BRIEF TECHNICAL PLAN – Cyber Security Track, IBCAST-2021 (12-15 January, 2021).

CONFERENCE OPENING MESSAGE: 0930-0945 Hrs (12 January, 2021).

	Session – 1 (1000-1130 Hrs.)	Break: 1130-1150 Hrs.	Session – 2 (1150-1300 Hrs.)	Break: 1300-1400 Hrs.	Session – 3 (1400-1600 Hrs.)
DAY-1: 12 Jan	**LOCAL INVITED TALKS** **Dr. Haider Abbas, Military College of Signals (MCS), and National Cyber Security Auditing and Evaluation Lab, NUST, Pakistan.** (35 Mins: 1000-1035 Hrs.) **Topic:** Cyber Threats in the COVID'19 Pandemic Era. **Dr. Haroon Mehmood, Dept of CS, National Univ. of Computer & Emerging Sciences, Lahore, Pakistan.** (35 Mins: 1035-1110 Hrs.) **Topic:** Auditing of IoT Systems to identify hardware and software vulnerabilities. **CONTRIBUTED PAPER ID: CS-545**. (20 Mins: 1110-1130 Hrs.)		**FOREIGN INVITED TALK** **Mr. Andrey Golov, Security Code, Russia.** (35 Mins: 1150-1225 Hrs) **TOPIC:** Supply-chain attacks in interconnected world. **TECHNICAL WORKSHOP** **Mr. Yasir Emre Bulut, CC Lab, Tubitak BİLGEM, Turkey.** (40 Mins: 1225-1305 Hrs.) **TITLE:** IT Security Evaluations: Common Criteria and Effects of Security Analysis.		**FOREIGN & LOCAL INVITED TALKS** **Mr. Denis Legezo, Kaspersky, Russia.** (45 Mins: 1400-1445 Hrs) **TOPIC:** OrigamiElephant and other campaigns in Pakistan and around. **Mr. Adli Wahid, Asia Pacific Network Information Centre (APNIC), AP-CERT Brisbane, Australia.** (45 Mins: 1445-1530 Hrs) **TOPIC:** Observations and lessons learned from the APNIC Community Honeynet Project. **Dr. Rafi us Shan, KP CERC, Khyber Pakhtunkhwa Information Technology Board (KPITB), Pakistan.** (30 Mins: 1530-1600 Hrs.) **Topic:** Challenging in Conceptualizing Pakistan as Cyber Power.
DAY-2: 13 Jan	**TECHNICAL WORKSHOP** **Mr. Adli Wahid, Asia Pacific Network Information Centre (APNIC), AP-CERT, Brisbane, Australia.** (90 Mins: 1000-1130 Hrs.) **TITLE:** Practical packet analysis and intrusion detection with Suricata IDS.		**FOREIGN INVITED TALK** **Dr. Zahri Yunos, CyberSecurity Malaysia, Malaysia.** (45 Mins: 1150-1235 Hrs) **TOPIC:** Cyber Resiliency in Critical Infrastructure Environment. **CONTRIBUTED PAPER ID: CS-67.** (20 Mins: 1235-1255 Hrs.)		**LOCAL INVITED TALK & TECHNICAL WORKSHOPS** **Dr. Hanif Durad, PIEAS, Nilore, Pakistan.** (30 Mins: 1400-1430 Hrs.) **Topic:** Cyber Security Ecosystem – An integrated approach. **Dr. Rafi us Shan, KP CERC, KPITB, Pakistan.** (45 Mins: 1430-1515 Hrs.) **TITLE:** Android Mobile Application Pen-Testing: Methodologies and Tools. **Ms Ramsha Saeed, NCSAEL, MCS, NUST.** (45 Mins: 1515-1600 Hrs.) **TITLE:** Fake News detection using AI.
DAY-3: 14 Jan	**FOREIGN & LOCAL INVITED TALKS** **Dr. Ilya Trifalenkov, Cybersecurity Expert, Russia.** (45 Mins: 1000-1045 Hrs.) **Topic:** National PKI infrastructure: what is it and how to create? **Dr. Naveed Riaz Ansari, PAEC, Pakistan.** (30 Mins: 1045-1115 Hrs.) **Topic:** Block Cipher Evaluation Criteria. **CONTRIBUTED PAPER ID: CS-659.** (20 Mins: 1115-1135 Hrs.)		**FOREIGN INVITED TALK** **Mr. Mikahil Kudinov, Russian Quantum Centre, QApp, Bauman Moscow State Technical University, Moscow, Russia.** (50 Mins: 1150-1240 Hrs) **TOPIC:** Security analysis of SPHINCS+. **CONTRIBUTED PAPER ID: CS-154** (20 Mins: 1240-1300 Hrs.)		**CONTRIBUTED PAPER IDs: CS-420, CS-524, CS-477, CS-353, CS-667.** (20 Mins each: 1400-1540 Hrs.) **LOCAL INVITED TALK** **Dr. Abid Hussain, CESAT, Pakistan.** (30 Mins: 1540-1610 Hrs.) **Topic:** Unconventional Threats for Data Proliferation.
DAY-4: 15 Jan	**FOREIGN INVITED TALKS** **Mr. Evgeny Goncharov, Kaspersky Lab ICS CERT, Kaspersky, Russia.** (45 Mins: 1000-1045 Hrs.) **TOPIC:** Quality of Information on ICS Vulnerabilities. How to Establish Effective Vulnerability Assessment Process for an Industrial Enterprise? **Mr. Maxim Sirotkin, Security Code, Russia.** (45 Mins: 1045-1130 Hrs.) **TOPIC:** Cryptopods and anti-fraud calls application as tools to secure mobile voice communication.		**CONFERENCE CLOSING REMARKS: 1145-1200 Hrs (15 January, 2021).**		

Technical Program of Cyber Security Track (IBCAST-2021) – Day 1 (Tuesday 12 January, 2020)

TIME	TOPIC	SPEAKER / TRAINER
0930-0945	**CONFERENCE OPENING MESSAGE**	
1000-1035	Cyber Threats in the COVID'19 Pandemic Era.	Local Invited Talk by **Dr. Haider Abbas,** Military College of Signals, and National Cyber Security Auditing and Evaluation Lab, NUST, Pakistan.
1035-1110	Auditing of IoT Systems to identify hardware and software vulnerabilities.	Local Invited Talk by **Dr. Haroon Mehmood,** Dept of CS, National Univ. of Computer & Emerging Sciences, Lahore, Pakistan.
1110-1130	**PAPER ID: CS-545** – Cryptanalysis of Resource Constraint IoT Network Authentication Protocol.	**Osman Khan,** Bahria University Islamabad.
1130-1150	**BREAK**	
1150-1225	Supply-chain attacks in interconnected world.	Foreign Invited Talk by **Mr. Andrey Golov,** Security Code, Russia.
1235-1315	IT Security Evaluations: Common Criteria and Effects of Security Analysis.	Technical Workshop by **Mr. Yasir Emre Bulut,** CC Lab, Tubitak BİLGEM, Turkey.
1300-1400	**BREAK**	
1400-1445	OrigamiElephant and other campaigns in Pakistan and around.	Foreign Invited Talk by **Mr. Denis Legezo,** Kaspersky, Russia.
1445-1530	Observations and lessons learned from the APNIC Community Honeynet Project.	Foreign Invited Talk by **Mr. Adli Wahid,** Asia Pacific Network Information Centre (APNIC), AP-CERT, Brisbane, Australia.
1530-1600	Challenging in Conceptualizing Pakistan as Cyber Power.	Local Invited Talk by **Dr. Rafi us Shan,** KP CERC, Khyber Pakhtunkhwa Information Technology Board, Pakistan,

Technical Program of Cyber Security Track (IBCAST-2021) – Day 2 (Wednesday 13 January, 2020)

TIME	TOPIC	SPEAKER / TRAINER
1000-1130	Practical packet analysis and intrusion detection with Suricata IDS.	Technical Workshop by **Mr. Adli Wahid,** Asia Pacific Network Information Centre (APNIC), AP-CERT, Brisbane, Australia.
1130-1150	**BREAK**	
1150-1235	Cyber Resiliency in Critical Infrastructure Environment.	Foreign Invited Talk by **Dr. Zahri Yunos,** CyberSecurity Malaysia, Malaysia.
1235-1255	**PAPER ID: CS-67** – A Taxonomy of Insider Threat in isolated (air-gapped) Computer Networks.	**Arshad Masood,** Air University, Islamabad.
1300-1400	**BREAK**	
1400-1430	Cyber Security Ecosystem – An integrated approach.	Local Invited Talk by **Dr. Hanif Durad,** Dept of Comp. & Info Sciences (DCIS), Pakistan Institute of Engg & Applied Scs (PIEAS), Nilore, Pakistan.
1430-1515	Android Mobile Application Penetration Testing: Methodologies and Tools.	Technical Workshop by **Dr. Rafi us Shan,** KP CERC, KPITB, Pakistan.
1515-1600	Fake News detection using AI.	Technical Workshop by **Ms. Ramsha Saeed,** NCSAEL, MCS, NUST, Pakistan.

Technical Program of Cyber Security Track (IBCAST-2021) – Day 3 (Thursday 14 January, 2020)

TIME	TOPIC	SPEAKER / TRAINER
1000-1045	National PKI infrastructure: what is it and how to create?	Foreign Invited Talk by **Dr. Ilya Trifalenkov,** Cybersecurity Expert, Russia.
1045-1115	Block Cipher Evaluation Criteria.	Local Invited Talk by **Dr. Naveed Riaz Ansari,** PAEC, Pakistan.
1115-1135	**PAPER ID: CS-659** – Critical Analysis of Internet Country Code Top-level Domain (ccTLD) of Pakistan.	**Muhammad Salman Khan**, Independent Researcher, Islamabad, Pakistan.
1130-1150	**BREAK**	
1150-1240	Security analysis of SPHINCS+.	Foreign Invited Talk by **Mr. Mikahil Kudinov,** Dept of Info Security, Russian Quantum Centre, QApp, Bauman Moscow State Technical Univ., Moscow, Russia.
1240-1300	**PAPER ID: CS-154** – A Pragmatic Analysis of Pre- and Post-Quantum Cyber Security Scenarios.	**Mr. Shah Fahad** for Dr. Arshad Ali, CESAT, Islamabad.
1300-1400	**BREAK**	
1400-1420	**PAPER ID: CS-420** – Design and development of Noise Generator for protection of smart devices from eavesdropping.	**Syed Muhammad Sajjad,** Riphah International University, Islamabad, Pakistan.
1420-1440	**PAPER ID: CS-524** – An Investigation into Detection of Radio Frequency Receivers in a Noisy Environment.	**Iqra Shahzadi,** Institute of Space Technology, Islamabad.
1440-1500	**PAPER ID: CS-477** – Secure Framework to Resolve Security Issues and Malware Detection in Cloud Computing.	**Zahid Hussain,** Huazhong University of Science and Technology, Wuhan.
1500-1520	**PAPER ID: CS-353** – Optimality of Feature set for Intrusion Detection System.	**Muhammad Rizwan,** Capital University of Science and Technology, Islamabad.
1520-1540	**PAPER ID: CS-667** – On Parametric Hardware Troajns.	**Raeesa Naseem,** NUST, Islamabad.
1540-1610	Unconventional Threats for Data Proliferation.	Local Invited Talk by **Dr. Abid Hussain,** CESAT, Pakistan.

Technical Program of Cyber Security Track (IBCAST-2021) – Day 4 (Friday 15 January, 2020)

TIME	TOPIC	SPEAKER / TRAINER
1000-1045	Quality of Information on ICS Vulnerabilities. How to Establish Effective Vulnerability Assessment Process for an Industrial Enterprise?	Foreign Invited Talk by **Mr. Evgeny Goncharov,** Kaspersky Lab ICS CERT, Kaspersky, Russia.
1045-1130	Cryptopods and anti-fraud calls application as tools to secure mobile voice communication.	Foreign Invited Talk by **Mr. Maxim Sirotkin,** Security Code, Russia.
1130-1150	**BREAK**	
1145-1200	**CONFERENCE CLOSING REMARKS**	

FOREIGN INVITED SPEAKERS AND TECHNICAL WORKSHOP TRAINERS

Mr. Andrey Golov,

Chief Executive Officer (CEO),
Security Code Ltd.,
Moscow, Russia.

Biography:

Andrey Golov is the Chief Executive Officer at Trusted Access Technologies. He has more than 15 years of executive experience on IT and Security positions. He is responsible for overall strategy for overseeing all business functions, go-to-market activities, attainment of strategic, operational and financial goals. Andrey has degree in mathematics, financial analysis and MBA degree in IT management. Andrey also holds CISSP and CISA certificates.

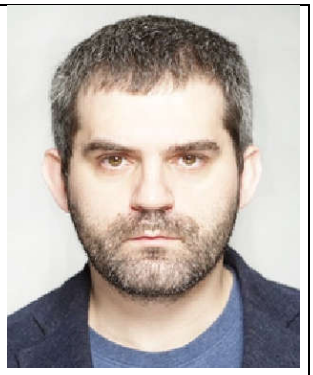
Topic of the Talk:

Supply-chain attacks in interconnected world.

Abstract:

The speaker will talk about IT software supply-chain attacks:

- Why risk averse customers should consider them as highly dangerous?
- Examples of such attacks (the recent SolarWinds incident among others) and lessons learned from them.
- How to prevent them or at least how to tackle them?



Mr. Evgeny Goncharov,

Head of Kaspersky Lab ICS CERT,
Kaspersky, Russia.

Biography:

Mr. Evgeny Goncharov has more than 16 years of experience in IT Security. He is the Head of Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT) since 2017. He has been driving ICS cybersecurity research and development since 2014.
He was the Head of Kaspersky Critical Infrastructure Defence, driving Kaspersky ICS cyber security research, product and services development during 2014-2016. From 2013-2014, he led the Kaspersky team protecting Sochi 2014 Olympic Games infrastructure from malware and targeted attacks. Before that he had managed Kaspersky Hosted Security Service and various Kaspersky 'nix product development.

Topic of the Talk:

Quality of Information on ICS Vulnerabilities. How to Establish Effective Vulnerability Assessment Process for an Industrial Enterprise?

Abstract: Continuous vulnerability assessment and mitigation is the keystone of any enterprise cybersecurity, recommended by each and every regulation authority and almost all security experts. But as the security outbreaks of the past showcase, in reality, that's not that simple for many organizations to implement it even for their IT systems. And when it comes to OT

infrastructures it requires approaches different from what normally works for IT environments. And it faces some problems systematically having no convenient solution and sometimes no any solution at all. How deep the rabbit whole is and how to overcome the security gap for industrial enterprises we will try and figure out during the talk.

Denis Legezo,

Senior Security Researcher,
Global Research and Analysis Team (GreAT),
Kaspersky Lab,
Russia.

Biography:

In Kaspersky Denis Legezo is working as Senior Security Researcher with Global Research and Analysis Team (GReAT). He specialized on targeted attacks research, reverse engineering for malware analysis. Denis regularly providing trainings for the customers on these matters. He got his degree at cybernetics and applied mathematics facility of Moscow State University in 2002. His diploma topic was directly related to information security. Then he started his career as a programmer in different public and commercial companies. Before joining Kaspersky Lab in the beginning of 2014, he worked as a technical expert for one of the Russian IT companies. He presented his targeted malware researches at RSA, HITB, SAS, VirusBulletin, MBLT Dev.

Topic of the Talk:

OrigamiElephant and other campaigns in Pakistan and around.

Abstract:

In 2020 we registered and reported malicious Android targeted campaign, which we attributed to OrigamiElephant. In this talk we would cover technical details of this campaign as well as others affected the region lately. In some samples' digital certificate real and existing IT-company was mentioned, but there is technical possibility that it was just spoofed
Our telemetry and Pakistani National Telecom & Information Technology Security Board reported it spreads through WhatsUp, SMS, social media. At least some of the targets were military ones. In this case Trojan mimics a set of popular Android applications as well. This time no publicly available trojan was the tool of choice: the custom modules written in Kotlin and Java with usage of SQLite database and JSON data format were signed. Seems like mobile development is more and more must have for the actors.

Dr. Zahri Yunos,

Chief Operating Officer,
CyberSecurity Malaysia,
Malaysia.

Biography:

Dr Zahri Yunos is currently the Chief Operating Officer of CyberSecurity Malaysia, an agency under the Ministry of Communications and Multimedia, Malaysia. Prior to joining CyberSecurity Malaysia, Zahri has served the Government of Malaysia as well as other private organizations. Zahri is a certified Associate Business Continuity Professional by the Disaster Recovery Institute International, USA and has been awarded Senior Information Security Professional by the (ISC)2, USA. Zahri also has contributed various publications and presented papers on topics related to cyber security, cyber terrorism and business continuity management. Zahri holds a PhD in Information Security from the Universiti Teknikal Malaysia Melaka (UTeM), Malaysia.

Topic of the Talk:

Cyber Resiliency in Critical Infrastructure Environment

Abstract:

Cyber threats are evolving at an exponential rate with new methods for infection, infiltration and evasion. Any successful cyber-attacks on critical infrastructure systems can have serious cascading effects on other systems as well, resulting in potential catastrophic damages and disruptions. There are several cyber incidents in Malaysia which involve critical infrastructure organizations such as ransomware, business email compromise and data breaches. In view of this, organizations which face Advanced Persistent Threat (APT) in the form of malware attacks should tackle such challenges in more innovative ways in order to protect the interests of their various stakeholders and customers. This presentation provides an insight on CyberSecurity Malaysia initiatives in protecting critical infrastructure organizations against malware threats. CyberSecurity Malaysia has developed an application called CMERP (Coordinated Malware Eradication & Remediation Platform). The application is able to detect, quarantine, eradicate and remediate malware threats. Continued research in this area can be further conducted, which may lead to the development of strategic and technological framework to counter global cyber threats.

Mr. Maxim Sirotkin,

Deputy Chief Technical Officer (Innovations and Development),
Security Code Ltd.,
Moscow, Russia.

Biography:

Maxim Sirotkin is the Deputy Chief Technical Officer in innovations and development at Security Code, Russia – the TOP 3 biggest players in IT-security in Russia. He is experienced as marketing and innovations director at different tech and non-tech companies focusing on new products development, digital transformations and strategic marketing leading to commercial results with up to x10 annual growth pace. Sirotkin is ESADE Business School (the #1 in Entrepreneurship in Europe, FT2019) EMBA graduate with good understanding of global markets managing and studying business in US, Brazil, Russia, India, CIS countries and Spain. His current role at Security Code includes development of innovative customers protection products in IT sector based on the latest global and local trends.

Topic of the Talk:

Cryptopods and anti-fraud calls application as tools to secure mobile voice communication.

Abstract:

Global pandemic and 5G development drives the annual double digit growth of global voice and mobile traffic. Fraud-calls and encryption of voice communication starts to attract greater attention of governments in the world. Even special military services and governmental structures appear on the list of the victims of so called «number substitution» leading to the leak of classified data. Entrepreneurs are suffering from unfair competition and banks clients are facing fraud credit card transactions. In Russia fraud calls from so called banks led to 50M. USD losses and amount of fraud operations reached 360K with 40% annual growth in 2020.

Dr. Ilya Trifalenkov,

Independent Cybersecurity Expert,
Russia.

Biography:

Dr. Ilya Trifalenkov was born in 1963. He graduated from the physical department of Moscow University, Russia in 1986. Since 1995 he is specialized in computer security and trusted services. He has worked both for private and state companies in the field of IT security. In 2006 he got his PhD in information security. During 2011-2013 he worked as head of security department in Rostelecom, the largest IT and telecom operator in Russia. During this time he was leader in a project for Russian government electronic infrastructure in the fields of security and trusted services. Now Dr. Ilya is an independent expert in cybersecurity trusted services and security compliance.

Topic of the Talk:

National PKI infrastructure: what is it and how to create.

Abstract:

Most PKI solutions deal with business services. But in the case of governmental services, we need to take into account some important specifics. As a result, the problem of national PKI is not covered by traditional PKI solutions. We faced the following challenges and problems: **National PKI infrastructure model** (PKI infrastructure can be designed in different models of management and interactions: hierarchical model, cross-certification model, bridges model); **Authentication** (To apply a digital signature, we need to associate signature service and subject. It requires strong authentication to get access to services. Therefore we need to design both PKI and authentication infrastructures); **Rights and powers** (The digital signature can be different for various cases. During PKI infrastructure design, we have to understand, how we will get/assign rights for digital signature applications for each case); **M2M PKI application** (Trust mechanisms can be used not only for people's actions but also for IT systems and services. In these cases, we have to understand and determine rules and conditions for digital signature applications. Those will be special conditions and they need be taken into consideration both in legal regulation and in technical solutions); **Indemnity & Insurance** (We use trust services to support legally significant actions. The main government's purpose is to guarantee all legal significant actions, so the government is responsible for services, based on national PKI. Therefore we need to develop standards and requirements for PKI-based services, indemnity, and insurance measures to deal with trust services utilization in case of possible losses).
Based on Russian experience we suggest hierarchical PKI architecture as a base of national PKI. In this architecture it is possible to use all necessary services, such as: Authentication and rights management; Certificate authorities SLA monitoring; Time service; Certificates archiving; Digital signature service; Trans-border digital legitimacy, etc.
To design national PKI we need not only to understand technical services and solutions to provide these services but also a set of standards to implement PKI-based services as a national framework. As main conclusions, we declare that:

- We don't need PKI infrastructure, but we need PKI-based services
- National PKI is not only a technical but multi-discipline project
- National PKI has to be integrated with authentication and rights management services
- A number of standards and regulations are necessary for national PKI
- We have necessary components for national PKI on market, but we need a System and it's a different task

Also, we take into account the Russian experience of national PKI system design and main conclusions from this experience.

Mr. Yasir Emre Bulut,

OKTEM LAB Manager,
TÜBİTAK BİLGEM,
Turkey.

Biography:

Yasir Emre Bulut is an Electronics Engineer and Cyber Security specialist who is currently working as Laboratory Manager at OKTEM Laboratory (TUBITAK). He graduated from Istanbul Technical University with bachelor's degree in Electronics Engineering in 2010. After graduating, he went to Goldey - Beacom College in Delaware, USA for Master's degree and completed Master of Business Administration with concentration in IT in 2012. In addition, he completed second Master's degree of Cyber Security Engineering in Turkey. Currently, he is continuing his PhD in Industrial Engineering by working in the field of artificial intelligence. He is currently managing Common Criteria Evaluations, Crypto Module Tests and participating into security related projects.

Title of the Workshop:

IT Security Evaluations: Common Criteria and Effects of Security Analysis

Brief Description:

Common Criteria provides a comprehensive methodology for specifying, implementing, and evaluating the security of IT products and systems. It details commonly accepted criteria for the design, development and evaluation with regard to cyber security considerations. While evaluating all development stages of a product, it questions all kinds of security-related controls throughout the entire life cycle. It examines the requirements for the secure delivery and secure usage of the product after development. With functional and penetration tests, the features offered by the products will be verified and security breaches will not be revealed. Emerging security vulnerabilities show that the main reasons of breaches are the deficiencies in the development stages and configuration errors. For these reasons, standards such as common criteria and testing and evaluation processes are of great importance. The speech will mostly be on these issues, and life-saving testing and evaluation processes will be mentioned.

Mr. Adli Wahid,

Senior Internet Security Specialist,
Asia Pacific Network Information Centre (APNIC), AP-CERT
Brisbane, Australia.

Biography:

Adli Wahid is a Security Specialist at the Asia Pacific Network Information Centre (APNIC). He is responsible for the APNIC's security engagement and outreach program. His engagement activities include providing technical support & training for network operators, Law Enforcement Agencies and CERTs/CSIRTs. Adli is also the technical lead for the APNIC Community Honeynet Project. Adli has more than 10 years of experience with the security response community. Prior to joining APNIC, Adli was the Head of Malaysia CERT (MYCERT) and had served as a member of Bank of Tokyo Mitsubishi UFJ Security Response Team (MUFG-CERT). Adli has also served as the Board member of the Forum of Incident Response and Security Teams (FIRST.org) from 2014-2019.

Topic of the Talk:

Observations and lessons learned from the APNIC Community Honeynet Project.

Abstract:

Honeypots are resources deployed to be attacked and probed. The value of honeypots to security defenders are immense. Not only it can be useful for detection of anomalies and malicious activities but also used to understand the gaps in security practices. The APNIC community honeynet project has been running for more than 2 years with partners in the Asia Pacific region. The talk will highlight key observations and some thoughts on security realities that can benefit researchers and practitioners.

Title of the Workshop:

Practical packet analysis and intrusion detection with Suricata IDS.

Brief Description:

Suricata is an open source rule-based intrusion detection and security monitoring engine. The tutorial will highlight some of the functionalities through analysis of network packet captures.

Note: Participants will be asked to download a Linux VirtualBox image pre-installed with the tools & pcaps if they would like to do the exercises.

Mr. Mikhail Kudinov,

Researcher, Department of Information Security,
Bauman Moscow State Technical University, Moscow, Russia.

Biography:

Mikhail Kudinov is a research fellow at the Russian Quantum Centre, QApp, Bauman Moscow State University, Skolkovo, Russia. His current field of study is mathematical approach for information security. He is working on cryptography and his main specialization is in post-quantum cryptography, especially the hash-based signatures.

Topic of the Talk:

Security analysis of SPHINCS+.

Abstract:

In this talk, Mikhail will discuss the security of SPHINCS+. SPHINCS+ is a hash-based signature algorithm, which is considered in the NIST Round 3 post-quantum competition. He will discuss the details of the security proof of this algorithm with a focus on W-OTS+ part.

LOCAL INVITED SPEAKERS AND TECHNICAL WORKSHOP TRAINERS

Dr. Haider Abbas,

Head of Department (Research),
Military College of Signals, NUST.
Director National Cyber Security Auditing and Evaluation Lab,
NUST, Pakistan.

Biography:

Dr. Haider Abbas is the Director of National Cyber Security Auditing and Evaluation Lab (NCSAEL) and the Head of R&D at MCS- NUST, Pakistan. He is a Cyber Security professional, academician, researcher and industry consultant who took professional trainings and certifications from Massachusetts Institute of Technology (MIT), United States, Stockholm University, Sweden, Stockholm School of Entrepreneurship, Sweden, IBM, USA and EC-Council. He received his MS in Engineering and Management of Information Systems (2006) and PhD in Information Security (2010) from KTH- Royal Institute of Technology, Sweden.

Dr. Abbas has been appointed by Springer as fulltime Regional Editor for the Neural Computing and Application (ISI-Indexed, Q1, IF 4.6) for all submission from Iran and Pakistan. He is also serving as fulltime Associate Editor for the IEEE Communication Magazine (ISI-Indexed, Q1, IF 10.2), IEEE Transactions on Information Technology in Biomedicine/IEEE Journal of Biomedical and Health Informatics (ISI-Indexed, Q1, IF 4.2), Journal of Network and Computer Applications (ISI-Indexed, Q1, IF 4.9), Electronic Commerce Research (Springer) (ISI-Indexed, Q2, IF 2.2), IEEE Access (ISI-Indexed, Q1, IF 4.0), Cluster Computing (Springer) (ISI-Indexed, Q2, IF 2.5) and KSII Transactions on Internet and Information Systems (ISI-Indexed). He has also served as Lead Guest Editor for Future Generations Computer Systems (ISI-Indexed, Q1, IF 4.9), Peer to Peer Networking and Applications (Springer) (ISI-Indexed)., IEEE Access (ISI-Indexed), Electronic Markets (ISI-Indexed) and Annals of Telecommunications (Springer) (ISI-Indexed). He has also served as Track Chair for several international conferences including IEEE ECBS-EERC'11, Serbia, IEEE CCNC'15, Nevada, USA, IEEE MobiSPC'15 Belfort, France, IEEE WETICE'18, Paris France, IEEE Healthcom'17, Dalian, China, IEEE BHI'19, University of Illinois at Chicago, IL, USA, (2019), IEEE WETICE'19 Capri, Italy, IWCMC'19, Tangier, Morocco, IEEE DASC'19, Fukuoka, Japan and IEEE MobiSPC'19, Halifax Nova Scotia, Canada.

Dr. Abbas has received several research grants totaling 300+ Million for ICT related projects from various research funding authorities (including Horizon2020, Erasmus+ etc.) and has been working on scientific projects in US, EU, KSA and Pakistan. His professional services include - but are not limited to - Journal Editorships, Industry Consultations, Workshops Chair, Technical Program Committee Member, Invited/Keynote Speaker and reviewer for several international journals and conferences. He has authored over 120 scientific research articles (with cumulative Impact Factor 360+, Citations: 6000+, H-Index: 34) in prestigious international journals (ISI-Indexed) and conferences. He is also serving as an adjunct Faculty Member at Florida Institute of Technology, United States. He is the principal advisor for several graduate and doctoral students at Florida Institute of Technology, United States, Manchester Metropolitan University, United Kingdom, National University of Sciences and Technology, Pakistan, King Saud University, KSA, and Al-Farabi Kazakh National University, Kazakhstan. He has also worked as Information Security Consultant for various multinational firms which include Government and Private organizations based in US, EU, Middle East and Pakistan.

Dr. Abbas has received many awards from National and International organizations. He has been declared Overall NUST University Best Researcher for 2017-2018 among all NUST constituent Colleges and Schools across Pakistan. Some of the significant awards include Research Productivity Award from Pakistan Council for Science and Technology, Best researcher award from MCS, NUST, CyberPatriot from US Airforce Association, USA and Research Excellence from COEIA, KSA. Also, in recognition of Dr. Abbas services to the international research community and excellence in professional standing, he has been awarded

one of the youngest Fellows of The Institution of Engineering and Technology (IET) UK; a Fellow of The British Computer Society (BCS), UK and a Fellow of The Institute of Science and Technology, UK. He has been appointed as 1st ACM distinguished speaker from Pakistan by ACM - Association for Computing Machinery, United States. He has also been elected to the grade of Senior Member of Institute of Electrical and Electronics Engineers (IEEE), USA. He has been appointed as a Member of the Board of Governors for National Information Technology Board (NITB), headed by the President of Pakisan.

Topic of the Talk:

Cyber Threats in the COVID'19 Pandemic Era.

Abstract:

The initial surge of covid-19 started at the end of 2019 and gained peak in 2020 whole world has been enduring from this pandemic. The world took their business activities from physical domain to cyber domain that also resulted in escalation of cyber threats. Increase in online activity reciprocated in sophisticated cyber-attacks, keeping this scenario in mind workload for cyber security professionals boosted as never before in known history. Online business and other activities are being exploited in many ways. Cyber security experts are struggling hard to keep the menace of hackers at bay. The talk shall discuss some of the cyber threats of COVID era and highlight some basic principles that the users should follow to keep their devices safe from cyber threats.

Dr. Muhammad Hanif Durad,

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 Incharge of Critical Infrastructure Protection and Malware Analysis Lab constituent part of National Center for Cyber Security, Pakistan. He is reviewer of reputed journals many 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 Cybersecurity, Cluster/ Grid/ Cloud/ Fog computing.

Topic of the Talk:

Cyber Security Ecosystem- An integrated approach.

Abstract:

Cyber threats are becoming more multipart and sophisticated, a holistic approach is required to implement security strategies. We need careful integration of multi-faceted solutions. This offers an efficient way to address the frequency, complexity, and rapidly-changing-nature of cyber-attacks. In this talk I will give insightful review of how various standardization efforts has focused on mitigating risks and enabling faster incident response to secure our cyber systems.

Dr. Haroon Mehmood,

UET Lahore (IOT Lab)

Biography:

Dr. Haroon Mahmood is currently working as an Assistant Professor in the department of Computer Science at National University of Computer and Emerging Sciences, Lahore. He has received his doctoral degree in Computer and Control Engineering from Politecnico di Torino, Italy with specialization in energy-efficient multi-core systems-on-chip.
In the past, he has been associated with various European projects including STORK, an EU funded project for European Identity Management System and COMPLEX, an EU FP7 integrated Project to develop an architecture for memory optimization. His research interests include several aspects of embedded system design with particular emphasis on the design and modeling of reliable and power-efficient solutions. He is also working in the field of IoT security to analyze the architecture of hardware devices, their firmware and communication mechanism to find security vulnerabilities.

Topic of the Talk:

Auditing of IoT Systems to identify hardware and software vulnerabilities.

Abstract:

Internet of things (IoT) devices, despite gaining tremendous acceptance over the past few years, are still vulnerable to cyber-attacks, e.g., information stealth, intervention of personal devices and usurp the object's functionality. For effective working of these IoT objects, we need to ensure the security of hardware, software and network connectivity of these systems.
Although much has been said about the software stack of IoT but such systems are undoubtedly prone to hardware attacks. Hackers can easily exploit the weaknesses, once the IoT device is acquired. Additionally, security of software components needed to operate hardware can be a challenging task. This talk will unbust the security issues in hardware and low level software of IoT devices. We will discuss and highlight the existing threats and upcoming challenges in the field of IoT, associated vulnerabilities and their exploitations.
One major objective of this talk is to create security awareness among users as the lack of IoT security awareness leaves users and associated companies increasingly exposed to potentially damaging cyber-attacks.

Dr. Rafi us Shan,

Chief Cyber Security,
KP CERC,
Khyber Pakhtunkhwa Information Technology Board (KPITB),
Government of Khyber Pakhtunkhwa, Pakistan.

Biography:

Dr Rafi us Shan is Chief Cyber Security at Khyber Pakhtunkhwa Cyber Emergency Response Center (KP-CERC); an initiative of KPITB to complement the digital ecosystem of Khyber Pakhtunkhwa. Dr Shan is responsible for setting up provincial CERT, standardization of ICT based services, risk and vulnerability assessment & penetration testing of digital assets of the Government of Khyber Pakhtunkhwa. His role is to design, lead and drive Information security framework and information security related initiatives, complementing the digital ecosystem and promoting e-governance solutions in Khyber Pakhtunkhwa. Working in a role of provincial CISO Dr. Shan is steering provincial information security policy and providing services to various provincial and national bodies in relation to information security. He is a member of the President of Pakistan committee on information security and member evaluation board National Center for Cybersecurity (NCCS) and various other national and international forums / bodies. He has served at COMSATS University Islamabad, for over 13 years and has been promoting innovation, product development and technology based startups.

Topic of the Talk:

Challenging in Conceptualizing Pakistan as Cyber Power.

Abstract: Awaited.

Title of the Workshop:

Android Mobile application Penetration Testing: Methodologies and Tools.

Brief Description: Session will cover basic techniques for mobile application Pen-testing.

Dr. Naveed Riaz Ansari,

PAEC, Islamabad.

Biography:

Dr. Naveed Riaz has degrees in Software Engineering (NUST, Pakistan, MS) and Computer Engineering (Graz University of Technology, PhD.) with specialization in Cryptography, Verification and Testing. He has research and application experience in the areas of Hardware verification, Cryptography, Digital Image processing, and distributed computing. He has been associated with NUST and University of Dammam in teaching capacity. He also has over 12 years of industry experience in the field of information security.

Topic of the Talk:

Block Cipher Evaluation Criteria.

Abstract:

Block ciphers are the most commonly used cryptographic primitives. AES is the most widely used block cipher and accounts for the largest proportion of encrypted data. Cryptographers continue to study the cryptanalysis of existing cipher algorithms and design new cipher algorithms for several reasons including and not limited to better performance, better security guarantees, lower costs, resistance to new attacks, and suitability for a particular task and/or platform. Moreover, almost all major nations of the world are looking for achieving cryptographic sovereignty and developing national algorithms due to their reluctance to employ foreign developed cryptographic schemes. Thus, the problem of evaluating the new cryptographic algorithms remains topical.

In this session, I will discuss different criteria that may be used for evaluating block ciphers including security level, key size, throughput, block size, computational complexity, data expansion, error propagation, statistical and implementation characteristics, benchmark performance, cryptanalysis, and resistance to known attacks.

Although AES is considered the best choice for the majority of the block cipher applications and has undergone various implementation advances, it is not considered suitable for resource constraint environments. The objective of Lightweight cryptography is to provide solutions tailored for small computing devices. Lightweight cryptography poses a unique set of security challenges as different devices have different limitations and the suitability of solutions tend to be platform-specific; Tradeoffs between performance, speed, security, cost, and energy consumption are highly important. If time permits, I will discuss some evaluation parameters specific to lightweight cryptographic algorithms like RAM size, chip area, energy consumption, program code size (ROM size), communication bandwidth, execution time, and latency.

Dr. Abid Hussain, CESAT, Islamabad.

Biography: Dr. Abid Hussain, received his MS and PhD degrees in Information Technology from National University of Sciences and Technology (NUST) in 2010 and 2016 respectively. He has above 10 years of experience in the field of Information Technology and Information Security at both public and private organizations. Currently Dr. Abid Hussain is working as Manager (Technical) at a public sector R&D organization in Pakistan. He has 07 research publications in well renowned international journals. His areas of interest include Cyber security threat assessment, Wireless channel band adaptation, physical and MAC layer attacks in wireless networks and stochastic modelling of physical and MAC layer behaviour of wireless networks.

Topic of the Talk:

Unconventional Threats for Data Proliferation.

Abstract: The world is already witnessing the knowledge, informational and technological revolution that is fundamentally changing the way we work, communicate and live. At the same time this ongoing digital transformation and expanding cyberspace, the growing prevalence and severity of cyber-attacks are posing a serious threat to the global economy, job market, national security and relations between nations and regions. While majority of the enterprises are aware of conventional cyber security threats to confidentiality, integrity and availability (CIA) of information and systems they possess, the attackers in today's world are exploiting several un-conventional ways to attack the organizations. The attackers (especially state sponsored) have developed large number of un-conventional attack vectors which are hard to detect and even harder to protect. This talk will generally focus some areas of unconventional cyber security threats and ways attackers use to materialize such attacks.

Ms. Ramsha Saeed,

Researcher,
National Cyber Security Auditing and Evaluation Lab (NCSAEL),
Military College of Signals, NUST, Pakistan.

Biography:

Ramsha Saeed holds a Masters degree in Software Engineering from Military College of Signals (MCS), National University of Science and Technology (NUST), Islamabad, Pakistan. She is currently working as a researcher at National Cyber Security Auditing and Evaluation Lab (NCSAEL), MCS, NUST. Her research interests include machine learning, data science, data mining, and natural language processing.

Title of the Workshop:

Fake News Detection using AI.

Brief Description:

The brief outline of the workshop is as under.

1. Data extraction using Twitter API
2. Content based feature extraction
    a. Embeddings based feature extraction
    b. Sentiment extraction
    c. Writing style feature extraction such as the use of punctuation marks, caps and emojis
3. Social context-based feature extraction
    a. Number of likes
    b. Number of retweets
4. Development of an AI algorithm to classify fake and real news

Prerequisites:
The users should have basic knowledge of python programming language. Python and required libraries (pandas, genism, numpy, tweepy, keras, sklearn, VADER) should be installed.