network sniffing, spoofing and poisoning; port scanning and vulnerability analysis; offline and online password attacks; buffer overflow; and root-kits and trojans.

FINANCIAL SUPPORT

Partial or full financial support will be provided to selected foreign participants from Member States of COMSATS, ISESCO and INIT.

FOR FURTHER INFORMATION, PLEASE CONTACT

ISESCO:

Dr. Tariq Mahmood
Director (Science and Technology), ISESCO
Rabat, Morocco.
Tel: +212-537-566052/53, Fax: +212-537-566012/13
Email: sciences@isesco.org.ma, mahmood@isesco.org.ma

Dr. Aicha Bammoun
Science Directorate, ISESCO
Rabat, Morocco.
Tel: +212- 5-37566052-53, Fax: +212- 5-37566012-13
Email: aicha_bammoun@yahoo.fr; bammoun@isesco.org.ma

INIT:

Mr. Tahir Naeem
Executive Director
Inter Islamic Network on Information Technology (INIT)
Islamabad, Pakistan.
Tel: +92-51-90495169, Fax: +92-51-9247006
Email: tnaeem@comsats.edu.pk

Mr. M. Atiq ur Rehman
Sr. Program Officer
Inter Islamic Network on Information Technology (INIT)
Islamabad, Pakistan.
Tel: +92-51-90495024, Fax: +92-51-9247006
Email: muhammad_atiq@comsats.edu.pk

COMSATS:

Mr. Tajammul Hussain
Advisor (Programmes)
COMSATS Headquarters
Islamabad, Pakistan.
Tel: +92-51-9204892, Fax: +92-51-9216539
Email: tajammul@comsats.org

Mr. Farhan Ansari
Sr. Assistant Director (Programmes)
COMSATS Headquarters
Islamabad, Pakistan.
Tel: +92 51 9214515-7, Fax: +92 51 9216539
Email: farhan@comsats.org

KazNU:

Prof. Dr. Tlekkabul Ramazanov
Vice-Rector for Research & Innovations, KazNU)
Almaty, Kazakhstan.
Tel.: (+7-727) 3773333-1122, Fax: (+7-727) 3773189
E-mail: tlekkabul.ramazanov@kaznu.kz

7th
ISESCO-COMSATS-INIT
International Workshop on

Internet Security: Enhancing Information Exchange Safeguards

19-23 December 2017
Almaty, Kazakhstan

Organized by

BACKGROUND

Information Technology is now considered a necessity for the general public and organizations in various sectors. However, it presents various risks in the form of cyber-attacks and has, therefore, evoked many privacy and security concerns. The frequency of cyber-attacks is considerably increasing every year, and the nature of security risks is constantly evolving. Therefore, effective surveillance networks are needed to ensure that the information and networks are protected from attacks, damage and unauthorized access, through the use of appropriate technologies, processes and practices.

In view of the above, the Commission on Science and Technology for Sustainable Development in the South (COMSATS); the Islamic Educational, Scientific and Cultural Organization (ISESCO); and the Inter Islamic Network on Information Technology (INIT) took the initiative of spreading awareness on this important field in the developing countries, particularly in their Member States, by means of organizing a series of training workshops. The earlier events of this series were held in Syria (2011), Jordan (2012), Tunisia (2013), Tanzania (2014), Turkey (2015) and Morocco (2016).

INTRODUCTION

The seventh five-day International Workshop on 'Internet Security: Enhancing Information Exchange Safeguards' is being jointly organized by ISESCO; COMSATS, INIT and Al-Farabi Kazakh National University (KazNU) on 19-23 December 2017, in Almaty, Kazakhstan.

AIMS AND OBJECTIVES

The workshop aims to provide a forum to the young scientists/professionals from the developing countries to learn about the latest advancements in the field of Internet security; promote the use of state-of-the-art technologies for protection of network and network-accessible resources from different types of malicious attacks; and identify effective Internet/information security solutions for general public, governmental organizations and commercial ventures through rigorous risk-analyses and security management approaches.

FORMAT

The workshop includes technical presentations, tutorials and hands-on training sessions by a group of renowned subject experts. It will cover major aspects of Internet/information security, ranging from theoretical understanding of cryptographic algorithms to practical subtleties of the network systems, and will also address the related managerial and technical issues. Moreover, a handful of network security tools will be demonstrated to provide opportunities to the participants to update their knowledge-base and interact with experts for further collaborative undertakings.

KEY AREAS

Following are the key topics of the workshop:

- Information Security Risk Assessment/ Management
- Network Security: Modern Attacks, Evasion Techniques and Defenses
- Malicious Code Analysis and Detection
- Measuring Security
- Ethical Issues of ICT Security
- Organizational Security Standards, Policies and Guidelines
- Cryptographic Techniques for Network Security
- Web Security
- Social Network Security
- Cloud Computing Security
- Digital Forensics Procedures and Tools

TARGETED INDIVIDUALS

Young researchers, practitioners, academicians, executives, system administrators, system programmers, and students working in the field of Internet/information security and cryptography are invited to participate in the workshop.

EXPECTED OUTCOMES

The workshop is expected to enable the participants to:

- Understand Organizational Security Structure and their particular security requirements
- Analyzing and mitigating the Information security risks
- Understand network protocols, models, topologies and related security threats;
- Understand major modern-day cryptographic algorithms and protocols;
- Understand how to send secure emails
- Use Full Disk Encryption (FDE) tools, including TrueCrypt;
- Understand the anti-virus, anti-spyware tools and firewalls;
- Understand the working of major web-security applications;
- Understand the working of contemporary biometrics systems;
- Understand organizational security measures, risk assessment tools and techniques and implement appropriate policies and procedures for a given organization;
- Understand different aspects of cyber security; and
- Understand and use various types of ethical hacking tools to secure the networks, including: