

Public Key Infrastructure (PKI) and Trust Management

Overview

Public Key Infrastructure (PKI) has played a vital role with four major components of digital security: authentication, integrity, confidentiality, and non-repudiation. As the Internet is spread out into business, government, the legal system, the military, and other areas that depend on secure communications, the need of PKI has intensified since PKI is paving the way for secure communications within organizations and on the public Internet.

Trust computing and management area has attracted many researchers, practitioners, academia and industrial people. Trust management has become popular in implementing security policies. It offers the automated verification of actions against security policies. Researchers are focusing on extending trust management for securing recent technologies viz; Social networks, Cloud computing, Internet of Things, Wireless sensor networks, Web etc.; as security is the major concerns in these technologies. However, calculating and establishing trust is a major challenge in such dynamic environments.

This course focuses on fundamental concepts of PKI, its motivation and challenges. It offers analysis of PKI standards and hands-on treatment of their implementations. It discusses security analysis and concepts of public key encryption, authentication, access control and key management through different protocols, standards and algorithms. This course then leads to participants through various trust models, trust management systems and trust based security, which will help them to understand the concept of trust and to incorporate trust mechanism in recent technologies in order to improve security. Finally, current implementations of the PKI and trust based systems will be discussed with their challenges and involved risks. The primary focus of this course will be on the fundamentals of PKI and Trust Management with their current implementations, applications, challenges and involved risks.

Modules	A: Introduction of Public Key Infrastructure (PKI): November 5, 2016 B: PKI Architectures and Standards: November 6 - 7, 2016 C: Public Key Cryptosystems: November 8 - 9, 2016 D: Trust Management: November 10 - 12, 2016 E: Application Systems on PKI and Trust Management: November 13 - 14, 2016 <i>Number of participants for the course will be limited to fifty.</i> <i>All modules are compulsory to attend</i>
You Should Attend If...	<ul style="list-style-type: none">▪ you are an executive, engineer and researcher from industry and government organizations, including R&D laboratories interested in learning of PKI and Trust Management, a growing area of information security▪ you are a student at all levels (B.Tech/M.Sc/M.Tech/Ph.D) or Faculty from the reputed academic institutions interested in pursuing research in PKI and Trust Management
Fees	The participation fees for taking the course is as follows: Participants from abroad : US \$300 Industry participants: Rs. 12000/- Academic Institutions/Research Organizations: Rs. 2,000/-(Student) & Rs. 8000/- (Others) (For SC/ST students 50% fee is waived) The above fee includes all instructional materials, computer use for tutorials and assignments, laboratory equipment usage and Internet facility.

The Faculty



Prof. Audun Jøsang is working at the Department of Informatics, Network and Distributed System (ND) Group, University of Oslo, Oslo, Norway. He is an Adjunct Professor at QUT. Prior to that he was research leader of the Security Unit at DSTC in Brisbane, worked in the telecommunications industry for Alcatel in Belgium and for Telenor in Norway. He has worked as an Associate Professor at the Norwegian University of Science and Technology (NTNU). Dr. Jøsang's research interest includes Identity Management, Trust & Reputation Management, Network Security, Security Usability and Subjective logic. His current research activities include Oslo Analytics, OffPAD, Advanced Belief Reasoning in Intelligence (ABRI), Concurrent Security and Robustness for Networked Systems (ConSeRNS), Intelligent Advice, FRISC. His past research projects include Local User-Centric Identity Management (Lucidman), Web Services Trust, Norwegian Information Security Network (NISNet).

Dr. Jøsang has received the William Winsborough Commemorative Award (2012) for the contributions to research and community building in trust management at IFIPTM. In 2011, he has received Most cited article award in the area of technology in the time window 2005-2011. He has been involved as Co-Editor, Guest Editor, Conference Chair, Track chair, Event organizer and PC Co-Chair for many reputed international journals, conferences and workshops.



Dr. Modi Chirag Navinchandra is an Assistant Professor of Computer Science and Engineering at National Institute of Technology Goa. His research interest include Information Security and Privacy, Cryptography, Cloud computing Security, Network Security, Intrusion Detection and Privacy Preserving Data Mining. He has received the Young scientist award (2015) by VIFRA, Chennai. He holds Best Paper Award (2015), from JNCA, Elsevier, San Diego, USA.



Dr. Pravati Swain is working as an Assistant Professor in the Department of Computer Science and Engineering, National Institute of Technology Goa, India. Her research interests include Analysis of high-speed communication networks, Virtual Data Center, Wireless network, Mobile computing, Stochastic process, Formal Verification.



Dr. Keshavamurthy B. N. is working as an Assistant Professor in the Department of Computer Science and Engineering, National Institute of Technology Goa, India. His research interests include Privacy preserving mining, Stream mining and Social network analysis.

Location:



National Institute of Technology Goa
Farmagudi, Ponda, Goa-403401, India

Course Duration:

Two Weeks: November 5-14, 2016

Course Coordinator

Dr. Modi Chirag Navinchandra
Contact: 0832-2404212/ 09423918821
E-mail: cnmodi@nitgoa.ac.in

.....
Course Registration Link:

<http://www.gian.iitkgp.ac.in/GREGN>
<http://www.nitgoa.ac.in/gian/>