Course guides
230993 - TMA - Network Traffic Monitoring and Analysis

Last modified: 30/06/2020

Unit in charge: Barcelona School of Telecommunications Engineering
Teaching unit: 701 - DAC - Department of Computer Architecture.

Degree: MASTER'S DEGREE IN CYBERSECURITY (Syllabus 2020). (Compulsory subject).

Academic year: 2020 **ECTS Credits:** 5.0 **Languages:** English

LECTURER

Coordinating lecturer: Barlet Ros, Pere

Others: Barlet Ros, Pere

PRIOR SKILLS

Basic knowledge about computer networks

TEACHING METHODOLOGY

- Lectures
- Laboratory practical work / Project
- Group work (distance)
- Individual work (distance)
- Oral presentations
- Short answer test (Control)
- Extended answer test (Final Exam)

LEARNING OBJECTIVES OF THE SUBJECT

Learning objectives of the subject:

The objective of this subject is to study the main techniques, technologies and tools for monitoring and analyzing the network traffic, and their applications to cyber-security. The course will review the main approaches to measure the Internet (passive and active monitoring), the techniques used for identifying the traffic of applications and services (traffic classification), and methods employed for network security, such as the detection and mitigation of Distributed Denial of Service (DDoS) attacks using Machine Learning. It will also address the main technical challenges involved in network monitoring due to the ever-increasing link speeds and volume of network traffic. Finally, it will discuss about the privacy and ethical implications of measuring network traffic, as well as current regulations such as the EU General Data Protection Regulation (GDPR).

Learning results of the subject:

- Understand the technological challenges associated to network monitoring and traffic analysis as well as the required methods to address them.
- Understand and be able to apply the existing network monitoring tools and methods for traffic classification and anomaly detection.
- Understand the ethical, social and legal implications associated to network monitoring and traffic analysis as well as the mechanisms and regulations in data protection.

STUDY LOAD

Type	Hours	Percentage
Hours large group	26,0	20.80
Hours small group	13,0	10.40
Self study	86,0	68.80

Total learning time: 125 h

CONTENTS

Introduction

Description:
- Why measuring the Internet?
- Challenges of measuring the Internet
- Classification of monitoring techniques
- Active vs Passive Monitoring
- Measurement community: venues, forums, etc.
- Review of the Internet architecture

Full-or-part-time: 12h
Theory classes: 4h
Self study : 8h

Network monitoring: Methods and challenges

Description:
- Packet-level measurements: Libpcap
- Flow-level measurements: Netflow
- Algorithms and data structures: Traffic sampling, Bloom filters, Sketches
- Tools, repositories and infrastructures

Full-or-part-time: 35h
Theory classes: 7h
Laboratory classes: 4h
Self study : 24h

Network traffic classification

Description:
- Port-based methods
- Deep Packet Inspection (DPI)
- Machine learning-based methods

Full-or-part-time: 26h
Theory classes: 5h
Laboratory classes: 3h
Self study : 18h

Network security monitoring

Description:
- Anomaly detection
- Intrusion and attack detection
- Botnet and malware detection

Full-or-part-time: 26h
Theory classes: 5h
Laboratory classes: 3h
Self study : 18h

Online privacy and ethical implications

Description:
- Privacy and ethical implications of network monitoring
- Traffic anonymization
- The General Data Protection Regulation (GDPR)
- Online tracking: mechanisms, implications and defenses

Full-or-part-time: 26h
Theory classes: 5h
Laboratory classes: 3h
Self study : 18h

GRADING SYSTEM

Midterm exam: 20%
Final exam: 30%
Laboratory / Project: 40%
Presentations: 10%

EXAMINATION RULES.

Laboratory classes (project) and paper presentations are done in groups of 4 students.
At least one laptop per group is required.

BIBLIOGRAPHY

Basic:
- Sanders, C.; Smith, J. Applied network security monitoring: collection, detection, and analysis [on line]. Waltham, MA: Syngress, 2014 [Consultation: 15/07/2020]. Available on: https://www.sciencedirect.com/science/book/9780124172081. ISBN 9780124172081.
- Bejtlich, Richard. The Practice of network security monitoring: understanding incident detection and response [on line]. San Francisco: No Starch Press, 2013 [Consultation: 02/07/2020]. Available on: https://ebookcentral.proquest.com/lib/upcatalunya-ebooks/detail.action?docID=1572876. ISBN 9781593275341.
- Crovella, M.; Krishnamurthy, B. Internet measurement: infrastructure, traffic, and applications. Chichester: John Wiley & Sons, 2006. ISBN 047001461X.

Complementary:
- Bejtlich, Richard. The Tao of network security monitoring : beyond intrusion detection. Boston [etc.]: Addison-Wesley, cop. 2005. ISBN 9780321246776.
- Kurose, James F; Ross, Keith W. Computer networking : a top-down approach [on line]. 7th ed. Boston (Mass.) ; London ; Paris [etc.]: Pearson, cop. 2017 [Consultation: 23/06/2020]. Available on:

https://ebookcentral.proquest.com/lib/upcatalunya-ebooks/detail.action?docID=5187270. ISBN 9781292153599.