TENTATIVE BRIEF TECHNICAL PLAN – CYBER SECURITY TRACK, IBCAST-2022 (16-20 AUGUST, 2022).

	Session – 1 (0900-1030 Hrs.)	Session – 2 (1100-1230 Hrs.)	Session – 3 (1400-1530 Hrs.)	Session – 4 (1600-1730 Hrs.)
DAY-1: 16 AUG	**Departure to Bhurban**		**OPENING REMARKS (10 Mins)** **INVITED TALK (40 Mins)** **DR. ZAHRI BIN YUNOS – MALAYSIA.** Strategic Cybersecurity Advisor, Securelytics, Malaysia. Member Board of Directors, University Teknikal Malaysia Melaka, Malaysia. **TOPIC: Common Criteria for ICT Security Evaluation: Malaysia's Case Study.** **Contributed Talks (40 Mins): CS-1, CS-2**	**INVITED TALK (40 Mins)** **DR. MOHAMMAD RICHARD DAHMAN – TURKEY.** Senior AI and Data Scientist, Co-Founder DAHMAN's Phi Services, Istanbul, Turkey. **TOPIC: The Treasure Trove of Data and the Shadow of CS.** **Contributed Talks (60 Mins): CS-3,CS-4,CS-5**
DAY-2: 17 AUG	**INVITED TALK (45 Mins)** **PROFESSOR DR. HAFIZ MALIK – USA.** Founding Director Information Systems, Security, and Forensics (ISSF) Laboratory, Dept. of Electrical & Computer Engineering, University of Michigan, Dearborn, USA. **TOPIC: Content Integrity Verification in the Age of Deepfakes and Social Networks.** **Contributed Talks (40 Mins): CS-6,CS-7**	**INVITED TALK (30 Mins)** **DR. ZUNERA JALIL – PAKISTAN.** Associate Professor and Chair, Department of Cyber Security, Air University, Islamabad, Pakistan. **TOPIC: Cyber Security for Artificial Intelligence (AI) and AI for Cyber Security.** **Contributed Talks (60 Mins): CS-8,CS-9,CS-10**	**TECHNICAL WORKSHOP (90 Mins)** **PROFESSOR DR. HAFIZ MALIK – USA.** Founding Director Information Systems, Security, and Forensics (ISSF) Laboratory, Dept. of Electrical & Computer Engineering, University of Michigan, Dearborn, USA. **TOPIC: Deepfakes from Generation to Detection.**	**TECHNICAL WORKSHOP (90 Mins)** **DR. MOHAMMAD RICHARD DAHMAN – TURKEY.** Senior AI and Data Scientist, Co-Founder DAHMAN's Phi Services, Istanbul, Turkey. **TOPIC: The Magic of Math seen through Prediction.**
DAY-3: 18 AUG	**INVITED TALK (45 Mins)** **DR. HASAN TAHIR BUTT – PAKISTAN.** Assistant Professor, Head of Information Security, NUST, Islamabad, Pakistan. **TOPIC: Physically Unclonable Functions - A Novel Root of Trust for Cryptographic Implementations.** **Contributed Talks (40 Mins): CS-11,CS-12**	**INVITED TALK (45 Mins)** **DR. SHAHZAIB TAHIR BUTT – PAKISTAN.** Assistant Professor, Head Information Security and Privacy (ISP) Research Group, NUST, Pakistan. **TOPIC: Securely Preserving Water Memory through Searchable Encryption.** **Contributed Talks (40 Mins): CS-13,CS-14**	**TECHNICAL WORKSHOP (90 Mins)** **MR. ALI FAYYAZ, MR. MUDDASSAR MASOOD, AND MR. ABID KHAN JADOON – PAKISTAN.** Malware Analysts and Researchers, CESAT, Islamabad, Pakistan. **TOPIC: Packed Malware Analysis.**	**TECHNICAL WORKSHOP (120 Mins)** **DR. ZAHRI BIN YUNOS – MALAYSIA.** Strategic Cybersecurity Advisor, Securelytics, Malaysia. Member Board of Directors, University Teknikal Malaysia Melaka, Malaysia. **TOPIC: CERT Establishment: Case Study of Malaysia Model.**
DAY-4: 19 AUG	**INVITED TALK (30 Mins)** **DR. SAAD ISLAM – USA.** Researcher, CESAT, Islamabad, Pakistan. Former Researcher at Vernam Lab, Dept of ECE, Worcester Polytechnic Institute (WPI), USA. **TOPIC: Rowhammer Attack.** **Contributed Talks (60 Mins): CS-15,CS-16,CS-17,CS-18**	**Conference Closing Ceremony & Checkout**	**Departure to Islamabad**	

BREAK / REFRESHMENT

BREAK / REFRESHMENT (LUNCH & PRAYER)

BREAK / REFRESHMENT

Special/ Extended Sessions: Discussions, Networking, etc. (1730-1930 Hrs)

INVITED SPEAKERS AND WORKSHOP TRAINERS (FOREIGN / LOCAL).

Dr. Zahri Bin Yunos,

Strategic Cybersecurity Advisor,
Securelytics, Malaysia.
Member Board of Directors,
University Teknikal Malaysia Melaka, Malaysia.

Biography:

Zahri started his career in 1988 as a computer analyst at the Ministry of Defence Malaysia and joined CyberSecurity Malaysia in 2001 (formerly known as National ICT Security and Emergency Response Centre – NISER), an agency under the Ministry of Communications and Multimedia Malaysia. He was appointed as Chief Operating Officer (COO) in 2007 and retired from the national service in January 2022 while working at CyberSecurity Malaysia.

At CyberSecurity Malaysia, Zahri actively sat in several committees at national level and participated in establishment of NISER's Panel of Experts (POE) in 2001, entrusted to develop the National Infrastructure Protection Agenda (NIPA) Report. The NIPA Report was later referred to during development of the National Cyber Security Policy in 2006 which boosted Malaysia's reputation in cybersecurity worldwide. He also led the execution of 9th (2006-2010), 10th (2011-2015), 11th (2016-2020) and 12th (2021-2025) CyberSecurity Malaysia Plan.

In 2008 to 2012, Zahri contributed to implement cybersecurity policy in Malaysia by becoming the Secretariat Head for National Cybersecurity Coordination Committee (NC3) and Cyber Law Review Committee. As COO of CyberSecurity Malaysia, he led the team in outlining National Cyber Security Awareness Master Plan chaired by National Security Council in 2014; National Cyber Drill Committee chaired by National Security Council during 2011-17; and Cybersecurity Framework for Public Sector chaired by Malaysian Administrative Modernization and Management Planning Unit (MAMPU) in 2016. He participated as a Working Group Member to develop Malaysia Standard 1970 Business Continuity Management, completed in 2008.

Zahri also participates in universities academic programs as Industry Advisor, Associate Fellow, Visiting Expert and Adjunct Professor. Alumni UTeM publication featured him in "Anjakan Paradigma Mendepani Cabaran Alumni UTeM", that reveals his journey fostering cybersecurity in Malaysia, then he was appointed as UTeM Board Member for the term 2020-2023.

At international front, Zahri's expertise and experience are significant in sustaining nation's prominence in cybersecurity, particularly in the Asia Pacific region and the Organisation of Islamic Cooperation (OIC) countries. He is a central figure in the establishment of OIC Computer Emergency Response Team (OIC-CERT – www.oic-cert.org), a collaborative effort of CERTs amongst the OIC countries in 2019. He managed research collaboration project on malware amongst OIC-CERT and Asia Pacific CERT (APCERT – www.apcert.org) in 2017.

As an expert, Zahri had been part of several working groups (OIC in 2015, International Cyber Policy Centre, Australian Strategic Policy Institute in 2015, United Nations Group of Government Experts in 2014-2015, and COMSTECH in 2015). Zahri was appointed as Scientific & Industrial Advisory Board for National Centre of Cyber Security, Pakistan in 2019 and Advisory Board Member for CyberCyte United Kingdom in 2021.

Zahri continuously contribute on topics related to cybersecurity, cyber terrorism and business continuity management. He holds a PhD in Information Security from Universiti Teknikal Malaysia Melaka (Malaysia) in 2015, MSc in Electrical Engineering from Universiti Teknologi Malaysia (Malaysia) in 1992 and BSc in Computer Science from the Fairleigh Dickinson University (New Jersey, USA) in 1987. He is registered with the Malaysia Board of Technologists (MBOT) as Professional Technologist in 2018 and was awarded Senior Information Security Professional by the (ISC)2, USA in 2010. In 2019, Zahri was conferred Paduka Mahkota Perak (P.M.P) in conjunction with Perak Ruler Sultan Nazrin Muizzuddin Shah's 63rd birthday, for his exceptional role in cybersecurity at national and international level.

Topic of the Talk:

Common Criteria for ICT Security Evaluation: Malaysia's Case Study.

Abstract:

Common Criteria for ICT Security Evaluation (Common Criteria or CC) is an international standard (ISO/IEC 15408) for ICT product security certification. A Common Criteria evaluation allows an objective evaluation to validate that a particular product satisfies a defined set of security requirements. Common Criteria provides methodology regarding preparation of evaluation deliverables such as Target of Evaluation (TOE) and operational documents in accordance with Evaluation Assurance Level (EAL).

Majority of ICT developers prepared evaluation deliverables after their products have been developed. As such, additional resources such as time and cost have been invested in order to ensure the products are ready for evaluation evidence. In this presentation, based on Malaysia's case study, discussion focuses on how Common Criteria utilizes the development process to improve product security while simultaneously reducing the time and cost associated with evaluating ICT security requirements.

Title of the Workshop:

CERT Establishment: Case Study of Malaysia Model.

Brief Description:

Many nations all over the world have increased their dependency on the use of Information and Communication Technology (ICT). Many stakeholders are concerned with cyber-attacks against Critical National Information Infrastructures (CNIIs) such as power distributions, transportations, telecommunications, financial services and essential public utility services. Successful cyber-attacks on these CNIIs can have serious catastrophic damages and disruptions.

The capability to have a functional national or enterprise CERT is seen as closely connected to the concept of CNII protection. It is proposed for CNII organisations to establish a CERT to provide systematic guidance regarding organisation's information security risk management to an acceptable level. A narrative of CERT operations such as structure, responsibilities, workflow and international cooperation will be covered. In addition, participants will manage scenario based cyber incident. The exercise will consist of an interactive, escalating, cyber policy desktop exercise, involving a serious regional cyber incident that targets CNII.

Dr. Mohammad Richard Dahman,

Senior AI and Data Scientist, Finance & Business Developer,
Co-Founder DAHMAN's Phi Services, İstanbul, Turkey.

Biography:

Dr. Mohammad Richard Dahman is a Senior AI and Data Scientist. He has more than 14 years of experience in management and information technology. His experience spans employing AI problem-solving paradigm for social science research problems, business development, and research & innovation initiatives. Thanks to his interdisciplinary background, he has a successful record of accomplishments in both industry and academia.

In his current position, Dahman helps organizations employing AI problem-solving paradigm, based on his invented academic framework AISS V2.1.0, to their business processes to achieve increased efficiency and innovation. In addition, he utilizes the same framework to assist and supervise research studies for undergraduates, postgraduates and scholars.

Dahman holds a Ph.D. in management information system. He has a number of peer-reviewed scientific publications as well as several drafts and presentations in the media. His certifications include MCP, MCSE, MCITP, PRINCE2 Agile, and AI.

Dahman has lived and worked in different countries around the world. His real nationality is HUMAN. His colleagues and friends describe him as analytical, creative, goal-oriented and above all humanitarian.

Topic of the Talk:

The Treasure Trove of Data and the Shadow of CS.

Abstract:

Data security refers to the process of protecting data from unauthorized access and data corruption throughout its lifecycle. Data security includes data encryption, hashing, tokenization, and key management practices that protect data across all applications and platforms. Firewalls, password protection, and multi-factor authentication are all types of data security measures typically employed.

The talk will cover mathematical and realistic perspective on the subject of data and protection, including:

(a) what is data in the real and the digital world,

(b) the life-cycle of transformation,

(c) where is the gap, and mathematical proof for that, and

(d) what is the limit?

Title of the Workshop:

The Magic of Math seen through Prediction.

Brief Description:

A host of new and evolving cybersecurity threats has the information security industry on high alert. Ever-more sophisticated cyberattacks involving malware, phishing, and more have placed the data and assets of corporations, governments and individuals at constant risk.

The workshop will propose a framework on the design of **Home Made Protection Shield** to help stakeholders to be independent from external ready-to use tools. The endeavor is to predict possible attacks on a private digital asset. Pure mathematical induction underlies the framework. The session will include an illustration of fictional demo on the use of the algorithm.

Use-Case: Framework of a mathematical solution to predict the action of a cyber attack.

Uniqueness of the Proposal: The mathematical proposal will use two pillars: **historical data foundation** and **simulative modeling data** based on the mathematical algorithm designed by the author.

Prof. Dr. Hafiz Malik,

Professor, Electrical and Computer Engineering,
Founding Director Information Systems, Security, and Forensics (ISSF) Laboratory,
Department of Electrical and Computer Engineering,
University of Michigan-Dearborn, Dearborn, MI 48128, USA.

Biography:

Hafiz Malik is Processor of Electrical and Computer Engineering (ECE) at the University of Michigan – Dearborn. His research in the areas of automotive cybersecurity, deepfakes, IoT security, sensor security, multimedia forensics, steganography/steganalysis, information hiding, pattern recognition, and information fusion is funded by the National Science Foundation, National Academies, Ford Motor Company, Marelli, Inc. N.A., and other agencies. He has published over 100 articles in leading peer-reviewed journals, conferences, and workshops. He is a founding member and chief operating officer (COO) of the Global Foundation for Cyber Studies and Research, a founding member of the Cybersecurity Center for Research, Education, and Outreach at UM-Dearborn and member of leadership circle for the Dearborn Artificial Intelligence Research Center at UM-Dearborn. He is also a member of the Scientific and Industrial Advisory Board (SIAB) of the National Center of Cyber Security Pakistan. He is a member of MCity Working Group on Cybersecurity, since 2015.

Further info about his research can be found at: http://www-personal.umd.umich.edu/~hafiz/

Topic of the Talk:

Content Integrity Verification in the Age of Deepfakes and Social Networks.

Abstract:

Advances in artificial intelligence and multimedia (audio, video, and image) synthesis and generation technologies are the main driver behind exponential growth of deepfakes and shallowfakes. The deepfake technology can be used to generate audios and videos of a real people saying or doing things they never said or did. Deepfake technology is weaponizing information and social media platforms are adding fuel to the fire. Bad actors are taking advantage of deepfake technologies and social media platforms to spread misinformation, amplify rumors, propagate disinformation, influence election outcomes, increase social polarization, distort facts and introducing alternate realities. Stung by interference in elections of the United State and other democracies, governments and intelligence agencies around the world have started preparing for future malign operations. Despite of limited successes in detecting and countering disinformation and misinformation campaigns, the bad actors keep on taking advantage of emerging AI technologies and re-tooling social platforms to spread falsehood and manipulate the political discourse.

This talk will discuss trajectory of deepfake and shallowfake technologies and the threats it poses to national security, democratic institutions, financial institutions, and the society at large. This talk will present a framework to debunk deepfake attacks in real-time. This talk will also present state-of-the-art on information authentication and findings of our-on-going research on content verification for digital audios and videos and influencer-based framework to mitigate the damages of disinformation.

Title of the Workshop:

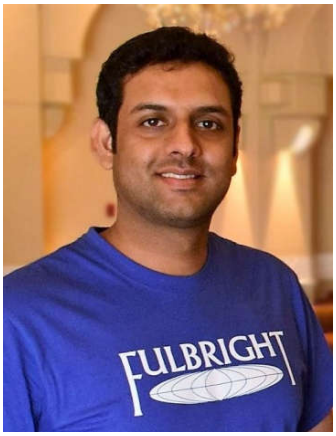
Deepfakes from Generation to Detection.

Brief Description:

Easy access to audio-visual content on social media, combined with the availability of modern tools such as Tensorflow or Keras, and open-source trained models, along with economical computing infrastructure, and the rapid evolution of deep-learning (DL) methods have heralded a new and frightening trend. Particularly, the advent of easily available and ready to use Generative Adversarial Networks (GANs) have made it possible to generate deepfakes media partially or completely fabricated with the intent to deceive to disseminate disinformation and revenge porn, to perpetrate financial frauds and other hoaxes, and to disrupt government functioning. A comprehensive review and detailed analysis of existing tools and machine learning (ML) based approaches for deepfake generation, and the methodologies used to detect such manipulations in both audio and video will be covered. For each category of deepfake, information related to manipulation approaches, current public datasets, and key standards for the evaluation of the performance of deepfake detection techniques, along with their results will also be discussed. Additionally, open challenges and future directions will be discussed which need to be considered in order to improve the domains of both deepfake generation and detection. This workshop is expected to assist audience in understanding how deepfakes are created and detected, along with their current limitations and where future research may lead.

Dr. Saad Islam,

Researcher,
CESAT, Islamabad, Pakistan.
Fulbright Scholar and Former Researcher at Vernam Lab,
Worcester Polytechnic Institute, United States of America.



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.

Topic of the Talk:

Rowhammer Attack.

Abstract:

Every computer process has its own virtual address space which is divided into virtual pages, typically of size 4 kB. Memory Management Unit (MMU) translates the virtual addresses into physical addresses and keeps track in form of page tables. The memory controller integrated in modern processor then translates these physical addresses into channels, ranks and banks inside the DRAM. This DRAM addressing varies from system to system and is not publicly disclosed for Intel CPUs. Each bank then further consists of rows and columns sharing the same row buffer. A DRAM row consists of 64K cells and a cell is composed of a transistor and a capacitor. Data is stored in these capacitors in form of charge and interpreted as a zero or a one according to predefined threshold levels. As capacitors leak charge over time, there is a refresh mechanism to restore the charge of all the DRAM cells every 64ms.

As the DRAM manufacturers are trying to make memories more compact, these rows of cells are getting physically closer leading to disturbance errors from one DRAM row to another. If one row is accessed repeatedly, it might cause electrical interference with the neighboring row due to insufficient insulation and the cells in the neighboring row may leak faster. If the leakage is faster than the refresh frequency, the cells can not maintain their state, which may lead to bit-flips. This is known as the Rowhammer effect which was first introduced by Kim et al. in 2014. Using Rowhammer, an attacker with access to a row next to the victim row in DRAM is able to cause bit-flips in the victim's memory, even when the attacker resides in a process completely separate from the victim process. If the attacker hammers one row which causes bit-flips in the neighboring row, it is called single-sided Rowhammer.

After this discovery, Seaborn et al. introduced the double-sided Rowhammer which is far more effective than the earlier single-sided Rowhammer. In a double-sided Rowhammer, the attacker hammers two rows sandwiching the victim row, leaking the victim cells even faster. Veen et al. in 2016 showed that it is also applicable on mobile platforms. Gruss et al. introduced one-location hammering and achieved root access with opcode flipping in sudo binary in 2018. Gruss et al. and Ridder et al. have shown that Rowhammer can be applied through JavaScript remotely. Tatar et al. and Lip et al. have proved that it can be executed over the network. Rowhammer is also applicable in cloud environments and heterogeneous FPGA-CPU platforms. In 2020, Kwong et al. demonstrated that Rowhammer is not just an integrity problem but also a confidentiality problem.

There have been many efforts on Rowhammer detection and neutralization but are found ineffective. Some countermeasures require hardware modification, bootloader or BIOS update but they are not all implemented. Cojocar et al. in 2019 reverse-engineered the Error Correction Code (ECC) memories showing that ECC countermeasure are not secure either. Another hardware countermeasure Target Row Refresh (TRR) has also been recently bypassed by Frigo et al. using many-sided Rowhammer on DDR4 chips. The same work has been extended by Ridder et al. to attack TRR-enabled DDR4 chips from JavaScript. They claim that more than 80% of the DRAM chips in the market are still vulnerable to the Rowhammer attack.

Dr. Zunera Jalil,

Associate Professor and Chair,
Department of Cyber Security, Air University, Islamabad.

Biography:

Dr. Zunera Jalil is Associate Professor & Chair at Department of Cyber Security, Faculty of Computing & Artificial Intelligence, Air University, Islamabad. She is also engaged as Co-Investigator with National Cybercrimes and Forensics Lab, National Center for Cyber Security, Air University, Islamabad. Dr. Zunera has over 18 years of national as well as international academic experience as a Full-Time Faculty (Cyber Security/Computing/Software Engineering), teaching courses in Cyber Security (Digital Forensics, Network Security, and Information Assurance), Computing, and Software Engineering. She has contributed with over 50 research articles in international journals and conferences. She has contributed in multiple international conferences in diverse roles.

She is EC-Council's Certified Computer Hacking Forensic Investigator (CHFI). Dr. Zunera has delivered guest talks, conducted seminar and trainings at numerous national and international forums in past. She is Chief Trainer at National Cybercrimes and Forensics Lab and also involved in R&D of cyber security solutions using Artificial Intelligence. She is reviewer and editor of multiple renowned international journals in computing and cyber security domain.

Her research interests include but are not limited computer forensics & AI, computational intelligence for audio, video and log data processing, data privacy protection, information security management, digital forensics for cyber-physical systems, cyber-attacks detection using deep learning, and Digital Forensics as a Service (DFaaS).

Topic of the Talk:

Cyber Security for Artificial Intelligence (AI) and AI for Cyber Security.

Abstract:

Artificial intelligence and Machine Learning has created a huge impact in current digital world and has been shown to be able to create machines that exhibit intelligence comparable to or in some cases even better than human intelligence. AI has been used in medical applications, security applications, cloud computing, smart cities, web, and in many other domains. Pakistan is moving towards digitalization and the emphasis is on using technology to enhance productivity, economic stability, security and reachability. In this shift towards digitalization, cybersecurity cannot be neglected. AI is helping to achieve cybersecurity by detecting anomalies, adapting security parameters based on ongoing cyber-attacks, and to combat cyber-adversaries. However, AI systems can be controlled, compromised, biased, and misled through flawed learning models and poisonous input data. Therefore, AI systems need robust security. One should know: How to use AI to secure existing digital systems and at the same time how to use these AI models securely? How to safeguard AI models from malicious inputs? How to not make adversaries take advantage of your smart moves? The integration of cybersecurity and AI can boost progress through secure, smooth and smart shift towards digitalization.

Engr. Dr. Hasan Tahir Butt,

Assistant Professor,
Head of Information Security,
Associate Dean for Computing in School,
NUST, Islamabad, Pakistan.

Biography:

Dr Hasan Tahir is an Assistant Professor in National University of Sciences and Technology and the Head of Information Security. He is also the Associate Dean for Computing in School. Dr Hasan did his PhD from the University of Essex, UK and MS from College of EME, NUST. Dr Hasan has completed two HEC funded projects in the field of cyber security. His research interests include Physically Unclonable Functions, network security, IoT security, cloud security. He is a senior member IEEE and an Associate Fellow of Higher Education Academy UK.

Topic of the Talk:

Physically Unclonable Functions - A Novel Root of Trust for Cryptographic Implementations.

Abstract:

Cryptographic algorithms typically rely on algorithmic intractability thus making it difficult for adversaries to break the mathematical basis. As computation power becomes common particularly with the advent of cloud. It is only a matter of time that through computation the algorithmic intractability will be defeated. This talk will look into Physically Unclonable Functions (PUF) as modern / novel roots of trust that can be used to form the basis of cryptographic implementations. The talk will bring to light innovative hardware fingerprinting concepts and how they can revolutionize cryptography. The talk will also focus on the inherent limitations of PUFs and how these can be overcome.

Dr. Shahzaib Tahir Butt,

Assistant Professor,
Co-PI Information Security and Privacy Lab,
Department of Information Security,
Military College of Signals (MCS),
NUST, Islamabad, Pakistan.

Biography:

Dr Shahzaib Tahir, is an entrepreneur, security advisor and an academician with several years of experience in the Cyber Security sector. He specializes in Cloud Security and has been involved in several industrial Cyber Security projects that helped him identify the gap within the Cloud Security sector. Hence, he Co-founded CityDefend Cyber Security Solutions Limited, UK and currently holds the position of Chief Technical Officer (CTO) at CityDefend. CityDefend is the result of his PhD work at City, University of London; and amongst many accomplishments, CityDefend has been successful through the InnovateUK Cyber Security Academic Startup Accelerator Programme (CyberASAP). In 2020, CityDefend was listed among the top five enterprise security start-ups in the UK, by The Enterprise Security Magazine.

Shahzaib has a passion for teaching where he seeks to bridge the gap between academia and the industry. He is an Assistant Professor at the National University of Sciences and Technology (NUST), Pakistan, where he leads the Information Security and Privacy (ISP) Research Group. ISP carries out cutting edge research on topics including Searchable Encryption and Privacy-preserving techniques in the Cloud, Aviation and Maritime security, and Blockchains. Shahzaib is a senior member of IEEE and has won several grants from the UK, EU and Pakistan.

Topic of the Talk:

Securely Preserving Water Memory through Searchable Encryption.

Abstract:

It is purported that water has memory of its own and the ability to retain memory of the substances that are dissolved into it, even after being substantially and serially diluted. It is observed that the microscopic pattern of water obtained from the same vessel by different people is unique but can easily distinguish those individuals if the same experiment is executed repeatedly. Furthermore, extensive research is already underway that explores the storage of data on water and liquids. This leads to the requirement of taking the security and privacy concerns related to the storage of data on water into consideration, especially when the real-time collection of data related to water through the IoT devices is of interest. Otherwise, the water memory aspect may lead to leakage of the data and, consequently, the data owner's identity. Therefore, this talk for the first time highlights the security and privacy implications related to water memory and discuss the possible countermeasures to effectively handle these potential threats. The talk will also present a framework to securely store sensitive data on water.

Biography of Malware Workshop Trainers

Ali Fayyaz

Ali Fayyaz is an Information Security Engineer and Researcher. He is currently leading a Malware Analysis Group. He has spent over 15 years as a security professional focusing on: Digital and Network Forensics, vulnerability assessment, auditing, penetration testing, and incident response. He has also served as a cyber security trainer. He holds an MS in Information Security and has taken many certifications and trainings, including: CHFI | CEH | CISCO | HUAWEI | CISSP.

Muddassar Masood

Muddassar has 12+ years experience in information security domain. He has worked as a Security Consultant with Symantec Partners in Pakistan and is a Symantec Certified Security Specialist. He has also worked as Senior Researcher at NUST to develop a Web Application Firewall (WAF). He has six research publications to his credit. His research interests, include: threat Intelligence, threat hunting, malware analysis, network forensic, anti-virus IDS / IPS & WAF signatures development, vulnerability assessment, and penetration testing. He has an MS in Information Technology from NUST.

Abid Khan Jadoon

Abid Khan Jadoon is a security researcher primarily focused on malware analysis, IDS, and Threat hunting. During his MS he has done research on Tor browser forensics. He loves to code small scripts which help his team in malware analysis and signature development. During his free time, he is mostly busy in researching about new APT attacks, malware trends and lately Russia-Ukraine cyberwar.

Title of the Workshop:

Packed Malware Analysis.

Abstract:

Malware writers now pack malwares and use anti-analysis techniques to hide full functionality of malwares. This workshop will build foundations to analyze packed malware through advance static and dynamic analyses by using disassembler, debugger and other freely available tools. Interactive workshop will cover essential assembly concepts relevant to reverse engineering and core OS concepts to deal an executable in perspective of malware analysis. Live demonstration will cover analysis of packed malicious windows 32-bit executable with brief outline as:

- Recognizing packed Windows malware
- Unpacking malicious code
- Retrieving malicious code from dumped memory
- Understanding core Intel x86 key disassembling constructs
- Reverse Engineering, Disassembling with IDA Pro
- Unpacking via Advance Dynamic Analysis, Payload extraction