IEEE

1st Annual

International Conference On CYBER WARFARE & SECURITY

2020

20th - 21st October 2020

Islamabad, Pakistan

2020 International Conference on Cyber Warfare and Security (ICCWS)

20-21 October 2020
Islamabad, Pakistan // Virtual Conference

Conference Booklet

IEEE Catalog Number: CFP20V89-CDR
IEEE ISBN: 978-1-7281-6838-8

Contents

Welcome Note by Conference Patron

Javaid Ahmed

Vice Chancellor, Air University

Dear Participants,

I am pleased to welcome you in this 1st Annual International Conference on Cyber Warfare and Security (ICCWS) organized by National Centre for Cyber Security (NCCS) Pakistan. Cyber Security is a big challenge costing the world billions of dollars losses annually. There is indeed dearth of professionals as this field is constantly evolving with new vulnerabilities and attacks emerging every day. The fast growth of this technology domain demands that we train lot of professionals at a matching pace. Covid-19 pandemic has proved to be another big game changer as we are adapting to the dynamics of cyber world but at the same time the associated vulnerabilities with digital space are required to be adequately dealt with.

From academia perspective, quality cyber security education and trainings are crucial for bridging this very important gap. One of the key challenge is to equip students with practical knowledge and skills to effectively tackle cyber security threats. To abridge this gap, NCCS is playing a vital role to promote research and development activities and establishing academia-industry linkages across the country. ICCWS-2020 is a key initiative of NCCS to provide a scientific platform to the researchers and experts from across the world to share their experiences and proficiencies related to the cyber security domain.

ICCWS-2020 will include high-quality and focused technical program on cyber security with keynote talks from prominent industry and academia experts. The research presented in this conference will be good contribution and value addition in the educational resources and knowledge repositories. The conference will provide networking opportunities to the researchers, students, developers and cyber security professionals from the industry, academia and government organizations. I believe that this conference will provide new opportunities for more national and international collaborations among the stakeholders.

I would like to thank national and international speakers, researchers as well as participants for joining us in this virtual conference. We are especially pleased with the generous support of international speakers including Mr. Fred Baker and Prof. Vern Paxson from USA, Mr. Andrey Golov, Mr. Dmitry Zryachikh and Mr. Evgeny Goncharov from Russia, Dr. Mehmat Akif Nacar, Mr. Murat Husseiyn Candan, and Mr. Abdullah Erten from Turkey, Prof. Dr. Siraj Shaikh from UK, Prof. Dr. Olaf Maennel from Estonia and Ms. Jean Daka from Belgium. I convey my best wishes to all the organizers of 1st IEEE ICCWS 2020.

Welcome Note by Conference Chair

Prof. Dr. Kashif Kifayat

Director NCCS

Dear Participants,

National Centre for Cyber Security (NCCS) was established in June 2018 by Planning Commission of Pakistan through Higher Education Commission (HEC). The Centre constitutes Research and Development (R&D) Labs in 11 reputed universities of Pakistan. These partner Labs were established in different specialized areas of cyber security such as software security, networks security, smart devices and IoT security, Internet security and privacy, security auditing and testing, critical infrastructure security, Blockchain security, digital forensics and cybercrimes. The objective of NCCS is to instigate R&D activities, producing skilled human resource as well as the development of indigenous products and practical applications/toolkits in the specialized domain of Cyber Security to contribute its part in the protection of national cyberspace. The secretariat of NCCS is housed at Air University Islamabad.

ICCWS-2020 is the first IEEE technical sponsored educational conference in Pakistan that is solely focused on cyber security. The agenda of this conference covers a wide range of topics related to recent advances in the field of cyber security and its allied areas. In this two days conference event, researchers and practitioners working in cyber security and related domains will share their research ideas and experiences related to the state-of-the-art as well as in the emerging areas of cyber security. In total, 171 papers were submitted from 16 different countries out of which 23 papers will be presented in ICCWS. These papers were selected through a double blind peer-review process by the technical program committee comprised of renowned cyber security academicians from national and international universities. Moreover, keynote speeches and technical talks by leading cyber security experts from across the world will be part of conference program along with 2 well-focused panel discussions. I hope that the challenges and opportunities identified by the keynote speakers and panelists will help well in recognizing cyber security importance, developing better understanding and resilience within the respective organizations, stakeholders as well in personal life.

We warmly welcome all the national and international participants and encourage them to share their knowledge and discuss the way forward for creating cyber security awareness and making Pakistan a digitally secure and safe place to live and work online. We also appreciate our collaborators, sponsors and supporters, without their support we would not be able to organize this event. We hope you find ICCWS-2020 a valuable experience.

1st IEEE INTERNATIONAL CONFERENCE ON CYBER WARFARE AND SECURITY 2020 (ICCWS)

Call for Paper:

Cyber Security is a rapidly growing global challenge with new sophisticated zero-day attacks costing economies billions of dollars annually. Cyber-attacks may particularly affect the developed world, but developing countries are also at higher risk due to the lack of expertise and shortage of security professionals with adequate skills and experience to effectively combat the rising threats. There is a persistent need for initiatives that can produce skilled resources and carry out Research and Development (R&D) activities in the specialized areas of Cyber Security. National Centre for Cyber Security (NCCS) is an R&D initiative of Government of Pakistan to promote research and human resource development in the fields of Cyber Security. NCCS in technical co-sponsorship and joint collaboration with IEEE Islamabad Section (R-10) is organizing a three days conference event, i.e. ICCWS-2020; to invite researchers and practitioners around the World to share their original research ideas and experiences related to the state-of-the-art as well as the emerging areas of Cyber Security. ICCWS-2020 will include high-quality and focused technical program on Cyber Security with keynote talks from prominent industry and academia experts. The conference will also feature an attractive Lab-to- Market Event aimed at industry practitioners, vendors and local start-up companies.

Main topics of interests:

Following areas and others closely related topics:

- Networks and infrastructure security
- Hardware and systems security
- Operating systems and software security
- Embedded systems, IoT and Cyber Physical Systems (CPS) security
- Web, Big data and Cloud security
- Edge/Fog computing and data centre security
- Information security and data provenance
- Cyber warfare
- Information assurance
- Cryptology, cryptanalysis and security analysis of cryptographic primitives and protocols
- Prevention, detection and investigation of APTs, Botnets, DDoS and other cyber attacks
- Anti-malware techniques: detection, analysis, and prevention
- Security and privacy of systems based on Machine Learning and Artificial Intelligence
- Artificial Intelligence aided security and privacy concerns
- (Adversarial) Machine learning and cyber deception
- (Anti-) Reverse engineering, side channels and physical attacks
- Protection of Digital Services
- Digital forensics, social media, networks, computer and mobile forensics
- Automated security analysis of protocols, source code and binaries
- Measurements and monitoring of human behavior in cyberspace
- Security, Privacy, and Trust in Digital Payments and Crypto-currencies
- Security and privacy issues in Blockchain
- Security, privacy and resilience in critical infrastructures
- Testing, auditing and evaluation of security architectures and models
- 5G Security issues and architectural requirements with privacy considerations
- Energy efficient security in IoT and CPS
- Security for future Internet architectures and designs
- Authentication, Identification, Authorization and Biometrics
- Cybercrime defense (anti-phishing, anti-blackmailing, anti-fraud, etc.) techniques
- Legal Aspects of Cyber Security (Cyber Laws and Regulations)

HINTS FOR ATTENDING ONLINE CONFERENCE

On behalf of the programs committee that helped to set up various sessions for this conference, we invite you to get ready to learn and network with other researchers and professionals. This conference truly has something for everyone. The committee has worked diligently to create the best lineup of keynote speakers.

Attending the online session

Program Schedule

The conference schedule has been designed to deliver comprehensive, timely session. We expect most of the sessions to be complete in time, so please join the sessions timely. While joining please identify yourself and keep your full name as joining Id. Use chat option to seek any guidance from organizers or convey your concerns to session chairs.

Be a Good Audience Member

Presenting your research is very important and it requires time, effort to prepare, it is not easy as it seems. Please be vigilant about timing, be considerate about Q/A option and Chat Panel available in Zoom Meeting Software to coordinate with organizers. Please be patient and avoid disruption by unmuting your mic or any other methods.

Your Feedback is Important

This conference purpose is to create cyber security awareness and promote its related R&D activities by providing a networking platform. As your presence is valued to us we really appreciate you to share your feedback and suggestions. We will definitely consider it to further improve this event.

The Conference Staff

Conference organizers are available to answer any questions or address any concerns you may have about the conference or facilities.

ORGANIZING COMMITTEE

Patron:

Javaid Ahmed, Air University Islamabad, Pakistan

General Chair:

Kashif Kifayat, National Centre for Cyber Security, Air University Islamabad, Pakistan

Program Chair:

Amir Qayyum, Capital University of Science and Technology, Lahore, Pakistan

Technical Program Committee Chair:

Haider Abbas, MCS, National University of Science and Technology, Pakistan

Tracks and Workshops Chairs:

Adil Sultan, Air University Islamabad, Pakistan
Asad Arfeen, NED University of Engineering and Technology, Karachi, Pakistan
Ghalib A. Shah, University of Engineering and Technology Lahore, Pakistan
M. Hanif Durad Pakistan Institute of Engineering and Applied Sciences, Islamabad, Pakistan
Muhammad Imran, Air University, Islamabad, Pakistan
Najam us Siraj, Sir-Syed CASE Institute of Technology, Islamabad, Pakistan
Nazir A. Malik, Bahria University Islamabad, Pakistan
Sadeeq Jan, University of Engineering and Technology Peshawar, Pakistan
Umar Janjua, Information Technology University, Lahore, Pakistan
Zunera Jalil, National Centre for Cyber Security, Air University Islamabad, Pakistan

Publication Committee Chairs:

Chair: **Ammar Masood**, Air University Islamabad, Pakistan
Co-Chair**: Bilal Afzal**, National Centre for Cyber Security, Air University Islamabad, Pakistan
Co-Chair: **Muhammad Najam ul Islam**, Bahria University Islamabad, Pakistan
Co-Chair**: Uzair Khan**, National University of Computer &Emerging Sciences, Islamabad

Panel Chairs:

Adil Sultan, Air University Islamabad, Pakistan
Shoab A. Khan, National University of Sciences and Technology, Islamabad, Pakistan

Operations and Arrangements Chairs:

Chair: **Afzaal Ahmed Khan**, Air University Islamabad, Pakistan
Co-Chair: **Bilal Afzal**, National Centre for Cyber Security, Air University Islamabad, Pakistan
Co-Chair: **Farooq Arshad**, Air University Islamabad, Pakistan
Co-Chair: **Usman Afzal**, National Centre for Cyber Security, Air University, Pakistan
Co-Chair: **Farhan Babar**, National Centre for Cyber Security, Air University, Pakistan
Co-Chair: **Naveed Bhatti**, National Centre for Cyber Security, Air University, Pakistan
Co-Chair: **Qanaita Mehmood**, National Centre for Cyber Security, Air University, Pakistan

Publicity and Sponsorship Committee:

Chair: **Usman Afzal**, National Centre for Cyber Security, Air University Islamabad, Pakistan
Co-Chair: **Farhan Babar**, National Centre for Cyber Security, Air University, Pakistan

Web and Registration Chairs

Chair: **Zunera Jalil**, National Centre for Cyber Security, Air University, Islamabad, Pakistan
Co-Chair: **Asim Ali Fayyaz**, Air University, Pakistan
Co-Chair: **Noor ul Ain Ashraf**, National Centre for Cyber Security, Air University, Pakistan

Finance Committee:

Chair: **Tariq Javed Kamboh**, Air University Islamabad, Pakistan
Co-Chair: **Usman Ghani**, National Centre for Cyber Security, Air University, Pakistan

TECHNICAL PROGRAM COMMITTEE

	Name	Affiliation
1.	Vern Paxson	(UC Berkeley, USA)
2.	Qi Shi	(Liverpool John Moores, UK)
3.	Olaf Manuel	(Tallinn University of Technology, Estonia)
4.	Dan DongSeong KIM	(University of Queensland, Australia)
5.	Hafiz Malik	(Dearborn Michigan, USA)
6.	Siraj Ahmed Shaikh	(Coventry University, UK)
7.	Zahri Yunos	(CyberSecurity Malaysia, Malaysia)
8.	Syed Naqvi	(Birmingham City University, UK)
9.	Jean Daka	(DELOITTE, Belgium)
10.	Kashif Kifayat	(Air University, Islamabad, Pakistan)
11.	Haider Abbas	(MCS, NUST, Rawalpindi, Pakistan)
12.	Zartash Uzmi	(LUMS, Lahore, Pakistan)
13.	Mudassar Farooq	(Air University, Islamabad, Pakistan)
14.	Ejad Ahmed	(University of Malaya, Malaysia)
15.	Ammar Masood	(Air University, Islamabad, Pakistan)
16.	Mehdi Hassan	(Air University, Islamabad, Pakistan)
17.	Zunera Jalil	(Air University, Islamabad, Pakistan)
18.	Bilal Afzal	(NCCS, Air University, Islamabad, Pakistan)
19.	Naveed Bhatti	(Air University, Islamabad, Pakistan)
20.	Jawad Manzoor	(Air University, Islamabad, Pakistan)
21.	Sidra Siddique	(Air University, Islamabad, Pakistan)
22.	Fawad Khan	(MCS, NUST, Islamabad, Pakistan)
23.	Ghalib A. Shah	(UET Lahore, Pakistan)
24.	M. Waseem Iqbal	(MCS, NUST, Islamabad, Pakistan)
25.	Khawaja Mansoor	(Air University, Islamabad, Pakistan)
26.	Ali Hammad Akbar	(UET Lahore, Pakistan)
27.	Ubaid Ullah Fayyaz	(UET Lahore, Pakistan)
28.	Amir Mehmood	(UET Lahore, Pakistan)
29.	Haroon Mahmood	(FAST Lahore, Pakistan)

30. Ashraf Masood (MCS, NUST Rawalpindi, Pakistan)
31. Imran Rashid (MCS, NUST Rawalpindi, Pakistan)
32. Faisal Amjad (MCS, NUST Rawalpindi, Pakistan)
33. Waleed Bin Shahid (MCS, NUST Rawalpindi, Pakistan)
34. Asad Arfeen (NED UET Karachi , Pakistan)
35. M. Mubashir Khan (NED UET Karachi , Pakistan)
36. Iqbal Murtaza (Air University, Islamabad, Pakistan)
37. Muhammad Najam ul Islam (Bahria University, Islamabad, Pakistan)
38. Kashif Naseer Qureshi (Bahria University, Islamabad, Pakistan)
39. Nazir Malik (Bahria University, Islamabad, Pakistan)
40. Faisal Bashir Hussain (Bahria University, Islamabad, Pakistan)
41. Mureed Hussain (PIEAS, Islamabad, Pakistan)
42. M. Hanif Durad (PIEAS, Islamabad, Pakistan)
43. Naeem Iqbal (PIEAS, Islamabad, Pakistan)
44. Ghulam Mustafa (PIEAS, Islamabad, Pakistan)
45. Atif Raza Jafri (Bahria University, Islamabad, Pakistan)
46. Adeel Akram (UET Taxila, Pakistan)
47. Anees Ullah (CASE UET Taxila, Pakistan)
48. Najam-Us-Siraj (CASE, Islamabad, Pakistan)
49. Zain Tariq (Air University, Islamabad, Pakistan)
50. Fahad Tahir (Air University, Islamabad, Pakistan)
51. Mudassar Mushtaq (Air University, Islamabad, Pakistan)
52. Atif Moqurrab (Air University, Islamabad, Pakistan)
53. Hina Shaharyar (Air University, Islamabad, Pakistan)
54. Atiq Ur Rehman (UET Lahore, Pakistan)
55. Suleman Khan (Air University Islamabad, Pakistan)
56. Shehzad Ashraf (Istanbul Gelisim University Istanbul, Turkey)
57. Shahryar Kamal (Air University, Islamabad, Pakistan)
58. Asim Ikram (Air University, Islamabad, Pakistan)
59. Aiza Aqeel Abbasi (Air University, Islamabad, Pakistan)
60. Zaka Ullah (Lahore Garrison University, Lahore, Pakistan)
61. Researchers (National Centre for Cyber Security, Pakistan)

KEYNOTE TALKS

Mr. Fred Baker

ICANN RSSAC Chair / Former IETF Chair, USA

Talk Title: Management of Security in the Domain Name System

Abstract: One fundamental principle in the Internet is the End to End Principle. It could be stated in this way: the one valid thing for any layer of service software (including the Internet Protocol and common transports) is to carry out the intent of its user. Almost all Internet attacks can be described in terms of a violation of that principle - the packet is inspected by or delivered to an unauthorized party, not delivered at all, the predictable response is sent to a different party, the service is overwhelmed, the user is confused in some way that results in an access to an unintended service, or any of a long list of similar schemes. The talk will discuss technologies in use in the DNS to prevent such attacks in what might seem the simple posing of a question and it's a resulting answer

Professor Vern Paxson

University of California, Berkeley / Corelight, Inc. Berkeley, USA

Talk Title: Finding Very Damaging Needles in Very Large Haystacks

Abstract: Many of the most costly security compromises that enterprises suffer manifest as tiny trickles of behavior hidden within oceans of other site activity. This talk will examine the problem of developing robust detectors for particular forms of such activity. The themes include research pitfalls, the crucial need to leverage domain knowledge in an apt fashion, and why machine learning is difficult to effectively apply to such problems

.

Mr. Dmitry Zryachikh

Security Code, Russia

Talk Title: Russian semiconductor / microelectronic industry overview

Abstract: Standard x86 architecture is far from enough when it comes to trusted system developing. It doesn't matter how solid your software is if you cannot be fully sure in hardware level. Dmitry will give a brief overview about key factors of x86 substitution for network security appliances and describe key challenges we met during this process

Mr. Evgeny Goncharov

Kaspersky ICS CERT, Russia

Talk Title: Trends and challenges of Industrial Cyber Security highlighted by Covid-19 pandemic

Abstract: Covid-19 pandemic is definitely the most spoken topic of the year. The pandemic has brought struggling and sorrow to millions. Billions had to adjust their life habits. And it made almost every single person on the planet feel insecure. It did not even make us more vulnerable. Rather, it highlighted our existing vulnerability. From this perspective the current pandemics situation is not only a challenge, but also a huge potential game changer, which may give us an opportunity to see things different, and to see some things important that we did not see before. As the team conducting threat research and vulnerability analysis to Industrial Control Systems, we notice it has also highlighted some major vulnerabilities and cyber security problems of industrial infrastructures. And many of the problems highlighted we believe are absolutely important to solve for the vast majority of modern industrial enterprises to unlock possibility of the IoT and Industry 4.0 technological benefits. This talk will cover the facts discovered during the pandemic period, major challenges noticed and some trends and tendencies we may foresee from where we are now.

Mr. Andrey Golov

Security Code, Russia

Bio: 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 in different civil and military organizations. Andrey also is CEO of Security Code ltd (Russia), one of the famous leading vendors in Russia related to Network, Endpoint and Virtual security. Andrey has degree in mathematics/cryptography, financial analysis and MBA degree in IT management. And he got numerous industry awards and certifications including Certified Information Systems Security Professional (CISSP), Certified Information Security Auditor (CISA) and Business Continuity Institute specialist. Andrey has also experience in Cyber Security of International Cyber Space and global international cooperation. Andrey has also participated in various international MOU and intergovernmental missions

Dr. Mehmet Akif NACAR

HAVELSAN, Turkey

Bio: Mehmet Akif NACAR was born in Sanliurfa, Turkey in 1972. He received the B.S. degree in Computer Engineering from Trakya University, Edirne, Turkey in 1995. Then M.S. degrees in computer education from Gazi University, Ankara, Turkey in 1998 and computer science in Syracuse University, Syracuse, NY in 2000. He completed his Ph.D. degree in computer science in Indiana University, Bloomington, IN in 2008. From 2001 to 2008, he was a Graduate Assistant with Indiana University Community Grids Lab. Since 2008, he has been an Assistant Professor with the Computer Engineering Department, Harran University, Sanliurfa, Turkey. He has involved in many research projects supported by NSF and DoE. During the work with Harran University, he was awarded for a few research projects. He has worked as the vice president in HAVELSAN Training and Simulation Technologies Department since 2017. He is the general manager of HAVELSAN since 2020. His research interests include high-performance systems within parallel and grid computing, cloud computing and developing software models for energy efficiency applications.

Professor Dr. Siraj Shaikh

Coventry University, UK

Talk Title: Cyber-Physical Systems Security: Research Challenges and Opportunities

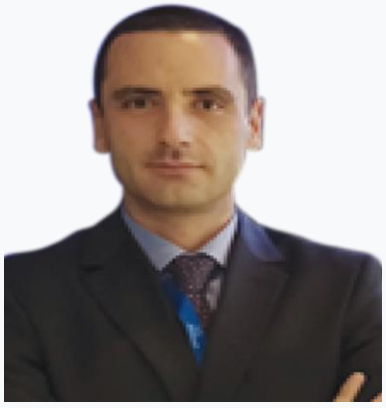
Abstract: The talk would provide a brief overview of some of the challenges in defending cyber-physical systems, and then run through some key areas of development in this domain. It will dive into some technical areas to reflect on some areas of design, policy and behavior, and engineering to address systems security.

Professor Dr. Olaf Maennel

Tallinn University of Technology, Estonia

Talk Title::Critical Infrastructure Protection: An Aviation Cybersecurity Perspective

Abstract: The aviation industry has embraced a safety-oriented culture probably more than any other transport sector. However, from a cybersecurity perspective it is increasingly vulnerable. Previously separate systems are now being interconnected in order to enhance efficiencies, reduce costs and improve the customer experience. However, this exposes new vulnerabilities that may be exploited by a variety of threat actors. These range from nation states to cyber criminals who will see aviation as an attractive target for financial gain, invading privacy or just creating chaos. Airport systems running commercial software are also at risk from indiscriminate attacks targeting any insecure Internet connected network that can be remotely accessed. The unique attributes of the aviation sector serve as a good example of how cybersecurity research needs to develop systems able to resist and counter multiple attack vectors. In our research we demonstrate that securing the aviation industry requires a holistic and wide-ranging approach incorporating aspects from both technical and social science disciplines.



Abdullah Erten

HAVELSAN, Turkey

Talk Title: Post quantum state of cryptology

Abstract: His talk will be mainly around the post quantum state of cryptology. The challenges that the whole cyber world will suffer when the computer power dramatically rises will be assessed. How cryptology will evolve to compensate for the rising computing power will be discussed as well. Post quantum changes in terms of battlefield and warfare will be analyzed

Ms. Jean Daka

Deloitte's Enterprise Risk Services, Belgium

Talk Title: The challenges of digital forensics

Abstract: Digital evidence has transformed from a single host such as a desktop computer with an attached usb drive to different physical or virtual locations such as the cloud and social networks. This makes the challenge of reconstructing the evidence to find 'the smoking gun' more complex. Digital forensic investigators need to keep the pace with advancement in technology and the intricacies of perpetrators by using the right tools that allow them to do their work in a manner that allows evidence to be admissible in a court of law whilst maintaining a forensically sound audit trail. We will look into some challenges faced and some tools investigators use to accomplish this.

Ahrar Naqvi

Ebryx, Pakistan

Talk Title: Zero Day Trust Architecture

Bio: Ahrar Naqvi is the CEO of Ebryx, a company he founded in 2008 in the US and Pakistan. Ebryx is the developer of a Zero Trust Network Access product. Its R&D services power some of the world's leading products in network security, endpoint security and insider threat detection. Ebryx also offers security assessments, compliance, SOC, incident response and digital forensics services. Its customers include local banks, Silicon Valley tech startups and Fortune 500 companies. Before Ebryx, Ahrar was EVP Engineering at Silicon Valley based Palmchip; Chief Architect at Veraz Networks and a product architect at Oracle. Ahrar has an MS in Electrical Engineering from Stanford University.

Mr. Murat Huseyin CANDAN

Barikat Cyber Security,Turkey

Talk Title: State of Cyber Security

Bio: Mr. Murat H. CANDAN is the CEO of Barikat Cyber Security. He has been working on various cyber security roles for the last 20 years and has presented among many security events discussing state and improvements for cyber security.

PAPER PRESENTATIONS: ABSTRACTS

Identifying Mirai-Exploitable Vulnerabilities in IOT Firmware through Static Analysis

Authors: Zafeer Ahmed**,** Ibrahim Nadir, Haroon Mahmood**,** Ali Hammad Akbar**,** Ghalib Asadullah Shah

Abstract: The prevalent use of IoT has raised numerous security concerns in recent times. One particular vulnerability in IoT ecosystem is weak authentication credentials. A large number of IoT attacks exploit such vulnerabilities. Emerged in 2016, the famous Mirai malware conducts attacks that benefits from poorly chosen username and passwords. Since its advent, Mirai attacks have only increased with time. Although multiple solutions have been suggested in literature based on dynamic packet analysis but existing solutions are expensive and are mostly based on reactionary measures. In this research work, we propose a scalable solution to audit the security of IoT firmware against the Mirai attack. Furthermore, we test our system by statically analyzing more than 1200 recent firmware images to inspect their resistance against Mirai botnet. Our results show that 193 out of 1200+ firmware images are susceptible to Mirai malware. To get effective results, we tested our solution against a variety of IoT devices' firmware images. We conclude that our solution is more scalable, less expensive and proactive as compared to other solutions.

Lightweight Encryption Algorithm Implementation for Internet of Thing Application

Authors: Syed Jahanzeb Hussain Pirzada, Tongge Xu, Liu Jianwei

Abstract: Internet of Things (IoT) application utilizes devices with limited hardware resources such as the wireless sensor network application and devices with sufficient hardware resources such as satellite applications. The main challenge is to design a lightweight encryption algorithm to be implementable on devices with limited hardware resources in IoT applications. This work proposes a lightweight encryption algorithm with the provision of protection against the side channel and nonce misuse attack. The lightweight encryption algorithm utilizes an AES like rounds architecture with reduced rounds to reduce area consumption and high-throughput provision. Its implementation of software and hardware validates the lightweight encryption algorithm. The lightweight encryption algorithm provides similar avalanche effects, as shown by the Advanced Encryption Standard (AES) algorithm. The lightweight encryption algorithm utilizes sub-algorithms for the randomization of Initialization Vector (IV) and the generation of randomizing keys for every cipher text. The encryption algorithm is compared with the recent implementations for resource comparison and security analysis.

Elixir A 128-bit Stream Cipher Protocol for Lightweight IOT Devices

Authors: Muhammad Umair Tariq**,** Danial Gohar**,** Talal Hassan**,** Ali Afzal Awan

Abstract: Over time, the Internet of Things (IoT) has turned out to be most prevalent in the field of research and its applications. However, IoT devices are resource constraints and thus, require lightweight and secure ciphering protocols. This paper proposes a new lightweight stream cipher algorithm named as 'Elixer', based upon classical 128-bit non-linear feedback shift register technique. This stream cipher is based on static and dynamic substitution-boxes with shift operations and results in an output key stream. Confusion and diffusion properties are added with the help of substitution and transposition techniques respectively. In the core design of Elixir, there are eight static 6 x 8 s-boxes and two dynamic s-boxes. The correctness of the proposed stream cipher is tested according to NIST randomness standards and Stream tests. Elixir is designed to be implemented easily and efficiently for both Hardware and Software implementations.

Nondeterministic Secure LSB Steganography for Digital Images

Authors: Khan Farhan Rafat

Abstract: The practice of obscuring information on a 'need to know' basis, but still sharing it with others, is called 'secrecy. 'The information that requires fortification is known as the secret. However, the pace at which data gets generated, gathered, disseminated, and analyzed in today's Internet of Things (IoT)has inhibited the individuals from keeping their secrets 'secret.' Cloud computing further hardened the situation by providing a pay-as-you-go method for data processing and information retention (persistent storage). Although the cloud service providers are bound to maintain data integrity, confidentiality, and the privacy of users, yet the gray areas of proxy points still await a resolution. The judicial endorsement on gaining and having access to the encrypted data and the pre-shared keys to the law-enforcing authorities by the Australian parliament – the first amongst the five-eye countries inspecting the global communication has worsened the situation further. Hence, the current state of affairs not just demand for information hiding but the evolution of 'secure' information hiding solutions to maintain secrecy both at the personal and national level. Least Significant Bit embedding technique for hiding data has brought a stir in the information security arena and since its inception has remained a topic of research for the said purpose. This research endeavor proposes an enhancement to the existing LSB embedding mechanism to deceive attackers from detecting hidden information but without compromising image perceptibility. The results confer on the effectiveness of the proposed algorithm with regard to Peak Signal to Noise Ratio and known-cover attack scenario.

An Efficient Forensic Approach for Copy-move Forgery Detection via Discrete Wavelet Transform

Authors: Rehan Ashraf**,** Muhammad Sheraz Mehmood**,** Toqeer Mahmood**,** Junaid Rashid**,** Muhammad Wasif Nisar**,** Mohsin Shah

Abstract: In this modern era, due to advancements in image processing applications; image forgery can be easily performed and difficult to locate by the bare eye. Therefore, the digital images and its content are becoming doubtful thereby losing credibility and truthfulness. Therefore, proving the content realism of an image is an imperative matter. Commonly used type of digital image forgery is copy-move that is carried out in the same image by pasting specific region to another semantically similar region. In this study, a technique is proposed for detecting image forgery by using discrete wavelet transform (DWT). Compared to Fourier transform (FT), DWT is more suitable to analyze image contents on edges or abrupt changes in color contrast. The DWT decomposes the image into 4 sub-bands. Approximation sub-band is employed to implement the present method. DWT reduces the size of the image which in turn minimizes the execution time of the algorithm. The experiment results of the proposed technique revealed that this approach is effective in detecting and localizing the copy-moved region. Therefore, the presented technique can be used for CMIF detection and benefits can be obtained in different fields such as the judiciary, media, and crime investigation.

Byte-Level Object Identification for Forensic

Authors: Dr. Zunera Jalil, Abdul Rehman

Abstract: Lately, digital data has increased a key role in providing and sharing information. Pictures and video recordings are utilized to pass on convincing messages to be utilized under a few unique situations, from propaganda to coercing. The majority of the effort in the present digital crime investigation network lies in the acquisition, retrieval, and investigation of existing data from digital machines. It is a time consuming and a humanly difficult task to collect, process and analyze each media content manually. In this paper, we provide a novel approach that solves a real-time problem for an investigator while investigating the suspect machine. Our approach acquires all image data at byte level from the suspect machine, perform fast and accurate object detection resorting to the deep learning-based algorithm and present high-level illustration of images containing suspicious object and unique objects that can be presented as evidence. Our approach aims to flag photos where suspicious objects are detected. Performance and time consumption wise, this study confirms the importance of automated object detection in digital forensics.

Vulnerabilities and Digital Violations in Software Products: Logistic Regression Analysis

Authors: Shahid Anjum, Effah Wafiyyah bintiAwangMohd. Hanafi

Abstract: Human beings are living in an era where network communication over 5G cellular infrastructure is gaining in fashion. In an environment of integrated technologies along with distributed architectures, there are variety of software spaces which need to be managed. Software, whether proprietor one or open source, may have variety of vulnerabilities which an attacker can exploit and which may compromise the CIA triad of a system. This article performs an analysis of various software vulnerabilities in diverse software products of major OS software vendors by using the logistic regression technique on Common Vulnerabilities and Exposures (CVE) details data which is derived from National Vulnerability Database. The logistic regressions have been estimated, with the help of STATA, for software vulnerability types of various kinds as dependent binary variables and several independent variables like vulnerability scores, a continuous variable and CIA triad, gained access level, access, authenticity and complexity as categorical variables.

Web Server Attack Detection using Machine Learning

Authors: Saima Saleem, Muhammad Sheeraz, Dr. Muhammad Hanif, Dr. Umar Farooq

Abstract: Today, every single organization is utilizing web applications for extension of its business as a result of the high accessibility of web and simple access. With the expansion of web use, the danger of attacks has increased likewise. An efficient monitoring software which can detect these attacks timely is required. HTML, PHP and Java script are used for websites development and SQL is used for database management extensively. Most common web server attacks include SQL injection, DOS (Denial of Service) and XSS (Cross Site Scripting). Rule based intrusion detection systems work on keywords and patterns and are unable to detect unknown attacks. This paper proposes machine learning based model for intrusion detection using web server logs. This model detects whether a specific log is normal or an attack log and also specifies the type of attack. Web server logs are generated and collected by creating a private network using an Apache WAMP server.

An Enhanced and Secure Multiserver-based User Authentication Protocol

Authors: Mehmood Hassan, Aiman Sultan, Ali Afzal Awan, Shahzaib Tahir, Imran Ihsan

Abstract: The extensive use of the internet and web-based applications spot the multi-server authentication as a significant component. The users can get their services after authenticating with the service provider by using similar registration records. Various protocol schemes are developed for multi-server authentication, but the existing schemes are not secure and often lead towards various vulnerabilities and different security issues. Recently, Zhao et al. put forward a proposal for smart card and user's password-based authentication protocol for the multi-server environment and showed that their proposed protocol is efficient and secure against various security attacks. This paper points out that Zhao et al.'s authentication scheme is susceptive to traceability as well as anonymity attacks. Thus, it is not feasible for the multi-server environment. Furthermore, in their scheme, it is observed that a user while authenticating does not send any information with any mention of specific server identity. Therefore, this paper proposes an enhanced, efficient and secure user authentication scheme for use in any multi-server environment. The formal security analysis and verification of the protocol is performed using state-of-the-art tool "ProVerif" yielding that the proposed scheme provides higher levels of security.

Improving Discrimination Accuracy Rate of DDoS Attacks and Flash Events

Authors: Sahareesh Agha, Osama Rehman

Abstract: Millions of people across the world are using internet for their day to day activities. People are highly dependent on internet as they are using internet resources for their work in every field. It connects billions of people across the world. Internet Security has become a big issue and with passage of time. Among many threats, the Distributed Denial-of-Service (DDoS) attack is the most frequent threats in the networks. Consequences of these attacks are more powerful when launched during flash events which are legitimate traffic and cause denial of service. This paper focuses on improving discrimination accuracy rate of DDoS Attacks and Flash events. Random forest is used for classification. Symmetric uncertainty is used for feature selection. NSL KDD data set used to evaluate performance of classifier. Weka is used for implementing algorithms.

Analysis of Fileless Malware and its Evasive Behavior

Authors: Asad Afreen, Moosa Aslam, Saad Ahmed

Abstract: Malware is any software that causes harm to the user information, computer systems or network. Modern computing and internet systems are facing increase in malware threats from the internet. It is observed that different malware follows the same patterns in their structure with minimal alterations. The type of threats has evolved, from file-based malware to fileless malware, such kinds of threats are also known as Advance Volatile Threat (AVT). Fileless malware is complex and evasive; exploiting pre-installed trusted programs to infiltrate information with its malicious intent. Fileless malware is designed to run in system memory with a very small footprint, leaving no artifacts on physical hard drives. Traditional antivirus signatures and heuristic analysis are unable to detect this kind of malware due to its sophisticated and evasive nature. This paper provides information relating to detection, mitigation and analysis for such kind of threat.

Automatic YARA Rule Generation

Authors: Myra Khalid, Maliha Ismail, Mureed Hussain, Muhammad Hanif Durad

Abstract: Since 2010, the numbers of new malware released daily have become so high, that manual analysis is not an option anymore. The purpose of this work is to focus on the increased modern cyber-attacks and malware campaigns. This work devises a framework that automates the process of generating high quality, effective and efficient malware signatures in considerably less amount of time and effort. It also facilitates in the tedious task of malware analysis. The proposed framework presents a generic approach to automatic YARA rule-based signature generation. This approach is based upon cherry picking the most promising core ideas of the related work. The testing of the prototype shows that it is capable of detecting samples with an average precision of 0.95.

An Enhanced SIP Authentication Protocol for Preserving User Privacy

Authors: Sarah Naveed, Aiman Sultan, Khwaja Mansoor

Abstract: Owing to the advancements in communication media and devices all over the globe, there has arisen a dire need for to limit the alarming number of attacks targeting these and to enhance their security. Multiple techniques have been incorporated in different researches and various protocols and schemes have been put forward to cater security issues of session initiation protocol (SIP). In 2008, Qiu et al. presented a proposal for SIP authentication which while effective than many existing schemes, was still found vulnerable to many security attacks. To overcome those issues, Zhang et al. proposed an authentication protocol. This paper presents the analysis of Zhang et al. authentication scheme and concludes that their proposed scheme is susceptible to user traceability. It also presents an improved SIP authentication scheme that eliminates the possibility of traceability of user's activities. The proposed scheme is also verified by contemporary verification tool, ProVerif and it is found to be more secure, efficient and practical than many similar SIP authentication scheme.

Cluster Analysis and Statistical Modeling: A Unified Approach for Packet Inspection

Authors: Sheikh Muhammad Farjad, Asad Arfeeny

Abstract: A secure network layer capable of distinguishing between malicious and genuine traffic flows is the need of every transit service provider, edge network, corporate customer, and a common Internet user. With the emergence of advanced technologies, the demand for security has been drastically increased over the past decade. The analysis of network traffic is essential for various tasks like security, capacity planning, and visibility at various levels. In this paper, a novel architecture is proposed which exploits two powerful techniques for network traffic inspection that is, cluster analysis and statistical modeling, and unifies them in a single framework. The proposed architecture leverages the clustering technique and statistical modeling for analyzing and inspecting the network traffic. Instead of selecting NetFlow records as the

primary format, this research paper presents an approach that employs Packet Capture (PCAP) data format for network analysis. The clustering technique can be used for classifying benign and malicious traffic but there may arise many uncertainties caused by various dynamic factors due to emerging application mixture. Our proposed model uses statistical modeling for supplementing the results obtained from clustering. This unified approach for traffic analysis reduces the chances of the false alert generation that substantially deteriorates the security ecosystem. The proposed architecture inspects different parameters of network traffic to uncover any strong correlation for identifying malicious network traffic flows.

Design and Analysis of Secure RoF Based Communication in 5G Front haul

Authors: Arsalan Ali**,** Romana Shahzadi**,** Nouman Qamar

Abstract: An analytical study is presented in this paper related to the emerging 5G network based on radio over fiber communication. Security of 5G front haul is ensured by using chaos in optical domain. Optical chaos generated by semiconductor laser is used for this purpose. Optical fiber is chosen to provide high bandwidth and minimum latency whereas chaos masking technique is used to implement the security features. In this work, a Radio over fiber (RoF) communication system is designed in licensed version of Opti-system software v.14.0 in which radio frequency signal is modulated on optical signal by using laser and Mach-Zehnder modulator (MZM). Chaos generation is represented by rate equations of laser. Message signal is secured by hiding it in the chaotic carrier produced by semiconductor laser. After transmission the original signal is retrieved through perfect synchronization between transmitter and receiver, thus maximizing not only Q-factor but reduced bit error rate (BER) as well. System performance is evaluated by using different lengths of optical fiber and varying laser power.

Detection of Slow Port Scanning Attacks

Authors: Mehrul Nisaa**,** Kashif Kifayat

Abstract: Cyber Security can be thought of as a set of techniques used to protect the secrecy, integrity, and availability of computer data against threats. Scanning attack itself is not a technique; In fact, it is a two-step procedure in which scanning is the first step where the vulnerability of communication channels are discovered and then the attack is launched in the second step. Since a port is an attack surface as all the information goes into and out of a computer through this medium. Therefore in port scanning, available open ports are searched over the network to find out the vulnerable machine that can be exploited. Many slow port scan detection solutions were proposed in the literature; however, all of these approaches use methods to detect the slow port scan attacks over the static time period. The approach proposed in this paper can detect the slow port scanning attacks not just over the static time interval but also all the attacks that are made with a gradual increase or decrease in the time duration. Moreover, this new proposed approach is employed to detect attacks over live data also. Further packet-based analysis is performed to detect the different types of port scan attacks. The best of all the accuracy of different scans is implemented. The proposed approach also classifies the single and parallel port scans based on attempts made. Therefore the difference between the faster scans and the slower ones is achieved.

Role of User and Entity Behavior Analytics in Detecting Insider Attacks

Authors: Salman Khaliq**,** Zain ul Abideen Tariq**,** Ammar Masood

Abstract: Traditional cyber security products are neither designed nor capable of detecting sophisticated and carefully crafted insider attacks. The main focus of these cyber security products is on the red interface, the outside attackers; ignoring the green side, the legitimate users. Moreover traditional cyber security products do not provide complete vision of user activities within the organization. User and Entity Behavior Analytics (UEBA) has become an important aspect in organization's security because the legitimate users have more rights and access over the organization resources as compared to outsiders. Also, the users are not aware of the security threats that may cause huge damage to organization's confidential information and intellectual property. We discuss the different approaches used in User and Entity Behavior Analytics (UEBA) including user and role-based detection, user and entity activity mapping, user profiling techniques and risk score calculations of individuals. We present the UEBA approaches proposed in literature and generalized design and feature set of top level commercially available UEBA solutions. We also highlight the fact that open source community still lags behind in giving a sophisticated UEBA solution.

Hardware-Assisted Isolation Technologies: Security Architecture and Vulnerability Analysis

Authors: Fatima Khalid**,** Ammar Masood

Abstract: Hardware-assisted isolation technology provides a Trusted Execution Environment (TEE) for the Trusted Computing Base (TCB) of a system. Since there is no standardization for such systems, many technologies using different approaches have been implemented over time. Before selecting or implementing a TEE, it is essential to understand the security architecture, features and analyze the technologies with respect to the new security vulnerabilities (i.e. Micro-architectural class of vulnerabilities). These technologies can be divided into two main types: 1) Isolation by software virtualization and 2) Isolation by hardware. In this paper, we discuss technology implementation of each type i.e. Intel SGX and ARM Trust Zone for type-1; Intel ME and AMD Secure Processor for type-2. We also cover the vulnerability analysis against each technology with respect to the latest discovered attacks. This would enable a user to precisely appreciate the security capabilities of each technology.

CONFERENCE PROGRAM

Day 1 | Tuesday, 20th October 2020 | ICCWS -2020

Opening Ceremony	
09:30 AM - 10:00 AM	Meeting Room Open (Participants Registration, Joining & Opening)
10:00 AM - 10:05 AM	Recitation from Holy Quran
10:05 AM - 10:20 AM	Introductory Remarks by Prof. Dr. Kashif Kifyat, Director NCCS
10:20 AM - 10:30 AM	Chief Guest's Address
10:30 AM - 10:40 AM	Key Note Speech by: Fred Baker, ICANN RSSAC Chair, USA
10:40 AM - 10:50 AM	Key Note Speech by: Andrey Golov, CEO Security Code, Russia
10:50 AM - 11:00 AM	Key Note Speech by: Dr. Mehmet Akif NACAR, CEO HAVELSAN, Turkey
11:00 AM - 11:05 AM	Address by Air Marshal Javaid Ahmed HI (M) (Retd), Vice Chancellor Air University

Day 2 | Tuesday, 21st October 2020 | ICCWS -2020

09:00 AM - 09: 05 AM	Opening of the day with brief overview of full day conference plan					
09:05 AM - 10: 00 AM	**Keynote Speaker: Prof. Vern Paxson, UC Berkley, USA** **Topic:** Finding Very Damaging Needles in Very Large Haystacks					
10:05 AM - 11:35 AM	**Main Room** Tech Talks by Industry Expert		**Room 1 Track - V** (Web & Big Data Security)	**Room 2** Parallel Session C-1	**Room 3** Parallel Session C-2	**Room 4** Parallel Session C-3
	Invited Talks (45 minutes for each Speakers)		**Parralel Session C-0** (15 Mins for Each Paper Presentations)	**Workshop - 1**	**Workshop - 2**	**Workshop - 3**
	Talk 1	**Trends and challenges of Industrial Cybersecurity highlighted by Covid-19 pandemic** by Mr. Evgeny Goncharov, *Head of Kaspersky ICS CERT*	**Paper 12:** Vulnerabilities and Digital Violations in Software Products: Logistic Regression Analysis **Paper 13:** Web Server Attack Detection using Machine Learning **Paper 14:** An Enhanced and Secure Multiserver-based User Authentication Protocol **Paper 15:** Improving Discrimination Accuracy Rate Of DDoS Attacks and Flash Events	**Topic:** Network Security Monitoring Using IDS **Resource(s):** Dr. Faisal Bashir CRC Lab, Bahria University, Islamabad	**Topic:** Threat Modeling for IoT platforms **Resource(s):** Dr. Ghalib Shah, Dr. Ubaid Fayyaz Mr. Bilal Imran *IoT Security Lab, UET Lahore*	**Topic:** Layer 7 Protocol Extractions **Resource(s):** Mr. Najm us Siraj Mr. Baqir Kazmi *DPI Lab, UET Taxila /CASE*
	Talk 2	**Post Quantum Cryptographic Resistance** by Mr. Abdullah A. ERTEN, *Product Manager, HAVELSAN*				
11:40 AM - 01:10 PM	**Talk 3**	**Its Time to Adopt a Zero-Trust Architecture** by Mr. Ahrar Naqvi *CEO Ebryx Pvt. Ltd Pakistan*	**Room 1 Track - VI** **(Software Security)** **Paper 16:** Analysis of Fileless Malware and its Evasive Behavior **Paper 17:** Automatic Yara Rule Generation **Paper 18:** An Enhanced SIP Authentication Protocol for Preserving User Privacy **Paper 19:** Cluster Analysis and Statistical Modeling: A Unified Approach for Packet Inspection			
	Talk 4	**Challenges of Digital Forensics** by Ms. Jean Daka, *Director Deloitte, Belgium*				
01:10 PM - 01:50 PM	**Lunch and Prayer Break**					

Day 2 (Continue)

02:00 PM - 04:00 PM	Main Room		Room 1 Track - VII (Hardware, Infrastructure & 5G Security)	Room 2 Parallel Session C-4	Room 3 Parallel Session C-5	Room 4 Parallel Session C-6
	Invited Talks		**Parralel Session C-4** (15 Mins for Each Paper Presentations)	**Workshop - 4**	**Workshop - 5**	**Workshop - 6**
02:00 PM - 02:30 PM	**Talk 5**	**Building Effective Cyber Threat Intelligence Programs** by Mr. Mahir Mohsin *CEO TISS (Pakistan)* 30 minutes	**Paper 20:** Design and Analysis of Secure RoF Based Communication in 5G Fronthaul **Paper 21:** Detection of Slow Port Scanning Attacks **Paper 22:** Role of User and Entity Behavior Analytics in Detecting Insider Attacks **Paper 23:** Hardware-Assisted Isolation Technologies: Security Architecture and Vulnerability Analysis	**Topic:** Art of Rooting and Flashing Android OS **Resource(s):** Mr. Mudassar Waheed DNS Lab, Air University Islamabad	**Topic:** Networks and Communication Security with Linux **Resource(s):** Mr. Jahanzaib Shahid NCSAEL Lab, MCS-NUST Rawalpindi	**Topic:** A Workshop on Malware Analysis **Resource(s):** Ms. Faiza Babar, Ms. Umm-e-Hani *CIPMA Lab, PIEAS*
02:35 PM - 03:15 PM	**Talk 6**	**State of Cyber Security** by Mr. Murat Huseyin CANDAN *CEO Barikat Cyber Security (Turkey)* 40 minutes				
03:15 PM - 04:05 PM	**Panel Discussion**	**Cyber Security Challenges in Digital Transformation: Post Covid-19 Era (Stakeholders Discussion)** 50 minutes				

Closing Ceremony	
04:10 PM - 04:15 PM	Meeting Room Open (Participants Registration, Joining & Opening)
04:15 PM - 04:20 PM	Recitation from Holy Quran
04:20 PM - 04:35 PM	Concluding Remarks by Prof. Dr. Kashif Kifyat, Director NCCS
04:35 PM - 04:40 PM	Address by Air Marshal Javaid Ahmed HI (M) (Retd), Vice Chancellor Air University
04:40 PM - 04:50 PM	Chief Guest's Address
04:50 PM - 05:00 PM	Closing Remarks and Thank you Note

ICCWS 2020

ORGANIZING TEAM

Prof. Dr. Kashif Kifayat, Director NCCS
Email: director@nccs.pk

Bilal Afzal, Program Manager, NCCS
Email: bilalafzal@nccs.pk

Usman Afzal, Business Development Manager, NCCS
Email: bdm@nccs.pk

EVENT DETAILS

When: October 20th – 21st 2020, 09.00 am- 5.00 pm (GMT+5)

Where: Online, Live on Zoom / Social Media

Inquiry: iccws.secretariat@nccs.pk
+92 (51) 9153655

www.nccs.pk
Securing Your Cyber Future

Notes

Notes