techniques to adopt appropriate policies and procedures;
- Understand different aspects of cyber security; and
- Understand and use various types of ethical hacking tools to secure the networks against a number of threats, including: 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 ISESCO, COMSATS, and INIT.

FOR FURTHER INFORMATION, PLEASE CONTACT

Dr. Tariq Mahmood
Director (Science and Technology)
Islamic Educational, Scientific and Cultural Organization (ISESCO)
Avenue des F.A.R, P.O. Box 2275, PC Code 10104
Hay Ryad-Rabat, Kingdom of Morocco.
Tel: +212-537-566052/53
Fax: +212-537-566012/13
Email: sciences@isesco.org.ma, tmahmood@isesco.org.ma

Mr. Tahir Naeem
Executive Director
Inter Islamic Network on InformationTechnology (INIT),
COMSATS Institute of Information Technology (CIIT)
Park Road, ChakShehzad
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)
COMSATS Institute of Information Technology (CIIT),
Park Road, Chak Shehzad
Islamabad, Pakistan.
Tel: +92-51-90495024
Fax: +92-51-9247006
Email: muhammad_atiq@comsats.edu.pk

Mr. Tajammul Hussain
Advisor (Programmes)
Commission on Science and Technology for Sustainable Development in the South (COMSATS) Headquarters
Shahrah-e-Jamhuriat, G-5/2, Islamabad, Pakistan.
Tel: +92-51-9204892
Fax: +92-51-9216539
Email: husseint@comsats.net.pk

Mr. Farhan Ansari
Sr. Assistant Director (Programmes)
Commission on Science and Technology for Sustainable Development in the South (COMSATS) Headquarters
Shahrah-e-Jamhuriat, G-5/2, Islamabad, Pakistan.
Tel: +92-51-9214515-7
Fax: +92-51-9216539
Email: fansari@comsats.net.pk

6th COMSATS-ISESCO-INIT International Workshop on

Internet Security: Enhancing Information Exchange Safeguards

19-23 December 2016
Rabat, Morocco

Organized by

COMSATS ISESCO INIT

INTRODUCTION & BACKGROUND

Since soon after the mainstreaming of computer systems for use by organizations, business enterprises and general public, the ever-increasing reliance on Internet, wireless networks and 'smart' devices especially smartphones, has been exposing societies across the globe to a number of security and privacy threats. This growing technological advancement is also accompanied by more sophisticated and complicated malicious techniques endangering end-users and enterprises that are active participants of the cyber environment. In order to prevent and mitigate the impact of these threats, the need for ensuring Internet/cyber security cannot be emphasized enough for, inter alia, protecting information systems from damage to the hardware and software, or theft of the information of sensitive nature processed by computer systems and networks; as well as avoiding disruption of the crucial services. All this can be ensured by adopting consistent cyber security policies and practices, and spreading the necessary technical information.

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 about cyber security in the developing countries, particularly in their Member States by means of organizing a series of training workshops on the theme. The earlier events of this series were held in Syria (2011), Jordan (2012), Tunisia (2013), Tanzania (2014) and Turkey (2015).

The 6th five-day International Workshop on 'Internet Security: Enhancing Information Exchange Safeguards' is being jointly organized by ISESCO, COMSATS, and INIT on 19-23 December 2016, in Rabat, Kingdom of Morocco.

AIMS AND OBJECTIVES

The workshop aims to provide a forum to the relevant young scientists and 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 against different types of malicious attacks; and identify effective Internet/ information security solutions for governmental organizations, commercial ventures and general public, through rigorous risk-analyses and security management approaches.

FORMAT

The workshop includes technical presentations, tutorials and hands-on training sessions by a group of 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 also highlight the related managerial and technical issues. Moreover, the use of a handful of network security tools will be demonstrated by the experts to enhance the participants' knowledge-base.

KEY AREAS

Following are the key topics of the workshop:

- Information Security Risk Assessment/ Management Ethical Issues of ICT Security;
- Organizational Security Standards, Policies and Guidelines;
- Network Security: Modern Attacks, Evasion Techniques and Defenses;
- Malware Detection and Analyses;
- Cryptographic Techniques for Network Security;
- Wireless Network Security;
- Web Security;
- Social Network Security;
- Cloud Computing Security; and
- Digital Forensics: Procedures and Tools.

WHO SHOULD ATTEND

Young researchers, practitioners, academicians, system administrators, system programmers, IT company executives, and students working/ studying 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 structures and their specific security requirements;
- Analyze and mitigate the information security risks;
- Understand security threats related to network protocols, models, topologies;
- Understand modern-day cryptographic algorithms and protocols;
- Understand how to send secure emails;
- Understand the anti-virus, anti-spyware tools and firewalls;
- Understand the engineering behind modern malwares;
- Understand the consequences of using weak security protocols and vulnerable software application;
- Understand the security issues in web applications;
- Understand risk assessment tools and