

Newsletter/ July 2020—Issue 4

## SECONDO

# a Security ECONomics service platform for smart security investments and cyber insur- ance pricing in the beyond 2020 networking era

### PROJECT COORDINATION

**Prof. Christos Xenakis**

School of Information and  
Communication Technologies  
Department of Digital Systems  
University of Piraeus  
Karaoli and Dimitriou 80,  
PC 18534, Piraeus, Greece  
Tel: +30 210 4142776  
email: xenakis@unipi.gr

**SECONDO** consortium is still in the process while it goes through its 18th Month. During this research period, the project is editing the WP3 “Quantitative Risk Analysis and Data Analytics” with Task 3.1 “Methods for pricing tangible and intangible digital assets” and Task 3.2 “Risk modeling” has been completed. While Task 3.3 “Big data collection and processing” is a work in progress and will be delivered at the end of 28th Month.

Currently, the secondees work on an econometric module that provides estimates of all kinds of costs of potential attacks as well as costs, of each possible security control, using a set of existing econometric models.

### PROJECT DETAILS

Project number: 823997

Project Website: [secondo-h2020.eu](https://secondo-h2020.eu)

Project start: 1st January 2019

Duration: 48 Months

Total cost: EUR 1 600 800

EC Contribution: EUR 1 600 800

**SECONDO** later in the year will launch the first Workshop on September 17-18, which will take place remotely. **SECONDO** researchers work to publish technical documents in well-known conferences in high impact journals.



This project has received funding from the European Union’s H2020-MSCA-RISE-2017 program under grant agreement No 823997.



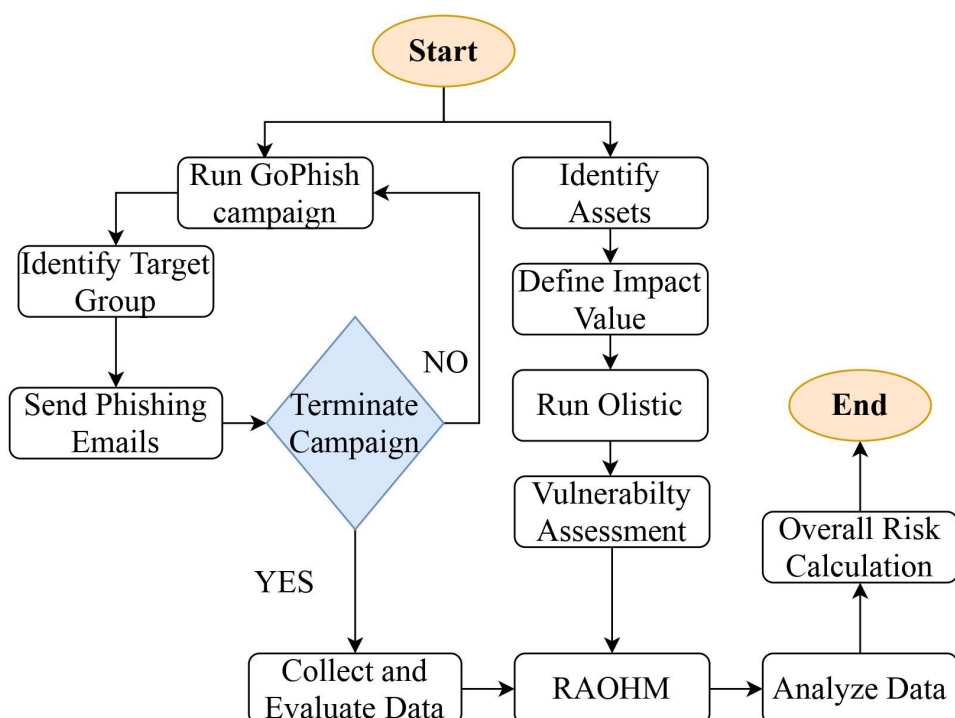
## Quantitative Risk Analysis and Data Analytics (GRAM)

GRAM provides the Metamodel Quantitative Risk Analysis which makes the cyber risk assessment in the **SECONDO** ecosystem. GRAM consists of RAOHM, SEAM, and an external risk assessment tool.

- **RAOHM**: analyzes the components of the existing risk analysis tools. Then harmonizes the data and translates it appropriately so that it can be used by GRAM.
- **SEAM**: interacts with users to invent their behavior, using penetration test approaches and provides specific numerical results for dangerous actions.
- **OLISTIC**: performs dynamically, continuously and near-real-time cyber-physical security risk assessment.

Considering the above analysis, D3.1 (Pricing Methods and Risk Modelling) uses the methods of Tasks 3.1 and 3.2, delivering an analytical report on the design, implementation, and evaluation of the various modules.

The valuation of an organization's asset is carried out considering both tangible and intangible metrics such as the cost of an asset, reputation damage, and impact on business continuity. Using the **SECONDO** risk model, we compute the lower and upper bound of the value of an asset to be used in Task 3.2 to determine the associated cyber risk from an asset.





## Use Cases: D2.1 “Technical Requirements, Business Cases and Reference Architecture”

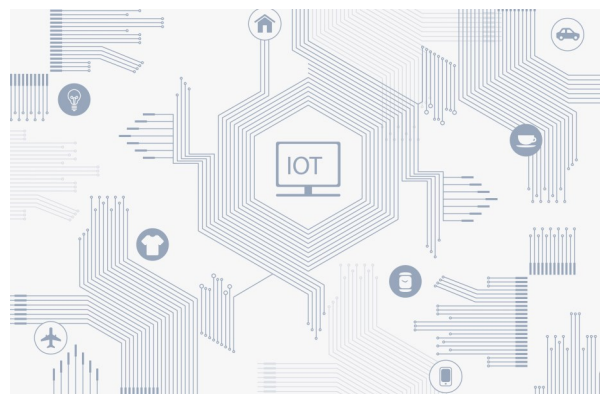
### Use Case 3 - Cyber insurance for an Innovative SME.



An innovative SME offers Business-to-Business (B2B) solutions for big data analytics and intelligent algorithms as well as professional services related to cloud computing and development. There is no physical infrastructure. The development and production environments are hosted in the Google Cloud.

### SEONDO Platform Actions

- 1) Identification and Prioritization of Assets
- 2) Asset Valuation
- 3) Social Engineering Assessment on SME Employees
- 4) Risk analysis per asset based on user behavior
- 5) Visualize and Evaluate Data



This project has received funding from the European Union’s H2020-MSCA-RISE-2017 program under grant agreement No 823997.



## NEWS AND EVENTS



**SECONDO** researchers work from home during these days

### NEW SECONDMENT FOR SAKSHYAM PANDA



### NEW SECONDMENT FOR EMILY PARSONS

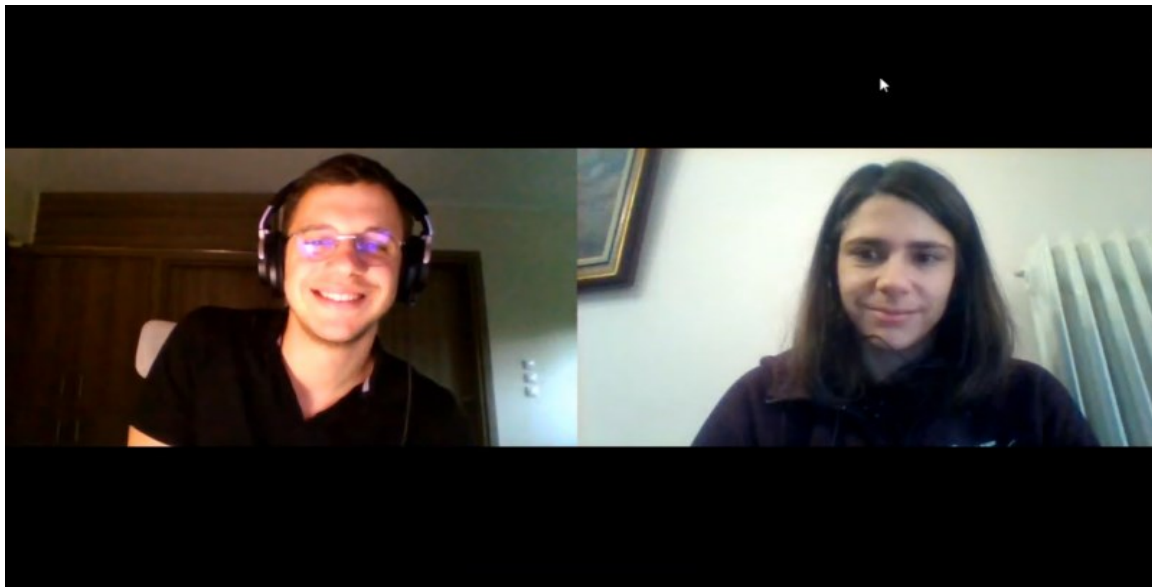
### SECONDO CONFERENCE CALL



This project has received funding from the European Union's H2020-MSCA-RISE-2017 program under grant agreement No 823997.



## NEWS AND EVENTS



### CONFERENCE CALL BETWEEN UPRC AND UBITECH ABOUT THE RAOHM



### SECONDO CONFERENCE CALL



This project has received funding from the European Union's H2020-MSCA-RISE-2017 program under grant agreement No 823997.



**cyberwatching.eu**  
The European watch  
on cybersecurity & privacy

 **SECONDO**

You can find more about the SECONDO Project at [Cyberwatching.eu](https://cyberwatching.eu) in the link <https://cyberwatching.eu/projects/1972/secondo>. More upcoming news/events so stay tuned and up to date for more information!!





## WORK IN PROGRESS ON D3.1



UPRC ON EAB CYBER MEETING



**This project has received funding from the European Union's H2020-MSCA-RISE-2017 program under grant agreement No 823997.**



## UPCOMING EVENTS



The goal of the DeSECSys workshop is to foster collaboration and discussion among cyber-security researchers and practitioners to discuss the various applications, opportunities and possible shortcomings of these technologies and their integration.

Effectively we aim to produce a collection of state-of-the-art research about emerging security technologies, their applications, their shortcomings and their verification with a focus on their uncompromised, in terms of security, safety and dependability, integration. Industry experience reports and empirical studies are also welcome.

### Topics

- Emerging security and privacy technologies and solutions
- Next-generation trustworthy computing security solutions and attacks (e.g., TPMs, TEEs, SGX, SE), and their impact
- Utilization of novel artificial intelligence and machine learning based technologies in the context of security
- Blockchain / Smart contracts for auditability and accountability
- Fog Computing
- Runtime risk assessment
- Vulnerability Analysis
- Formal Verification/Validation of design
- Advanced cryptographic techniques (e.g., homomorphic encryption, secure multi-party computation and differential privacy)
- Impact of quantum computing on cyber-security (not limited to cryptography)
- Novel attacks and protection solutions in mobile, IoT and Cloud
- Standardization of cyber security and trust techniques
- Novel schemes for Trust and Reputation in Distributed Environments
- Policy languages for advanced Access and Usage Control
- Consensus mechanisms
- Security in 5G networks

### Important Dates

**Submission deadline:** July 5th, 2020

**Notification to Authors:** August 2nd, 2020

**Camera-ready versions:** August 9th, 2020



This project has received funding from the European Union's H2020-MSCA-RISE-2017 program under grant agreement No 823997.



## During Events:

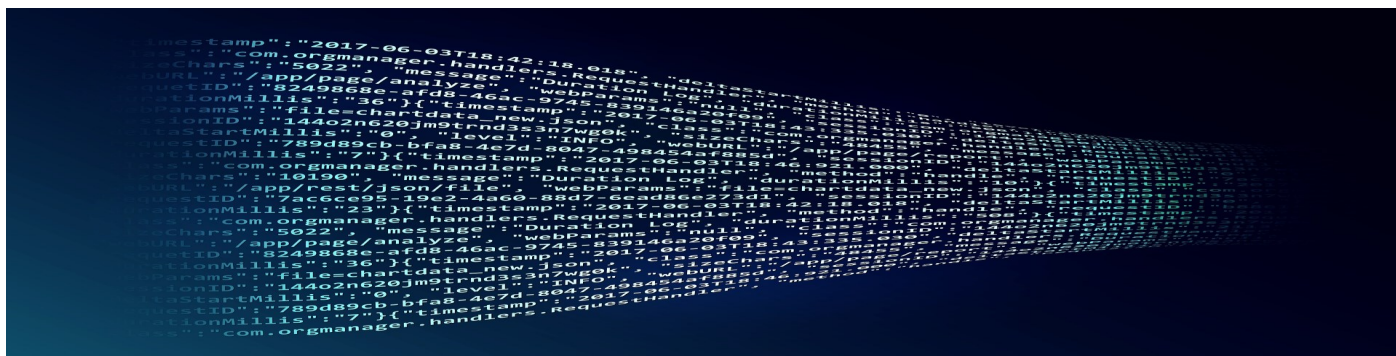
- ◆ First **SECONDO** Workshop on “DEPENDABILITY AND SAFETY EMERGING CLOUD AND FOG SYSTEMS (DESECSYS)” September 17-18, 2020

## UPCOMING DELIVERABLES

- ◆ D4.1 Econometrics
- ◆ D5.1 Cyber Insurance Market, Attributes and Sources
- ◆ D5.2 Cyber Insurance Policy Ontology



This project has received funding from the European Union’s H2020-MSCA-RISE-2017 program under grant agreement No 823997.



FOLLOW US FOR OUR LATEST NEWS

VITIS US FOR OUR LATEST NEWS

@H2020Secondo

@H2020Secondo

SECONDO Project

[www.secondo-h2020.eu](http://www.secondo-h2020.eu)



This project has received funding from the European Union's H2020-MSCA-RISE-2017 program under grant agreement No 823997.