21ST IBCAST – 2024

INTERNATIONAL BHURBAN CONFERENCE ON APPLIED SCIENCES & TECHNOLOGY

20–23 August,

Technical Program (Version 2.0) of

Cyber Security Track

ORGANIZED BY

Centers of Excellence in Science & Applied Technologies (CESAT), Islamabad, PAKISTAN.

IN COLLABORATION WITH

Beihang University (BUAA), Beijing (China);
Beijing Institute of Technology (BIT), Beijing (China);
Nanjing University of Aeronautics and Astronautics (NUAA), Nanjing (China);
Northwestern Polytechnical University (NPU), Xi'an, (China);
Harbin Engineering University (HEU), Harbin (China);
Shanghai Jiao Tong University (SJTU), Shanghai (China); and
Wuhan Institute of Virology (WIV), Chinese Academy of Sciences (CAS), Wuhan (China).

Program Coordinator
DR. MUREED HUSSAIN.

Deputy Program Coordinator
DR. SHIRAZ AHMAD.

TECHNICAL PROGRAM – CYBER SECURITY TRACK, 21st IBCAST-2024 (20-23 AUGUST, 2024).

(Version 2.0)

					Session-A (1600-1830 Hrs.)
Day-1: 20 Aug	**ARRIVAL ON VENUE AND CONFERENCE REGISTRATION.**	**Lunch Break: 1300-1400 Hrs.**	**CHECK-IN: 1400-1600 Hrs AND SETTLEMENT / REST.**	**Break: 1530-1600 Hrs.**	**RECITATION FROM THE HOLY QURAN, WELCOME ADDRESS** (10 Mins) **INVITED TALKS** **INVITED SPEAKER-1:** **Dr. Deniz Dahman, Dahman's Phi Services, TURKIYE.** **Topic:** The Norm Culture: To protect learning AI models against data and label poisoning attacks. (45 Mins) **INVITED SPEAKER-2:** **Dr. Qadeer Ahmed, The Ohio State University, USA.** **Topic:** Security by Design in Cyber Physical Systems. (30 Mins) **CONTRIBUTED PAPERS** **ID-93, ID-391, ID-254, ID-439, ID-187** (15 Mins Each)

	Session-B1 (0930-1100 Hrs.)		Session-B2 (1130-1300 Hrs.)		Session-B3 (1400-1530 Hrs.)		Session-B4 (1600-1830 Hrs.)
Day-2: 21 Aug	**INVITED TALK** **INVITED SPEAKER-3:** **Dr. Cihangir Tezcan, METU, TURKIYE.** **Topic:** Cryptanalysis: Theory vs. Practice. (45 Mins) **CONTRIBUTED PAPERS** **ID-412, ID-408, ID-241** (15 Mins Each)	**Break: 1100-1130 Hrs.**	**INVITED TALK** **INVITED SPEAKER-4:** **Prof. Dr. Jian Wei Liu, Beihang University, CHINA.** **Topic:** Key Technologies for Satellite Internet Security. (40 Mins) **CONTRIBUTED PAPERS** **ID-26, ID-14, ID-420** (15 Mins Each)	**Break: 1300-1400 Hrs.**	**TECHNICAL WORKSHOP-1** (120 Mins) **WORKSHOP TRAINER-1:** **Dr. Cihangir Tezcan, METU, TURKIYE.** **Topic:** Optimization of Symmetric Cryptography Algorithms on GPUs.	**Break: 1530-1600 Hrs.**	**INVITED TALK** **INVITED SPEAKER-5: Mr. Evgeny Goncharov, Kaspersky, RUSSIA.** **Topic:** Hacktivism, Ransomware, APT – Top cyber threat domains for OT environments, transportation and industrial infrastructures. (30 Mins) **TECHNICAL WORKSHOP-2** (120 Mins) **WORKSHOP TRAINER-2:** **Dr. Deniz Dahman, Dahman's Phi Services, TURKIYE.** **Topic:** Simulation of "The Norm Culture" (Demonstration of attack on an AI model during the continuous learning pipeline process and prevention against such an attack).

	Session-C (0930-1200 Hrs.)	
Day-3: 22 Aug	**INVITED TALKS** **INVITED SPEAKER-6: Dr. Abid Rauf, UET Taxila, PAKISTAN.** **Topic:** Zero-Knowledge Proofs and Their Applications in Cybersecurity. (30 Mins) **INVITED SPEAKER-7: Dr. Muhammad Hanif Durad, PIEAS, PAKISTAN.** **Topic:** Zero Trust Architecture: The Future of Cyber Security. (30 Mins) **INVITED SPEAKER-8: Dr. Syed Nasir Mehmood Shah, KICSIT, IST, PAKISTAN.** **Topic:** Shadow IT and Insider Threat: A Dangerous Combination. (30 Mins) **CONTRIBUTED PAPERS** **ID-104, ID-409, ID-50, ID-312** (15 Mins Each)	**CONFERENCE CLOSING** **CHECK-OUT: 1200 Hrs.**

TECHNICAL PROGRAM – CYBER SECURITY TRACK, 21st IBCAST-2024 (20-23 AUGUST, 2024).

DAY-1: 20 AUGUST, 2024.

	Time (Hrs)		TOPIC	SPEAKER
SESSION-A	1600-1610		**RECITATION FROM THE HOLY QURAN** **WELCOME ADDRESS AND CONFERENCE OPENING REMARKS**	**DR. MUREED HUSSAIN – PAKISTAN.** Program Coordinator, Cyber Security Track. **DR. SHIRAZ AHMAD – PAKISTAN.** Deputy Program Coordinator, Cyber Security Track.
	1610-1655		**INVITED TALK-1: The Norm Culture: To Protect Learning AI Models against Data and Label Poisoning Attacks.**	**DR. DENIZ DAHMAN – TURKIYE.** AI Developer & Independent Researcher, Self-Employed – DAHMAN'S PHI SERVICES, ISTANBUL, TURKIYE.
	1655-1725		**INVITED TALK-2: Security by Design in Cyber Physical Systems.**	**DR. QADEER AHMED – USA.** The Ohio State University, USA.
	1725-1740	**ID-93**	**AI-Driven APT Detection Framework: Early Threat Identification Using ML**	**Hidayat Ur Rehman,** Air University, Islamabad, PAKISTAN.
	1740-1755	**ID-391**	**Machine Learning-Based Anomaly Detection for MITM Attack Identification in Cloud Computing Infrastructures**	**Adnan Shahbaz,** The Millennium Universal College, PAKISTAN.
	1755-1810	**ID-254**	**A Password Strength Classifier using Supervised Machine Learning**	**Nida Khalid,** Military College of Signals (MCS), NUST, Rawalpindi, PAKISTAN.
	1810-1825	**ID-439**	**Anomaly Detection in HTTP Logs: Leveraging Machine Learning for Uncovering Anomalous Traffic Patterns with SIEM Integration**	**Waqas Ahmad,** Military College of Signals (MCS), NUST, Rawalpindi, PAKISTAN.
	1825-1840	**ID-187**	**Optimizing Distributed Denial of Service (DDoS) Attack Detection Techniques on Software Defined Network (SDN) using Feature Selection**	**Inamul Haq,** Karachi Institute of Economics and Technology, Karachi, PAKISTAN.
SESSION AND DAY CLOSING				

TECHNICAL PROGRAM – CYBER SECURITY TRACK, 21st IBCAST-2024 (20-23 AUGUST, 2024).

DAY-2: 21 AUGUST, 2023.

	Time (Hrs)	TOPIC		SPEAKER
SESSION-B1	0930-1015	**INVITED TALK-3: Cryptanalysis: Theory vs. Practice.**		**DR. CIHANGIR TEZCAN – TURKIYE.** Director of Cyber Security Center, METU, ANKARA, TURKIYE.
	1015-1030	**ID-412**	**The Effect of Affine and Extended Affine Equivalence Class Against Various Cryptographic Profile**	**Ijaz Khalid,** CESAT, Islamabad, PAKISTAN.
	1030-1045	**ID-408**	**A Post Quantum Light Weight Cryptographic Algorithm over Quaternion Integers**	**Tanveer Ul Haq,** CESAT, Islamabad, PAKISTAN.
	1045-1100	**ID-241**	**A Secure and Distributed Decision Based Handover Scheme for LEO Satellites in 6G Internet**	**Muhammad Arshad,** School of Cyber Science and Technology, Beihang University, Beijing, CHINA.
TEA BREAK: 1100-1130 Hrs.				
SESSION-B2	1130-1210	**INVITED TALK-4: Key Technologies for Satellite Internet Security.**		**JIAN WEI LIU – CHINA.** School of Cyber Science and Technology, Beihang University, Beijing, CHINA.
	1210-1225	**ID-26**	**Exploit Mitigations : A Call for Enhanced Windows Memory Protection**	**Moiz Abdullah,** Air University, Islamabad, PAKISTAN.
	1225-1240	**ID-14**	**An Efficient Smart Contract-Enabled Blockchain Framework for Data Sharing in Cloud based IoT Systems**	**Attiq Ur Rehman,** UMT, Lahore, PAKISTAN.
	1240-1255	**ID-420**	**Leveraging Occlusion Sensitivity for Malicious Code Localization**	**Dr. Muhammad Rizwan,** CESAT, Islamabad, PAKISTAN.
LUNCH & PRAYER BREAK: 1300-1400 Hrs.				
B3	1400-1600	**TECHNICAL WORKSHOP-1: Optimization of Symmetric Cryptography Algorithms on GPUs.**		**DR. CIHANGIR TEZCAN – TURKIYE.** Director of Cyber Security Center, METU, ANKARA, TURKIYE.
TEA BREAK: 1530-1600 AND 1730-1800 Hrs.				
SESSION-B4	1600-1630	**INVITED TALK-5: Hacktivism, Ransomware, APT – Top cyber threat domains for OT environments, transportation and industrial infrastructures.**		**MR. EVGENY GONCHAROV – RUSSIA.** HEAD ICS CERT, Kaspersky, RUSSIA.
	1630-1830	**TECHNICAL WORKSHOP-2:** **Simulation of "The Norm Culture" (Demonstration of attack on an AI model during the continuous learning pipeline process and prevention against such an attack).**		**DR. DENIZ DAHMAN – TURKIYE.** AI Developer & Independent Researcher, Self-Employed – DAHMAN'S PHI SERVICES, ISTANBUL, TURKIYE.
DAY CLOSING				

TECHNICAL PROGRAM – CYBER SECURITY TRACK, 21st IBCAST-2024 (20-23 AUGUST, 2024).

DAY-3: 22 AUGUST, 2023.

	Time (Hrs)	TOPIC		SPEAKER
SESSION-C	0930-1000	**INVITED TALK-6: Zero-Knowledge Proofs and Their Applications in Cybersecurity.**		**DR. ABID RAUF – PAKISTAN.** UET Taxila, PAKISTAN.
	1000-1030	**INVITED TALK-7: Zero Trust Architecture: The Future of Cyber Security.**		**DR. HANIF DURAD – PAKISTAN.** Head Information System Security Group, CIPMA Lab, DCIS, PIEAS, PAKISTAN.
	1030-1100	**INVITED TALK-8: Shadow IT and Insider Threat: A Dangerous Combination.**		**DR. SYED NASIR MEHMOOD SHAH – PAKISTAN.** KICSIT, IST, PAKISTAN.
	1100-1115	**ID-104**	**IMA- An Intelligent Obfuscated Malware Analysis Model**	**Abrar Ahmad,** CEME, NUST, Islamabad, PAKISTAN.
	1115-1130	**ID-409**	**Assessing Concept Drift in Malware: A Comprehensive Analysis**	**Ezza Ali,** CESAT, Islamabad, PAKISTAN.
	1130-1145	**ID-50**	**Malware Identification: A Benign File Synthesizer Using GANs**	**Asad Mehmood,** PIEAS, Nilore, Islamabad, PAKISTAN.
	1145-1200	**ID-312**	**Unveiling Android Malware Behavior: A Hybrid Approach for Comprehensive Analysis and Classification**	**Sheikh Muhammad Zeeshan Javed,** CESAT, Islamabad, PAKISTAN.
DAY CLOSING AND CHECKOUT: 1200 Hrs.				

DAY-4: 23 AUGUST, 2023.

CONFERENCE CLOSING CEREMONY – BY INVITATION ONLY.

INVITED SPEAKERS &

WORKSHOP TRAINERS

(FOREIGN / LOCAL)

DENIZ DAHMAN, PHD.

AI Developer specializing in Data Science and Machine Learning,
Independent Researcher | Self Employed,
Istanbul,
TURKIYE.

BIOGRAPHY:

Deniz Dahman, a Senior AI Developer, Data Scientist, and Inventor, boasts over 18 years of experience in management and information technology. His areas of expertise encompass the application of AI problem-solving techniques across social science research, business development, financial product solutions, and R&D in diverse industries. With his extensive interdisciplinary background, he has achieved success in both the industrial and academic sectors. Through his initiative, **Dahman's Phi Services,** Deniz assists organizations in adopting AI problem-solving methodologies, thereby improving their business processes, efficiency, and innovation. The initiative also provides support and supervision for research conducted by undergraduates, postgraduates, and scholars. **His current research focuses on two main areas:** *crafting a comprehensive guide for the implementation of AI solutions and fortifying the data privacy and security of AI models against various threats.* Deniz has developed numerous algorithms and penned 'The Big Bang of Data Science—from Academia to Industry.' He has a wealth of peer-reviewed scientific publications, drafts, and media presentations to his name. His peers acknowledge him as analytical, inventive, goal-driven, and profoundly humanitarian.

TITLE OF THE TALK:

The Norm Culture: To Protect Learning AI Models against Data and Label Poisoning Attacks.

ABSTRACT:

This talk presents a method **to protect learning AI models against data and label poisoning attacks;** *The Norm Culture method* posits that each class **in an image classification problem** possesses an inherent structure that serves as a primary defense against attacks—such as data or label poisoning—that can corrupt new training and testing samples during the parameter update phase of an AI predictive model within a conventional deep learning framework. The method requires calculating three elements from the essential training and testing samples. The first element is the flattened matrix representing the class image. The second element is the class alpha, a scalar that represents the weight norm of the class. The final element is the most recently validated AI predictive model. The experimental outcomes on a binary class image classification dataset from health domains indicate that the proposed method effectively identifies training and testing sample images compromised by either type of attack one or two. Additionally, there is potential for enhancing the method within the mathematical functions of the AI framework.

TITLE OF THE WORKSHOP:

Simulation of "The Norm Culture" (Demonstration of attack on an AI model during the continuous learning pipeline process and prevention against such an attack).

WORKSHOP BRIEF OUTLINE / CONTENTS:

1. Walking through the case study simulation storyline,
2. Setting up the lab and simulating the workflow,
3. Reviewing initial AI prediction results before an attack,
4. Simulating two types of AI model attacks using the "attackai 1.0.0" Python package,
5. Examining the results after the attack,
6. Implementing the "Norm Culture" security layer using the "protectai 1.0.0" Python package,
7. Analyzing the results after integrating the security layer,
8. Discussion on the future enhancement of method,
9. Engaging in an open discussion.

Further details related to the project are available online.

1. https://www.scienceopen.com/hosted-document?doi=10.14293/PR2199.000907.v1
2. https://dahmansphi.com/2024/06/27/the-norm-culture-advocates-for-the-introduction-of-a-security-layer-in-continuously-learning-ai-models-to-protect-against-data-and-label-poisoning-attacks/

ATTACK AI TOOL for ATTACK AI MODEL SIMULATION:

1. Test tool to simulate two types of poisoning attack on AI model is available at: https://github.com/dahmansphi/attackai
2. ATTACK AI TOOL related documentation and downloadable code repositories are available at: https://pypi.org/project/attackai/

PROTECT AI TOOL for PROTECT AI MODEL SIMULATION:

1. Test tool to simulate defense from poisoning attack on AI model is available at: https://github.com/dahmansphi/protectai
2. ATTACK AI TOOL related documentation and downloadable code repositories are available at: https://pypi.org/project/protectai/

DR. CIHANGIR TEZCAN,

Director of Cyber Security Center,
Head of Department of Cyber Security, Informatics Institute,

Middle East Technical University (METU),
Ankara,
TURKIYE.

BIOGRAPHY:

Dr. Cihangir Tezcan is a prominent academician in the field of cryptography. He earned his Master's and Doctoral degrees in Cryptography from the Institute of Applied Mathematics, Middle East Technical University (METU) in 2009 and 2014, respectively. Dr. Tezcan is a leading figure in Turkish cyber security academia, currently holding the positions of Head of the Department of Cyber Security and Director of the Cyber Defense and Security Research Center at METU. Prior to his tenure at METU, he served as a teaching assistant at the prestigious École Polytechnique Fédérale de Lausanne (EPFL) in Switzerland and as a postdoctoral researcher at Ruhr-Universität Bochum in Germany. His research interests encompass a broad spectrum of cyber security and cryptographic domains, including: cryptanalysis, quantum cryptography, wireless communications security, blockchain and cryptocurrency technologies, parallel computing, randomness, number theory, probability theory, algebraic geometry, GPU computing, and algebraic number theory.

TITLE OF THE TALK:

Cryptanalysis: Theory vs. Practice.

ABSTRACT:

Many cryptanalysis results are obtained theoretically and they are not verified since they have huge time, memory, or data complexities. Moreover, it is not a common practice to experimentally verify the reduced versions of these results. The probability of the theoretically obtained distinguishers might be different in practice and this affects the time, memory, and data complexities of the attacks that use these distinguishers. We used the parallelism and the computation power of the GPUs to experimentally verify theoretical cryptanalysis results. We observed that some attacks on symmetric key encryption algorithms require more time, memory, and data complexities in practice. Finally, our bitsliced implementation of ASCON and SERPENT allowed us to find the best distinguishers that we could not obtain theoretically by known methods and showed that theoretically obtained best distinguishers have better probabilities in practice. In this talk I am going to explain our optimizations and results.

TITLE OF THE WORKSHOP:

Optimization of Symmetric Cryptography Algorithms on GPUs.

ABSTRACT / SYNOPSIS:

Parallel computing power of GPUs can be used to optimize symmetric key encryption algorithms and these efficient implementations can be used to obtain fast encryption, perform brute force attacks on short keys, and verify theoretical results in practice. We can implement these algorithms generally in three ways: naïve, table-based, and bitsliced. In our recent works, we optimized 3DES, AES, ASCON, CRYPTO1, DES, and PRESENT algorithms for GPUs. By implementing CRYPTO1 in a bitsliced manner, we reduced the time required for offline attacks to clone Mifare Classic cards from months to hours. Our table-based implementation of AES-128 achieves 878.6 Gbps in counter mode on an RTX 2070 Super GPU which is 4.087 Gbps per Watt. Our table based optimizations provides 3.87 billion keys searches for DES and 3DES and 1.89 billion key searches per second for PRESENT. This result shows that 20 million RTX 3070 GPUs can capture an 80-bit PRESENT key in a year. In this Workshop I am going to explain our optimizations and results.

PROF. DR. LIU JIANWEI,

Professor and Dean,
School of Cyber Science and Technology,
Beihang University,
Beijing, China.

BIOGRAPHY:

Dr. Jianwei Liu received his Ph.D in communication engineering from Xidian University, China in 1998, and his B.S. and M.S. degrees in electronic engineering from Shandong University, China in 1985 and 1988. He is currently a professor and dean of School of Cyber Science and Technology, Beihang University. His current research interests include cryptographic protocol design, wireless and mobile network security, space-air-ground integrated network security, and 5G network security. He has published 6 books and nearly 200 papers in his research fields. He is a senior member of the Chinese Institute of Electronics and director of the Chinese Association for Cryptologic Research. He has been awarded the first prize of technological invention of China.

TITLE OF THE TALK:

Key Technologies for Satellite Internet Security.

ABSTRACT:

TBA.

EVGENY GONCHAROV,

Head of Kaspersky Industrial Control Systems (ICS) Cyber Emergency Response Team (CERT),
Kaspersky,
Leningradskoe Shosse, Moscow,
Russian Federation.

BIOGRAPHY:

Evgeny Goncharov has worked in software development since 1999, with 18 years' experience in the IT Security industry. Evgeny joined Kaspersky Lab in 2007 as software development team lead. Since then, he has worked on notable projects such as leading the Kaspersky Lab team at Sochi 2014 Olympic Games to protect their critical IT infrastructure from malware and targeted attacks. Since 2014, Evgeny has driven Kaspersky Lab's ICS cyber security research, product and services development. He is currently the Head of Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT).

TITLE OF THE TALK:

Hacktivism, Ransomware, APT – Top cyber threat domains for OT environments, transportation and industrial infrastructures.

ABSTRACT:

Different factors are influencing cyberthreat landscape for OT environments and industrial enterprises. From one hand, we see that the investments in IT and OT cybersecurity are working as they should that results in flattening the peaks of cyberthreat exposure of OT infrastructures in the hottest regions of the World. From the other hand we witness a qualitative leap in the hacktivists' attack severity – again and again they demonstrate an ability to reach out to OT systems, and more and more often – with a non-zero consequences to the attacked facility. The ransomware gangs keep reminding of themselves as of the TOP 1 severity threat for the industrial enterprises, here and there causing denials of operation and shipment, making $ hundred million damages and killing businesses. And no one should forget of APT actors, that are capable of building a devastating attack scenario based on their deep presence in the industrial enterprise infrastructure, telecom compromise and sophisticated supply chain infiltration – that are becoming especially possible as soon as the international relations run in an instability phase.

In my presentation I'll be talking about our OT telemetry analysis results, I will recall some recent attack cases that have been publicly disclosed and couple ones that our team investigated and have not disclosed yet. I'll be also talking on some of the OT and transportation products and the underlying technologies systematic security problems we identified in course of our vulnerability research projects that allow us to make a futuristic predictions on the shifts the sophisticated attack targeting may have should the conditions be met, which are not so impossible.

DR. QADEER AHMED,

Assistant Professor,
Department of Mechanical and Aerospace Engineering,
The Ohio State University,
Columbus, Ohio,
United States.

BIOGRAPHY:

Dr. Qadeer Ahmed has a decade-long research experience in smart mobility, energy-efficient vehicles, vehicular cyber security, and safety. He completed his BS in Mechatronics Engineering from UET Lahore, and his MS and PhD from Muhammad Ali Jinnah University. He is now an Assistant Professor at the Department of Mechanical and Aerospace Engineering at The Ohio State University. He also holds courtesy appointments with OSU's Departments of Electrical and Computer Engineering and Integrated Systems Engineering. He is also a fellow of OSU's Center for Automotive Research. He is a recipient of SAE's Ralph R. Teetor Educational Award in 2023, SAE's L. Ray Buckendale Award in 2019, and OSU's Lumley Research Award in 2018.

TITLE OF THE TALK:

Security by Design in Cyber Physical Systems.

ABSTRACT:

Cyber Physical Systems are increasingly becoming connected and automated to offer a variety of options including comfort, safety, and efficiency. However, alongside these benefits come potential risks, particularly in safety and cyber security. These risks may stem from technical vulnerabilities in the hardware and software due to the complexity required for deploying connected and autonomous features.

This presentation will delve into these critical issues, focusing on the unresolved cyber security issues in connected and automated vehicles. The talk will emphasize the importance of security by design by looking at optimal placement sensors for detecting the cyber-attacks based on the behavioral model of the system. Moreover, the talk will cover a method for analyzing the security implications of automotive systems, including designing robust residuals for attack detection, even with limited knowledge of the underlying dynamics.

DR. MUHAMMAD HANIF DURAD,

Associate Professor /Deputy Chief Scientist,
Department of Computer & Information Sciences (DCIS),
Pakistan Institute of Engineering & Applied Sciences (PIEAS),
P.O. Nilore, Islamabad, Pakistan.

BIOGRAPHY:

Dr. Muhammad Hanif Durad, did his M. Sc. Physics from Govt. College University Lahore in 1990. During his undergrad studies, he won the district government Merit Scholarship and Certificate of Merit from Government College University Lahore. In 1994, he did his M.S. in Systems Engineering from Pakistan Institute of Engineering & Applied Sciences (PIEAS) and joined Computer Division, PINSTECH where he worked on various projects related to computer interfacing, network deployment and development. In April 2003, he joined PIEAS faculty from where he won the HEC merit scholarship for PhD studies abroad. He completed his PhD. from Beijing Institute of Technology (BIT), P.R. China in July 2007.

He is heading Cyber Security group and is also Incharge of Critical Infrastructure Protection and Malware Analysis Lab, the constituent part of National Center for Cyber Security, Pakistan. He is reviewer of many reputed journals and international conferences. He has authored more than 66 papers in internationally reputed peer-reviewed journals and conferences. His research interests include Network Security, Cryptography, Embedded System Security, Industrial Control system Cybersecurity, Cluster/ Grid/ Cloud/ Fog computing.

TITLE OF THE TALK:

Zero Trust Architecture: The Future of Cyber Security.

ABSTRACT:

In an era where cyber threats are more sophisticated and pervasive than ever, traditional security models based on perimeter defenses are proving insufficient. The rise of cloud computing, remote work, and mobile devices has dissolved the clear boundaries that once protected enterprise networks, making the need for a more robust security framework critical. Enter Zero Trust Architecture (ZTA), a paradigm shift in cybersecurity that operates on the principle of “never trust, always verify.”

This talk will cover foundational concepts of Zero Trust, emphasizing its departure from legacy approaches and its relevance in today’s dynamic threat landscape. Attendees will gain insights into the core components of ZTA, including continuous authentication, least privilege access, and micro-segmentation, and understand how these elements work together to create a resilient security posture. The talk will also cover practical steps to implement Zero Trust in various organizational contexts, common challenges, and future implications of this as it becomes a new standard. Whether you are a cybersecurity professional, IT manager, or business leader, this session will equip you with the knowledge and strategies needed to safeguard your digital assets in an increasingly complex and hostile environment.

DR. ABID RAUF,

Faculty Member,
Department of Computer Science,
University of Engineering and Technology (UET),
Taxila, Pakistan.

BIOGRAPHY:

Dr. Abid Rauf is a faculty member in the Computer Science department at UET Taxila. He holds PhD degree in Computer Sciences from School of Electrical Engineering & Computer Science (SEECS), National University of Sciences and Technology (NUST), Islamabad. He has completed MS in Information Security from Sichuan University, Chengdu, China and MSc Statistics from Quaid-e-Azam University, Islamabad. He specializes in Security, Algorithm Design and Analysis, Information Theory, Formal Methods, and Statistical Methods in Data Science. His research interests also include Information Security and Internet of Things (IoT).

TITLE OF THE TALK:

Zero-Knowledge Proofs and Their Applications in Cybersecurity.

BRIEF OUTLINE:

- Introduction to Zero-Knowledge Proofs
- Fundamental Principles of Zero-Knowledge Proofs
- Cryptographic Foundations
- Applications of Zero-Knowledge Proofs in Cybersecurity
    - Authentication
    - Privacy-Preserving Transactions
    - Data Integrity and Confidentiality
    - Regulatory Compliance
- Real-World Use Cases
    - Crypto-currencies and Blockchain
    - Secure Voting Systems
    - Access Control Systems
- Implementation Challenges and Considerations
- Future Trends and Developments
    - Advancements in zk-SNARKs and zk-STARKs
    - Integration with Emerging Technologies
- Hands-On Session
    - Demo of Zero-Knowledge Proof Tools – Optional

DR. SYED NASIR MEHMOOD SHAH,

Head of Academics, KICSIT Campus,
Institute of Space Technology,
Islamabad, Pakistan.

BIOGRAPHY:

Dr. Syed Nasir Mehmood Shah earned his PhD in Information Technology from Universiti Teknologi PETRONAS, Malaysia in 2012. Presently, he is serving as Associate Professor in the department of Computer Sciences at KICSIT Campus, Institute of Space Technology, Islamabad, Pakistan. His research interest include Cyber Security, Cloud Computing, Grid Computing and Information Systems. He has published around 44 research papers in peer-reviewed conferences; quality journals and book chapters. He remained Conference Secretary for Annual Computational Science Conferences 2013-2015; and playing very active role in the development of Science and Technology at Pakistan.

TITLE OF THE TALK:

Shadow IT and Insider Threat: A Dangerous Combination.

ABSTRACT:

Shadow IT is a phenomenon where employees utilize hardware, software, or other technological solutions within an organization without the formal approval of the IT department.

The convergence of shadow IT and insider threats presents a significant challenge to effective organizational security. As employees increasingly adopt emerging technologies such as cloud collaboration tools, BYOD, IoT devices, blockchain applications, and AI-driven platforms without formal IT approval, they result in security gaps, which can be exploited by insiders. Shadow IT increases the organization's attack surface, complicating the ability of traditional security controls to monitor, manage, and defend against emerging threats, attacks and vulnerabilities.

This talk would address about major compliance frameworks, which discuss the concept of shadow IT and the importance of managing its security risks. This talk would also highlight how emerging technologies contribute to the growing risks of shadow IT and insider threats, and how organizations could deploy strategic controls such as Secure Computing Framework, Data Loss Detection and Prevention tools, and Zero Trust Architecture to ensure robust security implementation in organization. By understanding and mitigating the risks associated with these technologies, organizations can protect their critical infrastructure and maintain resilience in an increasingly complex digital landscape.