EPN

DOCTORAL COURSE ON R + D + I

HOMEWORK

A) OVERVIEW RESEARCH

Critical infrastructure of a country can be threatened by internal or external. To minimize negative impacts of such threats, the bodies in charge of those infrastructures should implement procedures to anticipate the development and course of possible attacks and to implement measures for mitigation.

Generally, the targets of an attack or intrusion are selected considering political, economic, social reasons, security, criminal issues, among others. In general, it establishes a phase of surveillance and close monitoring of the target using different techniques, including humans, operational and technological factors. When attacks or intrusions are in progress, they are masked using different techniques, which make hard their identification and therefore their neutralization.

The answer in both cases is to investigate and develop methods, techniques and technological tools in conjunction with operating procedures to detect and anticipate eminent or ongoing attacks to critical infrastructure of an organization or country. Such technologies must be both technically and economically accessible safeguarding certain technological independence.

KEY WORDS:

CIBERSECURITY, CRITICAL INFRAESTRUCTURE, TREATH, INTRUSION, SAFEGUARDING

B) RESEARCH CONTEXT

The rapid development of the Internet and the Web and its use by the population has had positive impacts in all areas of human endeavor but also negative impacts. One of these impacts is the violation or damage computer systems and critical- infrastructure of organizations and countries. Negative impacts may become a serious risk for individuals or organizations (including countries). The implementation of banking systems, e-commerce and e-government Web applications have attracted individuals to exploit technological or human failures to get economic benefit. However, recent years, attacks are also related to political/social issues or organized crime, among others. As a consequence has emerged a sense of insecurity in the Web and a series of behaviors in countries, organizations and individuals who have made unsafe to the Web. The cybersecurity management is the systematic response to those countries, organizations and inviduals, in regard to security in the Web. Cybersecurity is based on the political, organizational, human and technological management of threats and risks that now presents the Web and the Internet.

KEY WORDS:

INTERNET, WEB, CRITCAL-INFRAESTRUCTURE, CYBERSECURITY, E-COMMERCE

C) TWO CONGRESS

1.- Name:

10th IET System Safety and Cyber Security Conference

Acronym:

-

URL:

http://conferences.theiet.org/system-safety/

Deadline:

24 April 2015

Abstract Submission Procedure:

Online

Publisher:

Oxford Abstract

http://www.oxfordabstracts.com/

2.- Name:

12th International Conference on Trust, Privacy and Security in Digital Business

Acronym:

TrustBus’15

URL:

http://www.ds.unipi.gr/trustbus15/

Deadline:

30 April 2015

Abstract Submission Procedure:

Online

Publisher:

Springer

http://www.springer.com/computer/lncs/lncs+authors?SGWID=0-40209-0-0-0

D) TWO JOURNALS

1.- Name:

Cyber Security in the Critical Infrastructure: Advances and Future Directions

Acronym:

-

URL:

http://www.journals.elsevier.com/journal-of-computer-and-system-sciences/call-for-papers/cyber-security-in-the-critical-infrastructure-advances-and-f/

Deadline:

31 August 2015

Abstract Submission Procedure:

Online

Publisher:

Elsevier

http://www.journals.elsevier.com/journal-of-computer-and-system-sciences/call-for-papers/cyber-security-in-the-critical-infrastructure-advances-and-f/

2.- Name:

Journal on Information Security Special Issue on Recent Advances in Cybersecurity

Acronym:

EURASIP

URL:

http://jis.eurasipjournals.com/about/update/Cybersecurity

Deadline:

20 October, 2015

Abstract Submission Procedure:

Online

Publisher:

Springer Open Journal

http://jis.eurasipjournals.com/

Date: 2015-04-13

By: Manuel Rodriguez