Global Initiative of Academic Networks

Course (Dec. 18 - 30, 2017)

Computer Security from the Data Science Perspective

Department of Computer Science and Engineering

Indian Institute of Technology Ropar, Punjab

MHRD Govt. of India

सत्यमेव जयते

Overview

In today's highly-interconnected digital environment, attackers are regularly wreaking havoc on software, network infrastructure and hardware that were designed without security as a primary concern. Data science includes data mining, machine learning, natural language processing and statistics. Security analytics is the adaptation of techniques from data science for security challenges such as phishing/spear-phishing, intrusion and malware prevention and detection. It has proven to be helpful in analyzing, preventing and detecting many security attacks.

This course will cover the fundamentals of computer security and data science techniques applicable to security challenges. It aims at building in confidence and capability amongst the participants in mapping the security challenges to the analytical framework and applying security analytics tools and techniques. It will be useful for those interested in security and/or in the use of data sciences in security. The participants will learn these topics through ***lectures*** and ***hands-on lab sessions***.

Foreign Faculty: Prof. Rakesh M. Verma

He is a Professor of Computer Science at the University of Houston (UH) and Director of ReDAS Lab there. He has contributed to 100+ articles, with many in leading CS conferences/journals such as EATCS ICALP, IEEE FOCS, STACS, ESORICS, ACM CODASPY, SIAM Journal on Computing, IEEE Security and Privacy, and Journal of the ACM. He is a distinguished speaker of ACM and has given over 70 invited talks in the US, UK, France, Germany, India and the Netherlands. His research is funded by several competitive grants from the US National Science Foundation, National Security Agency and Department of Defense. (webpage)

Course Modules and Topics

Fundamentals of Security: Security goals, Basics of Cryptography, Intrusions, Malware, Email and Web security, Firewalls, Software Security, and Tools for penetration testing, vulnerability analysis, cryptography and malware detection

Data Mining Techniques for Security: Data Preprocessing and Visualization, Association Analysis, Classification, Clustering, Anomaly detection with applications to credit card fraud / intrusion, and Data Mining tools.

Machine Learning Techniques for Security: Intro to ML tools with illustration-Naive Bayes, Neural Networks, SVM, Online Learning tools and their applications to security challenges. Techniques for phishing URL detection and cost-sensitive learning.

Natural Language Processing (NLP) Techniques for Security: NLP tools, Linguistic Essentials and Language Modeling, Corpus & WWW based work, Hidden-Markov Models, and Anti-phishing Semantic Techniques.

Future Directions: Attacks on machine learning models and defenses.

Who Can Attend

- Executives, engineers and researchers from IT, service and government organizations including R&D laboratories who are interested in security and/or in the use of data sciences in security.
- Faculty members and Students (Sr. B.Tech / M.Sc / M.Tech / PhD) from academic / technical institutions who are interested in security and/or in the use of data sciences in security.

Course Fee

	Early Bird Registration	After 8th Nov
Academic Institutions (Faculty)	₹ 3500	₹ 4500
Industry/R&D Organizations	₹ 4500	₹ 5500
Students (UG/PG/PhD)	₹ 2000	₹ 3000
Participants from Abroad	US$ 200	US$ 250

The fee includes instruction material, computer usage for tutorials and assignments, and internet facility.

Limited Accommodation available on payment basis (around ₹ 120 per day).

Account Name : Registrar, IIT Ropar
Account No. : 30836125653
Bank | Branch : State Bank of India | IIT Ropar, Rupnagar, Punjab
IFSC Code : SBIN0013181 **Branch Code :** 013181

One may pay online (e.g. NEFT) or by using BHIM App or send a demand draft in favor of "Registrar, IIT Ropar" payable at Rupnagar 140001, Punjab.

How to Apply

Step 0 (For those who had not registered earlier on the GIAN website) :
One time web registration at GIAN portal by making a payment of ₹ 500.
GIAN portal - http://www.gian.iitkgp.ac.in/GREGN/register

Step 1: Login at http://www.gian.iitkgp.ac.in/GREGN/index
Go to "*Course Registration*" tab
Select THIS course to register, *Save* and *Confirm* your registration.
Wait for the email from Course Coordinator regarding short-listing.

Step 2: Pay the Course Fee as applicable for you.
Email the transaction receipt details to *gian.cse@iitrpr.ac.in*
Early Bird Registration deadline - **8th Nov 2017**

Limited Seats only! Apply ASAP. Early applicants will be given preference in short-listing process.

For any query regarding this course, please email at gian.cse@iitrpr.ac.in

Organizing Institute: IIT Ropar, Punjab

The Indian Institute of Technology Ropar (IIT Ropar) is an institute of national importance established in Punjab by the Government of India in 2008. It is located in Rupnagar (around 45 kms from Chandigarh) and the city is well connected to all parts of India via rail/road/air. IIT Ropar has a vision to be a trendsetter among the technology institutes born in this millennium and it is on a steep growth path under the able-leadership of **Director** - **Prof. Sarit K. Das.** Among all engineering institutes in India, IIT Ropar ranked 9th and 21st by NIRF in 2016 & 2017, respectively.

Host Faculty and Course Coordinator

Dr. Puneet Goyal is a faculty in Dept, of Computer Sc. & Engg. at IIT Ropar. He received his Ph.D degree in 2010 from Purdue Univ., USA.
Contact: puneet@iitrpr.ac.in 01881-242309
Office # 349, CSE, IIT Ropar, Nangal Road, Rupnagar 140001, Punjab, India