PRESS RELEASE
NOTA DE PRENSA

05 NOVEMBER 2018, MADRID

Publication date: 02 October 2018, Madrid

No more messing around with passwords

Network security based on data, not passwords

Source(s): IMDEA Networks Institute

Who doesn't have web accounts and faces a daily challenge of having to save and remember a plethora of usernames and passwords? An international team of researchers has unveiled a new secure authentication platform for mobile devices that links all of a user's online accounts to their identity, leaving their management to be handled by their cell phone.

Most mobile devices are linked to hundreds of accounts and applications, which imply all kinds of security settings, identities and passwords. The ReCRED project, funded by the European Union, has developed advanced software solutions to address the problem of password overload, enabling us to securely access our accounts without having to remember multiple passwords.

A single password to memorize

ReCRED leaves the era of passwords behind by developing an advanced, secure and flexible access system. "The adoption of authentication architecture based on the device is key to the elimination of passwords as the main method of authentication on the web," says project coordinator, Christos Xenakis of the University of Piraeus (Greece).

This method improves end-user security on the internet by using the cell phone as an authorization intermediary or proxy. "Authentication and authorization are simplified by the combined use of a short pin, biometric information (for example, voice, fingerprints or signature) and anonymous credentials (for example, a pseudonym)," says Rubén Cuevas, researcher at the University Carlos III of Madrid (UC3M), one of the entities that have contributed to the project.

User identity and account administration

Most Internet users are registered with many online services, such as email providers, social networks, electronic banking or corporate applications. This complicates the task of identifying a shared services domain associated to a single user.

ReCRED provides secure access to these services as well as making it possible to manage accounts from a single device, regardless of the authentication method used on each service. The online identity acquisition module that has been developed horizontally links the identities of the user that are fragmented across the web. The service allows the user to grant explicit authorization to ReCRED to access the information of each online account he owns.

Researchers have also created a physical identity acquisition module for those services that require a higher level of attribute guarantee. This service verifies all identity attributes included in the user's physical identity, such as their passport number or identity document, bank account number or photo.

With all these services ReCRED improves the guarantee of identity and reinforces the link between physical and virtual identities. "End users can now confirm that they own different accounts from different identity providers, link them together and consolidate their identity attributes," says Christos Xenakis.

Security based on data, not passwords

A common assumption that exemplifies everything connected to the management of the identity of users in the network is related to the diversity of services that require end users to log in for access.

Given this general assumption, ReCRED is committed to data-based security. Researchers have achieved that unique user characteristics such as age, nationality or occupation can be used to access data, resources or services. "We prioritize an authentication that requires using only essential data that act as anonymous credentials. It is not necessary to verify the e-mail address, for example, since it would reveal the identity of the user", explains Antonio Fernández Anta, researcher at IMDEA Networks Institute and UC3M collaborator in ReCRED.

Doubling security by strengthening the mobile device

The device that becomes the main authentication gateway has its own security challenges. This can become a single point of failure in case of loss or damage, or be vulnerable to being hacked after user authentication.

ReCRED (*From Real-world Identities to Privacy-preserving and Attribute-based CREDentials for Device-centric Access Control, H2020 Grant Agreement* 653417) has avoided these problems by creating additional security measures with blocking and recovery capabilities. In particular, researchers have taken advantage of an entity called Identity Consolidator (IDC) as well as the user's behavioral and physiological signatures and security protocols based on SIM cards to verify the identity of the user. The IDC allows for the consolidation and management of identities, whilst enabling efficient recovery in the event of failures. "In the event that a user loses their device, they can regain access to services by providing two-factor authentication, such as personal attributes scanned from physical characteristics or biometric behavioral data", Xenakis says.

Eliminating the need to use different passwords will make internet-based services safer and easier to use. In addition to the end users, other beneficiaries of this new open platform will be telecommunications operators, web hosting companies and manufacturers of mobile devices.

###

Traducción al español:
/noticias/2018/se-acabaron-lios-contrasenas
Original source:
/news/2018/more-messing-around-passwords

About Us

IMDEA Networks Institute is a **research organization on computer and communication networks** whose multinational team is engaged in cutting-edge fundamental science and technology. As a growing, English-speaking institute located in Madrid, Spain, IMDEA Networks offers a unique opportunity for pioneering scientists to develop their ideas. IMDEA Networks has established itself internationally at the forefront in the **development of future network principles and technologies.** Our **team** of highly-reputed researchers is designing and creating today the networks of tomorrow.

Read more on www.networks.imdea.org.

Some keywords that define us: *5G, Big Data, blockchains and distributed ledgers, cloud computing, content-delivery networks, data analytics, energy-efficient networks, fog and edge computing, indoor positioning, Internet of Things (IoT), machine learning, millimeter-wave communication, mobile computing, network economics, network measurements, network security, networked systems, network protocols and algorithms, network virtualization (software defined networks – SDN and network function virtualization – NFV), privacy, social networks, underwater networks, vehicular networks, wireless networks and more...*

IMDEA Networks Institute
Avda. del Mar Mediterráneo, 22
28918 Leganes (Madrid) Spain
@IMDEA_Networks | Linkedin | Facebook

Telephone: +34 91 481 6210
E-mail: mediarelations.networks@imdea.org
Web: www.networks.imdea.org