CRC

CYBER RECONNAISSANCE AND COMBAT

crc@bahria.edu.pk

Information and communication technologies have evolved over the last two decades and are now integrated into virtually every aspect of our lives. The transformation brought about by this digitalization creates new dependencies. Our economy, the administration of Pakistan government and the provision of essential services now rely on the integrity of cyberspace and on the infrastructure, systems and data which underpin it. As a nuclear state and Pakistan geopolitical position, the possibilities of various internal and external security concerns raised during last decade including Cyber Security. Government of Pakistan is implementing defense policies which shall stop the entry of terrorists in country and supervise territorial borders. Critical defense measures for important cyber services of the country such as NADRA, E-Government services and capital markets also requires attention of government in current security situation. In recent years, security solutions have been incorporated as various levels in public and private organizational networks. These solutions are comprising of firewalls, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) etc. The primitive line of defense in any security solution is IDS/IPS which safe guards against both internal and external threats. An IDS is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. Intrusion detection systems offer organizations a number of benefits, starting with the ability to identify security incidents. An IDS can be used to help analyze the quantity and types of attacks, and organizations can use this information to change their security systems or implement more effective controls. An intrusion detection system can also help companies identify bugs or problems with their network device configurations. The basic application domain of Cyber Reconnaissance and Combat (CRC) is the development of indigenous IDS software that can monitor and raise alarms in case of cyber-attacks. Although, a number of open source and commercial IDS are available but they cannot be trusted to protect Critical Information Infrastructure. Indigenous IDS will serve as main line of defense to identify threats/ attacks on National Information Infrastructure.

OBJECTIVES

- To become the country premier academic research Centre in Cyber Security and privacy, addressing the major technical and policy challenges.
- To develop both proof of concept and state-of-the art software/hardware for monitoring, detection and mitigation of cyber-attacks.
- To become the first choice for the government, industry, and public media in need of innovative research, technical insights, and policy guidance about Cyber Security .
- To be a catalyst of the information security industry in Pakistan through joint research projects with companies as well as successful start-up companies by Pakistan Tech faculty members and graduates.
- Detect, understand, investigate and disrupt hostile action, pursuing and prosecuting offenders and take offensive action in cyberspace.
- Develop an innovative, growing Cyber Security Centre, underpinned by world leading scientific research and development.
- Provide a self-sustaining pipeline of talent providing the skills to meet our national needs across the public and private sectors and overcome future threats and challenges.

SALIENT FEATURES

- Industrial Cases and Adoption: To design, develop and implement IDS systems.
- Small applications for attack detections and preventions
- Software and Solutions: to develop, enhance and deploy intelligent and adaptive platforms and systems with and for industry.
- Hardware Prototypes and Solutions: To research and develop hardware enabled solutions, with key focus on intrusion detection and prevention.

CONSULTING SERVICES

Provide advance research, academic and industrial services to small, medium-sized and large businesses. Core competencies in Cyber Security domain with specializations in:

- Design and implementation of intrusion detection systems.
- Design of defense/depth architecture for organizations.
- Designing Communication Protocols to secure the Wireless Ad hoc Networks and Internet of Things

RESEARCH & SERVICES PORTFOLIO

Intrusion Detection Systems

An IDS is a network security technology originally built for detecting vulnerability exploits against a target application or computer. Intrusion Prevention Systems (IPS) extend IDS solutions by adding the ability to block threats in addition to detecting them and has become the dominant deployment option for IDS/IPS technologies. A n IDS needs only to detect threats and as such is placed out-of-band on the network infrastructure, meaning that it is not in the true real-time communication path between the sender and receiver of information. The IDS monitors traffic and reports its results to an administrator, but cannot automatically take action to prevent a detected exploit from taking over the system. Attackers are capable of exploiting vulnerabilities very quickly once they enter the network, rendering the IDS an inadequate deployment for prevention device

Dynamic Application Security Testing and Assurance

To test a new software, you need to hire multiple people, which leads to more expenses and a chance of errors. Test automation aims to reduce the costs of software testing and to improve its reliability. Despite advances in test automation, there are some domains for which automation seems to be difficult, mostly in terms of security software. The project has enhanced the context of software security testing and provide substantial basis for understanding and executing automated and dynamic application security testing and assurance.

Smart IoT Communication Architecture

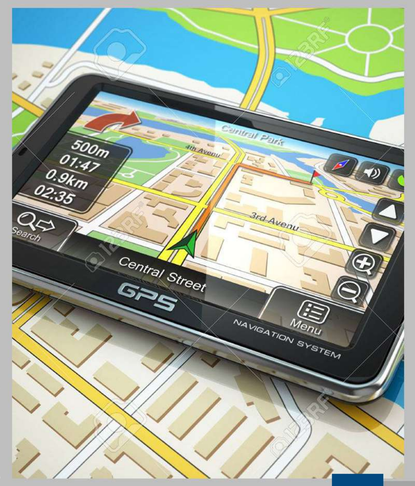
IoT devices are inherently connected and need a way of interacting with them, often with firewalls, network address translation (NAT) and other obstacles are in the way. There are billions of these devices for which, we need an architecture for scalability. In addition, these devices are typically interacting 24x7, so we need a highly-available approach that supports deployment across data centers to allow disaster recovery. The devices may not have user interface and certainly are designed to be "everyday" usage, so we need to support automatic and managed updates, as well as being able to remotely manage these devices. A model for managing the identity and access control for IoT devices and the data they publish and consume is a key requirement. This research aim is to provide an architecture that supports integration between systems and device.

Vulnerability Analysis

SQL Injection Attack (SQLIA) is one of the most severe attack that can be used against web database-driven applications. Attackers use SQLIA to obtain unauthorized access and perform unauthorized data modifications due to initial improper input validation by the web application developer. Various studies have shown that, on average, 64% of web applications worldwide are vulnerable to SQLIA due to improper input. To mitigate the devastating problem of SQLIA, this research proposes an automatic black box testing for SQL Injection Vulnerability (SQLIV). This acts to automate an SQLIV assessment in SQLIA. This research also focuses on improving the effectiveness of SQLIVS by proposing an object-oriented approach in its development. To test and validate the accuracy of research work, three vulnerable web applications were developed. The result of the experimental analysis shows significant improvement by achieving high accuracy compared to existing studies. Similarly, the analytical evaluations showed that the proposed scanner is capable of analyzing attacked page response using four different techniques.

Geographical Routing protocol for Vehicular Ad hoc Networks

Geographical routing protocols have suffered with neighbor discovery in urban scenarios. The network requires an efficient geographical routing protocol based on more realistic routing metrics for urban environment. In addition, large number of safety messages make communication channel more congested and cause of network overhead, packet loss and delay issues in the network. In order to handle congestion, there is a need of dynamic channel detection and controlling scheme for in time safety messages delivery in the network. The proposed geographical protocols are designed for urban scenarios. The more realistic routing metrics help the network for better data forwarding decisions and improve the frequent disconnectivity, packet forwarding and reduce delay in the network. Designed protocol also minimizing the network overhead, improve data delivery, reduce delay and secure the data. This work will be beneficial for communication channels to prevent from the congestion and controlling the channels to timely delivery of safety messages in VANETs.



KEY RESEARCHERS

Dr. Muhammad Najam Ul Islam

Dr. Muhammad Najam Ul Islam is working as Dean (Engineering Sciences) & Professor in the Bahria University, Islamabad. Najam did his PhD in Electrical Engineering from Telecom ParisTech, France. During his doctoral studies, he was working at EURECOM, Sophia Antipolis on the research theme of flexible radios for multi-standard wireless communication devices. He received his Master's Degree in Embedded Systems from University of Nice-Sophia Antipolis. Najam has also worked for NESCOM. Najam has worked on various research projects including NEWCOM, European Project: Flexible Baseband Design for Evolving Wireless Communication Standards, NESCOM: Modelling cyberattacks with empirical correlations, Bahria University: Design & FPGA implementation of Ultralight weight cryptography for low cost passive RFID tags, NESCOM: Pulse shaping and synchronization: Digital front end of telemetry system and IDROMEL: French National Project of FPGA Prototype Development of LTE Systems.

Dr. Faisal Bashir Hussain

Dr. Faisal Bashir Hussain is working as Professor in the Bahria University, Islamabad. He received his Ph.D. Computer Engineering in year 2008 degree from Dokuz Eylul Univeristy, Izmir, Turkey, where he worked on providing reliable communication in Wireless Sensor and Actuator Networks. He has also done Post Doctorate from Chosun University, South Korea, where he has worked on the association of devices in Wireless Personal Area Networks. He has worked as Assistant Professor in Department of Computer Software Engineering, MCS, NUST, Islamabad, from 2008 to 2013. Areas of interest are designing communication protocols for wireless ad-hoc networks, low power wireless networks, IoTs and security issues in wireless networks. Dr. Faisal Bashir is a recipient of Cultural Exchange Scholarship from Ministry of Education, Pakistan, PhD Research Scholarship, TUBITAK, Turkey and Post Doctorate Researcher Support from Chosun University, South Korea.

Dr. Kashif Naseer Qureshi

Dr. Kashif Naseer Qureshi is currently working as Senior Assistant Professor with Bahria University. He received his doctorate from the University of Technology Malaysia. His research interest focuses on but are not limited to Ad hoc communication, Internet of Vehicles, Body area Networks, Cloud Computing and Internet of Things and provision of security in these domains. He is a Cisco and Microsoft Certified Network Professional. He has been a reviewer for various reputable academic journals. He is an active researcher with around 80 international publications in various renowned journals with the cumulative impact factor of 50. He has lead Ministry of Higher Education Malaysia Project by Ministry of Education Malaysia and conducted in collaboration with Research Management Center at Universiti Teknologi Malaysia in Malaysia. Currently working with Ministry of Planning Commission and HEC Project Cyber Reconnaissance and Combat.