National Workshop on
Technology Trends in Cyber Security 2018
(WORTICS 2018)
29 - 30 June 2018

WORTICS 2018

Strategy and Synergy for Security

Organised by
Society for Electronic Transactions and Security (SETS)
(A Government of India Initiative)
In association with
IEEE Computer Society, Madras Chapter
Computer Society of India, Chennai Chapter
ISACA, Chennai Chapter

ABOUT SETS

Society for Electronic Transactions and Security (SETS) is an initiative of the Central Government through the Office of the Principal Scientific Adviser (PSA) to the Government of India. SETS was established for the purpose of nucleating, sensitising and developing technologies that can protect the information wealth of the country. Such an idea to form a specialized organisation in the area of information security was conceived by Dr. A.P.J. Abdul Kalam, former President of India and was implemented in 2002 by then PSA to GoI, Dr R Chidambaram. SETS is engaged in the research areas of systems security, network security and cryptology. SETS has signed MoUs with leading institutions specialising in information security.

THEME OF THE WORKSHOP

The world is embracing ICT technologies and our nation is marching towards Digital India with increased penetration of Internet usage and smart phones resulting in growing use of Internet for financial, banking, e-Health, e-Governance, e-Commerce in the form of mobile applications. The exponential growth and use of social media has made technology as an essential part of our day to day lives. While the objectives of the use of technology for improved performance, productivity, transparency are being met, the concerns of increasing threat canvass, cyber-attacks, financial frauds is quite alarming.

The cyber fraudsters/hackers are improving their skills and developing the easy to attack tools. These negative elements are even finding the ways and means of countering the preventive security measures being deployed in the computing systems and networks. An Advanced Persistent Threat (APT) is a malware which first infiltrates a system and does long-term damage/eavesdropping silently. While Internet of Things (IoT) gave lot of flexibility with anywhere, anytime monitoring and control of various systems, in applications such as Smart Cities, Smart Grids, Smart Homes, Smart Governance etc. it has also resulted in raising the cyber-attacks exponentially.

Use of technology is inevitable. The need of the hour is to work ahead of the adversaries and provide solutions which would enhance the value and provide safe and secure operations in the midst of growing threat surface. It may be imperative to use concepts such as security by design, secure SDLC, secure software coding etc., and also use AI, Machine Learning, Game Theory ideas in providing state-of-the art cyber security solutions to prevent, respond, analyse the cyber-attacks.

This workshop aims to give bird's eye view of the technology trends happening in the present and the future Cyber security. Secure solutions and products in the areas of hardware security (PUFs: Physically Unclonable Functions, HTs: Hardware Trojans, SCA: Side-Channel Analysis); advancements in Cryptology (with focus on PQC: Post-Quantum Cryptography, QKD: Quantum Key Distribution); Network security with focus on innovative Unified Threat Management (UTM) appliance, Denial-of-Service (DoS) solutions; Game theoretic approaches; use of Big Data, Blockchain, IoT and Cloud, Artificial Intelligence (AI) and Machine Learning techniques. The talks will be delivered by experts from leading R&D labs, Academia and Industry.

WORKSHOP CONTENT

- Cyber Security Threats and Challenges
- Secure Coding & Secure SDLC
- Security by Design
- DoS Attacks Detection and Mitigation
- Game Theoretic Approaches to Cyber Security
- Hardware Security (PUFs, Hardware Trojans, SCA)
- Security using Blockchain Technology

- Big Data Security & Security Analytics using Big Data tools
- Quantum & Post-Quantum Cryptography
- Cloud and IoT Security
- AI and Machine Learning for Cyber Security / Network Traffic Analysis
- Intrusion Detection/Prevention Systems
- Host System Hardening (Windows & Linux)

SPEAKERS

- **Eminent Professors**
- **Scientists and**
- **Researchers from leading Academic and R&D institutions.**

TARGET PARTICIPANTS

- Scientists
- Engineers from R&D Labs & Industry
- Cyber Security Professionals
- System Administrators

- Network Administrators
- Faculties
- Researchers and
- Post-Graduate Students

REGISTRATION FEE

Rs. 1500/- for Students   **Rs. 3000/- for Faculties and**   **Rs. 4000/- for Others**

Number of participants is limited to 90 only. Spot registration can be done Subject to availability.

Registration fee includes workshop Kit, Working Lunch, Tea and Snacks. The Registration fee may be paid through Cheque / Demand Draft / NEFT in favour of SETS payable at Chennai.

A/C No. 430969098   Bank Name: Indian Bank   Branch: LB Road
IFSC: IDIB000L006   GST IN 33AACTS6338P1ZY

Registration fee along with registration form should be sent to the Workshop Coordinator on or before **22nd June 2018**.

Dr. R. Jothi Ramalingam
Technical Coordinator
Scientist 'C', SETS
Society for Electronic Transactions and Security (SETS)
MGR Knowledge City, CIT Campus,
Taramani, Chennai – 600 113
Mobile: 9962055208 Phone: 044 – 66632521

All communications should be addressed to:
Dr. P. Nageswara Rao
Workshop Coordinator
Society for Electronic Transactions and Security (SETS)
MGR Knowledge City, CIT Campus,
Taramani, Chennai – 600 113
Mobile: 9884143131   Phone: 044 – 66632506
Fax: 044–66632501
Email: nageswar@setsindia.net