Advanced network security systems

Academic Year: (2019 / 2020) **Review date: 05-05-2020**

Department assigned to the subject:

Coordinating teacher: PASTRANA PORTILLO, SERGIO

Type: Electives ECTS Credits : 3.0

Year : 1 Semester : 2

REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)

Recommended, but not mandatory, to have taken a course on cryptography.

OBJECTIVES

Basic competences:
- Understand and analyze principles and methods for information and system security.
- Apply and assess network security mechanisms.
- Know trends and challenges in network security.

DESCRIPTION OF CONTENTS: PROGRAMME

1. Cyberthreats
1.1. Origins
1.2. Cyberattacks galore
1.3. A brief history of malware
1.4. Welcome to the underground economy
1.5. The cyberthreat landscape 2013-2018
1.6. Trends

2. Security in smart devices
2.1. Smart devices
2.1. Security models in current smart devices
2.2. Malware in smart devices
2.3. Threat detection and analysis
2.4. Open security problems

3. Coordinated attacks and denial of service
3.1. Coordinated attacks
3.2. Collaborative Intrusion Detection Systems
3.3. Existing classifications of CIDS
3.4. Integrated solutions for CIDS

4. Traffic analysis
4.1. Introduction
4.2. Military roots
4.3. Civil traffic analysis
4.4. Contemporary computer and communications security
4.5. Exploiting location data
4.6. Resisting traffic analysis in Internet
4.7. Data retention

5. Botnets
5.1. Introduction
5.2. Structure and functions
5.3. Detection techniques
5.4. Defense techniques
5.5. New trends/platforms
5.6. Challenges

LEARNING ACTIVITIES AND METHODOLOGY

Activities:

- Lectures
- Mandatory readings of paper assigned by the lecturer
- Debates and participative group activities

Methodology:

- Lectures using whiteboard and slide projector to develop the main concepts and discuss bibliographic references.
- Critical reading of texts recommended by the lecturer, including but not limited to: scientific papers, reports, news in press, and book chapters. This will serve as basis for further discussion in class or to extend/consolidate concepts learnt in this module.
- Solve practical cases and problems proposed by the lecturer, either individually or in small groups.
- Prepare essays and final reports, either individually or in small groups, and present them in class.

ASSESSMENT SYSTEM

(1) Attendance and participation during lectures

Constitutes 20% of the final mark and encompasses reading the papers suggested by the lecturer and participation in debates/activites.

(2) Final assignment

Each student must prepare a final assignment previously discussed with the lecturer on a topic related to the course contents. A short presentation will be also expected.

For the extraordinary exam the student will choose between two options:
a) Keep the grade obtained during the term in the continuous assessment process and sit an exam for the remaining 80% of the final grade; or
b) Sit an exam for 100% of the final grade.

% end-of-term-examination:	80
% of continuous assessment (assigments, laboratory, practicals…):	20

BASIC BIBLIOGRAPHY

- Matt Bishop Computer Security: Art & Science, Addison-Wesley Professional, 2015
- W. Stallings Cryptography and Network Security (7th Edition), Pearson, 2016

ADDITIONAL BIBLIOGRAPHY

- C. Sanders, J. Smith Applied Network Security Monitoring: Collection, Detection, and Analysis, Syngress, 2013
- Rebecca G. Bace Intrusion Detection, Sams Publishing, 2000
- Stephen Northcutt, Judy Novak Network Intrusion Detection (3rd Edition), Sams Publishing; 3 edition, 2002

BASIC ELECTRONIC RESOURCES

- Chenfeng Vincent Zhou, Christopher Leckie, Shanika Karunasekera . A survey of coordinated attacks and collaborative intrusion detection: http://dx.doi.org/10.1016/j.cose.2009.06.008
- G. Suarez-Tangil, J.E. Tapiador, P. Peris, A. Ribagorda. . Evolution, Detection and Analysis of Malware in Smart Devices: http://dx.doi.org/10.1109/SURV.2013.101613.00077
- George Danezis and Richard Clayton . Introducing Traffic Analysis: https://www.cl.cam.ac.uk/~rnc1/TAIntro-book.pdf
- Sérgio S.C. Silva, Rodrigo M.P. Silva, Raquel C.G. Pinto, Ronaldo M. Salles . Botnets: A survey: http://dx.doi.org/10.1016/j.comnet.2012.07.021