

# Applied Cyber Security

## Overview

The transformation of physical systems into cyber-physical systems (CPS) by imbuing them with intelligence is an ongoing process that can substantially benefit the society and the environment by improving comfort, convenience and quality of life of the people, while reducing consumption of precious natural resources, and reducing environmental footprint. Examples of CPS include smart resource distribution systems (including electricity, water etc.), smart systems for transportation, smart living and public gathering spaces, mass health care systems, etc. and a coordinated interplay between them as in smart cities. There is a world-wide urgent need to build these systems in order to avail their numerous advantages over the traditional physical infrastructures. However, there is an inherent danger in this transformation – the very capabilities that allow for flexible control and resource optimization provide conduits for information leakage (leading to privacy violations), inadvertent misconfigurations and deliberate attacks by both outsiders and insiders (leading to malfunctioning and endangering property and lives), and interdependencies that make the systems more vulnerable. In addition, as we consider larger scale systems within the ambit of CPS, it becomes essential to consider heterogeneous scenarios with multiple control agents that need to cooperate and share data, and yet defend against the potential of malicious or disruptive behavior of one another. On the other hand, enabling intelligent control of physical systems is making its components dynamically configurable through a cyber interface. This added flexibility opens up new attack pathways and robustness concerns for the CPS. The vision of this course is to make the community aware of the security, privacy, and configuration robustness issues of cyber-physical systems from both fundamental theoretical and practical deployment perspectives. The course will cover various applied use cases of CPS across various domain and the potential security challenges of such systems. Internationally acclaimed academicians and researchers with proven knowledge, experience, and demonstrable ability in teaching, consultancy, research, and training in the field of applied cyber security will deliver lectures in the course. Furthermore, this course envisaged to inculcate development mind set of the participants especially of the students in order to build various security solutions for different and often complementary environment.

The course is organized in three modules that should be taken together. The Module A will expose the participants to information and network security fundamentals, different active and passive network attacks and protection technologies. This module will also cover web technologies and software involved attacks. The Module B will introduce applied cyber physical infrastructure such as Smart Grid AMI and SCADA network, Mass Healthcare system etc. It will also cover different state-of-art security problems in cyber-physical systems and various solutions such as, Cryptography, Data Provenance, and formal analytics tools. The Module C will introduce different Cyber Security Standards and various proactive and reactive techniques for Cyber Security Analytics and Remediation planning. It will also cover Risk Assessment, Threat Modeling and Impact Analysis methods and implementations. The participants will learn these topics through lectures, case studies and hands-on experiments.

<b>Modules</b>	<b>A: Introduction to Information and Network Security : August 5 – August 6</b> <b>B: Cyber Physical Systems Security and Forensics : August 8 – August 9</b> <b>C: Cyber Security Analytics and Remediation Planning : August 10 – August 12</b> <b>Number of participants for the course will be limited to fifty.</b>
<b>You Should Attend If...</b>	<ul style="list-style-type: none"><li>▪ you are a Computer Scientist or Electronic Engineer interested in designing tools for cyber security analytics, automation and protection.</li><li>▪ you are a student or faculty from academic institutions interested on Computer Networks and Cyber Physical Systems Security.</li></ul>
<b>Fees</b>	The participation fees for taking the course is as follows: <b>Participants from abroad : US \$500</b> <b>Industry/ Research Organizations: INR 10000</b> <b>Academic Institutions: INR 7000 (Faculties/Officials), INR 4000 (students)</b> The above fee include all instructional materials, computer use for tutorials and assignments, laboratory equipment usage charges, 24 hr free internet facility. The participants will be provided with accommodation on payment basis.

## The Faculty



**Prof. Ehab Al-Shaer**, is a Professor in Computer and Informatics and the director of the Cyber Defense and Network Assurability (CyberDNA) Center, and the director of NSF IUCRC Center on Security Configuration Analytics and Automation in University of North Carolina Charlotte, NC, USA. His research interests include security analytics and automation, configuration verification and hardening for enterprise and cloud computing, smart grid security, science of security metrics, intrusion detection, cyber agility and moving target defense.



**Prof. Sajal Das** is a Professor in Computer Science, the Daniel St. Clair Endowed Chair Professor and Chair, Dept of Computer Science, Missouri University of Science and Technology, Rolla. His research interest includes Wireless and Sensor Networks, Cyber-Physical Systems, mobile and Pervasive Computing, Smart Environments and Healthcare, Energy and Sustainability, Security and Privacy, Social Networks, Systems Biology, Distributed, Grid and Cloud Computing, Middleware Services, Applied Graph Theory and Game Theory



**Dr. Padmalochan Bera** is an Assistant Professor of School of Electrical Sciences, Indian Institute of Technology, Bhubaneswar. His research interest includes Network Security, Access Control Models, Security Configuration Synthesis, Security Automation for Cyber Physical Systems, Software Defined Networking, and Formal Verification.



**Prof. Soumya K Ghosh** is a Professor in Computer Science and Engineering, and Head, Institute Information Cell, Indian Institute of Technology Kharagpur, India. His research interest includes Spatial Informatics, Spatial Data Infrastructure, Spatial Data Mining, Cloud Computing, Cloud Security and Network Security

## Venue:

School of Electrical Science  
IIT Bhubaneswar  
Samantapuri, Bhubaneswar  
Odisha 751013

## Course Co-ordinator

**Dr. Padmalochan Bera**  
Phone: +91-674-2306307  
Mob: +91-8658578918  
E-mail: plb@iitbbs.ac.in

---

**Last Date for Registration:  
23<sup>rd</sup> July 2016 (Saturday)**