TECHNICAL PLAN – CYBER SECURITY TRACK, 20th IBCAST-2023 (22-25 AUGUST, 2023).

					Session-A (1600-1830 Hrs.)
Day-1: 22 Aug	**ARRIVAL ON VENUE,** **CONFERENCE REGISTRATION,** **AND CHECK-IN: 1200 Hrs.**	**Lunch Break: 1300-1400 Hrs.**	**SETTLEMENT AND REST**	**Break: 1530-1600 Hrs.**	**WELCOM ADDRESS** (10 Mins) **INVITED TALKS** **Speaker: Mr. Evgeny Goncharov, Kaspersky, RUSSIA.** (40 Mins) **Topic:** What to be Afraid of, what to fight, and what to sacrifice. A look at the current security challenges of industrial enterprises. **Speaker: Dr. Saad Islam, CESAT, PAKISTAN.** (40 Mins) **Topic:** Post Quantum Cryptography. **CONTRIBUTED PAPERS** **ID-493, ID-424, ID-142** (15 Mins Each)

	Session-B1 (0930-1100 Hrs.)		**Session-B2 (1130-1300 Hrs.)**		**Session-B3 (1400-1530 Hrs.)**		**Session-B4 (1600-1730 Hrs.)**		**Session-B5 (1800-1930 Hrs.)**
Day-2: 23 Aug	**INVITED TALK** **Speaker: Mr. Evgeny Goncharov, Kaspersky, RUSSIA.** (40 Mins) **Topic:** Kaspersky Global Threat Evaluation Mechanism, Modern Threat Analysis Approaches and Latest Trends. **CONTRIBUTED PAPERS** **ID-433, ID-460** (15 Mins Each)	**Break: 1100-1130 Hrs.**	**INVITED TALK** **Speaker: Dr. Haider Abbas, National CERT, Govt. of PAKISTAN.** (40 Mins) **Topic:** Pakistan's National CERT: Challenges and Way Forward. **CONTRIBUTED PAPERS** **ID-141, ID-520** (15 Mins Each)	**Break: 1300-1400 Hrs.**	**TALK & TECHNICAL WORKSHOP** **PART-1** (90 Mins) **Speaker: Dr. Ali Javed, UET Taxila, PAKISTAN.** **Demonstrators: Qurat-Ul-Ain and Hafsa Ilyas.** **Topic:** Multimedia Forensics Analyzer – AI tool to combat disinformation in Cyberspace.	**Break: 1530-1600 Hrs.**	**TECHNICAL WORKSHOP** **Multimedia Forensics Workshop PART-2** (50 Mins) **INVITED TALK** **Speaker: Dr. Hanif Durad, PIEAS, PAKISTAN.** (40 Mins) **Topic:** Security Challenges in the new paradigm of Mist Computing.	**Break: 1730-1800 Hrs.**	**INVITED TALK** **SPEAKER: MR. ASIF SOHAIL ABID, CESAT, PAKISTAN.** (40 MINS) **TOPIC:** OH CATCH'EM – THE GHOST RAN SOME WHERE IN THE WILD WITH PRECIOUS DATA. **Speaker: Dr. Sohail Sarwar, CESAT, PAKISTAN.** (40 Mins) **Topic:** An Era of Large Language Models: Technologies, Opportunities and Challenges by ChatGPT for Cyber Defenders.

	Session-1 (0930-1200 Hrs.)		
Day-3: 24 Aug	**INVITED TALK** **Speaker: Jian Wei Liu, Beihang University, CHINA.** (40 Mins) **Topic:** Emergency Secure Communication System Based on 5G Super SIM. **Speaker: Dr. A. S. Atilla Hasekioglu, BILGEM, TUBITAK, TURKIYE.** (40 Mins) **Topic:** Emerging Challenges in Quantum Random Number Generation (QRNG). **CONTRIBUTED PAPERS** **ID-336, ID-423** (15 Mins Each)	**CONFERENCE CLOSING** **CHECK-OUT: 1200 Hrs.**	**Version 2.0: Last Updated on 22 August, 2023.** **NOTE: All changes/ re-arrangements are highlighted in Red Color.**

TENTATIVE TECHNICAL PLAN – CYBER SECURITY TRACK, 20th IBCAST-2023 (22-25 AUGUST, 2023).

DAY-1: 22 AUGUST, 2023.

	Time (Hrs)	TOPIC		SPEAKER
SESSION-A	1600-1610	**RECITATION FROM 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.
	1610-1650	**INVITED TALK-1:** **What to be Afraid of, what to fight, and what to sacrifice.** **A look at the current security challenges of industrial enterprises.**		**MR. EVGENY GONCHAROV – RUSSIA.** HEAD ICS CERT, Kaspersky, RUSSIA.
	1650-1730	**INVITED TALK-2:** **Post Quantum Cryptography.**		**DR. SAAD ISLAM – PAKISTAN.** InfoSec Researcher, CESAT, PAKISTAN.
	1730-1745	**CS-493**	**Internet Voting in the Age of Quantum Computing**	**Khan Farhan Rafat,** Air University, Islamabad, PAKISTAN.
	1745-1800	**CS-424**	**An Ensemble Learning Model for the detection of phishing attacks**	**Hidayat Ur Rehman,** Air University, Islamabad, PAKISTAN.
	1800-1815	**CS-142**	**Enhancing IoT Security: Federated Learning with GANs for Effective Attack Detection**	**Bakhtawar Saeed,** Deep Packet Inspection Lab, Computer Engineering Department, UET, Taxila, PAKISTAN.
SESSION AND DAY CLOSING				

TENTATIVE TECHNICAL PLAN – CYBER SECURITY TRACK, 20th IBCAST-2023 (22-25 AUGUST, 2023).

DAY-2: 23 AUGUST, 2023.

	Time (Hrs)	TOPIC		SPEAKER
SESSION-B1	0930-1010	**INVITED TALK-3:** **Kaspersky Global Threat Evaluation Mechanism, Modern Threat Analysis Approaches and Latest Trends.**		**MR. EVGENY GONCHAROV – RUSSIA.** HEAD ICS CERT, Kaspersky, RUSSIA.
	1010-1025	**CS-433**	**Detection of Internet Layer DoS Attack on Cloud Using Deep Learning**	**Mansoor Ul-Haque,** PIEAS, Nilore, PAKISTAN.
	1025-1040	**CS-460**	**Sequential Heuristic Model for DDOS Attack Detection in Software-Defined Network**	**Tooba Shaikh,** NED UET, Karachi, PAKISTAN.
TEA BREAK: 1100-1130 Hrs.				
SESSION-B2	1130-1210	**INVITED TALK-4:** **Pakistan's National CERT: Challenges and Way Forward.**		**DR. HAIDER ABBAS – PAKISTAN.** Director General, National CERT, Govt. of PAKISTAN.
	1210-1225	**CS-141**	**Improving Botnet Detection with a Generative Adversarial Network-based Technique**	**Shehla Gul,** UET Taxila, PAKISTAN.
	1225-1240	**CS-520**	**A Hybrid Framework of Meta-Learning and Generative Adversarial Networks for Few-Shot Malware Detection**	**Faiza Babar Khan,** PIEAS, Nilore, PAKISTAN.
LUNCH & PRAYER BREAK: 1300-1400 Hrs.				
SESSION-B3,B4	1400-1530 1600-1650	**INVITED TALK & WORKSHOP-5:** **Multimedia Forensics Analyzer – AI tool to combat disinformation in Cyberspace.**		**DR. ALI JAVED – PAKISTAN.** Director Multimedia Signal Processing (MSP) Research Lab, UET Taxila, PAKISTAN.
	1650-1730	**INVITED TALK-6:** **Security Challenges in the new Paradigm of Mist Computing.**		**DR. HANIF DURAD – PAKISTAN.** Head Information System Security Group, CIPMA Lab, DCIS, PIEAS, PAKISTAN.
TEA BREAK: 1530-1600 AND 1730-1800 Hrs.				
SESSION-B5	1800-1840	**INVITED TALK-7:** **OH Catch'em – The GHOST Ran Some Where in the Wild with Precious Data.**		**MR. ASIF SOHAIL ABID – PAKISTAN.** InfoSec Researcher, CESAT, PAKISTAN.
	1840-1920	**INVITED TALK-8:** **An Era of Large Language Models: Technologies, Opportunities and Challenges by ChatGPT for Cyber Defenders.**		**DR. SOHAIL SARWAR – PAKISTAN.** InfoSec Researcher, CESAT, PAKISTAN.
DAY CLOSING				

TENTATIVE TECHNICAL PLAN – CYBER SECURITY TRACK, 20th IBCAST-2023 (22-25 AUGUST, 2023).

DAY-3: 24 AUGUST, 2023.

	Time (Hrs)	TOPIC		SPEAKER
SESSION-C	0930-1010	**INVITED TALK-9:** **Emergency Secure Communication System Based on 5G Super SIM.**		**JIAN WEI LIU – CHINA.** Professor and Dean, School of Cyber Science and Technology, Beihang University, Beijing, CHINA.
	1010-1050	**INVITED TALK-10:** **Emerging Challenges and Solutions in Quantum Random Number Generators (QRNG).**		**Dr. A. S. Atilla Hasekioglu – TURKIYE.** BILGEM, TUBITAK, TURKIYE.
	1050-1105	**CS-336**	**A Security Analysis of a Blockchain Based Decentralized Energy Trading Application**	**Muhammad Hasan Danish Khan,** Bahria University, Islamabad, PAKISTAN.
	1105-1120	**CS-423**	**ISLAP: Advancing RFID System Security through an Improved Succinct and Lightweight Authentication Protocol**	**Muhammad Ayaz Khan,** Air University, Islamabad, PAKISTAN.
CONFERENCE CLOSING AND CHECKOUT: 1200 Hrs.				

QUANTUM TECHNOLOGY SPECIAL SESSION PAPERS.

		TOPIC	SPEAKER
1.	CS-435	**Enhanced Variational Quantum Regression for Non-linear Curve Fitting in Higher Dimensions**	**Ali Hassan Jamal,** NUST, Islamabad, PAKISTAN.
2.	CS-396	**Scalable surface ion trap design for magnetic quantum sensing and gradiometry**	**Qirat Iqbal,** University of Sindh, Jamshoro, PAKISTAN.
3.	CS-137	**SQUID Sensor Technology: Fundamental Principle and Applications in ASW Operation and Geophysical Exploration**	**Sartaj Khan,** CESAT, Islamabad, PAKISTAN.
4.	CS-247	**Bearing Fault Diagnosis using Quantum Machine Learning**	**Misha Urooj Khan,** AITeC, NCP, PAKISTAN.

INVITED SPEAKERS AND WORKSHOP TRAINERS (FOREIGN / LOCAL).

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:

What to be afraid of, what to fight, and what to sacrifice.
A look at the current security challenges of industrial enterprises.

ABSTRACT:

In the laboratory and on the ground, researchers from Kaspersky ICS CERT encounter various security problems, many of which look significant, while some seem unsolvable at this stage. Technologies that are inherently insecure, vendor neglect of secure development culture, inability to guarantee all the staff follows even the basics of cyber hygiene, impossibility to put into practice all these "best practices," - all of this can ruin optimism and shake the faith in efforts yielding results.

However, facing the actual landscape of threats, many of the theoretical and emotional assessments require reconsideration. Adversaries are not only motivated, persistent, and inventive, but also short-sighted, careless, greedy, and lazy. Sophisticated threats are rare, and simple ones are generally not that dangerous if a few straightforward practices are followed. As a result, the multitude of intertwined risks, fears, and problems breaks down into a spectrum of tasks, each of which can be independently and reasonably solved using tools available to every organization.

In the presentation, we will share practical experience in addressing urgent security challenges to protect industrial enterprises from various types of threats using simple methods and available resources.

TITLE OF THE TALK:

Kaspersky Global Threat Evaluation Mechanism, Modern Threat Analysis Approaches, and Latest Trends.

ABSTRACT: TBA.

DR. A. S. ATILLA HASEKIOGLU,

Deputy Member for Quantum Community
Network (QCN) in Europe,
Representative of TUBITAK Informatics and
Information Security Research Center (BILGEM) for
Quantum Industry Consortium (QuIC) in Europe,
Gebze, Kocaeli,
TUBITAK, TURKIYE.

BIOGRAPHY:

Atilla Hasekioglu has earned PhD (RPI, USA), MS (RPI, USA), BS (Bogazici University, Turkey) in Electrical Engineering, BS (Bogazici University, Turkey) in Physics and MBA (Bogazici University, Turkey) degrees. During his PhD, he worked on semiconductor device modeling and simulating image sensors. After having received his PhD degree, he worked at the Canadian Space Agency, Montreal, Canada as a researcher working on simulating attitude sensors and health of the satellite systems. In 2002, he joined the National Research Institute of Electronics & Cryptology (UEKAE), the Scientific and Technological Research Council of Turkey (TUBITAK) as a lead researcher. In 2014, he became the Director of Cyber Security Institute. He is currently working as a project manager.

He has experience in software development for semiconductor device modeling, semiconductor device simulations, simulating image sensors and power devices, software development for space applications, satellite operations support analyses, cryptology, cyber security, quantum cryptography, quantum computing, quantum information and imaging. He has participated in several international projects in Turkey, US, Canada, EU and Japan. He has six years of working experience in research and operation environment in space industry and close to 20 years of experience in cryptology, cyber security and quantum related projects. His current interests include cryptography, cyber security, neuromorphic computing, quantum random number generators, quantum cryptography, quantum computation, imaging and information, quantum technologies in general and research management.

Currently, he participates in ETSI Quantum Key Distribution Standardization group activities as a vice-chair. He represents Turkey as a deputy member of Quantum Community Network (QCN) in Europe. He is a representative of TUBITAK Informatics and Information Security Research Center (BILGEM) for Quantum Industry Consortium (QuIC) in Europe.

TITLE OF THE TALK:

Emerging Challenges in Quantum Random Number Generation (QRNG).

ABSTRACT: TBA.

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:

Emergency Secure Communication System Based on 5G Super SIM.

ABSTRACT:

New cryptographic theories and technologies play a crucial role in the security design of communication terminals. This talk focuses on the communication security and confidentiality requirements of mobile communication terminals in complex emergency environments, and elaborates on the application practice of cryptographic technology in terminal security domain isolation, communication traffic security isolation, applications isolation, key distribution protocol design, identity authentication, communication encryption, and other aspects. It has a guiding significance for the design and development of high security and high trust communication terminals in the future.

DR. HAIDER ABBAS,

Director General
National CERT, Government of Pakistan.

BIOGRAPHY:

Dr. Haider Abbas is serving as Director General for National Cyber Emergency Response Team (National CERT), Government of Pakistan. He received his MS and PhD in Information Security from KTH, Sweden and took professional trainings and certifications from Massachusetts Institute of Technology (MIT), United States, Stockholm University, Sweden, Stockholm School of Entrepreneurship, Sweden, IBM, USA and Certified Ethical Hacker from EC-Council. Dr. Abbas has received many awards from National and International organizations including NUST University Best Researcher award, Research Productivity Award from PCST, best paper award from Elsevier, best paper award by IEEE, Asia-Pacific ICT Alliance Awards, P@SHA ICT Awards, MCS best researcher award and CyberPatriot from US Airforce Association, USA.

TITLE OF THE TALK:

Pakistan's National CERT: Challenges and Way Forward.

ABSTRACT:

PK-CERT/N-CERT, the latest undertaking of the Government of Pakistan, serves as the central body for managing cybersecurity events on a national scale. Its pivotal role involves detecting, assessing, and countering cyber risks and breaches, frequently engaging with different industries to enhance the nation's overall cybersecurity. This presentation will outline the strategy for fostering cooperation among the government, industry, and academia to establish a resilient cyber landscape for Pakistan. The outline of the talk is as under:-

- National CERT Intro
- NCERT Organisation / Sectoral CERTs
- NCERT Basic Functions
- The Future Strategy

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 Government 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).

After graduating from PIEAS, he 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. His thesis title was “Evaluation of trust in Open and Grid Networks”.

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 many papers in internationally reputed peer-reviewed journals and conferences. His research interests include Network Security, Cryptography, Embedded System Security, Industrial Control Cyber security, Cluster/ Grid/ Cloud/ fog computing and IoTs.

TITLE OF THE TALK:

Security Challenges in the new paradigm of Mist Computing.

ABSTRACT:

Despite the increasing usage of cloud computing, there are still unsolved issues due to the inherent problems of cloud computing as unreliable latency, lack of mobility support, and location-awareness. Fog computing, also termed edge computing, can address those problems by providing elastic resources and services to end users at the edge of the network, while cloud computing is more about providing resources distributed in the core network. Mist computing is a newer concept that involves distributing computing resources even further, closer to the source of data. In this talk, I will present a detailed analysis of the new security challenges introduced due to Mist computing.

DR. ALI JAVED,

Director/ Associate Professor,
Multimedia Signal Processing Lab,
Software Engineering Department. UET Taxila.

BIOGRAPHY:

Dr. Ali Javed is working as an Associate Professor of Software Engineering at the University of Engineering and Technology, Taxila, Pakistan. He has more than 15 years of experience involving teaching, research, and administrative duties including acting HOD Software Engineering Department at UET Taxila. He served as a Postdoctoral Scholar in the SMILES lab at Oakland University, MI, USA in 2019 and as a visiting Ph.D. scholar in the ISSF Lab at the University of Michigan, MI, USA in 2015. His research interests are in Image Processing, Computer Vision, Multimedia Forensics, Video Content Analysis, and Machine Learning. He is also the Director of the Multimedia Signal Processing (MSP) Research Lab at UET Taxila, Pakistan. He has secured many funded (Govt. & Industry) research projects in his areas of interest. He has published more than 140 research papers in peer-reviewed international conferences and journals. He has supervised 02 PhDs and more than 57 MS thesis in the domain of computer vision and image processing. Dr. Ali has delivered invited talks in the domain of multimedia forensics at multiple Conferences and also conducted two workshops in multimedia forensics and image processing. He has been providing reviewing services for many prestigious peer-reviewed journals and conferences. He has served on technical program committees at many international conferences. He has also served on the national-level expert's panel/board to review research grants. He has also served as a subject expert on multiple selection boards for faculty hiring at HITEC University. He is also a member of the HEC Accreditation Committee for reviewing BS Computing Programs. Dr. Ali got selected as an Ambassador of the Asian Council of Science Editors from Pakistan in 2016. He is a Senior Member of IEEE and member of IEEE SPS.

TITLE OF THE TALK:

Multimedia Forensics Analyzer- AI tool to combat disinformation in Cyberspace

ABSTRACT:

The rapid and unstoppable progress of fake multimedia generation technology has introduced unparalleled challenges in verifying the authenticity and reliability of digital content. Utilizing powerful deep learning algorithms, videos and images can be convincingly altered, giving rise to the potential dissemination of false information, manipulation of public opinion, and the gradual erosion of trust in media sources. Recognizing the urgency of this critical issue, our hands-on workshop is thoughtfully crafted to shed light on the profoundly negative impact fake multimedia have on our society. Throughout the workshop, participants will acquire a comprehensive and in-depth understanding of the diverse and harmful applications of fake content.

Additionally, attendees will explore the disquieting implications for privacy, as fake media generation technology can be maliciously used to fabricate content that invades the private lives of unsuspecting individuals. The goal of this training is to provide attendees with extremely practical and cutting-edge techniques for detecting and combating fake content. By immersing attendees in the realm of advanced deep learning models, we hope to furnish them with the necessary tools and expertise to distinguish truth from deceit in an ever-evolving digital landscape. With this knowledge and skill, our participants will emerge as vigilant protectors, leading the fight against deception and ensuring the integrity of digital media. We embark on this critical mission to discover fraud and protect the credibility of information in the digital era in a spirit of unity and collaboration. Together, we will strengthen the pillars of trust and construct a resilient society that remains steadfast and immune to the malevolent influence of fake content. As we stand united in the face of this formidable threat, let us join hands to uphold the principles of authenticity, transparency, and truth in the relentless pursuit of countering deception.

Workshop Outline:

- Introduction to Multimedia Forensics.
- Audio Forensics.
- Image Forensics.
- Video Forensics.
- Impact of Fake Multimedia Content.
- Fake Multimedia generation platforms.
- Multimedia Forensics: Techniques.
- Multimedia Forensics: Challenges and future directions.
- Our prototype.
- Hands-on practice (Training, Validation, Testing the model).

WORKSHOP TRAINERS/ ASSISTANTS.

Qurat-Ul-Ain, Research Associate, Multimedia Signal Processing Lab, UET Taxila.

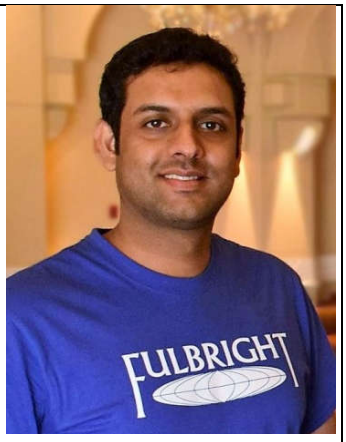
Qurat-ul-Ain is working as a Research Associate in Multimedia Signal (MSP) Research Lab at UET Taxila. She is a computer science Ph.D. scholar with more than 4 years of experience involving teaching and research. With two master's degrees and a bachelor's degree, she has a strong foundation in computer science, particularly in machine learning, computer vision, and image processing. She won several national-level competitions including 3-Minute Thesis at SZABIST, COMSATS, and NUST. She published work on deepfake and forged face detection, demonstrating her expertise in machine learning and computer vision.

Hafsa Ilyas, Research Assistant Multimedia Signal Processing Lab, UET Taxila.

Hafsa Ilyas is working as a Research Assistant in Multimedia Signal Processing Lab. She has done her B.Sc. and M.Sc. degree in Software Engineering from UET Taxila. She has more than three years of experience in research. Her research interests are in Deep-learning, Multimedia forensics, Image, audio and video processing, and Computer vision.

DR. SAAD ISLAM,

Senior Cyber Security Researcher,
CESAT, Islamabad, Pakistan.



BIOGRAPHY:

Saad Islam is a Fulbright scholar who has recently completed his PhD in Cyber Security from Worcester Polytechnic Institute, USA. Working in Vernam Lab in the field of side-channel attacks, he discovered a hardware bug named "SPOILER" in all generations of Intel Core processors which remained undiscovered since 2008. His work was published in one of the topmost security conferences USENIX'19 and received a lot of media attention. SPOILER helped him boosting a well-known software-induced fault attack called "Rowhammer", making it more efficient and practical. Using Rowhammer attack, he was able to successfully target two of the post-quantum signature schemes from the NIST PQC competition. These works were published in top tier security conferences ACM CCS 2020 and EuroS&P 2022.

TITLE OF THE TALK:

Post-Quantum Cryptography.

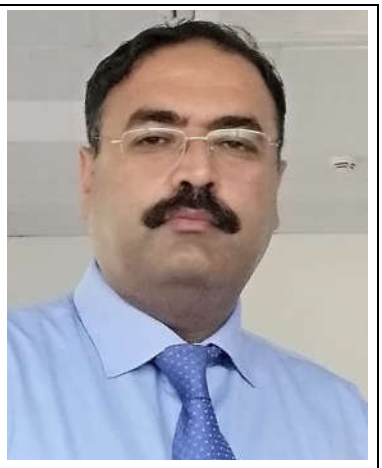
ABSTRACT:

Post-quantum cryptography (PQC) refers to cryptographic techniques that are designed to be secure against attacks from quantum computers. Traditional cryptographic methods, which rely on mathematical problems like factoring large numbers and discrete logarithms, can be efficiently broken by a powerful enough quantum computer using Shor's algorithm. As quantum computers become more feasible, there is growing concern about the potential impact on the security of current encryption systems.

Post-quantum cryptography aims to develop new encryption algorithms and protocols that are resistant to quantum attacks. These algorithms are based on different mathematical problems that are believed to be hard even for quantum computers to solve. The National Institute of Standards and Technology (NIST) has been actively involved in the standardization process of post-quantum cryptographic algorithms. They launched a competition in 2016 to select promising candidates for post-quantum encryption and digital signature schemes. The goal is to establish a set of standardized algorithms that can be used for secure communications in a post-quantum era.

DR. SOHAIL SARWAR,

Senior Cyber Security Researcher,
CESAT, Islamabad, Pakistan.



BIOGRAPHY:

Dr. Sohail has 17 years of R&D experience in public/ private, academia/ industry of Pakistan. Over these years, he got a chance to work in various professional roles as Software quality analyst at Bentley Systems, Software Architect at BizSol, Automation Engineer as academic researcher/ faculty at NUST SEECS and lately as Data Scientist at CESAT. He possesses diverse teaching experience as visiting faculty member for teaching undergraduate and postgraduate level courses at reputed universities of Pakistan. He has 40 international publications including high impact journals, book chapters, conference papers; centering AI, Machine Learning and NLP. Besides, He got a chance to present his research at international forums such as HONET Egypt, ICTL Dubai, UAI in Netherlands, HONET Malaysia and Basque University Spain.

His PhD was focused on “Ontology based Personalized and Adaptive E-Learning Frameworks” through NLP constructs for modeling learning objects. Hence, semantic information retrieval can be enabled, another step to Web 4.0. Moreover, modeling of learner profiles, ML based learner classification; content/collaborative recommenders were also developed for aligning learners and SCO (sharable Content Objects) adaptively. This research was carried out in collaboration with Ontology Engineering Group (OEG), Technical University of Madrid, Spain; a globally renowned group of Semantics and NLP technologies. Dr. Sohail completed his MS from NUST with specialization in Object Oriented Technologies. His industry based research was focused on developing “Predictive prefetching techniques via ML techniques” in collaboration with DTS Japan. At CESAT, he has worked on different RD projects including CMS development, testing tasks, AI based assignments, threat prediction, SDLC/PM design and NLP based assignments for digital media analysis, content crawling, scraping and parsing, sentiment analysis, Multi-lingual / aspect based sentiment analysis, speech to text translation, fake news detection and pattern / association mining. He has facilitated collaborations with NUST, FAST, PIEAS and Bahria University.

Dr. Sohail is also an active volunteer on avenue of community services as well. His mobilization enabled food / medicine supplies to 5000 families during COVID-21 along with volunteers from FAST. Also, they supported 7000 families during flood relief along with volunteers from NUST.

TITLE OF THE TALK:

An Era of Large Language Models: Technologies, Opportunities and Challenges by ChatGPT for Cyber Defenders.

ABSTRACT:

The emergence of large language models (LLMs), exemplified by the likes of Bard, Falcon and ChatGPT etc., have ushered in a new era of transformative potential across various domains.

However, as these AI-driven systems become increasingly sophisticated and pervasive, they present a range of unprecedented opportunities / challenges for cyber attackers / defenders.

This talk aims to shed light on the LLM technologies / components, distinct opportunities, challenges posed by similar technologies, emphasizing their implications in general as well as for cyber security. Moreover, a collaborative approach among AI researchers, cyber security professionals, and platform providers is to be discussed; for collective mitigation of the risks posed by LLMs and potential for indigenous development of similar platforms.

Mr. Asif Sohail Abid,

Senior Cyber Security Researcher,
CESAT, Islamabad, Pakistan.

Biography:

Asif Sohail Abid is an experienced Cyber Security professional and researcher having more than 10 years of experience. He has conducted penetration testing of multiple products including web applications/ services, Operating systems, Network infrastructure, Active Directory, Network devices, Mobile applications, IoT Devices, COTs solutions, Indigenous applications, Mobile Applications and Firewalls.

His domain specific specialized qualification, thorough knowledge and significant professional experience has helped him in comfortably profiling and navigating a target network utilizing attack vectors inside and outside the network. During his professional career, he has conducted manual and automated exploitation of various vulnerability classes.

He is also a trained malware analyst, who can perform static and dynamic analysis of windows and Linux malwares.

He is a certified "ISO/IEC 27001:2013 - Information Security Management Systems Auditor/ Lead Auditor". During his professional career, he has also contributed in secure SoPs development, Risk Analysis, governance, and policy making.

Topic of the Talk:

OH Catch'em – The GHOST Ran Some Where in the Wild with Precious Data.

Abstract:

In an era where digital transformation is reshaping industries and economies, the digital realm also becomes a breeding ground for various threats. One of the most pervasive and destructive threats that have emerged in recent years is ransomware. Ransomware attacks have gained notoriety for their ability to disrupt businesses, compromise personal data, and generate significant financial gains for cybercriminals.

The threat landscape of ransomware is a complex and evolving terrain, characterized by relentless innovation on the part of cybercriminals. Understanding this landscape is vital in comprehending the gravity of the issue and devising effective countermeasures. Ransomware attackers target a broad spectrum of victims, ranging from individuals and small businesses to large enterprises and even critical infrastructure. This wide scope highlights the universal vulnerability that these attacks exploit.

In this talk, we will delve into the world of ransomware, exploring its threat landscape, understanding its modus operandi, and discuss the strategies for defense and mitigation.