S^2 Hack4Energy HACKATHON

A joint SPEAR-SIT4Energy event

Call for participation

Introduction

The rapid progression of the Information and Communication Technology (ICT) transforms the electrical grid into a new paradigm called Smart Grid (SG). This new reality offers valuable benefits such as distributed generation, self-monitoring, self-healing, pervasive control, two-way communication between utilities and energy consumers as well as better utilization of the existing resources. SG enables the development of smart energy-related applications, considering both efficiency potentials in the local energy production and consumption. However, at the same time, this revolution raises severe cybersecurity issues since SG is characterized by multiple heterogeneous and interconnected technologies. In this context, the SPEAR (https://www.spear2020.eu/) and SIT4Energy (https://sit4energy.eu) projects join forces towards co-organizing a hackathon event that will focus on innovative approaches on energy-related cyber-security and end-user engagement, respectively.

Date

The hackathon event will consist of 4 challenges (2 per project) and will last two days on **23-24 October 2019**.

Location

The hackathon is available online through the F6S platform. For any parties that would like to attend physically, you will be able to do so at CERTH premises (6th km Harilaou-Thermis, Thessaloniki, Greece). So get your laptop, and get ready.

Schedule

Wednesday Oct 23rd		Thursday Oct 24th	
09:00	Welcome	16:00	S^2Hack4Energy ends
09:15	Welcome from the Hellenic Cybersecurity Team *Speaker: Dr. Christos Xenakis*	16:00	Ubitech
09:25	The SPEAR Project *Speaker: Dr. Panagiotis Sarigiannidis*	16:20	Watt & Volt
09:35	The SIT4Energy Project *Speaker: Dr. Dimitrios Tzovaras*	16:40	MLS
09:45	S^2Hack4Energy Event Guidelines *Speakers: Team Leaders*	17:00	Results & Awards
11:00	S^2Hack4Energy begins		

How to join

All you have to do is to get a ticket from S^{2} Hack4Energy (www.f6s.com/s2hack4energy).

Get yourself registered! *(But first, make sure you 've read the Terms & Conditions before joining!)*

Awards

To make the day even more exciting the winners will take home several prizes:

- **1st Prize**: Dell Latitude 5501, I7-9850H/15.6 FHD/16GB/512GB SSD/Webcam/Win10 Pro, Black
- **2nd Prize**: 300,00 € Amazon Gift Card
- **3rd Prize**: MLS Prime Tablet

The winners will be announced on 24th October 2019, after the end of the competition, according to the schedule.

S^2 Hack4Energy Challenges

SPEAR Challenge #1: Visual Analytics (VA) constitutes a significant weapon of the security administrator, providing the ability to identify possible anomalies when typical security mechanisms cannot address them. It can be considered as the science of analytical reasoning dealing with data analysis problems, utilizing visual interfaces. In particular, when automated security countermeasures are not capable of recognizing malicious patterns, visualization and interaction techniques can facilitate the decision-making process, contributing significantly to the human perception and intuition. This challenge aims at developing appropriate visualization mechanisms, which will illustrate operational-data related to electricity measurements in order that the security administrator will be able to understand their normal ranges without investigating thoroughly each metric.

SPEAR Challenge #2: Modern Intrusion Detection Systems (IDS) utilize classification Machine Learning (ML) techniques in order to identify possible cyberattacks timely. A significant advantage of such IDS systems compared to conventional signature-based IDS (like Snort and Suricata) is that they are able to identify possible zero-day cyberattacks and unknown anomalies. TCP/IP network flows enclose significant features, such as the flow duration, total packets/s, the total number of bytes sent in the initial window, etc. that can be used by anomaly-based IDS. The goal of this challenge is to develop a classification model with high detection performance which will employ ML techniques in order to identify various cyberattacks, including a) brute force attacks, b) Denial of Service (DoS), c) port scanning attacks, d) botnets, and e) infiltrations. Regarding the training process, a training dataset with labelled network flows will be provided. This dataset can be used by the participants for both training and testing. On the other hand, the evaluation process will test the performance of the provided models, utilizing a different testing dataset.

SIT4Energy Challenge #1: In our mission to engage end users and change their energy consumption behavior, visualizations constitute an integral tool. They offer an overview of the energy related data and add interactivity to the implementation. If they were not easily accessible, they would be useless, which is the reason we have chosen to incorporate them in a mobile application, since mobile devices are ubiquitous. Consequently, the user is able to view his energy behavior history in a concise and interactive environment, which in turn can be influential in motivating the user to energy friendly behaviors. This challenge aims to develop an Android application, which will visualize electricity-related data, micro-moments and occupancy, in an attractive and informative way. The provided data are energy consumption measurements and occupancy data from the SmartHome in CERTH's facilities and micro-moments from a user who works in the SmartHome.

SIT4Energy Challenge #2: Providing energy related recommendations is a fitting supplement to informative visual analytics. Although informing the user is crucial for behavioural change, the timing is of equal importance, because however interesting a recommendation is, the user will discard it, if busy. The detection of micro-moments addresses this issue by pinpointing the moments in which the user is idle. The user cannot be idle if he is currently performing a dynamic physical activity, so physical activity recognition is necessary. This challenge aims to develop a Machine Learning model, which will be able to identify physical activities by utilizing the WISDM (Wireless Sensor Data Mining) dataset efficiently. The WISDM dataset includes tri-axial accelerometer data, which correspond to specific physical activity labels. More specifically, the possible physical activities include a) going downstairs, b) jogging, c) sitting, d) standing, e) going upstairs and f) walking. The participants can use the provided dataset for both training and testing. Concerning the evaluation process, a different testing dataset will be used.

Terms & Conditions

By registering and getting a ticket all participants automatically accept the terms & conditions of the S^2 Hack4Energy hackathon. The terms & conditions can be found here.

Sponsors

A huge thank you to our sponsors. Their support is crucial to make this event really amazing!

UBITECH ubiquitous solutions WATT+VOLT ELECTRICITY | NATURAL GAS MLS Making Life Simple

Supported By:

CERTH:

Dr. Dimitrios Tzovaras, Director

Dr. Dimosthenis Ioannidis

iti Information Technologies Institute

UOWM:

Dr. Panagiotis Sarigiannidis

Mr. Dimitrios Pliatsios

Mr. Panagiotis Radoglou Grammatikis

UNIVERSITY OF WESTERN MACEDONIA

Contact Details:

SPEAR challenge #1: Mr. Nikolaos Vakakis, CERTH, Thessaloniki, Greece, nikovaka@iti.gr

SPEAR challenge #2: Mr. Odysseas Nikolis, CERTH, Thessaloniki, Greece, odynik@iti.gr

SIT4Energy challenge #1: Dr. Stelios Krinidis, CERTH, Thessaloniki, Greece, krinidis@iti.gr

SIT4Energy challenge #2: Mr. Konstantinos Peppas, CERTH, Thessaloniki, Greece, kpeppas@iti.gr