Marie Sklodowska Curie, Research and Innovation Staff Exchange (RISE)

Ref. Ares(2017)6386311 - 30/12/2017

European Commission

Horizon 2020
European Union funding
for Research & Innovation

ENhancing seCurity and privAcy in the Social wEb: a user-centered approach for the protection of minors

ENCASE
ENhancing seCurity and privAcy in the Social wEb

WP8- Exploitation and Dissemination

Deliverable D8.2 "Dissemination, Commercialization and IP Protection Activities (a)"

Editor(s):	Evangelos Kotsifakos (LST)
Author(s):	Evangelos Kotsifakos, Marios Vontas (LST) Antonis Papasavva, Savvas Zannettou, Michael Sirivianos (CUT)
Dissemination Level:	Confidential
Nature:	Report
Version:	0.3

ENCASE Project Profile

Contract Number	691025
Acronym	ENCASE
Title	ENhancing seCurity and privacy in the Social wEb: a user-centered approach for the protection of minors
Start Date	Jan 1st, 2016
Duration	48 Months

Partners

Τεχνολογικό Πανεπιστήμιο Κύπρου	Cyprus University of Technology	Cyprus
Telefonica Telefónica Investigación y Desarrollo	Telefonica Investigacion Y Desarrollo SA	Spain
UCL	University College London	United Kingdom
CyRIC	Cyprus Research and Innovation Center, Ltd	Cyprus
SignalGeneriX Advanced Signal Solutions	SignalGenerix Ltd	Cyprus
ARISTOTLE UNIVERSITY OF THESSALONIKI	Aristotle University	Greece
INNOVATORS HIGH TECHNOLOGY APPLICATIONS	Innovators, AE	Greece
ROMA TRE UNIVERSITÀ DEGLI STUDI	Universita Degli Studi, Roma Tre	Italy
Insightful LS Analytics TECH	LSTech Ltd	United Kingdom

Document History

AUTHORS

(LST) Evangelos Kotsifakos, Marios Vontas

(CUT) Antonis Papasavva, Savvas Zannettou, Michael Sirivianos

VERSIONS

Version	Date	Author	Remarks
0.1	18/12/2017	LST	Draft version
0.2	29/12/2017	LST, CUT	Revision and Restructuring
0.3	30/12/2017	CUT	Final Version

Executive Summary

This deliverable reports the Dissemination, Commercialization, and IP Protection activities that took place during the second year of the project. It includes information about the material that was created for specific target audiences, targeted press releases, popular press articles and conferences or workshops in which our results were published.

Recognizing the importance of the dissemination and communication activities, we employ various channels to promote the project’s goals and advantages. Specifically, the project establishes its presence on the Web via its website as well as its social media accounts in Facebook, Twitter, and LinkedIn.

Furthermore, the project and its goals are presented at various events with attendees from the industry and academia.

In terms of research articles, we managed to produce several papers in distinguished conferences, workshops, and journals. We consider the publication output of the project so far as very satisfactory.

While our communication activities are at a very good level, we are making efforts to further increase the project’s popularity and users’ engagement.

Table of Contents

Executive Summary..4
Table of Contents..5
List of Figures..7
List of Tables..7
1. Introduction..8
2. Dissemination Activities..9
2.1. Participation in Conferences..9
2.2. Participation in Workshops..13
2.3. Training Activities..13
2.3.1. Summer School..13
2.3.2. Seminars..14
2.3.3. Organization of a Workshop..16
2.3.4. Reviews and Plenary Meetings..17
3. Communication Activities..17
3.1. Articles in Mainstream Press (Press Releases)..17
3.2. Other Press Releases..18
3.3. Project website..19
3.4. Social Media..20
3.4.1. Facebook Page..20
3.4.2. LinkedIn Page..21
3.4.3. Twitter Page..21
3.5. ENCASE in Corporate Websites..22
3.6. Flyer..23
3.7. Participation in Events other than a Conference or Workshop..24
4. Standardization and Raising Awareness Efforts..25
4.1. Better Internet for Kids..25
4.2. Safe Internet..25
4.3. Saferinternet.gr..25
4.4. Cyber Safety..25
4.5. EU Kids Online..26

4.6. UNICEF 26
5. Intellectual Property Rights Management 26
5.1. Ownership of Results 26
5.2. Joint ownership 26
5.3. Transfer of Results 26
5.4. Dissemination of Results 27
5.5. Complementary skills for innovation training 27
5.6. Intellectual Property Rights (IPRs) 28
5.7. Plan for the Knowledge Management and Protection 28
5.7.1. Background IP Ownership 28
5.7.2. Foreground IP Ownership 28
5.7.3. Open Source 28
5.7.4. IPR Protection 29
5.7.5. Publishing Model 29
6. Conclusion and Future Activities 29

List of Figures

Figure 1. Number of ENCASE Dissemination and Communication activities..8
Figure 2. Number of persons reached by the ENCASE Dissemination and Communication activities...9
Figure 3. Summer School - Usable Security and Privacy in Online Social Networks schedule 14
Figure 4. ENCASE website 20
Figure 5. ENCASE Facebook page..20
Figure 6. ENCASE's Facebook page Likes statistics 21
Figure 7. ENCASE LinkedIn page 21
Figure 8. ENCASE Twitter page 22
Figure 9. ENCASE Kickoff announcement in CUT’s main page...22
Figure 10. ENCASE in SignalGenerix’s website..23
Figure 11. ENCASE Flyer Front Side...23
Figure 12. ENCASE Flyer Back Side..24

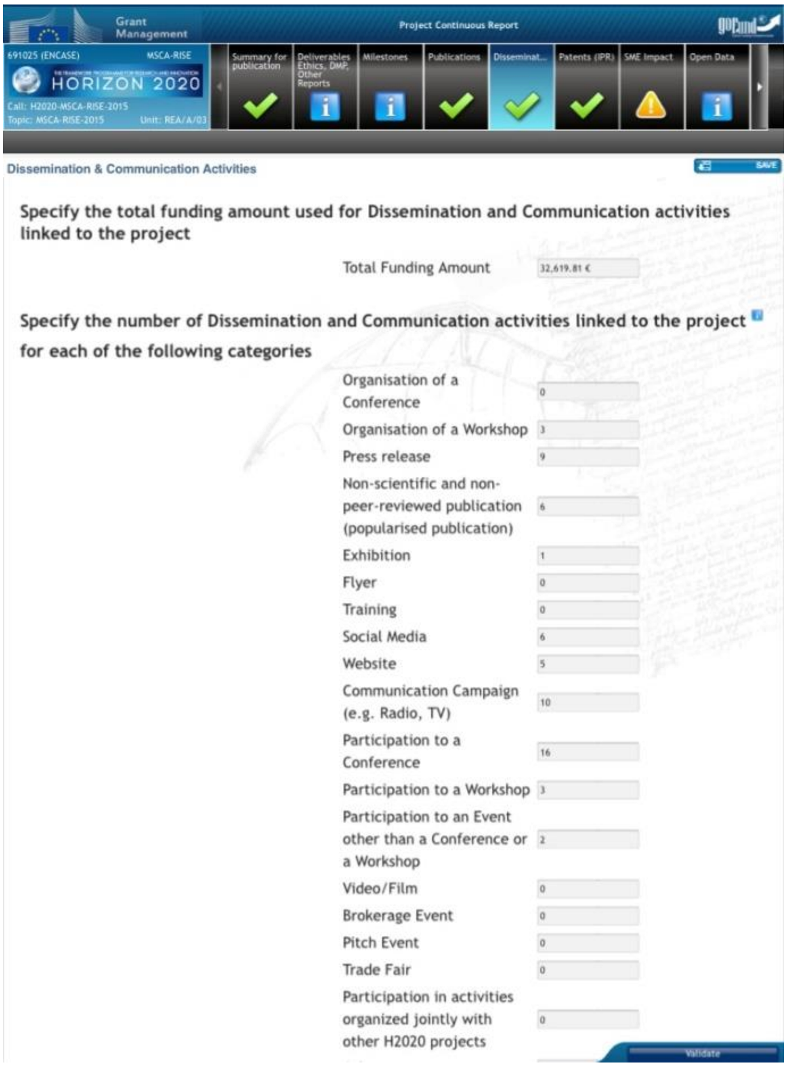
List of Tables

Table 1. ENCASE Pre-IMC Workshop schedule 16

1. Introduction

The purpose of this document is to report the Dissemination, Commercialization, and IP Protection activities that took place during the second year of the project. It includes information about the material that was created for specific target audiences, targeted press releases, and conferences in which our results were published.

In general, as specified in SyGMa, our Dissemination and Communication activities have costed 32619 Euro. The activities thus far executed are depicted in Figure 1.



Dissemination & Communication Activities

Specify the total funding amount used for Dissemination and Communication activities linked to the project

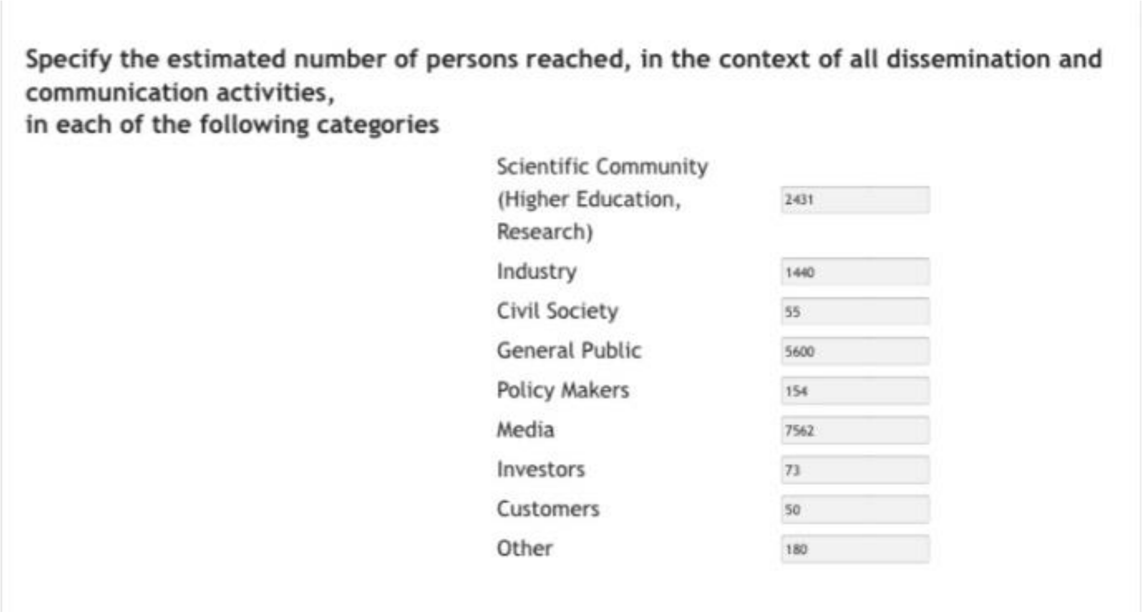
Total Funding Amount	32,619.81 €

Specify the number of Dissemination and Communication activities linked to the project for each of the following categories

Organisation of a Conference	0
Organisation of a Workshop	3
Press release	9
Non-scientific and non-peer-reviewed publication (popularised publication)	6
Exhibition	1
Flyer	0
Training	0
Social Media	6
Website	5
Communication Campaign (e.g. Radio, TV)	10
Participation to a Conference	16
Participation to a Workshop	3
Participation to an Event other than a Conference or a Workshop	2
Video/Film	0
Brokerage Event	0
Pitch Event	0
Trade Fair	0
Participation in activities organized jointly with other H2020 projects	0

Figure 1. Number of ENCASE Dissemination and Communication activities

Figure 2 lists, as specified in SyGMa, the number of persons reached by our Dissemination and Communication activities per type of audience.



Specify the estimated number of persons reached, in the context of all dissemination and communication activities,
in each of the following categories

Scientific Community (Higher Education, Research)	2431
Industry	1440
Civil Society	55
General Public	5600
Policy Makers	154
Media	7562
Investors	73
Customers	50
Other	180

Figure 2. Number of persons reached by the ENCASE Dissemination and Communication activities

2. Dissemination Activities

All the project’s scientific publications can be found in OpenAire (https://www.openaire.eu/search/project?projectId=corda__h2020::da30fe700e9d71002682b0782ee3f437) and on the project’s website (http://encase.socialcomputing.eu/publications).

2.1.Participation in Conferences

The multidisciplinary challenges that the ENCASE project takes on make the outcomes important for several scientific communities. During the second year, the consortium made the following publications:

1. “The Web Centipede: Understanding How Web Communities Influence Each Other Through the Lens of Mainstream and Alternative News Sources”, Savvas Zannettou, Tristan Caulfield, Emiliano De Cristofaro, Nicolas Kourtellis, Ilias Leontiadis, Michael Sirivianos, Gianluca Stringhini, and Jeremy Blackburn. ACM Internet Measurement Conference (IMC) 2017

   As the number and the diversity of news outlets on the Web grows, so does the opportunity for “alternative” sources of information to emerge. Using large social networks like Twitter and Facebook, misleading, false, or agenda-driven information can quickly and seamlessly spread online, deceiving people or influencing their opinions. Also, the increased engagement of tightly knit communities, such as Reddit and 4chan, further compounds the problem, as their users initiate and propagate alternative information, not only within their own communities, but also to different ones as well as various social media. In fact, these platforms have become an important piece of the modern information ecosystem, which, thus far, has not been studied as a whole.

In this paper, we begin to fill this gap by studying mainstream and alternative news shared on Twitter, Reddit, and 4chan. By analyzing millions of posts around several axes, we measure how mainstream and alternative news flows between these platforms. Our results indicate that alt-right communities within 4chan and Reddit can have a surprising level of influence on Twitter, providing evidence that “fringe” communities often succeed in spreading alternative news to mainstream social networks and the greater Web.

2. "Kek, Cucks, and God Emperor Trump: A Measurement Study of 4chan’s Politically Incorrect Forum and Its Effects on the Web”, Gabriel Emile Hine, Jeremiah Onaolapo, Emiliano De Cristofaro, Nicolas Kourtellis, Ilias Leontiadis, Riginos Samaras, Gianluca Stringhini and Jeremy Blackburn. ICWSM 2017

   The discussion-board site 4chan has been part of the Internet’s dark underbelly since its inception, and recent political events have put it increasingly in the spotlight. In particular, /pol/, the “Politically Incorrect” board, has been a central figure in the outlandish 2016 US election season, as it has often been linked to the alt-right movement and its rhetoric of hate and racism. However, 4chan remains relatively unstudied by the scientific community: little is known about its user base, the content it generates, and how it affects other parts of the Web. In this paper, we start addressing this gap by analyzing /pol/ along several axes, using a dataset of over 8M posts we collected over two and a half months. First, we perform a general characterization, showing that /pol/ users are well distributed around the world and that 4chan’s unique features encourage fresh discussions. We also analyze content, finding, for instance, that YouTube links and hate speech are predominant on /pol/. Overall, our analysis not only provides the first measurement study of /pol/, but also insight into online harassment and hate speech trends in social media.

3. "Class-based Prediction Errors to Detect Hate Speech with Out-of-vocabulary Words", Joan Serra, Ilias Leontiadis, Dimitris Spathis, Gianluca Stringhini, Jeremy Blackburn, Athena Vakali. ICLR 2017.

   Common approaches to text categorization essentially rely either on n-gram counts or on word embeddings. This presents important difficulties in highly dynamic or quickly-interacting environments, where the appearance of new words and/or varied misspellings is the norm. A paradigmatic example of this situation is abusive online behavior, with social networks and media platforms struggling to effectively combat uncommon or non- blacklisted hate words. To better deal with these issues in those fast-paced environments, we propose using the error signal of class-based language models as input to text classification algorithms. In particular, we train a next-character prediction model for any given class, and then exploit the error of such class-based models to inform a neural network classifier. This way, we shift from the ability to describe seen documents to the ability to predict unseen content. Preliminary studies us- ing out-of-vocabulary splits from abusive tweet data show promising results, out- performing competitive text categorization strategies by 4–11%.

4. “E-safety in Web 2.0 learning environments: a research synthesis and implications for researchers and practitioners”, Antigoni Parmaxi, Kostantinos Papadamou, Michael Sirivianos and Makis Stamatellatos, HCI International 2017.

   This study explores the research development pertaining to safety and security in online collaborative learning environments, as well as a review of web-based tools and applications that attempt to address security and privacy issues in Online Social Networks. Published research manuscripts related to safety and security in collaborative learning environments have been explored, and the research topics with which researchers and practitioners deal with are discussed, as well as implications for researchers and practitioners. This paper argues that online learning environments entail threats and challenges in the safety of both students and instructors, and further research needs to take place for handling and protecting the privacy of all involved stakeholders.

5. "On the Detection of Images Containing Child-Pornographic Material ", Emilios Yiallourou, Rafaella Demetriou, Andreas Lanitis, 24th International Conference on Telecommunication ICT 2017

   The vast increase in the use of social networks and other internet-based communication tools contributed to the escalation of the problem of exchanging child pornographic material over the internet. The problem of dissemination of child pornographic material could be addressed using dedicated image detection algorithms capable of rating the inappropriateness level of images exchanged through computer networks so that images with inappropriate content involving children are blocked. However, the complexity of the image detection task coupled with the nonexistence of suitable datasets, inhibit the development of efficient algorithms that can be used for detecting offensive images containing children. To deal with the problem, we propose a methodological approach that can be used for supporting the development of child pornography detectors through the generation of synthetic datasets and through the decomposition of the task into a set of simpler tasks for which training data is available. Preliminary results show the promise of the proposed approach.

6. "From Risk Factors to Detection and Intervention: A Metareview and Practical Proposal for Research on Cyberbullying", Ioannou, A., Blackburn J., Stringhini, G., De Cristofaro, E., Kourtellis N., Sirivianos, M., Zaphiris, P. (2017), IST-Africa 2017.

   We sought to determine the level of maturity of the Cyberbullying research community and identify knowledge gaps that could be addressed in future projects in this area. Our findings suggest that the vast majority of academic contributions on cyberbullying focus on understanding the phenomenon, risk factors, and threats, with the prospect of suggesting possible protection strategies. The review calls for more research tackling the problem by leveraging statistical models and computational mechanisms geared to detect, intervene, and prevent cyberbullying. We argue that a multidisciplinary approach is needed for current challenges to be addressed and significant progress to be made, in order to combat this social menace.

7. "Mean Birds: Detecting Aggression and Bullying on Twitter", Despoina Chatzakou, Nicolas Kourtellis, Jeremy Blackburn, Emiliano De Cristofaro, Gianluca Stringhini, Athena Vakali. ArXiv 2017.

   In recent years, bullying and aggression against social media users have grown significantly, causing serious consequences to victims of all demographics. Nowadays, cyberbullying affects more than half of young social media users worldwide, suffering from pro- longed and/or coordinated digital harassment. Also, tools and technologies geared to understand and mitigate it are scarce and mostly ineffective. In this paper, we present a principled and scalable approach to detect bullying and aggressive behavior on Twit- ter. We propose a robust methodology for extracting text, user, and network-based attributes, studying the properties of bullies and aggressors, and what features distinguish them from regular users. We find that bullies post less, participate in fewer online communities, and are less popular than normal users.

Aggressors are relatively popular and tend to include more negativity in their posts. We evaluate our methodology using a corpus of 1.6M tweets posted over 3 months, and show that machine learning classification algorithms can accurately detect users exhibiting bullying and aggressive behavior, with over 90% AUC.

8. "Hate is not binary: Studying abusive behavior of #GamerGate on Twitter", Despoina Chatzakou, Nicolas Kourtellis, Jeremy Blackburn, Emiliano De Cristofaro, Gianluca Stringhini, and Athena Vakali, Proceedings of the 2017 ACM Conference on Hypertext and Social Media (HyperText)

   Over the past few years, online bullying and aggression have be- come increasingly prominent, and manifested in many different forms on social media. However, there is little work analyzing the characteristics of abusive users and what distinguishes them from typical social media users. In this paper, we start addressing this gap by analyzing tweets containing a great large amount of abusive- ness. We focus on a Twitter dataset revolving around the Gamergate controversy, which led to many incidents of cyberbullying and cyberaggression on various gaming and social media platforms. We study the properties of the users tweeting about Gamergate, the content they post, and the differences in their behavior compared to typical Twitter users.

   We find that while their tweets are often seemingly about aggressive and hateful subjects, “Gamergaters” do not exhibit common expressions of online anger, and in fact primarily differ from typical users in that their tweets are less joyful. They are also more engaged than typical Twitter users, which is an indication as to how and why this controversy is still ongoing. Surprisingly, we find that Gamergaters are less likely to be suspended by Twitter, thus we analyze their properties to identify differences from typical users and what may have led to their suspension. We perform an unsupervised machine learning analysis to detect clusters of users who, though currently active, could be considered for suspension since they exhibit similar behaviors with suspended users. Finally, we confirm the usefulness of our analyzed features by emulating the Twitter suspension mechanism with a supervised learning method, achieving very good precision and recall.

9. "POISED: Spotting Twitter Spam Off the Beaten Paths", Shirin Nilizadeh, Francois Labreche, Alireza Sadighian, Jose Fernandez, Christopher Kruegel, Gianluca Stringhini, and Giovanni Vigna. ACM CCS, 2017.

   Cybercriminals have found in online social networks a propitious medium to spread spam and malicious content. Existing techniques for detecting spam include predicting the trustworthiness of ac- counts and analyzing the content of these messages. However, advanced attackers can still successfully evade these defenses.

   Online social networks bring people who have personal connections or share common interests to form communities. In this paper, we first show that users within a networked community share some topics of interest. Moreover, content shared on these social network tend to propagate according to the interests of people. Dissemination paths may emerge where some communities post similar messages, based on the interests of those communities. Spam and other malicious content, on the other hand, follow different spreading patterns.

   In this paper, we follow this insight and present POISED, a system that leverages the differences in propagation between benign and malicious messages on social networks to identify spam and other unwanted content. We test our system on a dataset of 1.3M tweets collected from 64K users, and we show that our approach is effective in detecting malicious messages, reaching 91% precision and 93% recall. We also show that POISED ’s detection is more comprehensive than previous systems, by comparing it to three state-of-the-art spam detection systems that have been proposed by the research community in the past. POISED significantly out- performs each of these systems. Moreover, through simulations, we show how POISED is effective in the early detection of spam messages and how it is resilient against two well-known adversarial machine learning attacks.

10. "Detecting Aggressors and Bullies on Twitter", Despoina Chatzakou, Nicolas Kourtellis, Jeremy Blackburn, Emiliano De Cristofaro, Gianluca Stringhini, Athena Vakali. WWW '17 Companion Proceedings of the 26th International Conference on World Wide Web Companion.

    Online social networks constitute an integral part of people’s every day social activity and the existence of aggressive and bullying phenomena in such spaces is inevitable. In this work, we analyze user behavior on Twitter in an effort to detect cyberbullies and cuberaggressors by considering specific attributes of their online activity using machine learning classifiers.

11. On June 24, 2017 Antonia Gogoglou from Aristotle University of Thessaloniki did a presentation about The ENCASE Project at the Data Intelligence Conference. Details can be found here: http://data-intelligence.ai/presentations/4

2.2. Participation in Workshops

1. "Measuring #GamerGate: A Tale of Hate, Sexism, and Bullying", Emiliano De Cristofaro, Despoina Chatzakou, Jeremy Bluckburn, Nicolas Kourtellis, Athina Vakali, Gianluca Stringhini , Cybersafety Workshop 2017

    Over the past few years, online aggression and abusive behaviors have occurred in many different forms and on a variety of plat- forms. In extreme cases, these incidents have evolved into hate, discrimination, and bullying, and even materialized into real-world threats and attacks against individuals or groups. In this paper, we study the Gamergate controversy. Started in August 2014 in the online gaming world, it quickly spread across various social networking platforms, ultimately leading to many incidents of cyber- bullying and cyberaggression. We focus on Twitter, presenting a measurement study of a dataset of 340k unique users and 1.6M tweets to study the properties of these users, the content they post, and how they differ from random Twitter users. We find that users involved in this “Twitter war” tend to have more friends and followers, are generally more engaged and post tweets with negative sentiment, less joy, and more hate than random users. We also perform preliminary measurements on how the Twitter suspension mechanism deals with such abusive behaviors. While we focus on Gamergate, our methodology to collect and analyze tweets related to aggressive and bullying activities is of independent interest.

2.3. Training Activities

2.3.1. Summer School

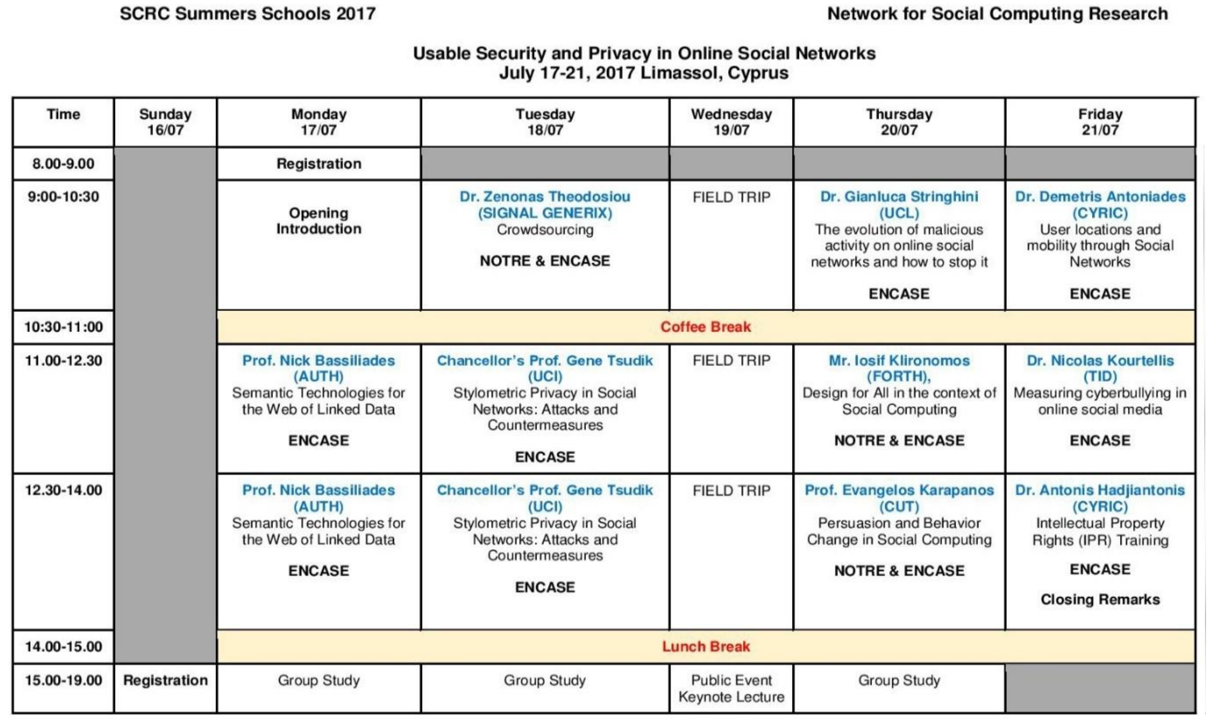
Usable Security and Privacy in Online Social Networks – July 17-21, 2017, Limassol, Cyprus http://summerschools.socialcomputing.eu/encase

The Social Computing Research Center (https://www.socialcomputing.eu/) at the Cyprus University of Technology (CUT) hosted a Summer School in the context of ENCASE with the title "Usable Security and Privacy in Online Social Networks".

The summer school took place between Monday 17th of July 2017 and Friday 21st of July 2017 from

9:00am until 14:00pm every day in the facilities of the Cyprus University of Technology in Limassol.

The summer school aimed to encourage participants to understand significant research issues commonly or increasingly studied in the field of Usable Security and Privacy for Online Social Networking. Such enhanced understanding will enable them to 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. Also to provide research and innovation contributions to end-user experience assessment, large scale data processing, machine learning and data mining, and content confidentiality. Furthermore, it will give opportunities to PhD students to interact and exchange research ideas with other PhD students, participate in discussions and focus group sessions on PhD studies and experiences and engage in discussions around research in Usable Security and Privacy for Online Social Networking. The daily schedule of the summerschool is shown in Figure 1.



SCRC Summers Schools 2017

Network for Social Computing Research

Usable Security and Privacy in Online Social Networks
July 17-21, 2017 Limassol, Cyprus

Time	Sunday 16/07	Monday 17/07	Tuesday 18/07	Wednesday 19/07	Thursday 20/07	Friday 21/07
8.00-9.00		Registration				
9:00-10:30		Opening Introduction	Dr. Zenonas Theodosiou (SIGNAL GENERIX) Crowdsourcing NOTRE & ENCASE	FIELD TRIP	Dr. Gianluca Stringhini (UCL) The evolution of malicious activity on online social networks and how to stop it ENCASE	Dr. Demetris Antoniades (CYRIC) User locations and mobility through Social Networks ENCASE
10:30-11:00		Coffee Break				
11.00-12.30		Prof. Nick Bassiliades (AUTH) Semantic Technologies for the Web of Linked Data ENCASE	Chancellor's Prof. Gene Tsudik (UCI) Stylometric Privacy in Social Networks: Attacks and Countermeasures ENCASE	FIELD TRIP	Mr. Iosif Klironomos (FORTH), Design for All in the context of Social Computing NOTRE & ENCASE	Dr. Nicolas Kourtellis (TID) Measuring cyberbullying in online social media ENCASE
12.30-14.00		Prof. Nick Bassiliades (AUTH) Semantic Technologies for the Web of Linked Data ENCASE	Chancellor's Prof. Gene Tsudik (UCI) Stylometric Privacy in Social Networks: Attacks and Countermeasures ENCASE	FIELD TRIP	Prof. Evangelos Karapanos (CUT) Persuasion and Behavior Change in Social Computing NOTRE & ENCASE	Dr. Antonis Hadjiantonis (CYRIC) Intellectual Property Rights (IPR) Training ENCASE Closing Remarks
14.00-15.00		Lunch Break				
15.00-19.00	Registration	Group Study	Group Study	Public Event Keynote Lecture	Group Study	

Figure 3. Summer School - Usable Security and Privacy in Online Social Networks schedule

2.3.2. Seminars

Cybersafety in Modern Online Social Networks – September 10-13, 2017, Dagstuhl, Germany http://encase.socialcomputing.eu/dagstuhl-seminar

The main goal of this seminar was to bring together researchers working on all aspects of cybersafety, including security, privacy, human factors, economics, sociology, law, and psychology. Examples of issues debated include:

- How do we define cyberbullying and online harassment in a way that captures their inherent ambiguities and subjectiveness?
- How do perpetrators of these activities exploit technological tools to increase their effectiveness? How do cyberbullies and online harassers organize and choose targets?
- What are the different types of cyber fraud activities and how might we cluster different

types of scams, based on psychological, sociological, situational and technical variables so as to better design countermeasures?

- What data are ethically and socially acceptable to draw upon in detection and prevention of cyber fraud?
- What variables are important in enabling us to distinguish those who have become single or repeat victims from nonvictims?
- What are the current mitigation schemes adopted by social networks to counter reputation manipulation and their limitations?
- What are the economics and legal mechanisms governing fake activities?
- What can be done to make it economically unviable for fraudsters to engage in reputation manipulation and fake activities?
- How does online radicalization happen?
- Are there specific demographics that are more susceptible to being radicalized? How is online radicalization different from other types of online abuse?

A report was authored based on this seminar: This report documents the program and the outcomes of Dagstuhl Seminar 17372 “Cybersafety in Modern Online Social Networks.” The main motivation behind the seminar stems from the increased relevance of threats and challenges in the context of cybersafety, especially in mod- ern online social networks, where the range of malicious activities perpetrated by malevolent actors is regrettably wide. These include spreading malware and spam, controlling and operating fake/compromised accounts, artificially manipulating the reputation of accounts and pages, and spreading false information as well as terrorist propaganda. The reasons for the success of such attacks are manifold. The users of social networking services tend to extend their trust of the services and profiles of their acquaintances to unknown users and other third parties: despite the service providers’ attempts at keeping their audiences identifiable and accountable, creating a fake profile, also in another person’s name, is very simple. Even partially or fully taking over a profile is comparatively easy, and comes with the benefit of the trust this profile has accrued over time, as many credentials are easy to acquire. Further, even seemingly innocuous issues such as the design and presentation of user interfaces can result in implications for cybersafety. The failure to understand the interfaces and ramifications of certain online actions can lead to extensive over-sharing. Even the limited information of partial profiles may be sufficient for abuse by inference on specific features only. This is especially worrisome for new or younger users of a system that might unknowingly expose information or have unwanted interactions simply due to not fully understanding the platform they are using.

Unfortunately, research in cybersafety has looked at the various sub-problems in isolation, almost exclusively relying on algorithms aimed at detecting malicious accounts that act similarly, or analyzing specific lingual patterns. This ultimately yields a cat-and-mouse game, mostly played on economic grounds, whereby social network operators attempt to make it more and more costly for fraudsters to evade detection, which unfortunately tends to fail to measure and address the impact of safety threats from the point of view of regular individuals. This prompts the need for a multi-faceted, multi-disciplinary, holistic approach to advancing the state of knowledge on cybersafety in online social networks, and the ways in which it can be researched and protected. Ultimately, we want to work towards development of a cutting-edge research agenda and technical roadmap that will allow the community to develop and embed tools to detect malice within the systems themselves, and to design effective ways to enhance their safety online.

This seminar was intended to bring together researchers from synergistic research communities, including experts working on information and system security on one hand, and those with expertise in human/economic/sociological factors of security on the other. More specifically, in the field of cybersafety, there exist a number of interconnected, complex issues that cannot be addressed in isolation, but have to be tackled and countered together. Moreover, it is necessary for these challenges to be studied under a multi-disciplinary light. Consequently, we identified and focused on the most relevant issues in cybersafety, and explored both current and emerging solutions. Specifically, we discussed four problems that are the most pressing both in terms of negative impact and potential danger on individuals and society, and challenging open research problems requiring a multi-disciplinary approach: Cyberbullying & Hate Speech, CyberFraud & Scams, Reputation Manipulation & Fake Activities, and Propaganda.

Overall, the seminar was organized to include a number of long talks from senior experts in the field, covering the four main topics above, followed by a series of short talks from the participants about work in progress and recent results, and finally working groups to foster collaborations, brainstorming, and setting of a research agenda forward. (http://encase.socialcomputing.eu/wp-content/uploads/2017/11/dagrep_v007_i009_pXXX_s17372.pdf)

2.3.3. Organization of a Workshop

ENCASE Pre-IMC Workshop – October 31st, 2017, London, UK

University College London (UCL) hosted a Workshop in the context of ENCASE with the title "ENCASE Pre-IMC Workshop". Table 1 shows the workshop schedule. The corresponding link is the following: http://encase.socialcomputing.eu/ucl-seminar

10.00-10.30	***Arrival; Coffee and Sweets***
10:30-10:35	Welcome, Emiliano De Cristofaro (UCL)
10.35-10.50	Overview, ENCASE EU Project (http://encase.socialcomputing.eu)
10.50-11.15	Jeremiah Onaolapo (UCL): Hives and Honeypots: Understanding Malicious Activity In Online Accounts
11.15-11.40	Narseo Vallina Rodriguez (IMDEA Networks, ICSI): Crowdsourcing Network and Traffic Measurements to Illuminate the Mobile Ecosystem with Lumen
11.40-12.05	Zubair Shafiq (University of Iowa): Measuring and Modeling Software Vulnerability Patching: Challenges and Future Opportunities
12.05-12.30	Nishanth Sastry (King's College London): How Do We Watch TV, and How Can Networks Adapt to This?
12.30-14.00	***Catered Lunch***
14.00-14.40	Ralph Holz (Sydney University): Measurements of Blockchain Networks
14.40-15.20	Roya Ensafi (University of Michigan): Investigating Internet Connectivity Disruptions
15.20-15.40	***Coffee Break***
15.40-16.05	Richard Mortier (University of Cambridge): Containing Personal Data Processing with the Databox
16.05-16.30	Emiliano De Cristofaro (UCL): How I Got Redpilled Measuring 4chan
16.30-16.55	Jon Crowcroft (University of Cambridge): Rewarding Reproducible Results
16.55-17.20	Mobin Javed (ICSI): Detecting Credential Spearphishing in Enterprise Settings

Table 1. ENCASE Pre-IMC Workshop schedule

2.3.4. Reviews and Plenary Meetings

1. On April 21, 2017 the first Review of ENCASE took successfully place at the Università Degli Studi Roma TRE – Italy.
2. On April 19 and 20, 2017 the second ENCASE Plenary Meeting of ENCASE took successfully place, at the Università Degli Studi Roma TRE – Italy.
3. On October 30-31, 2017. The third ENCASE Plenary Meeting successfully took place, at the UCL – London, UK.

3. Communication Activities

3.1. Articles in Mainstream Press (Press Releases)

1. On May 6, 2017, coverage of the 4chan paper and an interview of Jeremy Blackburn (Telefonica Research) on how forums that disseminate fake stories affect what news we see. More information can be found here: http://www.theneweuropean.co.uk/top-stories/a-beginners-guide-to-4chan-the-site-you-never-knew-was-influencing-you-1-5006102?platform=hootsuite
2. On June 11, 2017. Research examines fake news, hate speech and 4chan. The “fringe” alt-right movement using the politically incorrect board on 4chan have a “surprising level of influence” elsewhere. More information can be found here: http://news.sky.com/story/research-examines-fake-news-hate-speech-and-4chan-10910915?dcmp=snt-sf-twitter
3. On November 7, 2017, The New York Times published an example of how information that appeared on a “fringe” community, such as a parody website, managed to creep into mainstream web communities like Facebook and Fox News. This example highlights how fringe communities can influence mainstream web communities by manipulating and spreading unconfirmed information. Before our study, this phenomenon had not been rigorously investigated, and there was no thorough measurement and analysis on how information flows between online communities. http://hackingdistributed.com/2017/07/11/web-centipede
4. On November 17, 2017, The Atlantic highlighted ENCASE’s research on fringe web communities and their outsized influence over the mainstream. https://www.theatlantic.com/politics/archive/2017/11/how-much-attention-should-extremists-get/546152/
5. On November 22, 2017, Caroline Kitchener, associate editor at The Atlantic, talks about Political Extremism on the Internet and discusses ENCASE’s findings on the outsized influence of fringe communities over the mainstream. https://www.c-span.org/video/?437612-3/washington-journal-caroline-kitchener-discusses-political-extremism-internet
6. On November 24, 2017. Gianluca Stringhini discussed some of our ongoing work investigating fringe web communities and disinformation campaigns with Sky news. See more at: https://news.sky.com/story/long-read-key-evidence-linking-kremlin-to-social-media-trolls-is-lacking-11137255

3.2. Other Press Releases

1. On February 28, 2017, the Social Computing Research Center (http://socialcomputing.eu) at the Cyprus University of Technology (CUT) started a campaign to attract people to the Summer School of the Research Project “Enhancing security and privacy in the Social web: a user-centered approach for the protection of minors (ENCASE) (http://encase.socialcomputing.eu)”. This campaign was pushed to the public through our social media, press releases, the project’s website and the personnel of the consortium. More information can be found here: http://www.paideia-news.com/index.php?id=109&hid=24951&url=%CE%A4%CE%95%CE%A0%CE%91%CE%9A%3A-%CE%98%CE%B5%CF%81%CE%B9%CE%BD%CE%AC-%CE%A3%CF%87%CE%BF%CE%BB%CE%B5%CE%AF%CE%B1-%CF%84%CE%BF%CF%85-%CE%9A%CE%AD%CE%BD%CF%84%CF%81%CE%BF%CF%85-%CE%9A%CE%BF%CE%B9%CE%BD%CF%89%CE%BD%CE%B9%CE%BA%CE%AE%CF%82-%CE%A0%CE%BB%CE%B7%CF%81%CE%BF%CF%86%CE%BF%CF%81%CE%B9%CE%BA%CE%AE%CF%82 and http://m.city.sigmalive.com/article/21178/therina-sholeia-pliroforikis-gia-foitites-stin-kypro.

2. On April 11 2017, the ENCASE research project has been included in the Cypriot National Strategy actions for Security on the Internet relating to the creative and safe use of the internet. The aim is to present and make known the actions of the ENCASE programme as well as to provide an opportunity for information sharing and at the same time create opportunities for partnerships and synergies between those involved in safety issues on the Internet. The concept of the effective and creative use of the Internet with security, responsibility and creativity is one of the primary goals of the Republic of Cyprus. The optimal exploitation of the potentials provided by the Information and Communications Technologies (ICT) in order to promote innovation, financial growth and progress is promoted by the Digital Agenda presented in the European Commission in May 19th, 2010.The Republic of Cyprus is following the European and international standards in this respect, with the recent approval of the National Strategy on Cybersecurity for the Republic of Cyprus by the Ministry Council (Ref. Decision 74.721, Date of Decision 14/02/13, Date of Assignment 27 / 3/13) under the coordination of the Office of the Commissioner of Electronic Communications and Postal Services (OCECPR). In this context, the Ministry of Education and Culture has accepted the invitation to coordinate the Working Group on the Safe Internet for children, teachers and parents.The national strategy proposal aims to provide information and education on digital security issues, which will be addressed to children, teachers and parents in order to become critical and responsible users of digital technologies and develop culture of safe use of the possibilities of digital technologies.For more information, please visit the link: http://www.esafecyprus.ac.cy/parousiasi-drasewn.

3. On May 15, 2017, Michael Sirivianos from the Cyprus University of Technology was interviewed by the Politis Radio with Katerina Eliadi on ENCASE and fake news show. More information can be found here: http://politis.com.cy/politis-radio

4. On June 1, 2017, Jeremy Blackburn, a professor at the University of Alabama at Birmingham and one of the study’s authors, explained that 4Chan’s interaction structure (where, unlike more mainstream platforms like Facebook or Reddit, there is no like or upvote system, and the only way to gauge audience reaction is by the number of replies) encourages a constant attempt to galvanize a response by just about any means. More information can be found here: https://motherboard.vice.com/en_us/article/how-4chans-structure-creates-a-survival-

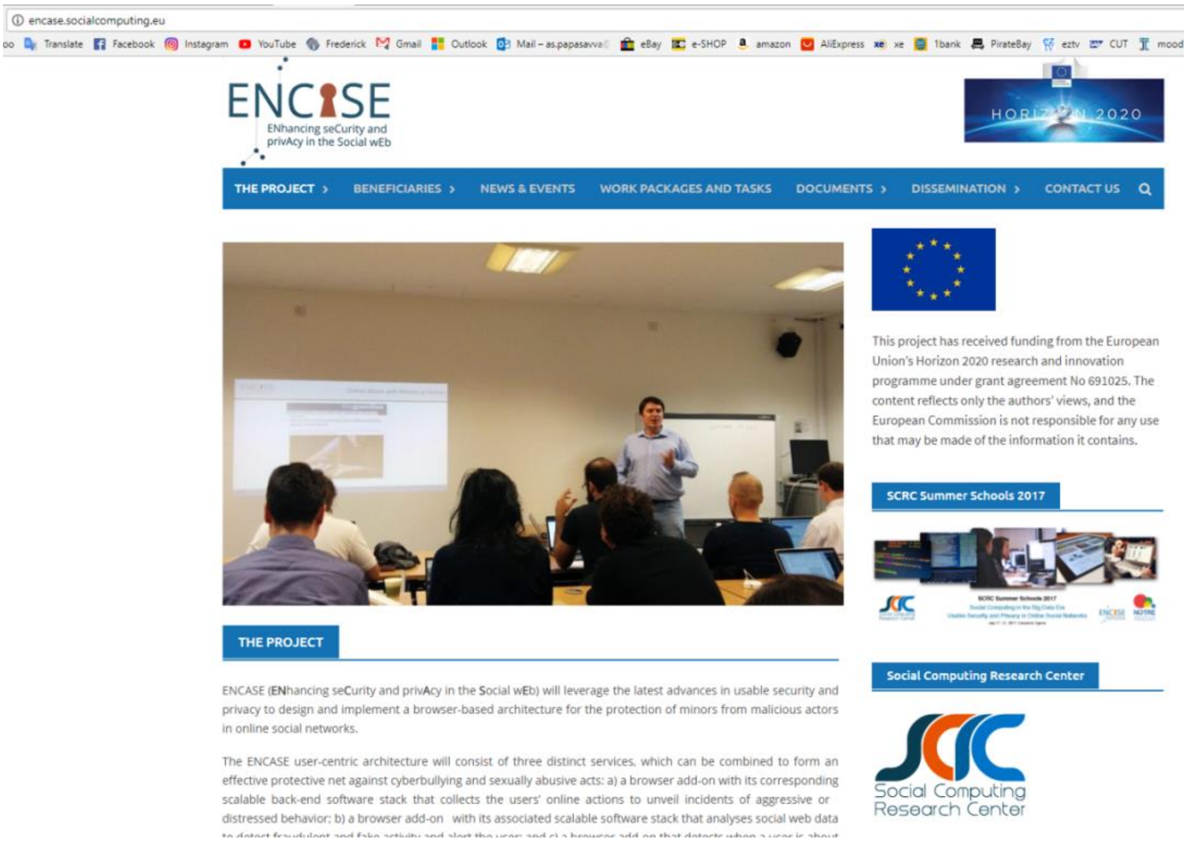
of-the-fittest-for-memes

5. On June 9, 2017, Gianluca Stringhini from the UCL was interviewed by the Nature International Weekly Journal of Science on Shining a light on the dark corners of the web. More information can be found here: http://www.nature.com/news/shining-a-light-on-the-dark-corners-of-the-web-1.22128
6. On June 26, 2017. Europol against online child sexual coercion and extortion!!Europol has launched the campaign “Say No!” to raise awareness on online sexual coercion and extortion affecting minors. A dedicated page has been published at the Europol website to provide information about this criminal phenomenon, the campaign and links to the materials in all languages: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/online-sexual-coercion-and-extortion-crime
7. On July 11, 2017. Twitter, Reddit and 4chan: The Web’s Fake News Centipede: http://hackingdistributed.com/2017/07/11/web-centipede
8. On September 25, 2017. Emiliano De Cristofaro gave an interview on Italian Radio channel “Radio 24” about our research on 4chan and fake news: http://www.radio24.ilsole24ore.com/programma/smart-city/puntate?refresh_ce=1
9. On August 8, 2017. Report of "The Web Centipede: Understanding How Web Communities Influence Each Other Through the Lens of Mainstream and Alternative News Sources", Publication in Paideia News. (http://www.paideia-news.com/index.php?id=109&hid=27059&url=%CE%94%CE%B9%CE%B5%CE%B8%CE%BD%CE%AE%CF%82-%CE%B1%CE%BD%CE%B1%CE%B3%CE%BD%CF%8E%CF%81%CE%B9%CF%83%CE%B7-%CF%84%CF%89%CE%BD-%CE%B5%CF%81%CE%B5%CF%85%CE%BD%CE%B7%CF%84%CE%B9%CE%BA%CF%8E%CE%BD-%CE%B1%CF%80%CE%BF%CF%84%CE%B5%CE%BB%CE%B5%CF%83%CE%BC%CE%AC%CF%84%CF%89%CE%BD-%CF%84%CE%BF%CF%85-%CE%A4%CE%95%CE%A0%CE%91%CE%9A)
10. On November 21, 2017 Caroline Kitchener, associate editor at The Atlantic talks about Political Extremism on the Internet and discusses ENCASE's findings on the outsized influence of fringe communities over the mainstream: https://www.c-span.org/video/?437612-3/washington-journal-caroline-kitchener-discusses-political-extremism-internet

3.3. Project website

ENCASE’s website was designed and released by CUT who is also hosting it. The corresponding link is http://encase.socialcomputing.eu. More specifically ENCASE’s website is compatible with Firefox, Chrome, MS IExplorer and can be viewed on mobile devices such as smartphones and tablets running Android, Windows or iOS.

Furthermore, a search function is offered so as viewers can search for any text in the entire website. A special section of the website has been devoted to dissemination, a snapshot of which can be found in Figure 2.



This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 691025. The content reflects only the authors’ views, and the European Commission is not responsible for any use that may be made of the information it contains.

THE PROJECT

ENCASE (ENhancing seCurity and privAcy in the Social wEb) 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.

The ENCASE user-centric architecture will consist of three distinct services, which can be combined to form an effective protective net against cyberbullying and sexually abusive acts: a) a browser add-on with its corresponding scalable back-end software stack that collects the users’ online actions to unveil incidents of aggressive or distressed behavior; b) a browser add-on with its associated scalable software stack that analyses social web data to detect fraudulent and fake activity and alert the user; and c) a browser add-on that detects when a user is about

Figure 4. ENCASE website

3.4.Social Media

ENCASE has appearance on social networking services such as Facebook, Twitter and LinkedIn.

3.4.1. Facebook Page

Our Facebook page link is https://www.facebook.com/ENCASE.H2020/. As of today, the Facebook page has 259 likes and 113 posts. Figure 3 shows the project’s Facebook page and Figure 4 shows the statistics of ENCASE Facebook page likes.

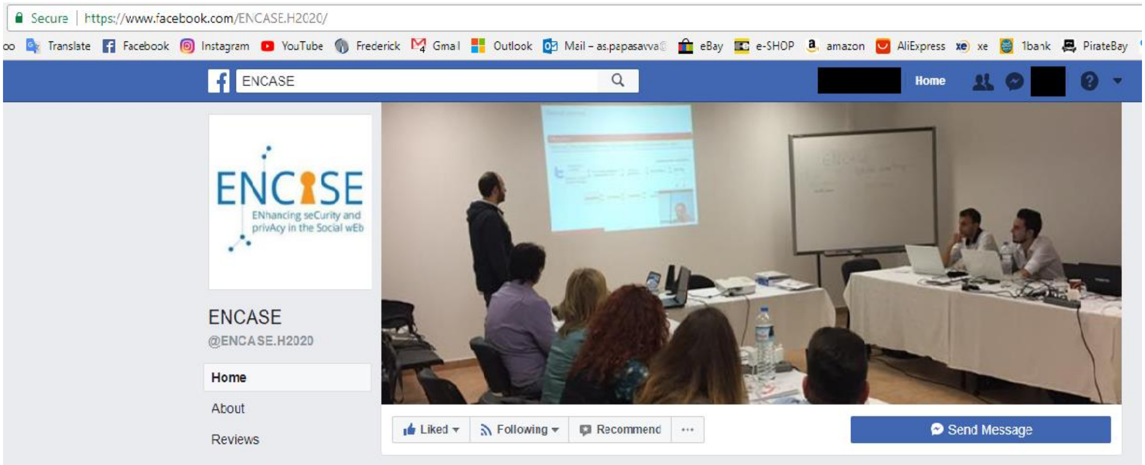
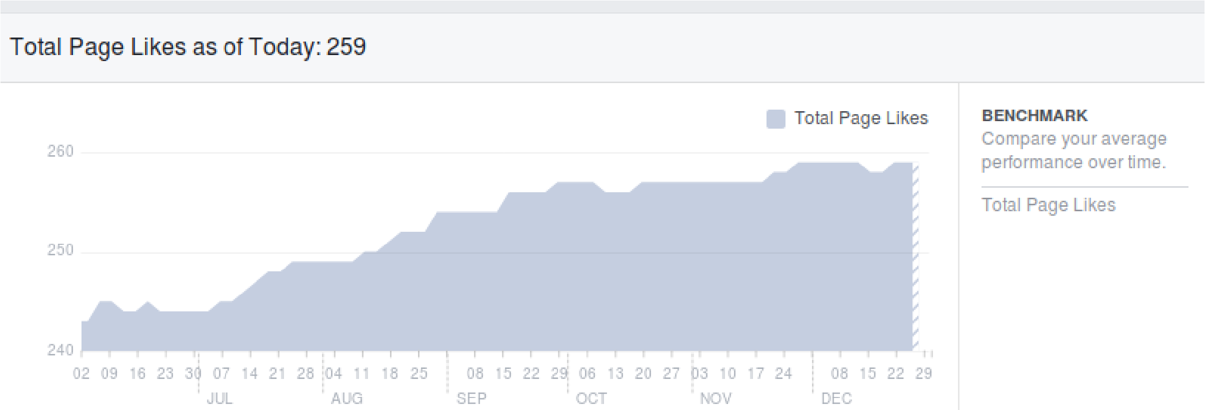


Figure 5. ENCASE Facebook page



Total Page Likes as of Today: 259

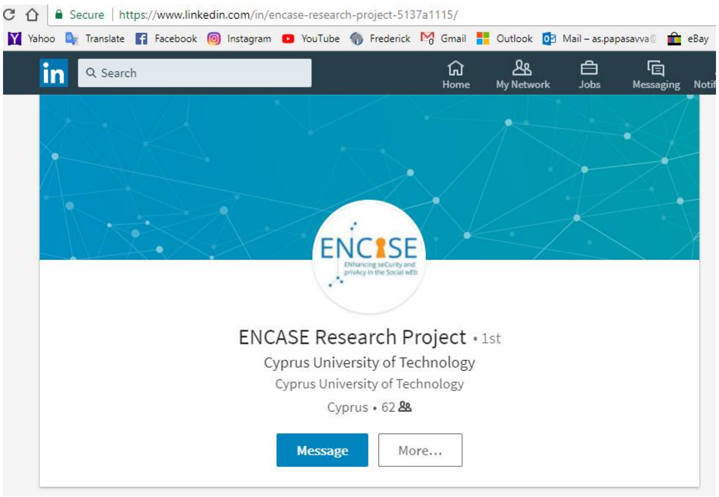
BENCHMARK
Compare your average performance over time.

Total Page Likes

Figure 6. ENCASE's Facebook page Likes statistics

3.4.2. LinkedIn Page

Our LinkedIn page link is https://www.linkein.com/in/encase-research-project-5137a1115/. As of today, the LinkedIn page has 62 followers and 6 posts. Figure 5 shows the project’s LinkedIn page.



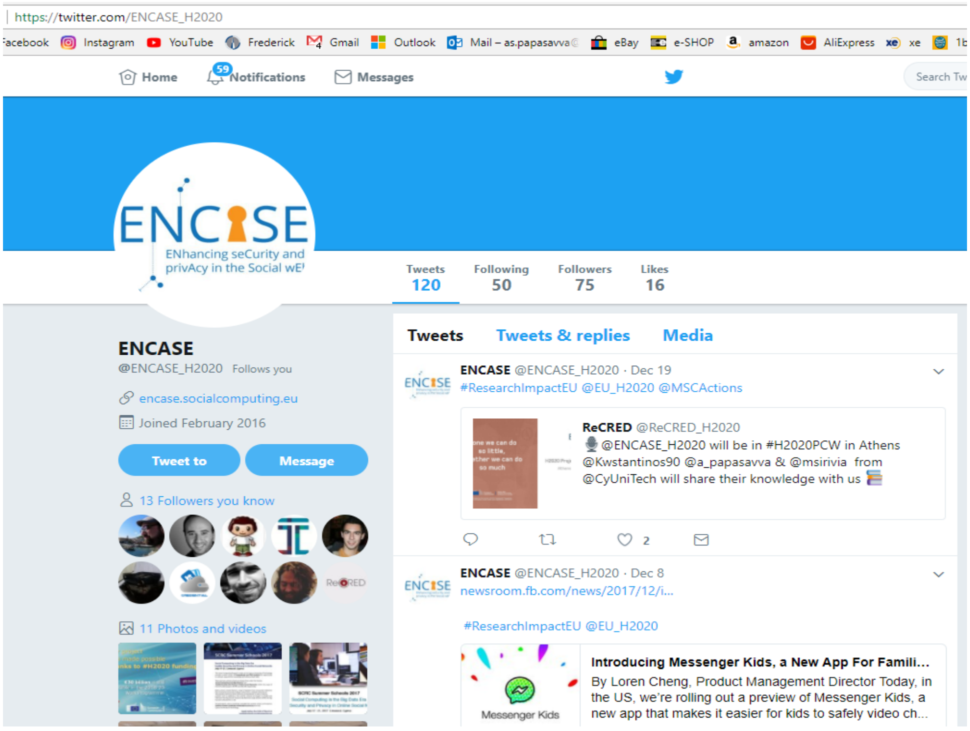
Secure | https://www.linkedin.com/in/encase-research-project-5137a1115/

ENCASE Research Project • 1st
Cyprus University of Technology
Cyprus University of Technology
Cyprus • 62

Figure 7. ENCASE LinkedIn page

3.4.3. Twitter Page

Our twitter page link is https://twitter.com/encase_h2020. As of today, the project’s Tweeter page has 75 followers and 120 tweets. Figure 6 below, shows the project’s Twitter page. It is worth mentioning that The University of Alabama at Birmingham wrote an article based on our research and posted it on its news site: http://www.uab.edu/news/research/item/8840-study-finds-alternative-news-communities-on-reddit-and-4chan-have-high-influence-on-flow-of-alternative-news-to-twitter. Phys.org then redistributed the same content on their website here: https://phys.org/news/2017-11-fringe-reddit-4chan-high-alternative.html. Both links about ENCASE’s research reached various social media, and especially Twitter where they both got approximately more than 1000 retweets.


https://twitter.com/ENCASE_H2020
Facebook Instagram YouTube Frederick Gmail Outlook Mail – as.papasavva@ eBay e-SHOP amazon AliExpress xe 1b
Home
59 Notifications
Messages
Search Tw
ENCASE ENhancing seCurity and privAcy in the Social wEb
Tweets 120
Following 50
Followers 75
Likes 16
Tweet to
Message
Tweets
Tweets & replies
Media
Messenger Kids

ENCASE
@ENCASE_H2020 Follows you
encase.socialcomputing.eu
Joined February 2016
13 Followers you know
11 Photos and videos

ENCASE @ENCASE_H2020 · Dec 19
#ResearchImpactEU @EU_H2020 @MSCActions

ReCRED @ReCRED_H2020
@ENCASE_H2020 will be in #H2020PCW in Athens @Kwstantinos90 @a_papasavva & @msirivia from @CyUniTech will share their knowledge with us

2

ENCASE @ENCASE_H2020 · Dec 8
newsroom.fb.com/news/2017/12/i...

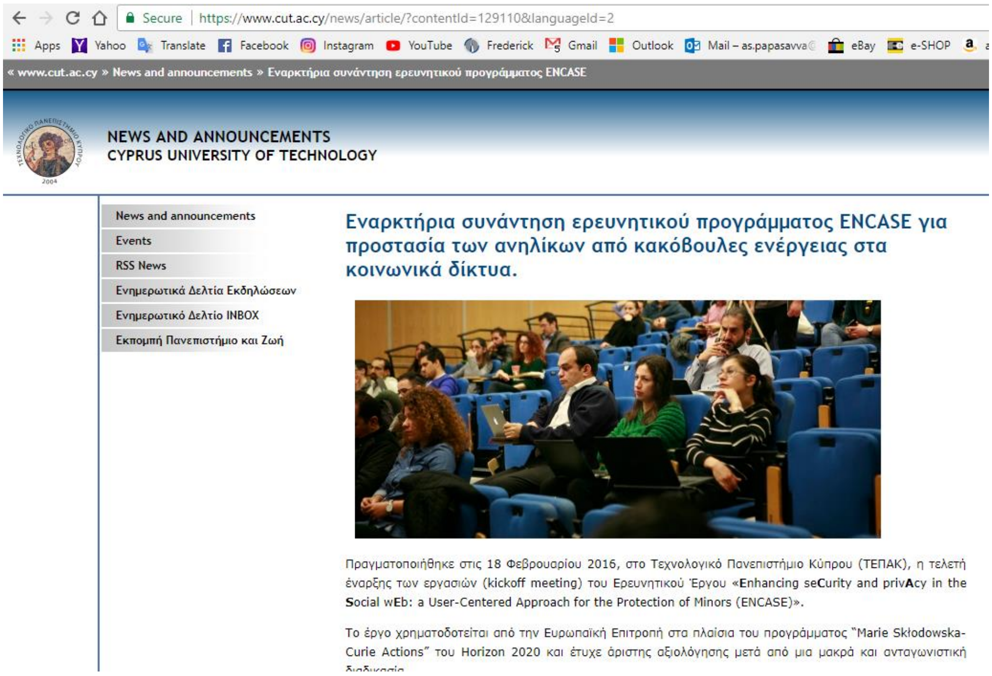
#ResearchImpactEU @EU_H2020

Introducing Messenger Kids, a New App For Famili...
By Loren Cheng, Product Management Director Today, in the US, we're rolling out a preview of Messenger Kids, a new app that makes it easier for kids to safely video ch...

Figure 8. ENCASE Twitter page

3.5. ENCASE in Corporate Websites

The consortium is communicating the project to its customers, the academic community and its associates, aiming to create potential for collaborations and of course to raise interest to possible partners. The University of Cyprus has as well published an article in its website. The corresponding link is the following: https://www.cut.ac.cy/news/article/?contentId=129110


Secure https://www.cut.ac.cy/news/article/?contentId=129110&languageId=2
Apps Yahoo Translate Facebook Instagram YouTube Frederick Gmail Outlook Mail – as.papasavva@ eBay e-SHOP
« www.cut.ac.cy » News and announcements » Εναρκτήρια συνάντηση ερευνητικού προγράμματος ENCASE
NEWS AND ANNOUNCEMENTS
CYPRUS UNIVERSITY OF TECHNOLOGY
News and announcements
Events
RSS News
Ενημερωτικά Δελτία Εκδηλώσεων
Ενημερωτικό Δελτίο INBOX
Εκπομπή Πανεπιστήμιο και Ζωή

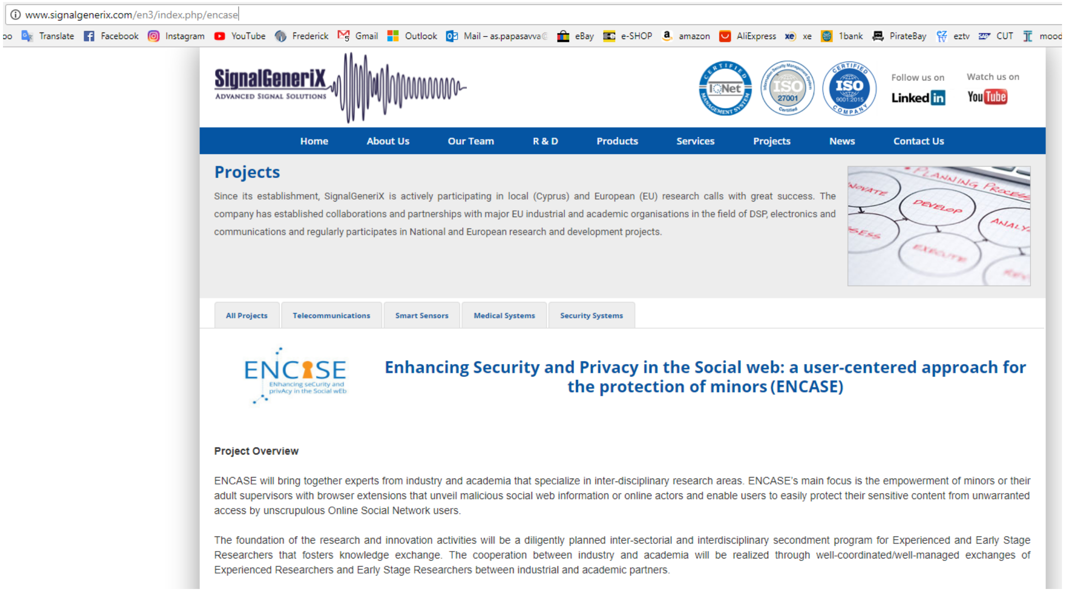
Εναρκτήρια συνάντηση ερευνητικού προγράμματος ENCASE για προστασία των ανηλίκων από κακόβουλες ενέργειας στα κοινωνικά δίκτυα.

Πραγματοποιήθηκε στις 18 Φεβρουαρίου 2016, στο Τεχνολογικό Πανεπιστήμιο Κύπρου (ΤΕΠΑΚ), η τελετή έναρξης των εργασιών (kickoff meeting) του Ερευνητικού Έργου «Enhancing seCurity and privAcy in the Social wEb: a User-Centered Approach for the Protection of Minors (ENCASE)».

Το έργο χρηματοδοτείται από την Ευρωπαϊκή Επιτροπή στα πλαίσια του προγράμματος "Marie Skłodowska-Curie Actions" του Horizon 2020 και έτυχε άριστης αξιολόγησης μετά από μια μακρά και ανταγωνιστική διαδικασία

Figure 9. ENCASE Kickoff announcement in CUT’s main page

The target audience of the website article was the General public, the industry and the scientific community. Also, Signal GeneriX has as well presented ENCASE to its website. The corresponding link is the following: http://www.signalgenerix.com/en3/index.php/encase



Projects

Since its establishment, SignalGeneriX is actively participating in local (Cyprus) and European (EU) research calls with great success. The company has established collaborations and partnerships with major EU industrial and academic organisations in the field of DSP, electronics and communications and regularly participates in National and European research and development projects.

Enhancing Security and Privacy in the Social web: a user-centered approach for the protection of minors (ENCASE)

Project Overview

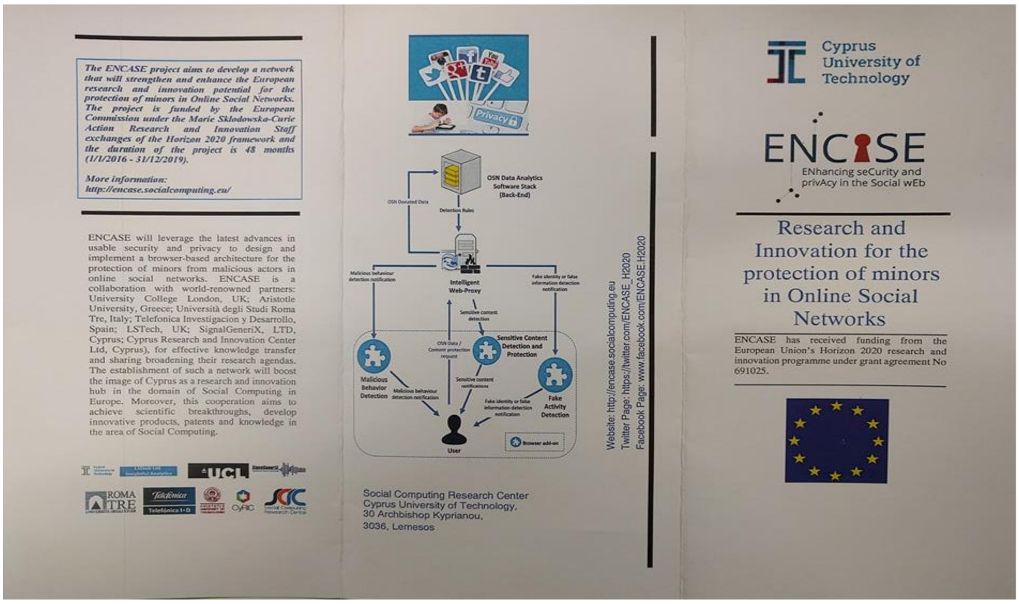
ENCASE will bring together experts from industry and academia that specialize in inter-disciplinary research areas. ENCASE’s main focus is the empowerment of minors or their adult supervisors with browser extensions that unveil malicious social web information or online actors and enable users to easily protect their sensitive content from unwarranted access by unscrupulous Online Social Network users.

The foundation of the research and innovation activities will be a diligently planned inter-sectorial and interdisciplinary secondment program for Experienced and Early Stage Researchers that fosters knowledge exchange. The cooperation between industry and academia will be realized through well-coordinated/well-managed exchanges of Experienced Researchers and Early Stage Researchers between industrial and academic partners.

Figure 10. ENCASE in SignalGenerix’s website

3.6. Flyer

The Cyprus University of Technology has created a Flyer that is distributed to all the academic and administrative personnel, as well as to the attendees of conferences and workshops. Also, this flyer is available to all the students of the University and is placed in multiple points within the University, like the main building entrance, Student Well-Fair offices etc.



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.

UCL
ROMA TRE
Telefónica
Telefónica I+D
CyRIC
SCRC Social Computing Research Center
Privacy
OSN Data Analytics Software Stack (Back-End)
OSN Donated Data
Detection Rules
Intelligent Web-Proxy
Malicious behaviour detection notification
Fake identity or false information detection notification
Sensitive content detection
OSN Data / Content protection request
Sensitive Content Detection and Protection
Malicious Behavior Detection
Sensitive content notifications
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

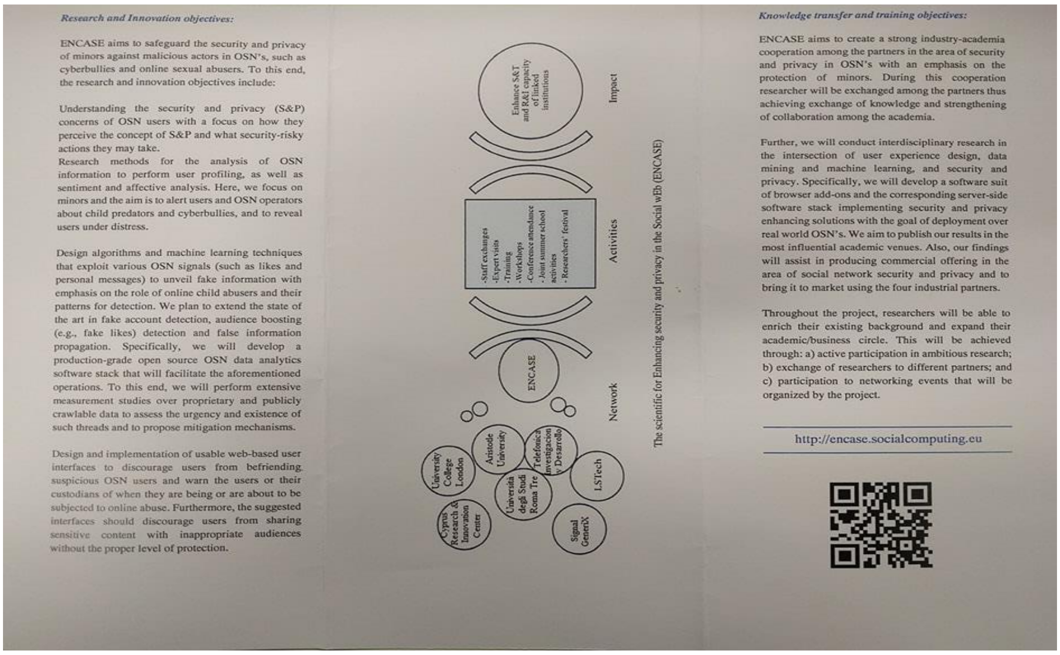
Cyprus University of Technology

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.

Figure 11. ENCASE Flyer Front Side



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.

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

http://encase.socialcomputing.eu

Figure 12. ENCASE Flyer Back Side

3.7. Participation in Events other than a Conference or Workshop

1. On March 08, 2017 Savvas Zannettou, a PhD student from the Cyprus University of Technology, covered the aspects of the clickbait problem on the YouTube platform during a talk at IMDEA premises on 08/03/17. During his talk, the participants were presented with several examples of clickbaits on the YouTube and the various misleading techniques that are used by the video uploaders. He also presented an innovative deep learning model for discerning clickbait videos in an automated manner. More information can be found here: http://netcom.it.uc3m.es/events/2017/good-bad-and-bait-detecting-and-characterizing-clickbait-videos-youtube.

2. On April 3, 2017, at the Kalamaria facilities of the Aristotle University, a presentation took place within the framework of sharing knowledge derived from the activities of the ENCASE European Marie Curie Program. More information can be found here: http://oswinds.csd.auth.gr/news/encase-cases-re-integration-secondees-%E2%80%93-sharing-knowledge.

3. On April 10, 2017, Associate Prof. Nick Bassiliades of the Aristotle University visited CUT to present a lecture on Web Information Extraction, Semantic Entity Identification and Linking. The talk covered some aspects of Web Information Extraction so that extracted entities can be uniquely identified by semantic similarity search in Web knowledge bases (a.k.a. Linked Open Data) and linked to their similar entities in these datasets. More information can be found here: http://www.cut.ac.cy/events/article/?contentId=134155 and http://www.cut.ac.cy/news/article/?contentId=134220.

4. On June 9, 2017, ENCASE participated in a Gravity Ventures speech event, hosted at CYRIC's premises with the title: “Identification of online harassment predator and victim through their chat behavior trails”. More details can be found here: http://gravity.ventures/encase-workshop-event-identification-of-online-harassment-predator-and-victim-through-their-chat-behavior-trails/

5. On September 11, 2017, ENCASE participated in a Gravity Ventures speech event, hosted at CYRIC’s premises with the title: “How Usable is Better Security or Is the World Ready for 2FA?”. More details can be found here: http://gravity.ventures/encase-workshop-event-how-usable-is-better-security-or-is-the-world-ready-for-2fa/
6. On October 10, 2017. “ENCASE vision and market applications”. A presentation to all major security vendor representatives in Cyprus for the ENCASE vision and the applicability of ENCASE within their business sector. http://gravity.ventures/encase-workshop-presentation

4. Standardization and Raising Awareness Efforts

The following organizations have been or will be contacted in order to seek ways of exploiting the results of the project.

4.1. Better Internet for Kids

Better Internet for Kids (https://www.betterinternetforkids.eu) vision, is to create a better internet for children and young people in line with the European Commission's Better Internet for Kids strategy (https://ec.europa.eu/digital-single-market/en/content/safer-internet-better-internet-kids). In more practical terms, their mission is to foster – through the BIK core service platform – the exchange of knowledge, expertise, resources and best practices between key online safety stakeholders, including industry, in order to increase access to high-quality content for children and young people, step up awareness and empowerment, create a safe environment for children online, and fight against child sexual abuse and child sexual exploitation.

4.2. Safe Internet

Safe Internet (https://www.saferinternet.org.uk/) is a partnership of three leading organisations: Childnet International, Internet Watch Foundation and SWGfL, with one mission - to promote the safe and responsible use of technology for young people. The partnership was appointed by the European Commission as the Safer Internet Centre for the UK in January 2011 and is one of the 31 Safer Internet Centres of the Insafe network.

4.3. Saferinternet.gr

Saferinternet.gr is the national representative for Greece for the Insafe network. (http://www.saferinternet.gr)

4.4. Cyber Safety

CYberSafety (https://www.cybersafety.cy) brings together major national stakeholders in order to create a safe internet culture, empowering creative, innovative and critical citizens in the digital society. CYberSafety aims to provide an awareness platform where actors can find resources and tools, share experiences, expertise and good practices. At the same time it aims to contribute towards a European approach and provide qualitative and quantitative feedback at European level, through the core service platform. The operation of the Helpline will ensure that all actors get advice and support by trained supporters/helpers in real time on issues related to their use of online technologies. The operation of the Hotline will ensure that all actors can report illegal content or actions related to illegal child sexual abuse material, racism and xenophobia. At the same time all illegal cases will be forwarded to the responsible body for action. CYberSafety will add to the existing work in Cyprus by focusing on new needs deriving from the evolvements on national and European level.

4.5. EU Kids Online

EU Kids Online (http://www.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx) is a multinational research network. It seeks to enhance knowledge of European children's online opportunities, risks and safety. It uses multiple methods to map children's and parents' experience of the internet, in dialogue with national and European policy stakeholders. It has been funded by the EC’s Better Internet for Kids programme.

4.6. UNICEF

UNICEF (https://www.unicef.gr) works to improve the policies and services that protect all children.

5. Intellectual Property Rights Management

The consortium has agreed on the following IP Protection rules, procedures, and activities:

5.1. Ownership of Results

Results are owned by the Party that generates them.

5.2. Joint ownership

The joint owners agree on the allocation and terms of exercise of their joint ownership, to ensure compliance with their obligations. Unless otherwise agreed each of the joint owners shall be entitled to use their jointly owned Results for non-commercial research activities on a royalty-free basis, and without requiring the prior consent of the other joint owner(s).

Unless otherwise agreed in the joint ownership agreement, each joint owner may grant non-exclusive licenses to third parties to exploit jointly-owned results (without any right to sub-license), if the other joint owners are given:

- at least 45 days prior notice must be given to the other joint owner(s); and
- fair and reasonable compensation must be provided to the other joint owner(s)

5.3. Transfer of Results

Each Party may transfer ownership of its own Results. A defaulting Party leaving the consortium shall transfer ownership of the entirety of each own Results to specified Parties. A non-defaulting Party leaving the consortium voluntarily shall maintain ownership of the entirety of each own Results.

Each Party may identify specific third parties it intends to transfer the ownership of its Results. The other Parties hereby waive their right to object to a transfer to listed third parties. In addition, each Party may transfer ownership of its own Results (including without limitation its share in Results that it owns jointly with another Party or Parties and all rights and obligations attached to such Results) to any of its Affiliated Entities without notification to any other Party.

The transferring Party shall, however, notify the other Parties of such transfer and shall ensure that the rights of the other Parties will not be affected by such transfer.

The Parties recognize that in the framework of a merger or an acquisition of an important part of its assets, it may be impossible under applicable EU and national laws on mergers and acquisitions for a Party to give the full 45 calendar days prior notice for the transfer.

The obligations above apply only for as long as other Parties still have - or still may request - Access Rights to the Results.

5.4. Dissemination of Results

During the Project and for a period of 1 year after the end of the Project, the dissemination of own Results by one or several Parties including but not restricted to publications and presentations, shall be governed by the procedure of Article 29.1 of the Grant Agreement subject to the following provisions.

Prior notice of any planned publication shall be given to the other Parties at least 45 calendar days before the publication. Any objection to the planned publication shall be made in accordance with the Grant Agreement in writing to the Coordinator and to the Party or Parties proposing the dissemination within 30 calendar days after receipt of the notice. If no objection is made within the time limit stated above, the publication is permitted.

An objection is justified if (a) the objecting Party's legitimate academic or commercial interests are compromised by the publication; or (b) the protection of the objecting Party's Results or Background is adversely affected. The objection has to include a precise request for necessary modifications.

If an objection has been raised the involved Parties shall discuss how to overcome the justified grounds for the objection on a timely basis (for example by amendment to the planned publication and/or by protecting information before publication) and the objecting Party shall not unreasonably continue the opposition if appropriate actions are performed following the discussion.

The objecting Party can request a publication delay of not more than 90 calendar days from the time it raises such an objection. After 90 calendar days the publication is permitted, provided that Confidential Information of the objecting Party has been removed from the Publication as indicated by the objecting Party.

A Party shall not publish Results or Background of another Party, even if such Results or Background is amalgamated with the Party’s Results, without the other Party’s prior written approval.

The Parties undertake to cooperate to allow the timely submission, examination, publication and defense of any dissertation or thesis for a degree which includes their Results or Background. However, confidentiality and publication clauses have to be respected.

Nothing in ENCASE Consortium Agreement shall be construed as conferring rights to use in advertising, publicity or otherwise the name of the Parties or any of their logos or trademarks without their prior written approval.

5.5. Complementary skills for innovation training

Apart from disciplinary and inter-disciplinary scientific skills and exposure to relevant sectors, ENCASE also places a strong emphasis on transferable complementary skills that aim to develop the ERs and ESRs to be well-rounded researchers beyond the traditional academic environment. Therefore, a package of complementary skills training programmes has been identified to provide the ERs and ESRs with necessary skills to become team leaders in academia or industry. Individual graduate courses available at each of the partner universities will be incorporated into the ESRs’ individual training plans. The ENCASE Summer School in July 2017, included a session on IPR training.

The workshop on “Entrepreneurship and innovation” will focus on the skills needed for turning technical prototypes into business ideas. Contents will include market analysis, the experience economy, writing business plans, and financing of start-ups. External speakers from our partners will be invited to give a lecture on the topic, and to have personalized discussions with the trainees. Secondly, intellectual property rights (IPR) training will be provided as part of the summer school. The project team will work with IPR consultants and European Patent Organization and its two organs (European Patent Office and Administrative Council) to provide training in the following areas: different types of IPR (copyright, patent, trademark), available legal protections, and the process of acquiring and protecting IPR.

5.6. Intellectual Property Rights (IPRs)

IPRs and patent applications will further contribute to the impact of the project. IPRs aim at stimulating innovation by temporarily restricting the use of new knowledge thus allowing its commercial exploitation by the innovating parties. A reason for the academic partners to be involved in IPRs is to make sure that the outcome of the research actually flows to society. The industrial partners will protect the achievements of the project in order to improve their own products and solutions, which could open additional business opportunities.

5.7. Plan for the Knowledge Management and Protection

The plan of ENCASE partners to exploit and commercialize the different technologies developed during the project will require a careful management of the Intellectual Properties Rights (IPR). The consortium will apply the IPR regulations for Horizon 2020 by respecting the principle of equality of all the partners towards the foreground knowledge and in full compliance with the general Commission policies regarding ownership, exploitation rights and confidentiality.

5.7.1. Background IP Ownership

Ownership of background knowledge provided by one (or several) partner(s) to the project is fully by that (those) partner(s). And then, access rights to that knowledge by a third partner must follow the general rules defined by the owner. There might be exception to this general procedure if there is any critical background item that is essential for the successful development of the project.

5.7.2. Foreground IP Ownership

The foreground IP generated by the work of a single partner will be owned by that partner. Moreover, for the foreground IP resulting from the joint work of two or more partners and in the case it is not possible to clearly establish a separation in individual pieces of the joint foreground IP provided by each partner (in which case each partner would own the IP of its piece), the foreground IP will be shared by all the contributors. This same general rule applies for inventions and patents generated during the project execution.

5.7.3. Open Source

As part of the commitment of ENCASE to contribute to the development of the European society and benefit the citizens of the member states some versions of the developed products and services will be release as open source under the applicable licenses. Note that licenses will be selected such that they do not prevent the commercialization of professional versions of the same services and products as those released as open source.

5.7.4. IPR Protection

The ENCASE partners agree that the different services, products and inventions with commercialization potential will be protected utilizing standard patenting processes.

5.7.5. Publishing Model

Following the EC’s guidelines, the scientific and industrial publications resulting from ENCASE will be made publicly available. For publication venues (journals or conference proceedings) that do not offer Open Access options, ENCASE will employ a Green Open Access strategy making the pre-print of the publication available in existing public repositories (e.g., OpenAire, ArXiv, etc) and on the project’s website.

6. Conclusion and Future Activities

During the first year of the project, the beneficiaries put a lot of effort to disseminate and communicate the project’s objectives and early results. These efforts have increased during the second year of the project resulting in reaching a wider audience and making the project and its results known to a wide industrial and academic audience, as well as to general public.

We will continue implementing our dissemination strategy throughout the project. Our future activities include but are not restricted to more publications, workshops, seminars, talks and lectures, participation in panels, articles in popular press, and appearances in TV and radio. In addition, ENCASE will participate in the H2020 project clustering event (https://www.recred.eu/news-article/170/h2020-project-clustering-event) organized in Athens on Dec 31st, where more than 16 EU funded projects will participate, present their objectives and results and share their implementation experiences.