ReCRED

From Real-world Identities to Privacy-preserving and Attribute-based CREDentials for Device-centric Access Control

Makes your digital life **safe** and definitely **easy**!

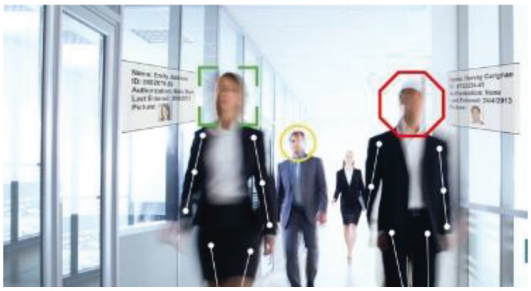
www.recred.eu

European Commission | Horizon 2020 European Union funding for Research & Innovation

Killing Passwords: Strong Authentication Beyond the Password Era

With e-commerce now exceeding 1 trillion € per annum and the emergence of Internet of Things, the need for reliable and user-friendly authentication mechanisms is more pressing than ever. Currently, user authentication relies on passwords, a technology developed in the '60s. Due to their simplicity and straightforwardness, passwords continue to remain the principle method of authentication, with over 98% of the websites using it without offering other ways of authentication. However, apart from being extremely popular, this method remains highly insecure, since users have the tendency to choose weak passwords, easy-to-remember and, therefore, easy-to-guess. Additionally, the security requirements of critical services, such as e-banking, far exceed those satisfied by ordinary passwords, which can be easily stolen or bypassed. Finally, according to several studies, 70% of users forget their password once a month and tend to try on average 2.4 passwords before they type the right one to connect to the service of their choice.

The issues described above created the need for new authentication mechanisms, of higher standards, that will leverage the potential of existing technologies and achieve the right balance between security and usability. Towards this direction, researchers are currently working to find alternative authentication methods to replace passwords, where user's identity will be verified using biometric characteristics, such as fingerprint, iris and face recognition, rather than a combination of username/password. The adoption of these new authentication methods is directly linked to the rapid increase of smartphone penetration, as they are equipped with high-end sensors, like fingerprint readers, that are widely used on mobiles for authentication and access control.



Recent developments in biometric authentication are also focusing on behavioral characteristics. The way we walk, move around the city, how we talk or type can identify us effectively enough to be used as authentication means. An example of behavioral biometric authentication is the Project Abacus of Google, which aims to eliminate passwords from Android OS and replace them with the way users interact with their devices. Project Abacus created a method where a set of metrics compose trust scores for device unlock and graded access to applications, based on their criticality. The project is currently under development by Google.

At the same time, a European research project is also under development, entitled **"ReCRED: From Real-world Identities to Privacy-preserving and Attribute-based CREDentials for Device-centric Access Control"**. The project is funded by the Horizon H2020 Framework Programme of the European Union and it is being carried out by 12 organizations in total,

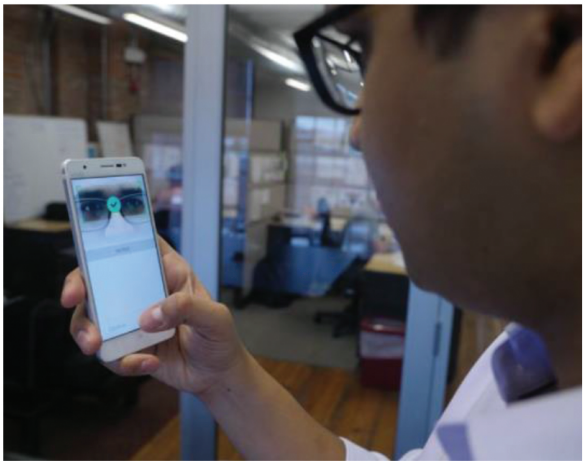
universities and companies working in unison from 8 European countries: University of Piraeus, Cyprus University of Technology, Telefonica, Verizon, CNIT, Universidad Carlos III de Madrid - IMDEA, UPCOM, EXUS, WEDIA, certSIGN, The Productizers, and Baker & McKenzie. ReCRED's goals are very similar to Abacus'. However, they differentiate in the way users' biometric identities are being collected, processed and stored. While Project Abacus exclusively depends on Google platforms and Google has total control over all the collected data, ReCRED was designed and implemented as an open platform for user authentication, where only the results of the authentication process are being collected rather than the biometric identities of the users.

Some of ReCRED's advantages are:

a) it was specifically designed following a privacy-by-design approach in order to protect users' personal data and to comply with the European privacy legal framework;

b) it provides a modular and flexible architecture, which can be deployed and used by any service provider; and

c) it gives the opportunity to organizations with registered subscribers to offer new type of services that are related to user identification, authentication and management.



ReCRED moves the burden of authentication from the user to the device itself, taking full advantage of smartphones' inherent capabilities. Smartphones evolve into authentication proxies, where every user account can be securely kept and managed on the device, following the most contemporary technological standards that leverage the benefits of asymmetric cryptography (e.g., FIDO Alliance). Users can be authenticated by their mobile devices, locally, using fingerprint, face recognition, how they walk, type, move around the city, etc., while the device in collaboration with the ReCRED platform provide access to the subscribed services (e.g. e-banking accounts, social media accounts, etc.). In case of device loss or theft, all user's personal data are securely encrypted in the device, using a new and promising technology called Trusted Execution Environment, which operates at both hardware and software level.

Apart from turning smartphones into authentication and authorization proxies towards the digital world, ReCRED also offers two additional innovations:

a) the consolidation and management of online user identities and accounts, and

b) the issuance of anonymous credentials that verify specific attributes or properties of the users, while guaranteeing the latters' anonymity.

Regarding the first, the majority of today's Internet users are registered to many online services, such as email providers (e.g. Gmail, Yahoo), social media (e.g. Facebook, Twitter,

LinkedIn), e-banking, corporate applications, etc. ReCRED can offer secure access to all the aforementioned services, as well as account management from a single device, regardless of the applied authentication method of each service. The ReCRED platform offers great flexibility and ease of use, without compromising users' security and privacy. Users are also able to tie their online identities with their real-world identity, in order to make electronic transactions on platforms such as eBay.

Anonymous credentials, on the other hand, offered by ReCRED, are in position to verify users' attributes (e.g., sex, age, student, etc.), without revealing any other personal data. Anonymous credentials are being issued by trusted authorities, which possess such data (e.g. e-government services, telecommunication providers, banking institutions, ReCRED platform, etc.), and are submitted encrypted by the users to online services using their mobile devices, proving attributes that could grant them benefits, such as discounts or access to specific resources. In this way, users can be securely authenticated, while at the same time maintaining their privacy.

The project is expected to be completed in April 2018, but ReCRED's first large-scale pilots will take place during summer 2017.

For more info, visit www.recred.eu or contact Prof. Xenakis at xenakis@unipi.gr.


ReCRED


ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS


EXUS


institute
imdea
networks


cnit


Cyprus
University of
Technology


Telefónica
Telefónica I+D


THE
PRODUCTIZERS


certSIGN


wedia


verizon


upcom
Bringing business and IT together


Baker
McKenzie.