

Webinar on IoT Security (WISE - 2022) on 30th May 2022

Inaugural function

Welcome Address: Mr. Mahesh Patil, Associate Director, C-DAC Hyderabad



Special Address: Dr. Sarat, Executive Director, SETS



Special Address: Dr. Sukumar Nandi, Senior Professor, IIT Guwahati



Inaugural Address: Dr. R Chidambaram, Chairman (Honorary) School for Advanced Studies in Nuclear Science and Technology and Former PSA to the GoI



Key Note Address: Dr. S D Sudarshan, Executive Director, C-DAC Bangalore



Vote of Thanks: Ms. A Suganya, Senior Scientist, Head of Hardware Security Research Group, SETS



TALKS



Dr. John Jose
Associate Professor,
IIT Guwahati

Title: Security Challenges in Edge and IoT devices

Abstract: IoT devices at the edge are now more intelligent and capable. Connected devices are gaining intelligence natively, and that's bringing numerous capabilities to the field and users on the move. This intelligence at the edge is bringing new capabilities but also a host of risks to the far reaches of the network. IoT practitioners need to adapt traditional methods to ensure IoT device security at the edge. At the edge, devices can gather data and deliver information in real time, without the latency constraints of sending data back and forth to the cloud. But a central trade-off is device security at the edge. As devices move from centralized architectures to the far reaches of the network, traditional security measures can become less relevant or practically impossible. There is a real opportunity to use machine learning to learn expected device behaviours out at edge and spot aberrant behaviours at scale that might correlate with security issues. This talk summarizes on a couple of such security threats and potential solutions.

Profile: Dr. John Jose is an Associate Professor in Department of Computer Science & Engineering, Indian Institute of Technology Guwahati, where he joined as an Assistant Professor in 2015. He completed his Ph.D. degree from Indian Institute of Technology Madras in the field of computer architecture. He was a rank holder in MTech degree from Vellore Institute of Technology (VIT University). He did his BTech degree from College of Engineering Adoor, Cochin University, Kerala. He is the recipient of the prestigious Qualcomm Faculty Award 2021. He is also serving as the Vice-Chair of IEEE India Council. His research group in Multicore Architecture and Systems Lab at IITG explores the domain of network on chips, cache management techniques for large multicore systems, non-volatile memories, hardware security, domain specific hardware accelerators and disaggregated storage systems. He is the associated editor for IEEE-Embedded System Letter Journal. He has over 35 IEEE & ACM peer reviewed conference publications, over 15 ACM & IEEE transactions papers as well as Springer and Elsevier journal papers to his credit. He is a reviewer for many national and international peer reviewed journals and member of technical program committee and organizing committee for many IEEE/ACM national and international conferences.

<p>Mr. Vikash Mishra, Founder, President of Myelin Innovation Pvt. Ltd.</p>	<p>Title: Drone Security</p> <p>Profile: Mr. Vikash Mishra is the Founder, President of Myelin Innovation Pvt. Ltd. Myelin Innovation Private Limited is a manufacturing firm based in Greater Noida, that develop drones through its in-house research and indigenous technology. Mr. Vikash Mishra is from Mechanical and Aerospace background and he has Massachusetts Institute of Technology, Cambridge; Florida Institute of Technology and University of Arkansas at Fayetteville to his alma mater. He was Summer Intern at CERN and Research Intern Idaho National Laboratory during his early phase of career. He has published paper in various journals and handled various project during his career.</p>
 <p>Mr. Suresh Chandra Director, STQC New Delhi</p>	<p>Title: IoT Security Standards</p> <p>Profile: Mr. Suresh Chandra is currently the Director & Head IT & eGov; Head certification body (Common Criteria); Head BDCS & QR code (Biometric device certification scheme) and Head of NCMC STQC Ministry of Electronics & IT. He pursued B.Tech in Electronics & Communications from A.M.U., Aligarh and M.B.A. From UBS, PU, Chandigarh. His Professional qualifications include "Intro' to the CMM" Course", ISMS Lead Auditor (IRCA), Common Criteria (CC) Evaluator, CSQP (Certified Software Quality Professional) and Software reliability. His work area includes Conformity assessment of e-Gov projects mainly for Functional, Performance, Security, SLA and project documentation. He is currently heading various Certification Schemes which include Common criteria certification scheme; BDCS (Biometric device certification scheme); QR code; NCMC (National common mobility card) and Trusted electronics value chain. He is involved in the Preparation of standards, framework & guidelines and part of various committees in ISO/IEC and BIS.</p>
 <p>Dr. Prem Laxman Das Senior Scientist, SETS</p>	<p>Title: Lightweight Cryptography for IoT Security</p> <p>Abstract: Ensuring authentication and confidentiality is essential for the security of IoT devices. Cryptographic primitives are used for achieving these goals in any practical network. We will discuss some cryptographic constructions that are used in this scenario. We will also discuss their efficiency and their practical relevance in a IoT network.</p> <p>Profile: Dr. Prem Laxman Das has completed his Ph.D. in Mathematics from Indian Statistical Institute. He works broadly in the domain of algorithmic aspects of algebra and</p>

	<p>number theory. In cryptology, his interests include: i) cryptanalysis of public key systems, ii) pairing-based crypto with applications to cloud computing security and iii) aspects of post-quantum cryptography. He is currently interested in understanding privacy, security and policy issues related to machine learning.</p>
 <p>Ms. Nalini Project Scientist, SETS</p>	<p>Title: Security Framework for IoT Devices</p> <p>Abstract: In recent years, the number of smart IoT devices has increased dramatically. The huge number of smart devices and the complexity of networks has made it impossible to secure the data and communication between devices. While manufacturing the IoT devices, a standardized security layer needs to be included to provide basic security. This talk explores popular attacks against IoT architecture and provides the necessary security mechanism at each layer to ensure optimal protection against cyberattacks.</p> <p>Profile: Ms. Nalini is working in Hardware Security R&D team of SETS, Chennai as a Project Scientist. She obtained her M.Tech in Digital Electronics Communication Systems from JNTU. She is a member in IETE and published papers in national and international journals. She received Sri LV Prasad Gold Medal and Pratibha Award for excellence in academics during her M.Tech. She has also received stipend from Technical Education Quality Improvement Programme (TEQIP), Government of India. Prior to joining SETS, she worked in CSIR-4PI, Bangalore. Her research interests include Hardware Security, IoT Security, Cryptography and efficient realization of secure network systems.</p>
 <p>Dr. S.V. Srikanth Joint Director, C-DAC Hyderabad</p>	<p>Title: IoT Penetration Testing</p> <p>Abstract</p> <p>An IoT device is a complex solution, with various potential entry doors for an attacker. There are three specific types of attacks on IoT devices and embedded systems such as software attacks, non-invasive hardware attacks and invasive hardware attacks. This session will familiarize you with the tools to assess, evaluate and pentest these wide range of IoT devices.</p> <p>Profile: Dr. S.V. Srikanth has been associated with C-DAC Hyderabad for the last 17+ years in the field of IoT and Embedded System Design. Currently he is designated as Joint Director. He obtained Masters in Networking and Telecom systems from UK and Ph.D. in the area of Wireless Heterogeneous Networks from JNT University, Hyderabad, India. His areas of interest include Internet of Things (IoT),</p>

	<p>Ubiquitous Computing, Wireless Technologies, Embedded System Design and Mobile Communications. He is a member of CSI SIG for IoT. He has executed around 14 projects and has published around 20 papers in various journals and conferences. He has also delivered talks in number of national workshops and conferences.</p>
 <p>Mr. Amalraj P C Project Engineer, C-DAC Hyderabad</p>	<p>Title: Exploitation of Radio Communication Protocols: Wi-Fi & BLE:</p> <ul style="list-style-type: none"> • BLE Security <p>Abstract: Bluetooth Low Energy (BLE) is becoming one of the most common wireless standards used today in IoT devices. It is also becoming more commonly used in applications where sensitive information is being transferred, security becomes more and more important. This session will cover the fundamentals of Bluetooth low energy (BLE) security including pairing, bonding & privacy.</p> <p>Profile: Amalraj P C is currently working as Project Engineer at C-DAC Hyderabad. He holds BTech in Electrical & Electronics Engineering from Govt Engineering College Barton hill, Trivandrum. He started working on embedded system design & testing since 2018 and working on IoT device Security/ Pen testing for more than a year.</p>
 <p>Mr. Mirza Abubaker Baig Project Engineer, C-DAC Hyderabad</p>	<p>Title: Exploitation of Radio Communication Protocols: Wi-Fi & BLE:</p> <ul style="list-style-type: none"> • Wi-Fi Security <p>Abstract: IoT devices are highly popular for their ability to connect to the Internet and its wireless connectivity. Therefore, Wi-Fi security plays a very important role for IoT Security. In Today's discussion we will cover the fundamentals of Wi-Fi security and how important it is for protection of IoT device security</p> <p>Profile: Mirza Abubaker Baig is currently working as Project Engineer at C-DAC Hyderabad. He holds BTech in Electronic and Communication Engineering & PG-Diploma in Embedded Systems Design. Started Working on Embedded devices since 2018 and working on pentesting of the IoT devices for more than a year in C-DAC Hyderabad.</p>



Mr. Hari Prasad R
Scientist, SETS

Title: Drone as Cybersecurity target and threat

Abstract: Drones are widely used for consumer and commercial business purposes. The talk will cover the basics of drones or Unmanned Aircraft System (UAS) security which is essential to mitigate the issues of data leakage and privacy. Counter UAS (C-UAS) measures are also being developed across the globe to prevent any attacks from adversarial drones.

Profile: Mr. Hari Prasad R is working as Scientist at SETS Chennai. He obtained BTech in Electronics and Communication from Calicut University, MTech in VLSI and Embedded Systems from CUSAT and MBA in Marketing from Pondicherry University. After a year of internship at Hardware Design Group at C-DAC Trivandrum, he worked in R&D department of ITI Limited Bangalore as Assistant Executive Engineer for four years. Then he moved to 5G and Datacentre group at VVDN Technologies at Cochin, as Senior FPGA Engineer. Currently he is working in the Hardware Security Research Group at SETS Chennai as Scientist, for the past two years. His experience includes cryptographic module implementations in FPGA, 1GE/10GE TCP/IP security and implementation of error correcting codes in FPGA for 5G. His research topic includes Cryptography, IoT security and Secure Drone design.



Mr. A. Vishnu Praveen
Project Associate, SETS

Title: Internet Key Exchange (IKE) for IoT

Abstract: Security in IP-based networks is established through Internet Protocol Security (IPsec) suite which is a collection of several protocols. One among them is Internet Key Exchange protocol (IKE) which is used for authentication and key exchange. It is often used in establishing Virtual Private Networks (VPNs). In the context of IoT security the existing protocol can be adapted to support constrained devices. This talk will cover the minimal implementation of IKE for use on constrained nodes that is interoperable with IKE version 2 (IKEv2).

Profile: Mr. A. Vishnu Praveen is part of the Hardware Security Research Group at SETS Chennai, working as Project Associate. He is post graduate in Electronics and Communication Engineering from PSG College of Technology Coimbatore and MTech Research in Photonics from IISc Bangalore and his area of interest is security in wireless communication and networks."