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


## Addressing the problems with passwords: the ReCRED's approach for device-centric access control

Christoforos Ntantogian
Department of Digital Systems
University of Piraeus Research Center

European Commission
Horizon 2020
European Union funding
for Research & Innovation

Co-funded by the Horizon H2020 Framework Programme of the European Union under grant agreement no 653417.

# ReCRED Project – Consortium

- Project funded by EU under H2020
- Call Identifier: H2020-DS2-2014-1


wedia

EXUS

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

THE PRODUCTIZERS

verizon

Telefónica
Telefónica I+D

cnit

institute imdea networks

upcom
Bringing business and IT together

certSIGN BY UTI

BAKER & McKENZIE

**www.recred.eu**

# Current state

- Nowadays **e-commerce** now exceeds **1 trillion € per annum**
- **Internet of Things** becomes a reality
- **Digital economy** & **digital life require** reliable and **user-friendly authentication mechanisms**
- Currently, **user authentication** relies **on passwords**, a **technology of the '60s**
  - **98%** of the **websites** use **password-based authentication**



# Problems, Problems, Problems!

- Users have the **tendency** to choose **weak** & **easy-to-remember** **password**
  - Therefore, **passwords** are **easy-to-guess** and **highly insecure**
- Today's Internet users are registered in **too many online services**
  - Passwords are **highly reused by users or forgotten or patterns are created**
- Regarding passwords **usability**:
  - **70%** of users **forget their password** **once in a month**
  - Users **tend to try** on average **2.4 passwords** before they **type the right one (think about typing in a mobile device)**

# Questions to answer…

- Can I **login without using passwords?**


- **Can I use a method to access internet which is usable but also secure?**

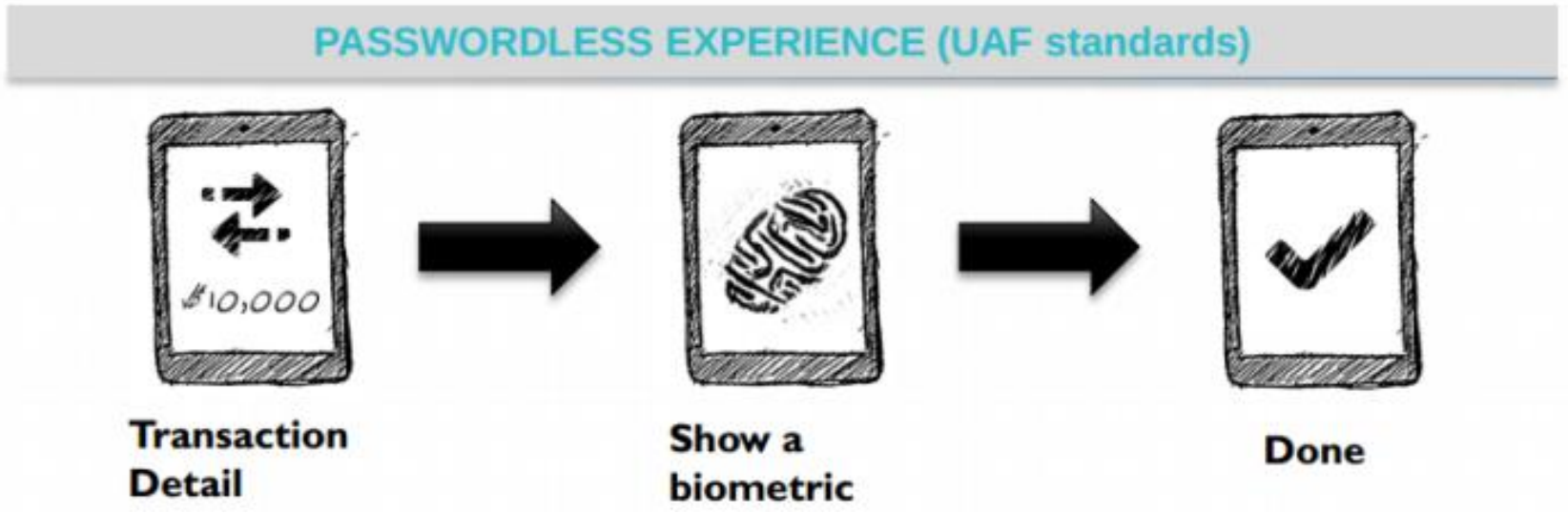

- Can I **ensure my anonymity when I access to webpages?**

# ReCRED's approach


**ReCRED** integrates existing as well upcoming techniques of **authentication**, **identity management**, **access control** and **privacy protection**

# Device Centric Authentication – The FIDO Protocol

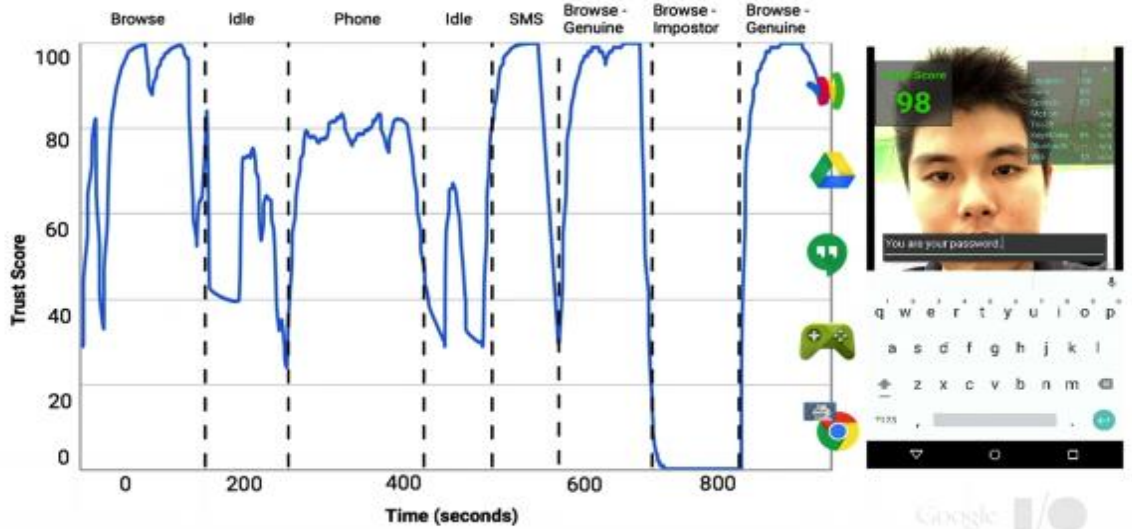
- The FIDO protocol is the base of Device Centric Authentication
- FIDO members → Google, Paypal, Microsoft, Visa, Samsung, Intel, American Express, Bank of America…



# Device Centric Authentication - Behavioral Authentication

- **For security critical services a second factor authentication is also required**
- Continuous authentication
- Captured attributes
  - Typing patterns
  - Browsing habits
  - Location
  - Walking habits
  - Speech recognition
  - Touch dynamics

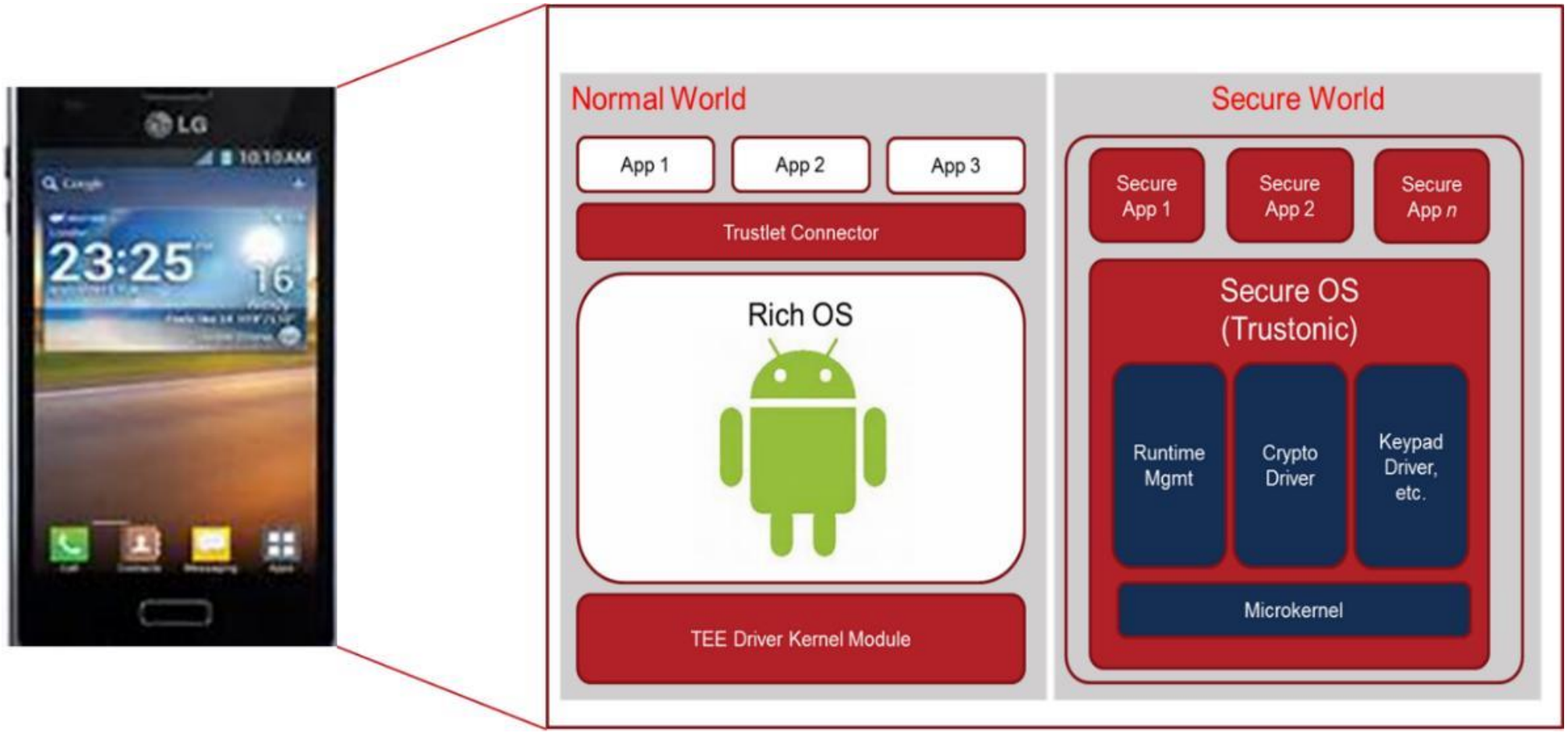
Google Project Abacus



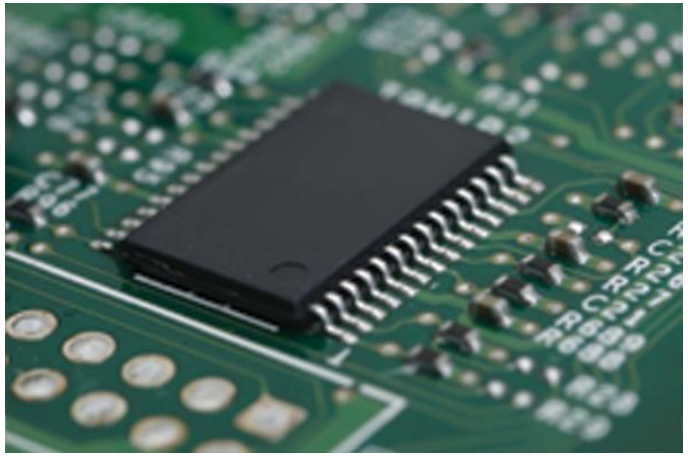
# Wait a minute!

- The device is the gateway to our digital life with FIDO
- What happens if the device gets infected with a malware installed??
- The malware will tamper with FIDO → Impersonation, data compromise…
- So with FIDO are we just transferring the problem?

# Trusted Execution Environment - TEE



# Hardware Root of Trust



- Transfer Security from software to hardware
- Trusted Execution Environment is a hardware technology to separate secure and normal worlds
- Malware is software → it cannot reach and tamper with hardware

# ReCRED's approach - employed technologies

- **OpenID Connect** (Single Sign On)
  - Online services authenticate their users by employing **Google**, **Microsoft**, Twitter, accounts
- **Less passwords to remember for users**
- **No need for password maintenance for service provides**
- **FIDo + OpenID Connect**

# Anonymous access

- **But with OpenID Connect, there is no anonymity**
- **Privacy preserving Attribute-based Access Control, aka Anonymous Credentials**
- **Two implementations**
  - **Idemix by IBM**
  - **U-Prove by Microsoft**


# Anonymity

- Authentication with pseudonyms
- **Account-less access through verified identity attributes (e.g., Age, Location, etc.)**
- Reveal to service providers only the minimum identity information that is required by the purpose of the access action
- Advanced cryptography
  - Zero knowledge
  - Blind signatures

# Anonymity Example

- I want to have access to an online bookstore **that has a discount if you have the specific attributes** or **properties**
  - That I am **above 18**
  - I am a **student**, **professor** or **researcher**
  - I belong to a **family** that has **more than two children**
- I want to **ensure my anonymity** controlling my privacy
  - **I do not want to reveal any additional personal information**

# Anonymity Example

- The bookstore service can mathematically verify that a user has specific properties
  - Indeed the user is above 18 and he is a student or professor or researcher and his family has more than two children.

- The bookstore service does not learn the exact age of the user, only that the user is above 18.

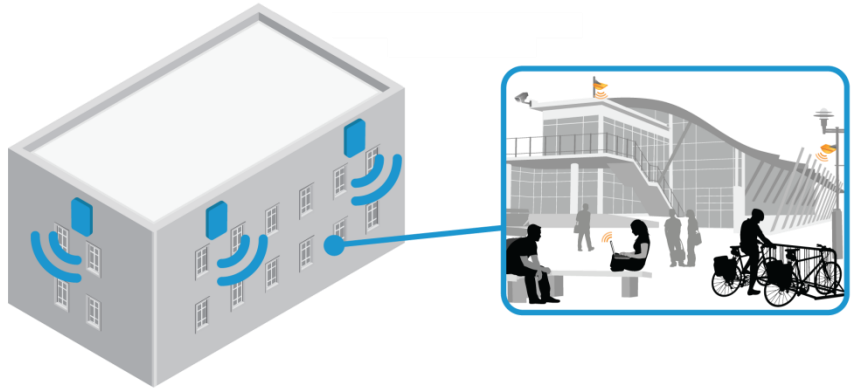
- The same holds also for the number of children and his occupation.

# ReCRED's Innovation

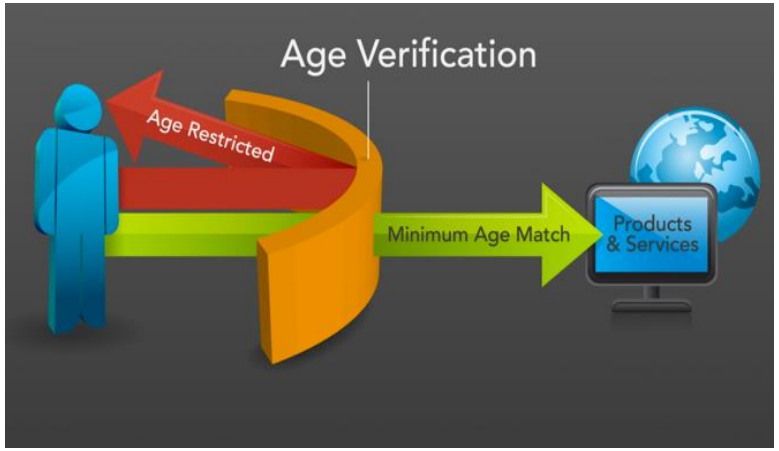
- Standardized and secure authentication using **FIDO**
  - **FIDO protocol implementation**
- Multifactor & easy to use password-less authentication
  - Biometrics and behavioral authentication
- Enhanced security & privacy by employing the crypto functions and secure storage of **TEE**
  - **Implementation of secure world applications with C programming language**
- Privacy of **online identities** using **anonymous credentials**
  - Idemix and U-Prove implementation
  - **Attribute-based Access Control policies**

# 4 ReCRED pilots → Business Cases!

Support to financial services



Campus Wi-Fi and Campus-restricted Web Services




Age Verification


Student Authentication and Offers

# Thank you

Christoforos Ntantogian

Systems Security Laboratory
Department of Digital Systems

http://ssl.ds.unipi.gr/
http://cgi.di.uoa.gr/~dadoyan
email: dadoyan@unipi.gr

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS