INCOGNITO NEWSLETTER

01
OBJECTIVE

The overarching goal of INCOGNITO (**I**de**N**tity verifi**C**ati**O**n with privacy-preservin**G** crede**N**t**I**als for anonymous access **T**o **O**nline services) is to combine state-of-the-art technologies in a platform that will allow users to easily understand what is needed to access online services with respect to their privacy and be able to prove specific attributes of their identity or their whole identity. We build on top of the framework that is being developed under the ReCRED project where we use advanced mobile software in order to convert online and physical identity proofs into validated and cryptographically strong proofs of identities that can be used for getting access to Online Services. INCOGNITO has the following objectives:

1. Design and implement an infrastructure that supports QUALIFIED ANONYMITY (QA) by leveraging state of the art cryptographic credentials schemes as well as Federated Login solutions.

2. Design and implement an Identity Acquisition and Management platform that will allow the user to quickly and securely acquire identity attributes from Physical ID documents and Online Identities.

3. Design and implement an advanced UI/UX AI-based assistant that will guide and inform the user about aspects of his identity management as well as possible actions to take.

4. Evaluate the results of the project through two pilot activities.

To achieve these objectives an inter-sectorial and interdisciplinary secondment program for Experienced and Early Stage Researchers that fosters knowledge exchange is proposed. Academic partners will offer their expertise on online identity acquisition and management, machine-learning algorithms and user experience assessment. Industry partners will offer their expertise on state-of-the-art IT security technologies, production-grade development processes, exposure to industrial research environment and relevant business issues and data.

MESSAGE FROM THE COORDINATOR

We are happy to introduce you to the INCOGNITO news-letter, a great vehicle for our consortium to communicate our project's achievements, activities and results. The intention of this newsletter is to open a new communication channel in order to provide news on the project progress and to discuss ongoing topics relevant to INCOGNITO for internal and external project partners, stakeholders and all other interested bodies

Contribution to address authentication methods weaknesses

Current authentication methods on the Web have serious weaknesses. First, services heavily rely on the traditional password paradigm, which diminishes the end-users' security and usability. Second, the lack of attribute-based authentication does not allow anonymity-preserving access to services. Third, users have multiple online accounts that often reflect distinct identity aspects. This makes proving combinations of identity attributes hard on the users.

Contribution to address authentication methods weaknesses

We address a way to help solving these weaknesses by proposing a privacy-preserving architecture for device-centric and attribute-based authentication based on:
1. the seamless integration between usable/strong device-centric authentication methods and federated login solutions;
2. the separation of the concerns for Authorization, Authentication, Behavioral Authentication and Identification to facilitate incremental deployability, wide adoption and compliance with NIST assurance levels;
3. a novel centralized component that allows end-users to perform identity profile and consent management, to prove combinations of fragmented identity aspects, and to perform account recovery in case of device loss

INCOGNITO

EUROPEAN UNION BENEFITS

At the moment, authentication on the web relies on the password paradigm, which was developed during the 60s for old computers. In addition we know that the 128-bit very complex and long (~20 characters) password used for a specific service is highly secure, but only when it is stored in the brain of the user and it is computationally hard to guess. However, as the needs and number of web services increases, the password paradigm ails an inextricable tension between security and usability as users become burdened with memorizing and managing multiple passwords. At the same time, passwords can be shoulder-surfed, key-logged, replayed, eavesdropped, brute-forced and phished. On the other hand, password databases can be leaked and even if the service follows security good practices, the attacker can guess the password by performing a dictionary-based brute-force attack.

In this concept, the vital contribution will be provided by the INCOGNITO as an in the current efforts for crewing a European research and development community with expertise in the authentication techniques that may combine cross-sectorial (industry and academia) backgrounds.

02

NEWS

INCOGNITO & ReCRED introduced Qualified Anonymity

INCOGNITO & ReCRED introduced Qualified Anonymity using Anonymous Credentials in the 13th Meeting of the Community of Users on Secure, Safe, Resilient Societies that took place in Brussels, 25 – 29 March 2019.
https://www.securityresearch-cou.eu/node/9200

Incognito in Researcher's Night Athens

The Systems Security Laboratory (SSL) of the University of Piraeus participated in the Researcher's Night event which took place in Athens, Greece on September 27, 2019. During this event, the researchers presented the Incognito project, its aims and the progress that is made in these early stages.

03

FOLLOW US FOR OUR LATEST NEWS

You can see more about the project in our website https://incognito.socialcomputing.eu/

Follow us in our Social Media

fb.me/IncognitoH2020

https://twitter.com/H2020Incognito

https://www.linkedin.com/company/incognito-h2020/

04

OUR PARTNERS

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

Cyprus University of Technology

certSIGN®

INCOGNITO BENEFICIARIES COUNTRIES

Telefónica
Telefónica I+D

FOGUS
INNOVATIONS & SERVICES

Insightful LS TECH Analytics