Press Release: BuildSEC’24 – Building a Secure and Empowered Cyberspace Successfully Concludes at IIIT-Delhi

New Delhi, India | *December 23, 2024*

BuildSEC’24, a premier cybersecurity and privacy conference, concluded on December 20, 2024, with resounding success. Held over two days at IIIT-Delhi, the event brought together leading academics, industry experts, and policymakers to address critical issues in safeguarding our increasingly digital society. Technically co-sponsored by the IEEE Society on Social Implications of Technology (SSIT), the conference emphasized collaborative and interdisciplinary approaches to building a safer and more trusted digital future.

Key Highlights

In his keynote titled *"Jailbreaking Large Language Models: Attacks and Defenses"*, **Prof. Atul Prakash from the University of Michigan** delved into the vulnerabilities of large language models (LLMs), focusing on their susceptibility to automated jailbreak attacks. Prof. Prakash reviewed the strategies behind previous jailbreak attacks and discussed how even recent LLMs with a Guard Model are still vulnerable to such attacks.

The afternoon featured interactive sessions:

Session 1: Cyberphysical Systems and Machine Learning
Innovations in secure data management and machine learning were explored, including topics such as privacy-preserving smart meter communications (NUS Singapore), privacy policy classification using LLMs (University of Sydney & UNSW, Australia), IoT camera traffic detection (BITS Pilani, India), and adversarial attacks on deep neural networks (IIT Patna, India).

Session 2: Blockchain and Organisational Security
This session highlighted blockchain’s transformative potential, discussing payment channel networks (New Mexico State University, USA), protecting EEG data with blockchain (IIT Jodhpur & IIT Gandhinagar, India), revolutionizing agricultural supply chains with blockchain (Bangladesh universities), and securing organizational data ecosystems (RWTH Aachen & Fraunhofer FIT, Germany).

Session 3: Privacy and Usability
Focused on privacy and usability, the session examined older adults’ experiences with online dating (University of Denver, USA), authentication habits in India (IIT Gandhinagar, India), accessible e-payment designs for older adults (University of Denver, USA), and privacy measures in healthcare apps for older adults (University of Denver, USA).

The day concluded with closing remarks from the **TPC chair, Dr. Sambuddho of IIIT Delhi**, who took a moment to reflect on the highlights of the day. He began by announcing the best paper award. He provided a thoughtful summary of the key discussions and sessions, and extended his sincere thanks to the speakers, session chairs, and attendees for their contributions in making the conference both highly engaging and interactive. Dr. Sambuddho also offered a preview of the upcoming day’s events, setting the stage for another productive and insightful day of the conference.

Day 2 Highlights

Day two focused on the practical aspects of implementing public digital infrastructure. The morning began with a keynote by Dr. Mainack Mondal, IIT Kharagpur, titled *"On Designing Social Norm-Grounded Privacy Preserving Systems"*. Dr. Mondal emphasized integrating technical and social perspectives to create systems that align with user-driven social norms for data collection, sharing, and storage.

Privacy Panel Discussion
Moderated by Dr. Sambuddho, the panel brought together experts to explore the intersection of privacy rights and digital freedoms. Participants included Mr. Apar Gupta, Founder and Director of Internet Freedom Foundation, India, Dr. Mainack Mondal, Dr. Abhishek Bichawat (IIT Gandhinagar), and Dr. Devashish Gosain (IIT Bombay). The discussion addressed privacy challenges from both technical and societal perspectives.

Invited Talk by Dr. Donghoon Chang, NIST and Strativia, USA & IIIT-Delhi, India
Dr. Donghoon Chang provided an overview of NIST’s work on developing the Accordion mode for block ciphers, highlighting cryptographic security enhancements in modern systems.

Keynote Session: Dr. Urbi Chatterjee, IIT Kanpur
Dr. Urbi Chatterjee’s keynote, *"The Present and Future of Hardware Security for Embedded Systems"*, discussed vulnerabilities in embedded systems like Arduino boards and Raspberry Pi, as well as emerging threats in network-on-chip architecture and machine learning accelerators.

Side-Channel Panel Discussion
Moderated by Dr. Ravi Anand, this panel explored side-channel attacks with presentations by Dr. Urbi Chatterjee, Dr. Chester Rebeiro (IIT Madras), and Col. (Dr.) Milan Patnaik, Co-Founder and CISO of Whizhack Technologies Pvt Ltd.

Other Events on Day 2

Research Report Launch
MDI Gurgaon and ISB Hyderabad presented findings from a critical report on digital safety, exploring emerging technologies and their role in shaping modern digital environments.

Keynote Address: The Cornerstones of Trust and Safety in Digital Environments
This keynote examined the foundational elements of trust and safety in the digital age, focusing on strategies and frameworks to protect users from emerging threats.

Panel 1: Emerging Technologies and Vulnerable Populations: A Security by Design Approach

Moderated by Dr. Rajiv Jain from the Intelligence Bureau, Government of India, this panel emphasized designing technology solutions that are secure and inclusive, featuring Dr. Subi Chaturvedi (InMobi Group), Samiran Gupta (ICANN), Varun Sakhuja (Mastercard), and Prof. Sanjay Jha (UNSW Sydney).

Paper Presentation

Academic and industry papers on digital security provided in-depth insights into contemporary challenges, advancing the discussion on vulnerabilities and safety in the digital ecosystem.

Panel 2: Risk Mitigation in Digital Environments

Moderated by Pradyot Chandra Haldar, President of the Policy Perspectives Foundation, this panel focused on improving grievance redressal mechanisms and trust-building in the digital age, with contributions from Bhajan Poonia (OLX India), Dr. Rakesh Maheshwari (Ministry of Electronics and Information Technology), Sudhir Sharma (Google Singapore), Dr. Aparajita Bhatt (National Law University), and Mahima Kaul (Netflix).

CyberPeace Honours and Awards

The ceremony recognized outstanding contributions to digital security, honoring eRaksha winners and CyberPeace Corps volunteers for their exceptional dedication to promoting cyber safety.

Valedictory Session by Suresh Yadav, Senior Director of the Secretariat’s Trade, Ocean & Natural Resources Directorate, The Commonwealth

The event concluded with a valedictory session by Suresh Yadav, summarizing key takeaways and reinforcing the importance of global collaboration to create safer digital spaces.

BuildSEC’24 successfully fostered collaboration and knowledge sharing across multiple sectors to address the challenges of digital security and privacy in a rapidly evolving landscape. The event’s diverse lineup of sessions, discussions, and expert contributions highlighted the need for innovative, interdisciplinary solutions to secure and empower our digital future.