NCCS
NATIONAL CENTRE FOR CYBER SECURITY

NATIONAL AEROSPACE S&T PARK AVIATION CITY PAKISTAN

AIR UNIVERSITY

ICCWS 2022

IEEE

3rd Annual International Conference On CYBER WARFARE & SECURITY 2022

» Securing Your Cyber Future

December 7th - 8th 2022 | 9:00 AM - 5:00 PM (GMT+5)
Air University, Sector E-9, Islamabad, Pakistan

ICCWS 2022 SPONSORS & PATRONS

HEC
ebryx
Department of Cyber Security Air University, Islamabad
NCCS CRYPTO CORNER
NCSA NATIONAL CYBER SECURITY ACADEMY Detect | Defend | Evolve
PAKISTAN Cyber Security Cluster
ORIC AIR UNIVERSITY
AU BIC
SECURE NETWORKS Be Secured
MINISTRY OF PLANNING, DEVELOPMENT & SPECIAL INITIATIVES

2022 International Conference on Cyber Warfare and Security (ICCWS)

7th – 8th December 2022

Air University, Islamabad, Pakistan

Conference Booklet

IEEE

Contents

Welcome Notes 01

Keynotes and Technical Talks... 05

Paper Abstracts 10

Welcome Note by Conference Patron

Air Marshal Javaid Ahmed (Rtd)

Vice Chancellor, Air University

Dear Participants,
I am pleased to welcome you to the 3rd Annual International Conference on Cyber Warfare and Security (ICCWS) organized by National Centre for Cyber Security (NCCS) Pakistan. Cyberspace has now emerged as an important pillar of a nation's strategic domain. The pervasive connectivity and mobility of digital assets exposes cyberspace to a host of new and evolving cyber security threats. A nation without a resilient, reliable and robust cyber security foundation is vulnerable to aggressive actions from rival states to cyber mercenaries. In this regard, NCCS, since its establishment in 2018, has played an important role in development of indigenous cyber security solutions to not only meet Pakistan's domestic requirements but also to promote national cyber security industry for meeting emerging challenges. In this regards since NCCS has always actively contributing its role in develop and promotion of the R&D activities and HR Development in the specialized field of Cyber Security.

The conduct of ICCWS provides NCCS a fundamental platform to showcase its cyber security solutions and also acts as a nucleus for cyber security professionals from the government, industry and academia to share their experiences and synergies efforts. In this regard, the ICCWS-2022 includes a high-quality focused technical program on cyber security with keynote talks from industry and academia The presented research will not only add value to academic resources and knowledge repositories; but, also provide avenues for undertaking collaborative research between all stakeholders. In addition, the conference will provide networking opportunities to researchers, students, developers and cyber security professionals from the industry, academia and government organizations around the world.

I wish to thank national and international speakers, researchers, and participants for joining us at this conference. We are especially pleased with the generous support of international speakers, including Prof. Dr. Olaf Maennel, Prof. Dr. Salman Basit , Professor Dr. Hafiz Malik, Dr. Zahri Yunos from Malaysia, Prof. Dr. Jawad Shamsi, Mr. Rizwan Mir, Dr. Aiman Erbad, and Dr. Roberto Di Pietro from Qatar.

Finally, I convey my best wishes to all the organizers of the 3rd IEEE ICCWS 2022

Welcome Note by Conference Chair

Prof. Dr. Kashif Kifayat

Director NCCS

Dear Participants,

I am delighted to arrange the third IEEE International Conference on Cyber Warfare and Security at Islamabad. Last year's conference ICCWS-2021 made a lasting impact on the international and national cyber security community. As a result, collaboration with the industry, academia, and other stakeholders has flourished. This year's ICCWS-2022 we expect to enhance further. We hope to make this year's conference more effective due to the involvement of national and international academia, industry experts and participation from government sector and new emerging stakeholders. We anticipate that the conference will enhance public awareness about cyber security and safety. In this regard, the National Centre for Cyber Security at Air University is committed to promoting and enhancing research work on cyber security to ensure safe internet facilities and a secure cyberspace. To facilitate the growth in cyber security and cyber infrastructure NCCS have not only participated in national level cyber policy making but also promoting start up and training in the field. The establishment of National Cyber Security academy (NCSA) is a next step in the progress as new curriculum for various BS/MS/PhD programs in the emerging/ futuristic areas of Cyber Security such as Cryptology, Digital Forensics, Criminology, Cyber psychology, Cybercrime Investigation, Cyber laws expected to improve national and international assets of cyber skill force.

The plan of this year's conference covers a wide range of topics related to recent advances in cyber security and its allied areas. In the two-day conference, researchers and practitioners working in cyber security and related domains will share their research ideas and experiences in relation to emerging areas of cyber security. For this year more than 100 papers from 5 countries have been submitted for selection. Out of these 12 selected papers will be presented in the 3rd ICCWS. The selection process for the papers has been conducted through a double blind peer-review process by the technical program committee of renowned cyber security academicians from national and international universities. Moreover, keynote speeches by leading cyber security experts worldwide will be a part of the conference program, along with two well-focused panel discussions. I hope that the challenges and opportunities identified by keynote speakers and panelists will help recognize the significance of cyber security and develop better understanding and resilience within respective organizations and stakeholders.

We warmly welcome all national and international participants and encourage them to share their knowledge and discuss ways and means to create cyber security awareness and make the Cyber world a digitally secure and safe place. We also express our appreciation for our collaborative sponsors, and supporters, whose continuous and dedicated support has enabled us to organize this event. We hope you find ICCWS-2022 a valuable experience.

3rd IEEE INTERNATIONAL CONFERENCE ON CYBER WARFARE ANDSECURITY 2022 (ICCWS)

NCCS
NATIONAL CENTRE FOR CYBER SECURITY
AIR UNIVERSITY
ICCWS 2022
IEEE
3rd Annual
International Conference On
CYBER WARFARE & SECURITY
2022
Securing Your Cyber Future

Call for Papers

- National Centre for Cyber Security (NCCS) at Air University Islamabad is going to organize a two-day event to invite researchers and cyber security practitioners across the world to share their research work and experiences related to the state-of-the-art and the emerging areas of cyber security. ICCWS-2022 will provide its participants an opportunity to learn, share and demonstrate their ideas, strategies, and policies pertaining to cyber security. Prospective authors are invited to submit their original technical papers for presentation at ICCWS 2022. Conference content will be submitted for inclusion into IEEE Xplore® as well as other Abstracting and Indexing (A&I) databases.

Main topics of interests:

Following areas and others closely related topics:

- Hardware and systems security
- Networks and infrastructure security
- Operating systems and software security
- Web, Big data and Cloud security
- Distributed systems and data center security
- Security and privacy for embedded systems, IoT and Cyber Physical Systems
- Information security, data provenance, and information assurance
- Cryptology, cryptanalysis and security analysis of cryptographic primitives and protocols
- Prevention, detection and investigation of APTs, DDoS and other cyber attacks
- Anti-malware techniques: detection, analysis, and prevention
- Artificial Intelligence aided security and privacy concerns
- (Adversarial) Machine learning and cyber deception
- (Anti-) Reverse engineering, side channel attacks and physical attacks
- Protection of digital services and applications
- Digital forensics, social media, networks, computer and mobile forensics
- Automated security analysis of protocols, source code and binaries
- Security, Privacy, and Trust in Digital Payments and Crypto-currencies
- Security and privacy issues in Block chain
- Security, privacy and resilience in critical infrastructures
- Testing, auditing and evaluation of security architectures and models
- Security issues in 5G Networks and Beyond
- Security for future Internet architectures and designs
- Measurements and monitoring of human behavior in cyberspace
- Interdisciplinary research connecting cyber security and privacy to psychology
- Usable security and privacy: human and societal aspects
- Cybercrime defense (anti-phishing, anti-blackmailing, anti-fraud, etc.) techniques
- Policy making and legal aspects of cyber security (cyber laws and regulations)

CONFERENCE ATTENDING RULES

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 line up of key note speakers.

Attending the session

Program Schedule

The conference schedule has been designed to ensure that sessions cover meaningful research. Punctuality is important to warrant timely start and completion of sessions, so be mindful of timings. Q/A will be entertaining at the end of each presentation session.

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.

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 will 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.

KEYNOTE TALKS

: **Prof. Dr. Olaf Maennel**

Centre of Digital Forensics and Cyber Security, Tallin University of Technology, Estonia

Talk Title: Evolving World of Cyber Operations

Abstract: “Cyber”, as the 5th domain of warfare, is getting more awareness recently. Our unpreparedness is also becoming apparent. In this talk, we will revisit some recent developments in the sector and discuss the underlying fundamentals of the problems we are seeing. How can we increase our cybersecurity posture as individuals and organizations? Simple cybersecurity awareness changes, combined with some common sense and essential critical thinking, can already bring us quite far. We will discuss some examples of offensive methods and understand how to build the required defensive culture

Dr. Salman Baset

Head Product Security, MongoDB, USA

Talk Title: State of Cloud Security and its Future

Abstract: The talk will cover the state of cloud security both from a cloud provider and cloud consumer perspective, the role of shared responsibility in cloud security, and why shared responsibility should not mean equal responsibility. It will then showcase the security of large cloud providers through the prism of security bulletins and advisories published on their websites. The talk will also describe the security challenges that organizations face in using SaaS providers, and future directions in cloud security.

Professor Dr. Hafiz Malik

Professor of Electrical and Computer Engineering (ECE) at the University of Michigan – Dearborn

Talk Title: Cyber security for Connected and Autonomous Vehicles: Challenges and Solutions

Abstract: Advances in artificial intelligence, development of deepfake - a new form of manipulated media technologies, and evolution of social media platforms are key drivers behind exponential rise of global disinformation pandemic. Deepfake technology is weaponizing information and social media platforms are adding fuel to the fire. Bad actors are taking advantage of deepfake technologies and social media platforms to spread falsehood, amplify rumors, propagate disinformation, distort facts, and influence election outcomes. Recent studies indicate that disinformation has a negative impact on society and well-being. Despite limited success in detecting and countering disinformation campaigns, the bad actors continue taking advantage of emerging AI technologies and re-tooling social platforms to spread falsehood and manipulate the political discourse. This talk will discuss key enablers for disinformation pandemic, e.g., deepfake and shallowfake technologies and threats they pose to Pakistan's national security, its democratic institutions, financial institutions, and the society at large. This talk will present state-of-the-art on information authentication, share findings of our-on-going research on content verification for digital media, and propose a framework to counter disinformation crisis

Dr. Zahri Yunos

Board Member, University Teknikal Malaysia Melaka, Strategic Cybersecurity Advisor, Securely tics, Malaysia

Talk Title: Documentation, procedures and testing profiles in Common Criteria

Abstract: In this talk, a high-level overview on documentations, procedures and testing profiles in Common Criteria are covered. Discussion will focus on how Common Criteria improves security of ICT products and systems, while at the same, increases confidence level in using these products and systems. At the end of the presentation, the audiences will have understanding on what Common Criteria is all about (with some case studies in Malaysia). The talk is intended for a wider audience, to have general know-how on Common Criteria and its related components.

Prof. Dr. Jawad Shamsi

National University of Computer and Emerging Sciences (FAST), Karachi, Pakistan

Talk Title: Deepfakes - Issues and Challenges

Abstract: Deepfakes technology allows creation of synthesized digital contents. This can be used to impersonate a person or initiate a disputation cyberattack. Emerging challenges and requirements in cybersecurity necessitate us to deeply understand the process of deepfakes, it's types, generation and detection methods, and research directions. This talk is focused on the above mentioned needs. The talk will cover the process of deepfakes detection and generation using deep learning technologies. It will also focus on existing issues and challenges in the domain. The talk will be useful for students, academicians, and researchers in getting a better understanding of the field.

Mr. Rizwan Mir

CISO, VideoJet Technologies Pvt Ltd, USA

Talk Title: Emerging Trends in Cyber Security

Abstract: The internet is now being used to run electronic transactions globally across personal, business, and government sectors. With the adoption of mission critical Internet services, cyber security is no longer an afterthought. The goal of this session is to describe the evolving trends in cyber threat and defense against the backdrop of developing countries like Pakistan. The initial part of the presentation will give the audience an appreciation of the new threat landscape which now includes nation-state actors waging cyber wars, as well as cyber-criminal operating as an organized industry. We will share examples of how these threat actors are disrupting web services, attacking citizens' privacy, hacking personal devices, leveraging deep fake technology, and causing a sharp rise in financial loss by deploying ransomware in IT systems. In the second part of the presentation, we will touch on the new frontiers of cyber defense. This includes the adoption of product security in the software development process, digital identity taking the center stage, the concept of zero-trust networks, and the importance of cyber resilience in response to a successful cyber-attack. We will also review new trends in personal data rights, emerging cyber laws, and the responsibility of web-scale companies as well as governments in protecting their consumers.

Dr. Aiman Erbad

Associate Professor and Head of Information and Computing Technology Division in the College of Science and Engineering, Hamad Bin Khalifa University (HBKU)

Talk Title (Online): Efficient and Privacy Preserving Distributed Inference in IoT Systems

Abstract: Traditional cloud-based Internet of Things (IoT) architectures cannot guarantee communication and computational efficiency in data intensive applications leading to issues in scalability, real-time interactions, and data privacy. This motivated the need for new emerging architecture such as edge, fog and pervasive computing, where we merge hierarchical computing with efficient communication, leveraging learning-based distributed optimization, in order to optimally allocate computations and communication while addressing the identified issues.

Dr. Roberto Di Pietro

Hamad Bin Khalifa University, Qatar

Talk Title: The Cybersecurity of Drones: Attacks, Defenses, and Future Challenges

Abstract: Unmanned Aerial Vehicles (UVAs), also known as drones, are the classical dual usage technology. On the one hand, their adoption and possible use cases in the civil sector are blooming. On the other hand, their usage in warfare matters is the news. In this latter context, drones represent the last frontier of cyber warfare. Indeed, UAVs can be seen as the archetypal cyber-physical systems. As such, their cyber component---think of the navigating assistant component, the communication component, and the data processing component, to cite a few---represent a valuable target for any rational adversary. In this talk, we will discuss some recent contributions intended to secure UAVs from the compromising of some elements of their cyber components. The talk will conclude with some highlights on the next challenges. UAVs will be confronted with in the cyber warfare context and what can be done to reduce the threats posed by this technology.

PAPER PRESENTATIONS: ABSTRACTS

Blockchain-based Security for Internet of Medical Things Application

Authors: Taha Ramzan, Saima Zafar

Abstract: Internet of Things (IoT) refers to the network comprising of devices called “things” that are equipped with sensors, batteries, microcontrollers and radio transceivers for collecting and exchanging data with other devices and systems over the Internet. Internet of Medical Things (IoMT) signifies IoT applications in the healthcare sector and aims to improve the healthcare sector's technological, economic, and social aspects. An important concern in the IoMT is the security and privacy preservation of patient data. For IoMT to be widely adopted, assurance of data security and prevention of unauthorized access is of paramount importance. Presently IoMT applications incorporate centralized data storage which suffers from issues such as a single point of failure, a lack of strong protection against record tampering, hacking, data theft, trust and reliability. All of these issues can be resolved if IoMT adopts the blockchain technology leading to Blockchain-based IoT (BIoT) applications. Blockchain is a technology that aids in tracking, coordinating, and information sharing for a significant number of devices by maintaining ledgers of transactions on all connected peers, eliminating the need for a central server. This paper presents work related to the integration of multi-ledger blockchain architecture in IoMT and analyzes its security and resource implications. The results show that transition from centralized IoMT to decentralized BIoT introduces independence from the third parties, improves security, and removes a single point of failure. Additionally, the presented multi-ledger blockchain architecture with limited nodes demonstrates blockchain's scalability and adaptability with resource-limited IoMT devices.

A Knowledge Graph-Based Framework for Integrated Network-Centric Warfare Strategies for Cyber-Physical-Social World

Authors: Rauf Ahmed Shams Malick, Mir Murtaza, Khubaib Ahmed Qureshi

Abstract: The availability of multichannel data in the cyber, physical and social world has challenged Artificial Intelligence (AI) based methods to develop novel tools for integrated modern warfare strategies. Networks are widely being used to represent enriched data in combination with AI tools for deeper insights. The formation of static and dynamic networks from audio, video, GPS, text and social data has shaped network-centric warfare strategies in an integrated setting. The present paper highlights a set of challenges related to inference methods in the cyber, physical and social world. A novel framework is presented in this paper that allows the representation of multidimensional data with a single network-driven viewpoint and representing multidimensional networks in the form of knowledge graphs. The knowledge graphs are presented as an effective tool that has the ability to be utilized in surveillance, strategy development and real-time information sharing for cyber-physical-social worlds. The presented components in the strategic framework are implemented and validated under certain constraints for better understanding.

Generic Application Layer Features for IoT Devices Identification

Authors: Sabeeha Tanveer, Muhammad Husnain, Habiba Akram, Syed Ghazanfar Abbas, Dr. Ghalib A. Shah

Abstract: The wide adoption of Internet of Things (IoT) in traditional networks and critical infrastructures has brought many advantages. At the same time, insecure IoT devices provide a loophole in existing infrastructure that miscreants can exploit. Mirai incident is a well-known example, where attackers exploited the internet using IoT devices. Hence, a quick, accurate and energy-efficient IoT device identification mechanism is required to cope with these emerging challenges. In this research, we have proposed a generic set of application layer features for IoT device identification. To show the effectiveness of proposed generic application layer features we have

compared them with network layer features using machine learning models and IoT devices traces. Previously most of the work was done on network layer features. However, for IoT devices network layer features show constancy in their pattern as compared to application layer features which are distinct and unique in nature. As a consequence, large number of network layer features are required for identification of devices causing use of higher prediction time, computational and feature extraction cost. We have also developed the first available open-source application layer feature extractor tool. Researchers can utilize this tool for acquiring application layer datasets and utilize them in different research domains.

Anonymity Preserving Secure Authentication for a Transparent Internet Voting Process

Authors: Khan Farhan Rafat

Abstract: The COVID'19 pandemic of recent times has changed the trends of socializing, that is, from physical to online (virtual) presence. Likewise, remote or work-from-home culture has flourished and resulted in business gains with the least maintenance cost. However, the situation has its downsides, like risking users' privacy and compromising their anonymity by getting hacked, which has caused distrust in online businesses/activities. i-voting is also not indifferent, where people fear compromising their anonymity by casting votes via digital electoral. In an attempt to rebuild trust in i-voting, this research, as a test case, focuses on the security aspects of the authentication mechanisms used in the i-voting System of Estonia. It is to pledge the significance of voter authentication just before a vote gets cast because admittance to internal applications may expose the network to instant attack. Following that is the suggested remedy for the limitations observed, such as using a static e/m-ID for online transactions and limited time verifiability of their casted vote, through our proposed digital authentication mechanism, which ensures the anonymity of both the ballot and the voter and is a novel contribution to date.

An MFCC-based Secure Framework for Voice Assistant Systems

Authors: Syed Fahad Ahmed, Rabeea Jaffari, Moazzam Jawaid, Shahnawaz Talpur, Syed Saad Ahmed

Abstract: Voice assistant systems accept voice commands to perform various routine tasks such as navigation, playing music, temperature control, and so on. Voice assistants are commonly employed in home automation to serve the elderly and disabled people. Despite of their popularity in our daily lives, voice assistants are still far from perfect as these systems suffer from lack of security and accessibility issues. Available voice assistants respond to voice commands from any individual without proper user authentication. Hence, these systems are vulnerable to various security attacks where any adversary can control the voice assistant and perform any desired action. Moreover, popular voice assistants are also platform-dependent and only function on specific kind of devices. In the light of these limitations, we propose a Mel-frequency cepstral coefficients MFCC-based framework to secure the voice assistants via user authentication. MFCC efficiently recognizes the voice features which are then employed to distinguish between authorized and unauthorized users. Moreover, the voice assistant for the proposed framework is also implemented via cross-platform technology to guarantee increased accessibility. The proposed framework is tested on authorized and unauthorized user voices under different conditions with positive outcomes. The positive results prove the feasibility of our proposed framework for securing the voice assistant systems.

Forensic Data Analysis of Delivery and Transport Applications

Authors: Syeda Sundus Zehra, Dr.Sana Qadir

Abstract: The COVID-19 pandemic has changed many aspects of human life during last three years. One of these aspects is the adaption of new trends and technologies for everyday activities such as delivery and transportation. People now prefer to shop online and get their products delivered at home without wasting any time. Therefore, the security and importance of online and delivery applications is the main concern these days. The payment mode of these applications is online which involves personal data like bank information and user details. This problem led to the research contribution of our work. The main objective and implication of this study is to find personally identifiable information (PII) of users which uniquely identifies a person at personal and organizational scopes. In this paper, we present the forensics analysis of eight popular Android delivery and transport applications i.e. Daraz.pk, Foodpanda, Grocer app, airlift express, Bykea, INdriver, Uber and Clicky shopping app. These applications have not been previously studied and investigated by other researchers. Furthermore, these applications are among the top android apps used by customers. It is expected that such an analysis can guide investigators towards obtaining useful information about a suspect who has used such an application on their device. The analysis process started with the installation of each application on a rooted Samsung S7 Edge smartphone. Then various activities were performed such as setting up an account, booking a ride, or ordering a delivery. After this, a physical image of the device was acquired. A detailed analysis of the image was carried out using Autopsy and all relevant artifacts were collected. A comparison of the results showed largest number of artifacts have been gathered from installation activity and the most number of unique artifacts have been collected from order and booking activity. A tabular form of analysis has also been shown with all of the source and path files from which the data has been gathered.

Software Implementation of AES-128: Side Channel Attacks Based on Power Traces Decomposition

Authors: 1st Fanliang Hu, 2nd Feng Ni

Abstract: Side Channel Attacks (SCAs), an attack that exploits the physical information generated when an encryption algorithm is executed on a device to recover the key, has become one of the key threats to the security of encrypted devices. Recently, with the development of deep learning, deep learning techniques have been applied to SCAs with good results on publicly available dataset experiences. In this paper, we propose a power traces decomposition method that divides the original power traces into two parts, where the data-influenced part is defined as data power traces (T_data) and the other part is defined as device constant power traces, and use the T_data for training the network model, which has more obvious advantages than using the original power traces for training the network model. To verify the effectiveness of the approach, we evaluated the ATXmega128D4 microcontroller by capturing the power traces generated when implementing AES-128. Experimental results show that network models trained using Tdata outperform network models trained using raw power traces (Traw) in terms of classification accuracy, training time, cross-sub key recovery key, and cross-device recovery key.

A Comprehensive Review of Endpoint Security: Threats and Defenses

Authors: Abu Kamruzzaman, Sadia Ismat, Joseph C. Brickley, Alvin Liu, Kutub Thakur

Abstract: Endpoint Security/Protection is vital to an enterprise's cybersecurity platform. There are many endpoints a malicious actor can attack to infiltrate and gain access to a system and steal data. These different endpoints are continuously growing as more people switch to remote work or even use their work devices. Due to this, endpoints are more susceptible now than before because of the increased pathways cybercriminals can take to infiltrate a system. This paper will discuss the importance of endpoint security management, the type of attacks a cybercriminal uses, the different types of endpoints, and how cybersecurity specialists can combat and prepare protection for these endpoints. In addition, there will be examples of other vendors that provide endpoint security and explain how their software/antivirus can mitigate endpoint attacks.

Implementation of Two Layered DLP Strategies

Authors: Muhammad Arsalan Paracha, Muhammad Sheeraz, Yuanyuan Chai, Saad Ahmad, Zubair Nasir Khan, Shah Hussain, Aftab-Ul-Haq, Muhammad Hanif Durad

Abstract: Data Loss Prevention or DLP system, is a cybersecurity system that identifies and stops data breaches. Organizations use it for internal security and regulatory compliance since it prevents sensitive data from being extracted. As organizations explore strategies to decrease the danger of sensitive data leaking outside the firm, data loss prevention solutions are becoming more popular. A DLP solution is built on a set of core technologies that enable its engine to properly detect the sensitive data and protect that data from possible insider breaches which businesses must safeguard and take remedial action to avert accidents. This paper gives a comprehensive overview of different DLP solutions and their effectiveness followed by our own indigenous and standalone DLP system design

and implementation. It begins by providing a solution to the aforementioned difficulties with universal serial bus (USB) memory devices. Then, at the application level, it displays an email filter to avoid the erroneous transmission of e-mail containing sensitive information and finally its integration with a SIEM solution

Sequential Embedding-based Attentive (SEA) classifier for malware classification

Authors: Muhammad Ahmed, Anam Qureshi, Jawwad Ahmed Shamsi, Murk Marvi

Abstract: The tremendous growth in smart devices has uplifted several security threats. One of the most prominent threats is malicious software also known as malware. Malware has the capability of corrupting a device and collapsing an entire network. Therefore, it’s early detection and mitigation are extremely important to avoid catastrophic effects. In this work, we came up with a solution for malware detection using state of-the-art natural language processing (NLP) techniques. Our main focus is to provide a lightweight yet effective classifier for malware detection which can be used for heterogeneous devices, be it a resource constraint device or a resourceful machine. Our proposed model is tested on the benchmark data set with an accuracy and log loss score of 99.13% and 0.04 respectively

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

EVENT DETAILS

When:7th –8th December 2022, 09.00 am- 5.00 pm (GMT+5)

Where: Air University, E-9, Islamabad

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

Securing Your Cyber Future

Notes

Notes

Notes