



UNIVERSITÀ
DEGLI STUDI
DI PADOVA

scuolagalileiana
di studi superiori



"...i diciotto anni migliori di tutta la mia età..."

Ciclo di incontri dal titolo "IT facing-challenges"

Organizzato dagli studenti della classe di Scienze Naturali della Scuola Galileiana di Studi Superiori. Tutti gli incontri si terranno presso l'aula Magna della Scuola Galileiana di Studi Superiori, via San Massimo 33, Padova.

Mercoledì 13 marzo, dalle 18.00

The future Internet: attacks and solutions

Speaker: Dr. Eleonora Losiouk – Spritz Group

Abstract: In the past few years, an astonishing consideration is rising: the current Internet architecture has reached its end. In fact, people are using Internet mostly for retrieving contents rather than for communicating with each other. This change in the usage pattern has pushed the research community towards the design of new architectures, among which there is the Information-Centric Networking (ICN). The motivation for its potential success is given by the switch from a host-based architecture to a content-based one. Therefore, clients just send an interest for a content in the network, without knowing the IP address of the server that will reply to their request. Even if ICN has been designed with the security in mind, there are still some issues to be addressed, such as the Denial of Service (DoS) attacks and the consumer/producer privacy. The potential for ICN deployment motivated the research group lead by Prof. Conti to start working on the topic, providing novel solutions that help with addressing the attacks that affect ICN networks. During this talk Dr. Losiouk will provide an overview of the most well-known attacks in ICN (i.e., cache pollution, content poisoning and interest flooding attacks) together with the solutions designed so far by the Spritz Group.

The Android Operating System: a Double-Edged Sword for Attacks and Defences

Speaker: Dr. Eleonora Losiouk – Spritz Group

Abstract: Today almost everyone owns a smartphone and, among all the different operating systems (OS) available on the market, chooses the most comfortable one according to his needs. Android is the leading OS according to users' choices since 2010 and, as well as other mobile platforms, it provides a lot of features in addition to the standard ones (e.g., navigating the web, exploiting the localization/mapping feature, using the social media). Those functionalities, as well as many others, are among the reasons for which users bring their smartphones everywhere and use them anytime. The popularity of the Android OS, together with the availability of its source-code and development kit, has motivated attackers towards the identification of a several effective attacks. During this talk, Dr. Losiouk will provide an overview of the best contributions of the Spritz Group towards the improvement of the Android OS from a security and privacy point of view.

Mercoledì 20 marzo, dalle 18.00

An Introduction to the Blockchain and Bitcoin Payment System

Speaker: Dr. Chhagan Lal – Spritz Group

Abstract: This talk aims to provide an overview of the blockchain technology with a specific focus on the Bitcoin concurrency. In particular, this talk will touch upon the following topics:

1. What is Bitcoin?
2. How is it different from the traditional payment system?
3. What the building blocks of Bitcoin: Wallet, Miner, Blockchain?
4. What is anonymity?
5. What is a Bitcoin address? What are their characteristics?
6. What is a Bitcoin Transaction? How they spread in the network? How do transactions are verified?
7. What is double spending problem?
8. What is the distributed consensus algorithm upon which blockchain systems rely?
9. What is Proof-of-Work concept in the blockchain systems?
10. Symmetric key vs. asymmetric key encryption. Hashes and Digital signature.

Lunedì 25 marzo, dalle 18.00

The second quantum revolution

Speaker: Prof. Simone Montangero – Physics professor, Unipd

Abstract: Quantum information theory has been developed to understand and characterize the processing of information encoded in hardware that obeys the laws of quantum mechanics. Exploiting the superposition principle and quantum correlations it has been shown that information can be processed in different and sometimes more efficient ways with respect to the classical information processing capabilities.

The possible applications of quantum information range from the development of novel algorithms to solve hard problems to communications.

In the last decades, there has been an increasing effort to develop and apply quantum information theory to solve practical problems, and nowadays we are experiencing an explosion of the developments of such quantum technologies.

In this seminar, I will review the fundamental quantum mechanical concepts that enable the development of quantum technologies and present an overview of their current status in quantum communications, computations, simulations, and sensing.

La Scuola Galileiana è sostenuta dalla: