2FA, But Better

By Zane Globus-O'Harra
and Doug Ure

Downsides of existing 2FA methods

PIN-2FA:

- PINs must be short enough for people to manually enter.
- Could be read by a nearby attacker (shoulder surfing)

PUSH-2FA:

- Requires a secure channel with trusted push-service providers.
- Vulnerable to careless user approvals

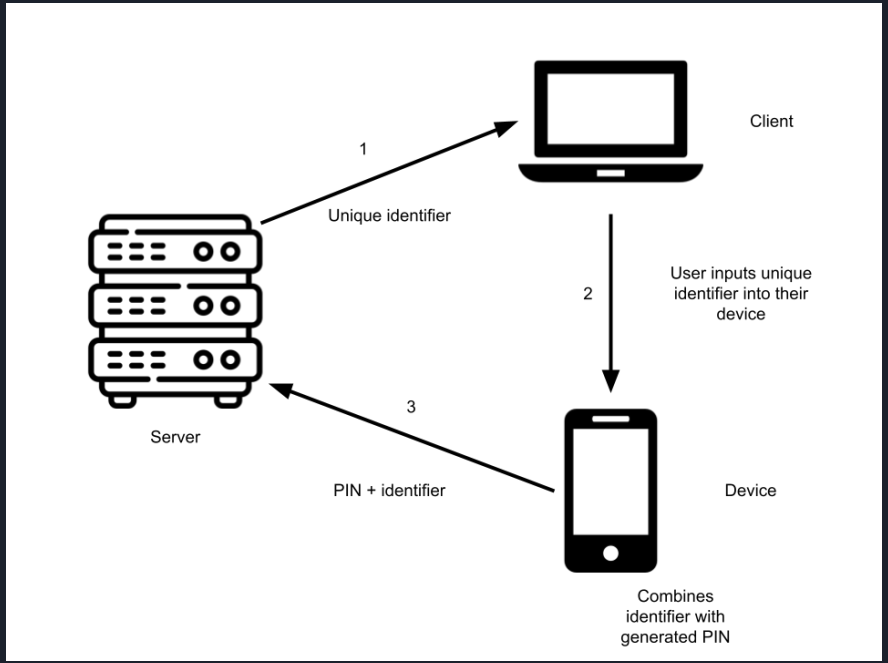
2D-2FA

Server sends a unique identifier to the client.

User inputs the identifier into their device.

The device combines the identifier with a PIN generated by the device (using time and a secret key).

The encoded combination is sent to the server; if correct, the client is approved.



Additional Security

“Typing-Proof”: the user’s device records them typing a code into the client. The server then compares the timing of both!