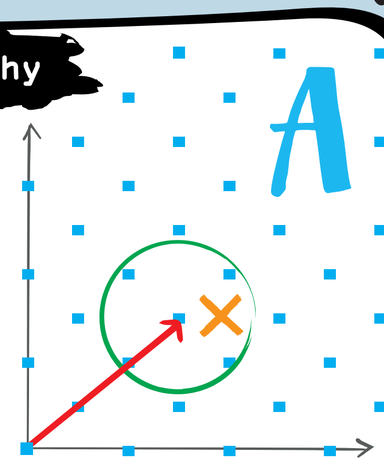
SOLUTION 3: Post-Quantum Cryptography

New mathematical techniques enable design of cryptography which resist quantum attacks!

We rebuilt our backup authenicator and account delegation protocol from polynomial lattices, based on the Learning with Errors (LWE) problem.

This requires new mathematical definitions and concepts to prove our protocols are quantum secure.

The noise added to this equation makes it hard for even quantum computers to find x!



LWE problem:
Given A and y, find x.

$$Ax + e = y$$

Public Key
Public Lattice
Secret Key
Small Gaussian Noise

daniel.gardham@surrey.ac.uk
https://sccs.pages.surrey.ac.uk/passwordless-auth

Surrey Centre for Cyber Security SCCS
UNIVERSITY OF SURREY
CRYSPEN
yubico