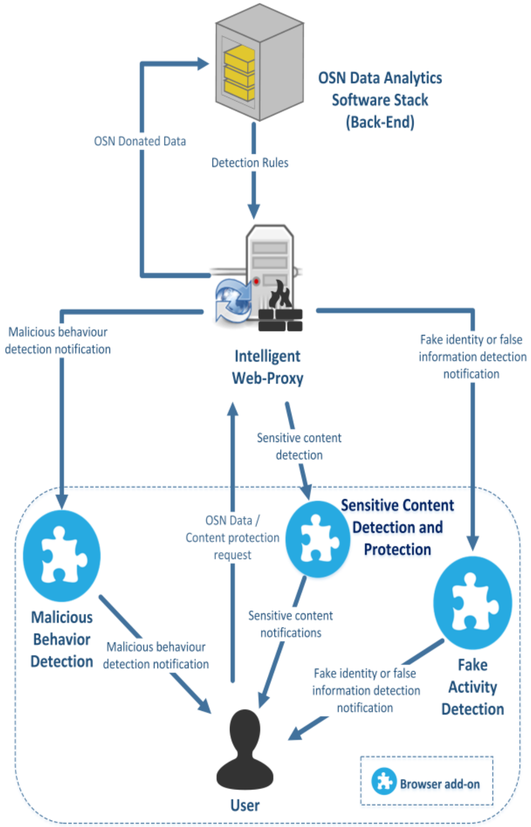
The ENCASE project aims to develop a network that will strengthen and enhance the European research and innovation potential for the protection of minors in Online Social Networks. The project is funded by the European Commission under the Marie Sklodowska-Curie Action Research and Innovation Staff exchanges of the Horizon 2020 framework and the duration of the project is 48 months (1/1/2016 - 31/12/2019).

More information: http://encase.socialcomputing.eu/

ENCASE will leverage the latest advances in usable security and privacy to design and implement a browser-based architecture for the protection of minors from malicious actors in online social networks. ENCASE is a collaboration with world-renowned partners: University College London, UK; Aristotle University, Greece; Università degli Studi Roma Tre, Italy; Telefonica Investigacion y Desarrollo, Spain; LSTech, UK; SignalGeneriX, LTD, Cyprus; Cyprus Research and Innovation Center Ltd, Cyprus), for effective knowledge transfer and sharing broadening their research agendas. The establishment of such a network will boost the image of Cyprus as a research and innovation hub in the domain of Social Computing in Europe. Moreover, this cooperation aims to achieve scientific breakthroughs, develop innovative products, patents and knowledge in the area of Social Computing.


OSN Data Analytics Software Stack (Back-End)
OSN Donated Data
Detection Rules
Malicious behaviour detection notification
Intelligent Web-Proxy
Fake identity or false information detection notification
Sensitive content detection
Sensitive Content Detection and Protection
OSN Data / Content protection request
Malicious Behavior Detection
Malicious behaviour detection notification
Sensitive content notifications
Fake identity or false information detection notification
Fake Activity Detection
User
Browser add-on

Social Computing Research Center
Cyprus University of Technology,
30 Archbishop Kyprianou,

3036, Lemesos

Website: http://encase.socialcomputing.eu
Twitter Page: https://twitter.com/ENCASE_H2020
Facebook Page: www.facebook.com/ENCASE.H2020

Cyprus University of Technology

ENCASE
ENhancing seCurity and privAcy in the Social wEb

Research and Innovation for the protection of minors in Online Social Networks

ENCASE has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 691025

Research and Innovation objectives:

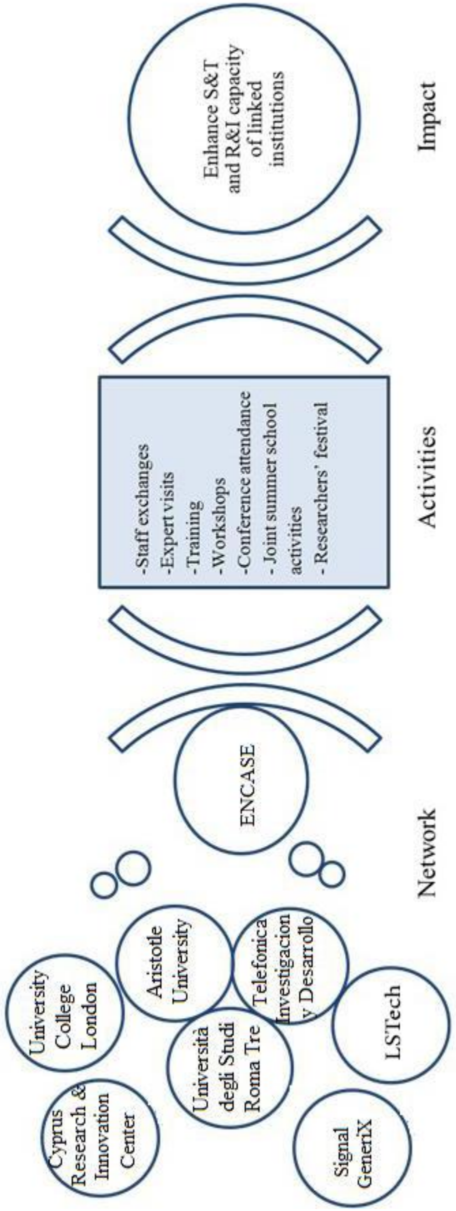
ENCASE aims to safeguard the security and privacy of minors against malicious actors in OSN’s, such as cyberbullies and online sexual abusers. To this end, the research and innovation objectives include:

Understanding the security and privacy (S&P) concerns of OSN users with a focus on how they perceive the concept of S&P and what security-risky actions they may take.

Research methods for the analysis of OSN information to perform user profiling, as well as sentiment and affective analysis. Here, we focus on minors and the aim is to alert users and OSN operators about child predators and cyberbullies, and to reveal users under distress.

Design algorithms and machine learning techniques that exploit various OSN signals (such as likes and personal messages) to unveil fake information with emphasis on the role of online child abusers and their patterns for detection. We plan to extend the state of the art in fake account detection, audience boosting (e.g., fake likes) detection and false information propagation. Specifically, we will develop a production-grade open source OSN data analytics software stack that will facilitate the aforementioned operations. To this end, we will perform extensive measurement studies over proprietary and publicly crawlable data to assess the urgency and existence of such threads and to propose mitigation mechanisms.

Design and implementation of usable web-based user interfaces to discourage users from befriending suspicious OSN users and warn the users or their custodians of when they are being or are about to be subjected to online abuse. Furthermore, the suggested interfaces should discourage users from sharing sensitive content with inappropriate audiences without the proper level of protection.


Impact
Enhance S&T and R&I capacity of linked institutions
Activities
-Staff exchanges
-Expert visits
-Training
-Workshops
-Conference attendance
- Joint summer school activities
- Researchers’ festival
Network
ENCASE
University College London
Aristotle University
Telefonica Investigacion y Desarrollo
Università degli Studi Roma Tre
LSTech
Cyprus Research & Innovation Center
Signal GeneriX

The scientific exchange for Enhancing security and privacy in the Social wEb (ENCASE)

Knowledge transfer and training objectives:

ENCASE aims to create a strong industry-academia cooperation among the partners in the area of security and privacy in OSN’s with an emphasis on the protection of minors. During this cooperation researcher will be exchanged among the partners thus achieving exchange of knowledge and strengthening of collaboration among the academia.

Further, we will conduct interdisciplinary research in the intersection of user experience design, data mining and machine learning, and security and privacy. Specifically, we will develop a software suit of browser add-ons and the corresponding server-side software stack implementing security and privacy enhancing solutions with the goal of deployment over real world OSN’s. We aim to publish our results in the most influential academic venues. Also, our findings will assist in producing commercial offering in the area of social network security and privacy and to bring it to market using the four industrial partners.

Throughout the project, researchers will be able to enrich their existing background and expand their academic/business circle. This will be achieved through:
a) active participation in ambitious research;
b) exchange of researchers to different partners; and
c) participation to networking events that will be organized by the project.

https://encase.socialcomputing.eu

facebook.com/ENCASE.H2020 **twitter.com/ENCASE_H2020**