ReCRED — Result In Brief

Project ID: 653417
Funded under: H2020-EU.3.7.
Country: Greece
Domain: Digital Economy

No more password mayhem

Anybody who uses online accounts knows how chaotic it can be to store and remember the location of a load of usernames and passwords. EU-funded researchers unveiled a new mobile authentication platform that connects all online accounts with the user's identity, putting the smartphone in charge.

Most mobile devices are linked with hundreds of accounts and applications, with all sorts of security settings, identities and passwords. The EU-funded project ReCRED produced advanced software solutions to address this so-called password overload issue, so that the user can safely access its accounts without having to remember multiple passwords.

Only one password to memorise

ReCRED moves beyond the password era by providing advanced and flexible architecture. "Embracing the device-centric authentication architecture is key to removing passwords as the main method of authentication on the web," notes project coordinator Christos Xenakis.

This scheme improves the end-user internet security by using the mobile as an authorisation proxy. Authentication and authorisation mandates the combined use of a short pin, biometric information and anonymous credentials.

User identity and account management

The majority of internet users are registered to many online services such as email providers, social media, e-banking, or corporate applications. This makes the task of proving joint-ownership of services hard.

ReCRED offers secure access to these services and account management from a single device, regardless of the applied authentication method of each service. The Online Identity Acquisition module is responsible for horizontally binding the fragmented online user identities. The service enables the user to give explicit authorisation to ReCRED to access the information of each online account that he maintains.

Researchers also implemented the 'Physical Identity Acquisition' module for services requiring higher attribute assurance level. This service verifies all the identity attributes included in the user's physical identity.

With all these services, ReCRED is improving identity assurance and tightens the binding amongst physical and online identities. "End users are now able to prove ownership of different accounts from different identity providers, link them together and consolidate their identity attributes," states project coordinator Xenakis.

Privacy-enhancing technology

A typical scenario that exposes the whole identity realm of users relates to some services that require end users to sign in to be given access.

Implementing attribute-based access control (ABAC) – dubbed the next-generation authorisation model – seems to be one of the best solutions to data-centric security. ReCRED combined ABAC with multifactor authentication schemes, granting a higher level of security and privacy. "User characteristics or attributes such as age, nationality or occupation comprise a unique identity that can provide authorisation privileges on accessing data, resources or services," outlines project coordinator Xenakis. As he further explains, "ABAC allows end users to be authenticated by providing only the necessary attributes that the service is requesting. Anonymous credentials provide access to services without requiring from the user to validate his email and thus reveal his entire identity."

Doubling up on security

The device becoming the main authentication gateway does not come without its security issues. It can either become a single point of failure in case of loss or damage or be vulnerable to hijacking after the user authentication.

ReCRED skirted these issues by building additional security layers with locking and recovery capabilities. In particular, researchers leveraged an entity called Identity Consolidator (IDC) along with behavioural and physiological user signatures and secure-SIM protocols to verify the user identity. The IDC enables identity consolidation and management, while also allows efficient failure recovery. "In case a user loses his device, his can recover access to services by providing two-factor authentication such as personal attributes mapped from physical characteristics or behavioural biometrics," notes project coordinator Xenakis.

Removing the need to employ separate passwords will ultimately make internet-based services more user-friendly while being secure. Besides end users, other beneficiaries of this brand new open platform will be telecom operators, web-hosting companies, and mobile device manufacturers.

Keywords

ReCRED, authentication, account, mobile device, user identity, attribute-based access control (ABAC), anonymous credentials, biometrics, device-centric authentication, two-factor authentication **Last updated on** 2018-08-13

Retrieved on 2018-11-05

Permalink : https://cordis.europa.eu/result/rcn/238602_en.html