NCCS
NATIONAL CENTRE FOR CYBER SECURITY

ICCWS 2021

IEEE

2nd Annual

International Conference On CYBER WARFARE & SECURITY

2021

ICCWS 2021

2021 International Conference on Cyber Warfare and Security (ICCWS)

23rd - 24th November 2021

PAFSOM, ARENA, Islamabad, Pakistan

Conference Booklet

IEEE

Contents

Welcome Note by Conference Patron

Air Marshal Javaid Ahmed (Rtd)

Vice Chancellor, Air University

Dear Participants,

I am pleased to welcome you to the 2nd Annual International Conference on Cyber Warfare and Security (ICCWS) organized by National Centre for Cyber Security (NCCS) Pakistan and the inauguration ceremony of the National Cyber Security Academy. 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.

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-2021 includes a high-quality focused technical program on cyber security with keynote talks from prominent industry and academia experts. 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. The inauguration of the National Cyber Security Academy will be another strategic step to enhance the role of academia in the Cyber domain.

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 Professor Dr. Hafiz Malik, Dr. Salman Base, and Mr. Razi Bin Rais from the US, Dr. Zahri Yunos from Malaysia, Professor Dr. Awais Rashid, Professor Siraj Shaikh, and Dr. Richard Thomas from UK, Professor Zoltan Rajnai from Hungary, Mr. Taylan Esen from Turkey and Mr. Ahrar Naqvi.

Finally, I convey my best wishes to all the organizers of the 2nd IEEE ICCWS 2021.

Welcome Note by Conference Chair

Prof. Dr. Kashif Kifayat

Director NCCS

Dear Participants,

I am delighted to arrange the second IEEE International Conference on Cyber Warfare and Security at Islamabad. Last year's online conference ICCWS-2020 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-2021 has more in store, as it is being arranged in hybrid mode. 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. Another important aspect of the conference is the inauguration of the National Cyber Security Academy. 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.

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 a total, of 147 papers from 9 countries have been submitted for selection. Out of these 21 selected papers will be presented in the 2nd 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 and technical talks 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 findICCWS-2021a valuable experience.

2nd IEEE INTERNATIONAL CONFERENCE ON CYBER WARFARE AND SECURITY 2021 (ICCWS)

Call for Papers

National Centre for Cyber Security (NCCS), in collaboration with IEEE Islamabad Section is organizing a two days' international conference, i.e. ICCWS-2021. Researchers and professionals around the World are invited to share their original research ideas and experiences related to the developments as well as the emerging areas of Cyber Security. ICCWS-2021 will include high quality and focused technical program 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, start-ups and local cyber security companies.

Main topics of interests:

Following areas and others closely related topics:

- Hardware and systems security
- Operating systems and software security
- Web, Big data and Cloud security
- Distributed systems and data centre 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 Feed back 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

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: Fully connected autonomous vehicles hold the promise to improve road safety and offer new mobility options to millions of people. The CAN protocol lacks basic security features such as message authentication, which makes it vulnerable to a wide array of attack vectors including man-in-the-middle and packet spoofing. In recent years, several researchers have successfully exploited these vulnerabilities. As, vehicle-centric technologies are expected to grow so are the associated attack surfaces. Therefore, there is an urgent need for developing robust and reliable tools and techniques for source identification and integrity verification of CAN packets. Existing solutions for CAN protocol security are limited in their ability and scope as they are unable to link received packet to the source (e.g., transmitting) ECU. This talk will provide an overview of growing attack surfaces for connected autonomous vehicles, emerging security threats, and existing solutions to mitigate them. This talk will present robust, computationally efficient, and practical solutions to message authentication problem for in-vehicle networks (IVN) including CAN. Specifically, this talk will discuss a new method based on physical attributes of CAN signals for linking IVN packets to transmitting ECU. It will also propose a layered-framework for design and development of intrusion detection and prevention system (IDPS) for connected vehicles and evaluate effectiveness of the proposed solutions.

Dr. Zahri Yunos

Chief Operating Officer of Cyber Security Malaysia under the Ministry of Communications and Multimedia

Talk Title: APT Malware Threat: Case Studies In Malaysia

Abstract: Issues on network security have escalated ever since the Internet was introduced. Many researchers have intensified their efforts to ensure that security threats are discovered and mitigated in a well-timed manner. Today, cyber criminals have introduced sophistication in their attack techniques that makes the traditional way of safeguarding the enterprise networks are not effective. Cyber Security Malaysia has developed a 'LebahNET' project, a computer security device evasive attacks detection based on honey pot distributed computer security mechanism. In addition, Cyber Security Malaysia has developed a Coordinated Malware Eradication & Remediation Platform project, a system that able to detect and mitigate cyber threat with identifying unknown malware threats, preventing data breaches and preventing wide malware infection. These projects help in understanding and mitigating unknown malware threats.

Professor Dr. Awais Rashid

Professor of Cyber Security at University of Bristol

Talk Title: Developing a programmed of research on privacy, harm reduction and adversarial influence online: The REPHRAIN Centre

Abstract: Digital technologies pervade our daily lives and bring many benefits through delivering of online services to billions of users globally. However, alongside the many positive benefits of such a data-driven digital economy, serious challenges – e.g., privacy violations, micro-targeting of individuals, online abuse/victimization, fraud, and disinformation – have emerged. With innovations such as smart cities, IoT and mobile connectivity leading to further growth in connected digital platforms and services, we must consider a holistic programme of research to anticipate and address issues of privacy and online harms. In this talk, I will discuss the programme of research — being undertaken within the REPHRAIN centre — to deliver interdisciplinary research drawing upon social and technical sciences to advance state-of-the-art in privacy enhancing technologies and online harm mitigation approaches.

Mr. Razi Bin Rais

Senior Technical Program Manager, Microsoft Identity Engineering, USA

Talk Title: Zero Trust Security: What it is and why it's important to embrace it to battle cyberattacks

Abstract: As cyber-attacks became sophisticated and prevalent across the globe, private organizations and governments alike must adopt a new security model that is effective against wide variety of attacks while embracing the mobile remote workforce. A new security model based on "Zero Trust" strategy is key to securing data, systems, and services. In 2021, United States White House issued an executive order mandating all federal agencies to adopt Zero Trust on urgent basis. Cloud providers like Microsoft, Google, Amazon, Alibaba have also made Zero Trust critical part of part of their security strategy. This session will explore key tenets and principles of the Zero Trust model and how it can be leveraged to improve the security posture of an organization.

Professor Zoltan Rajnai
National Cyber Coordinator of Hungary; Professor, Obuda University – Hungary

Talk Title: National cybersecurity challenges, coordination and cyber protection of critical infrastructure in Hungary

Abstract: In modern democracies the digital revolution has been stretching to all aspects of life which generates significant dependency. Nowadays members of the society are less viable if they do not use e-mail addresses, bank accounts and cards, or some sort of positioning system. The role and significance of digital infrastructures is undisputed, they became unquestionable components of transparent state functions, economic prosperity, and successful scientific research. One the one hand, modern information society considers information and communication technologies the engine of societal evolution. On the other hand, the challenges of dependency, the dynamics of development and the rate of penetration involve serious threats. Nowadays, all countries rely on the latest technologies to drive economic and social growth, and to make their most critical infrastructure systems operating smoothly. We all live in a digital landscape full of cyber threats and vulnerabilities. In the future both public and private sector cybersecurity professionals must be highly collaborative and interconnected to fight against cyber threats. To exchange information and share best practices about cyberspace issues and the resulting threats, is a good start to enhance cooperation and create trust between countries facing the same challenges to ensure the resiliency of critical infrastructure in the future. Evolving threats will continue. Users' awareness, training and education are the cornerstones of critical infrastructure cyber security. The speaker's presentation will highlight some issues of the Hungarian aspects of national cyber security.

Mr. Ahrar Naqvi
CEO Ebryx

Talk Title: Incident Readiness and Response

Abstract: Being well-prepared for incidents and effective incident response are key in limiting damage from incidents and minimizing recovery time. Lack of effectiveness here can lead to dire consequences. Yet most organizations tend to be ill-prepared and incident response tends to be chaotic and ill-executed, thus causing avoidable damage. The problem is especially acute in skill and resource constrained environments and extends beyond organizations to critical sectors. Market and organizational dynamics tend to compound the problem. This talk is aimed at highlighting key aspects of effective incident readiness and response and possible approaches to improving the situation in such environments.

Professor Siraj Shaikh
Head of System Security Group, Coventry University, UK

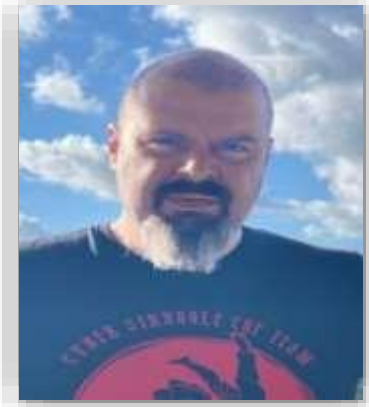
Talk Title (Online): Cyber security Challenges for Mobility and Transport Infrastructure

Abstract: While cyber-physical systems security poses technical challenges of design and verification, problems of in-life monitoring and risk perception for effective secure operation cannot be ignored. We focus on transport and mobility platforms for the security risks they pose, and examine what the current state of the art to address such risks. The concepts presented here sit at the intersection of computer science, cyber security and transport engineering.

Dr. Richard Thomas
UKRRIN - Industrial Fellow in Data Integration and Cyber security, University of Birmingham, UK

Talk Title (Online): The Cyber Security of Rail

Abstract: As the critical national infrastructure continues to digitalize, safety and cyber security now co-exist. These systems are designed with typical life spans measured in decades, meaning that they have to defend not only against current adversaries, but also emergent threats. This talk will explore the rail sector's journey in digitalization, from traditional line side signaling, to complex, inter-connected digital systems and how cyber security requirements and assurance are unavoidable in the digital railway, and how new legislation and regulation is driving a cyber-security culture change in the EU and international sectors.



Kubilay Onur Gungor
Cyber Struggle, Turkey

Talk Title: Warrior mindset and functional development for the irregular warfare side of the future cyber struggle

Abstract: On the contrary of the definition as an additional domain to Air, Land, Sea, and Space, Cyber is a truly irregular framework covering all other domains as well as carrying extreme uncertainty. We do not know when the attack will occur, how long it will take, how much power will be in use, where it will come from. Basically, we are trying to prepare ourselves to the unknown! On top of that, there is no border between war and peace. Therefore, this phenomenon is a struggle rather than a war, and unorthodox struggles require unorthodox approaches with teams and individuals.

Mr. Taylan Esen
CTO Angora Networks, Turkey

Talk Title (Online): Security Services Chaining

Abstract: Networks is the new circulatory system of the world. Everything is now irresistibly connected. From airplanes/fighter jets to the smallest sensors in the underground, all data generation or consuming points need to be engaged to better create a combined vision, holistic view and informed decision making. So we need to protect this environment consisting of unlimited data access, processes and subsystems where every byte may need a different approach for the best, but beyond that, useful security. The goal of the presentation is to share, how different measures should be combined inside a network to provide different level of security for distinct requirements. How to manage security services, how to monitor breaches, leaks or even simple steps taken by users, not only for protection but also, to understand the ecosystem of application and user. Understand how new technologies like, behavioral analysis, data mining, artificial intelligence and others would help your network, become more secure with optimal effort, time and cost.

Prof. Dr. Seref SAGIROGLU
Director of GAZI AI CENTER, Gazi University, Turkey

Talk Title: Data Analytics, Security and Privacy Issues in Smart Grid

Abstract: Big data has great potential to provide opportunities not only many fields but also smart gird enhancing technical, organizational, social and economic gains and contributions. The current potential of applying big data approaches for better planning; managing, designing, and securing power grid operations are very challenging tasks and needs significant efforts. This talk will cover the issues of computational complexity, data security and privacy, cost, management, planning and integration of big data into power grid systems and also focus on the key challenges in big data analytics, privacy and security issues. Finally, some issues supported by Gazi AI Center are summarized using big data analytic laboratory infrastructure and laboratory.

PAPER PRESENTATIONS: ABSTRACTS

Application Profiling from Encrypted Traffic

Authors: Alia Nawaz, Tariq Naeem and Muhammad Tayyab

Abstract: Everyday millions of people use Internet for various purposes including information access, communication, business, education, entertainment and more. As a result, huge amount of information is exchanged between billions of connected devices. This information can be encapsulated in different types of data packets. This information is also referred to as network traffic. The traffic analysis is a challenging task when the traffic is encrypted and the contents are not readable. So complex algorithms required to deduce the information and form patterns for traffic analysis. Many of currently available techniques rely on application specific attribute analysis, deep packet inspection (DPI) or content-based analysis that become ineffective on encrypted traffic. The article will have focused on analysis techniques for encrypted traffic that are adaptive to address the evolving nature and increasing volume of network traffic. The proposed solution is less dependent on application and protocol specific parameters so that it can adapt to new types of applications and protocols. Our results show that processing required for traffic analysis need to be in acceptable limits to ensure applicability in real-time applications without compromising performance.

Email Classification using LSTM: A Deep Learning Technique

Authors: Palwasha Bhatti, Asma Majeed, and Dr. Zunara jalil

Abstract: Electronic mail has been in use for decades and more than four billion users access their emails using different domains and servers. Emails are considered an official way of communication in remote working modes and in online businesses. Email labeling can reduce the amount of effort to manage this communication. Email classification is so far done to classify emails such as Spam, Non-spam, Junk, social media, etc. However, email classification keeping in view the types of cybercrimes committed through email is not done. Emails can be labeled as Spam, Phishing, fraudulent, harassing, bullying, or can be a general/normal email. This identification is one of the most challenging tasks for both email service providers and consumers. Several spam identification models have previously been proposed and tested but very limited work has been done so far on the multi-class classification of emails. Emails can be classified into more than two classes (spam and ham). In this paper, we have proposed a solution to classify emails into four classes: fraudulent, suspicious, harassment, and normal. A deep learning approach named Long Short Term Memory (LSTM) with stratified sampling has been used to identify the email classes. An effort has also been made to balance the input dataset using over-sampling methods. The proposed model obtained a classification accuracy of more than 90%. With stratified sampling only and more than 95% by applying data balancing techniques on the dataset.

A Generic Machine Learning Approach for IoT Device Identification

Authors: Zain Ali, Faisal Hussain, Syed Ghazanfa rAbbas, Muhammad Husnain, Shahzaib Zahid and Ghalib A.Shah

Abstract: The rapidly prevailing Internet of Things (IoT) Devices in numerous sectors, may jeopardize a vast amount of confidential data, raising threats to network security. Thereby, it is crucial to verify the data source and device identity to ensure network security. Thus, the identification of IoT devices is a substantial step in securing the underlying network system. The models which are proposed in previous studies are trained and tested on the same dataset, which leads to over fitting. In this work, we propose a generic machine learning approach for IoT device identification and test the trained models on four publically available datasets. To better identify IoT devices in the network through machine learning models, we first extracted 85 features from packet capture (.pcap) files using NF Stream. We then selected 20 features using the

information gain method and trained six machine learning models in our experiment son two publicly available datasets, i.e., UNSW IoT Traces, and Your Things dataset, for binary classification. In the training phase, we obtained the highest 99% accuracy for IoT device identification using Random Forest and Naiive Bayes classifiers over UNSW and Your Things dataset respectively. Further, we evaluated these models on two other publicly available datasets. Overall, the Na¨ıve Bayes classifier outperformed all other classifiers for detecting both IoT and non-IoT traffic, with 92% average accuracy.

Efficient Identification of Race Condition Vulnerability in C code by Abstract Interpretation and Value Analysis

Authors: Mehran Yousaf, Muddassar Sindhu, Muhammad Hassan Arif and Shafiq Ur Rehman

Abstract: The increased usage of information and communication technologies has changed the way industries look at things. This development of technology in terms of software utilization has resulted in various security vulnerabilities such as injection, data disclosure, authentication, and access control concerns. When working with concurrent applications, race conditions can trigger a number of these vulnerabilities. Formal approaches have been developed to detect the race condition vulnerability in the literature. Existing approaches for detecting race conditions have few drawbacks that include static checkers' inability to analyze the un interpreted programs, and minimal exploration of race condition types. Due to these weaknesses static checkers produce a large number of false alarms. This study proposes an algorithm AIT for analysis of un interpreted programs based on a formal static analysis technique called Abstract Interpretation (AI). It also proposes the T2RC and SyncRC algorithms for race condition detection. The proposed approach is validated using Juliet and Data Race Bench datasets. The proposed method yields an average accuracy of 84% and produces very few false alarms. Additionally, it not only handles un interpreted programs, but also analyzes for a wider range of Race Conditions thus performing better than other comparable approaches.

Reed: An Automated Scalable Multi-Language Vulnerability Dataset Generator for Open Source Software

Authors: Ahsan Yasin, Faisal Amjad, Haider Abbas and Ali Abidi

Abstract: The knowledge of potential vulnerabilities and their location in the software prior to its release can be very useful asset in preventing software from being compromised by an attacker. The tools currently available to detect vulnerabilities in software have many limitations including lack of automation in dataset creation. These tools are platform, language and purpose-specific. Furthermore, they do not cater for the fact that a given vulnerability may exist in multiple software categories or versions, which can have a negative effect on the accuracy of machine learning algorithms that depend on such datasets. In this paper, we present Reed, a customizable software vulnerability dataset generation tool which produces automated and scalable datasets for any language from open source software. Reed takes into account the possibility that a single vulnerability may exist in the raw data of multiple software packages and thus makes the generated dataset ideal for machine learning. To demonstrate the efficiency of Reed, we present the generation of three sample dataset of vulnerable software consisting of 301, 308 and 512 unique vulnerabilities extracted from git repositories of Ubuntu Bionic kernel, Ubuntu Xenial kernel and Ubuntu Trusty kernel respectively. These datasets were generated in few hours. Reed can gather CVE reported vulnerabilities of projects which have open-sourced their git repositories. This dataset generation method is considerably faster, cheaper and far more efficient than manual dataset generation which takes many months of effort to create relevant datasets of the similar sizes.

Secure Internet Voting using Block Chain Technology

Authors: Muhammad Ali Khan and Hafiz Shahbaz Rasheed

Abstract: Many countries have been using online voting systems instead of ballot papers. In such voting systems, voters can cast votes online using their cell phones, laptops, and other internet-connected devices. Online voting systems have centralized databases where a malicious attacker can hack, change or manipulate the database. Therefore, current online voting systems present a security concern for any government. Block chain is a peer-to-peer technology in which data is stored in a tamper-proof ledger and

maintained by participating peers. In this paper, we propose a secure online voting system using Ethereum Block chain and Ethereum Smart Contracts. A voter can cast her vote securely after scanning her fingerprint and iris recognition. Our proposed methodology uses Paillier homo-morphic encryption and the private key shifting technique to ensure voter privacy and identity security.

SSD Forensic: Evidence Generation and Forensic Research on Solid State Drives Using Trim Analysis

Authors: Hassan JalilHadi and Numan Mushtaq

Abstract: Traditional hard drives consisting of spinning magnetic media platters are becoming things of the past as with the emergence of the latest digital technologies and electronic equipment, the demand for faster, lighter, and more reliable alternate storage solutions is imperative. To attain these requirements, flash storage technologies like Solid State Drive (SSD) has overtaken traditional hard disk drives. In a forensic analysis of flash storage devices, forensic investigators are facing severe challenges for the reason that the sovereign behavior of solid-state storage media does not look favorable compared to traditional storage media devices. Wear Leveling, a fundamental mechanism in Solid State Drive (SSD), plays a severe challenge that most often destroys forensic evidence in many cases. It makes it complicated for forensic investigators to recover the necessary evidence. Persistence of deleted data in flash storage media depends on various factors like the Garbage Collection process, TRIM command, flash media type, manufacturer, capacity, file system, type of file saved, and the Operating System, etc. In view of this, extensive experiments conducted to identify the probability of data recovery and carving. Analyzed effects of Wear Leveling and Garbage Collection processes in Solid State Drive (SSD) of different manufacturers, having the same storage capacities and with a different type of files utilized. In conclusion, experimental findings established the fact that Wear Leveling in solid-state media can obfuscate digital evidence, and a conventional assumption regarding the behavior of storage media is no more valid. Moreover, data persistency also depends on the manufacturers, time-lapse of forensic analysis after data deletion, type of files, and size of files stored in Solid State Drives (SSD).

A Privacy-Preserving Cross-domain Network Access Services Using Sovrin Identifier

Authors: Farooq Ahmed and Syeda Azka Hussain

Abstract: The number of cross-domain roaming users through Wi-Fi has expanded considerably in recent years. It is important to authenticate users from various institutions to ensure the confidentiality and reliability of the network. Existing solutions like eduroam utilize a centralized framework to identify user's accounts that generate confidentiality and security concerns. We propose a block-chain-based cross-domain authentication mechanism that provides accountability and anonymity without any third-party dependence. In contrast to previous centralized ways, our scheme authenticates its user and server anonymously and widely distributed way of delivering roaming service without privacy breaching concerns. Using a Hyper-ledger block-chain, we integrate our system with Sovrin identifier to authenticate the user that retains confidentiality and reliability when the user accesses the network.

Endpoint Detection & Response A Malware Identification Solution for Enterprises

Authors: Asad Arfeen, Saad Ahmed and Muhammad Asim Khan

Abstract: Malicious hackers breach security perimeters, cause infrastructure disruptions as well as steal proprietary information, financial data, and violate consumers' privacy. Protection of the whole organization by using the firm's security officers can be besieged with faulty warnings. Engineers must shift from console to console to put together Investigative clues as a result of today have fragmented security technologies that cause frustratingly sluggish investigations. Endpoint Detection and Response (EDR) solutions add an extra layer of protection to prevent an endpoint action into a breach. EDR is the region's foremost detection and response tool that combines endpoint and network data to recognize and respond to sophisticated threats. Offering unrivaled security and operational effectiveness, it integrates prevention, investigation, detection, and responding in a single platform. EDR provides enterprise coverage and uninterrupted defense with its continuous monitoring and response to threats. Through various security layers, our EDR unifies and expands detection

and response capabilities, enabling security teams to have unified end-to-end corporate accessibility, powerful analytics, along with additional features such as web threat scan, external device scan, and automatic reaction across the whole technological tower, this allows security experts to detect and halt attacks in progress before they make an impact on enterprise security.

Image Steganography using Cryptographic Primitives

Authors: Zeeshan Abbas and Muhammad Qasim Saeed

Abstract: Information security has received exclusive consideration of numerous researchers in the recent past. Various methods for securing sensitive information have been devised either based on steganography or cryptography. The former method is a form of covert communication in which the information is hidden within some other medium like image, audio, video, or text. Whereas in the latter method, the information is encrypted using cryptographic primitives to generate the random-looking cipher text. Both approaches have their strengths and weaknesses. We devised a smart approach by combining the strengths of both methods; randomness from cryptography and data hiding using steganography. We used the most common technique of steganography in spatial domain called Least Significant Bit (LSB) based on RGB image steganography. Generally, in this method, the secret information bits are hidden in LSB of Red, Green, and Blue (RGB) channels of an image in a sequence. This approach is simple and efficient, however, it is prone to data recovery attacks. In order to destroy the sequential hiding, we used cryptographic primitives (AES-128, RC4 andSHA-256) to produce randomness. The randomness is used to determine the location and channel to hide the data. The random sequence generated by cryptographic primitives is only known to sender and receiver, thus an attacker eavesdropping on the message cannot recover the hidden information. After embedding the secret data in an image, we performed qualitative and quantitative analysis to measure the quality of the stego-image. Quantitative analysis includes Mean Square Error (MSE), Peak signal-to-noise ratio (PSNR) and Normalized Cross-Correlation (NCC). Histogram analysis is also performed on all three channels (Red, Green, and Blue) of both, original and stego-images. In the end, the proposed model is analyzed against various attacking scenarios.

SHA-3 Algorithm-based Authentication Scheme for Vehicular Ad-hoc Networks

Authors: Asjad Iqbal and Saima Zafar

Abstract: Vehicular Ad-hoc Networks (VANETs) are a subset of Mobile Ad-hoc Networks (MANETs), specifically designed for interconnection among vehicles and between vehicles and Road-Side-Units (RSU), in order to ensure efficient and secure transportation. Authentication is the process of identifying nodes or verifying messages and is of utmost importance in VANETs. Expedite Message Authentication Protocol (EMAP) is a notable authentication protocol specifically designed for VANETs which exploits the hash-based message authentication (HMAC) instead of certificate verification to minimize message loss-ratio and delay. On the downside, to generate the hash code, the EMAP uses Secure Hash Algorithm (SHA-1) which is an outdated algorithm susceptible to collision attack. Contrary to it, SHA-3 is a new hash standard that was not derived from the SHA family. Although the SHA-3 scheme is superior and different in structure from the previous family of standards, the feasibility analysis of SHA-3 scheme in VANETs is an open research problem. This paper presents the results of implementation of HMAC with SHA-3 algorithm in VANETs for authentication and analyzes its impact on Quality of Service (QoS) parameters of VANETs such as Packet Delivery Ratio (PDR), delay and throughput and compares these results against SHA-1 and SHA-2 algorithms. The simulations are carried out using the Network Simulator (NS3). Our results show that SHA-3 based algorithm provides improvement in PDR and end-to-end delay and is a viable choice for authentication in VANETs for providing superior security.

Decoy state HD QKD system for secure optical communication

Authors: Muhammad Kamran, Muhammad Mubashir Khan and Tahir Malik

Abstract: Quantum key distribution (QKD) is an unconditionally secure way of sharing secret

cryptographic keys on a public channel. Recently, high dimension QKD protocols have gained focus to achieve better security against various attack models. Here, we focus on the robustness of high dimensional QKD protocol against two realistic attack models, i.e. photon number splitting (PNS) attack and beam splitter (BS) attack. We present the high dimensional quantum key distribution system that incorporates a decoy-state scheme with complex structured light (OAM modes) using the KMB09 protocol. The complete QKD system design with experimental setup details and evaluation results are presented. The experimental results show that our proposed decoy-state scheme is robust against both PNS and BS attacks.

Enhancement in Buffer Overflow (BOF) Detection Capability of Cppcheck Static Analysis Tool

Authors: Younis Iqbal, Muddassar Sindhu, Muhammad Amir Javed and Muhammad Hassan Arif

Abstract: Buffer overflow (BOF) vulnerability is one of the most dangerous security vulnerability which can be exploited by unwanted users. This vulnerability can be detected by both static and dynamic analysis techniques. For dynamic analysis, execution of the program is required in which the behavior of the program according to specifications is checked while in static analysis the source code is analyzed for security vulnerabilities without execution of code. Despite the fact that many open source and commercial security analysis tools employ static and dynamic methods but there is still a margin for improvement in BOF vulnerability detection capability of these tools. We propose an enhancement in Cppcheck tool for statically detecting BOF vulnerability using data flow analysis in C programs. We have used the Juliet Test Suite to test our approach. We selected two best tools cited in the literature for BOF detection (i.e. Frama- C and Splint) to compare the performance and accuracy of our approach. From the experiments, our proposed approach generated Youden Index of 0.45, Frama-C has only 0.1 Youden's score and Splint generated Youden score of -0.47. These results show that our technique performs better as compared to both Frama-C and Splint static analysis tools.

Comparative Analysis of Anti-Virus Evasion Malware Creator Tools of Kali Linux, with Proposed Model for Obfuscation

Authors: Anas Kayani and Qasim Saeed

Abstract: Cyber security is one of the most important aspect for any organization as well as an individual against cyber threats which may leads to the destruction of their assets, personal information, and financial loss. Malwares are one of the most advanced and widely used software in this domain. Malware researchers are always looking forward for the ways to make their malicious file as legitimate and stealthy as possible. This study is highlighting the tools developed for the malware generation using the advance penetration testing operating system 'Kali Linux'. There are tools available which according to their writers "generates stealthy malware that has a capability to evade anti-viruses and hiding its capability to perform operations". We proposed a methodology to obfuscate the capabilities of software. The techniques used in the proposed methodology are packing and signing of an executable simultaneously, for packing (or compression) we used Lempel-Ziv and Huffman coding then the executable is signed by replicating the certificate of a legitimate website giving us the promising results.

A Deep Learning based Malware Images Classification

Authors: Muhammad MehmoodAlam, AdeelAkram, Talha Saeed and Sobia Arshad.

Abstract: The rapid development in the field of communication and networks has increased the size and complexity of the network. Due to these reasons, many malwares are generated that create challenges for systems to detect these malwares accurately. Moreover, the presence of malicious software (malware) with the aim of launching various malware files with in the network cannot be ignored. Although, there are numerous efforts by the researchers to develop procedures for automatic classification of malware. The methods of manually analyzing malware file is very time-consuming. Lately, deep learning-based methods are being used for the classification of malware. In this paper, we present a rapid and accurate malware classification based on different Convolutional Neural Network (CNN) architectures— including a custom CNN as well as commodity off-the-shelf CNN architectures such as AlexNet, VGG-16, ResNet-50, Inceptionv3 models. This has been demonstrated on benchmark datasets of Malimg dataset, which is

consists of malware images that were obtained after conversion of Malware binaries. The trained models allow accurate classification of malware and report a test accuracy of 98.90%.

Implementation of Cyber-Physical Systems with Modbus Communication for Security Studies

Authors: MuhammadMiftah Ur Rehman, Haseeb Ahmed Chattha, Ghulam Mustafa, Abdul Qayyum Khan, Muhammad Abid and EhtishamUlHaq.

Abstract: We present an implementation of cyber-physical systems with Modbus/TCP communication for real-time security testing. The proposed architecture consists of a process simulator, an IEC 61131-3 compliant programmable logic controller, and a human-machine interface, all communicating via Modbus/TCP protocol. We use Simulink as the process simulator. It does not have built-in support for the Modbus protocol. A contribution of the proposed work is to extend the functionality of Simulink with a custom block to enable Modbus communication. We use two case studies to demonstrate the utility of the cyber-physical system architecture. We can model complex cyber-physical processes using this architecture and can launch cyber-attacks and develop protection mechanisms.

Modeling and Simulation Challenges for Cyber Physical Systems from Operational Security Perspective

Authors: Kashif Rahim and HassaanKhaliq

Abstract: As Critical Infrastructures become more dependent on Cyber Physical Systems, their design and deployment in reliable, secure and safe manner has become more important. Such systems are bridging the gap between operational and information technologies as physical systems are interconnected and dependent upon underlying computational and communication infrastructure. The operational and information level vulnerabilities can cause physical damage and destruction in the event of system compromise. Appropriately verified modeling and simulation frameworks are therefore essential that may be incorporated from design till deployment stage of software, firmware, hardware and underlying connectivity fabric of physical systems or System of Systems. However, the heterogeneous nature of CPS limits full scale modeling and simulation in a single framework. In this study, state of art in CPS modeling and simulation is introduced for designing resilient systems with new methods and paradigms. Most relevant platforms are then analyzed for modeling CPS from mathematical, system theory, process control, interoperability and resiliency aspects. Lastly, we discuss challenges to CPS modeling and propose game theoretic approaches for formulation of operational security research through scenario building.

Electromagnetic Pulse (EMP): A Study of General Trends, Simulation Analysis of E1 HEMP Coupling and Protection Strategies

Authors: Rida Rashid and Amer Gilani

Abstract: Electromagnetic pulse (EMP) is considered as an element of electronic warfare (EW). EMP is an energy pulse that can damage electronic components. EMP events are considered as high impact low probability (HILP) events. In the current scenario, civil and military infrastructure are equally vulnerable to EMP attack whereas the risk of damage can be avoided by hardening the critical infrastructure. This paper will provide a study on EMP and its impact on modern society. To visualize the impact, simulation of E1 HEMP coupling on different cables is being performed using FEKO. The paper also includes protection strategies to harden vulnerable systems against EMP attack.

Physical Layer Authentication Security in Radio Communication- Emerging Trends

Authors: Fatima Khalil, Adnan Fazil, Ammar Masood and Muhammad Jawad Hussain

Abstract: Emerging mega-trends such as access control systems, wireless radio communication in active and passive wireless security systems and their promising applications are posing new challenges viz a viz new attacks to existing and future applications like Visible Light Communication (VLC), Radio Frequency Identification (RFID), Internet of Things (IoT) Electronic Ticketing, Electronic Passports etc. Consequently, dynamic management of additional measures and stepping ahead from mere reliance on cryptographic schemes deems crucial to smoothly garner the benefits of these technologies. Today, authentication between legitimate wireless systems without consideration of physical layer security attributes can provide attackers

an open cheque to exploit the communication. Recently, Physical-Layer Authentication (PLA) has emerged and enticed many researchers as it offers enhanced security, effective authentication with low computational complexity. The paper aims to give the reader a short but comprehensive view of PLA techniques, its implementation challenges along with emphasis to the emerging trends of PLA based applications for sound and secure authentication in wireless communication.

A Deep Ensemble Model for News Classification on Social Media

Authors: Javid Ur Rahman, Atif Khan, Shaukat Ali and Muhammad Fayaz

Abstract: In a biosphere where lots of people are associated through social networks for news stories, it is vital that accurate news be transmitted to quench the thirst of readers for knowing the world they live in. But, the transmission of fake news has become a great dilemma in the modern cyber world of which social media is an integral part. Therefore, the classification of news in real and fake on social sites has become a million-dollar question. Many machine and deep learning methods have been applied by various researchers for this task, but still space exist there to further improve the accuracy. We proposed a deep ensemble model comprised of Convolutional Neural Network (CNN), Deep Neural Network, and Recurrent Neural Network (RNN) where the final prediction has considered through majority of voting technique. The model provided 90.5 % accuracy on GloVe while 91.4 % accuracy on fastText embedding after evaluation.

Depression Analysis of social media activists using the Gated Architecture Bi-LSTM

Authors: Momina Rizwan Khan, Shereen Zehra Rizvi, Amanullah Yasin and Mohsan Ali

Abstract: Twitter is one of the social media platforms that has evolved into an incredible environment for users to communicate with friends and other users to trade thoughts, videos, and photographs that reflect their present mood. Using social media allows academics to investigate people' online data, revealing their moods and habits, and analyze their mental states. Since social media is becoming a part of our life, this study implies users' moods by what they post in their tweets. This study will analyze Twitter data for depression sentiment using a verified public internet portal. Social information is presented as an important predictor of depression. This study suggests distinct deep learning classification strategies which can perform as a competent and adaptable strategy and have already been effectively utilized in Natural Language Processing jobs to explore the impact of depression diagnosis on Twitter. LSTM and Convolutional Neural Networks were used to analyze Twitter data for depression analysis. Bi-LSTM proven the highest accuracy of 95% for real time depression Analysis. We also developed a depression analysis tool based on this study.

ICCWS 2021

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: 23rd – 24th November 2021, 09.00 am- 5.00 pm

Where: PAFSOM, ARENA, E-9, Islamabad

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

Notes

Notes

Notes