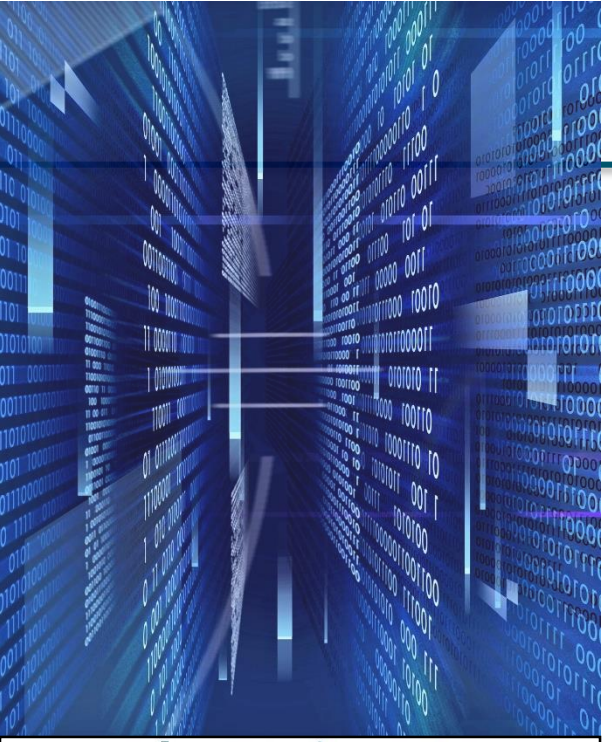


cybersecurity centre
GCHQ Academic Centre of Excellence EPSRC

Cybersecurity Southampton

Cyber Security Research Group

blog | twitter

UNIVERSITY OF Southampton

COMP6224 2019-20
Foundations of Cyber Security

Module Introduction

Week 1 – Tuesday 1st October 2019

Dr Leonardo Aniello

l.aniello@soton.ac.uk

COMP6224 2019-20 Teaching Team

UNIVERSITY OF Southampton

Leonardo Aniello
l.aniello@soton.ac.uk
Module Leader

Federico Lombardi
f.lombardi@soton.ac.uk
Lecturer

Nawfal Fadhel
n.fadhel@soton.ac.uk
Lecturer

Rob Thorburn
r.h.thorburn@soton.ac.uk
Teaching Assistant

Module Overview

UNIVERSITY OF Southampton

COMP6224 Foundations of Cyber Security

This module aims to give an overview of cyber security.

The module will equip students with a clear view of the current cyber security landscape considering not only technical measures and defences, but also the other subject areas that apply, including legal, management, crime, risk, social and human factors.

Learning Outcomes

UNIVERSITY OF Southampton

Knowledge and Understanding

Having successfully completed this module, you should be able to demonstrate knowledge and understanding of:

- A1. The importance of taking a multi-disciplinary approach to cyber security
- A2. The cyber threat landscape, both in terms of recent emergent issues and those issues which recur over time
- A3. The roles and influences of governments, commercial and other organisations, citizens and criminals in cyber security affairs
- A4. General principles and strategies that can be applied to systems to make them more robust to attack
- A5. Key factors in cyber security from different disciplinary views including computer science, management, law, criminology, and social sciences
- A6. Issues surrounding privacy, anonymity and pervasive passive monitoring
- A7. Managing security incidents, including digital forensic principles

Subject Specific Intellectual and Research Skills

Having successfully completed this module you should be able to:

- B1. Analyse case studies, to reinforce the different disciplinary perspectives of cyber security

Schedule

UNIVERSITY OF Southampton

October					November				December				January			
w1	w2	w3	w4	w5	w6	w7	w8	w9	w10	w11	w12	w13	w14	w15	w16	w17
Lectures											Christmas Vacation			Rev		
	Lab	Lab					Lab	Lab								
Tut	Tut	Tut			Tut	Tut	Tut	Tut	Tut							
		Assignment 1						Assignment 2							Exam	

- Lectures
  - Tuesday 9am
  - Wednesday 11am
  - Friday 2pm
- Tutorials: Thursday 2pm – for non-CS students
- Labs: 

Assessment

- Coursework on Password Cracking [15%]
  - Preparation Lab in week 2, start during Lab in week 3
  - Write a report
  - Deadline in week 5, feedback by week 8
- Coursework on Social Engineering [15%]
  - Preparation Lab in week 8, start during Lab in week 9
  - Write a report
  - Deadline in week 11, feedback by week 15
- Exam [70%]
  - Bookwork questions
  - Problem solving questions
  - Essay questions

Topics

1. Basic security concepts
2. Cyber Actors
3. User authentication
4. Cryptography
5. Secure communication
6. Privacy and anonymity
7. Access Control
8. Pervasive passive monitoring
9. Law aspects in cyber security
10. Social Engineering
11. Cyber Attacks and their Lifecycle
12. Corporate security
13. Cyber threat intelligence
14. Cyberwarfare and hacktivism
15. Security of Critical Infrastructures
16. Blockchain and cryptocurrencies
17. Risk Management
18. Managing security incidents
19. Digital forensic principles

Teaching/Learning Materials

- Main page: https://secure.ecs.soton.ac.uk/module/1920/COMP6224/33199/
  - Module information
  - Messages
  - Assignment submission
- Wiki: https://secure.ecs.soton.ac.uk/noteswiki/w/COMP6224-1920
  - Detailed schedule of lectures, tutorials and labs
  - Slides and links to audio recordings of sessions
  - Detailed assignment instructions
- Timetable: https://timetable.soton.ac.uk/Module/?department=5BBE9000144D2C9B4ACC35534ABD8D91&identifier=33199
- Additional resources will be referenced in the slides

Lecture Structure

- Usually, the lecturer doesn't talk for 45 minutes without interruptions
- You will be engaged in learning activities
  - Exercises in groups
  - Open discussions
  - Thought provoking questions

- Some basic guidelines
  - Feel free to ask questions during the lecture, as well as the end
  - If you feel you are lost or I'm going too fast/slow, please tell me
  - Please do not talk during the lecture
  - Please be on time

Warm-up Questions

In this module we will be looking at cyber vulnerabilities in the cyberspace, how they allow cyber attacks to succeed, and what the role of cyber security is.

- What is the cyberspace?
- What is a cyber vulnerability?
- What is a cyber attack?
- What is cyber security?

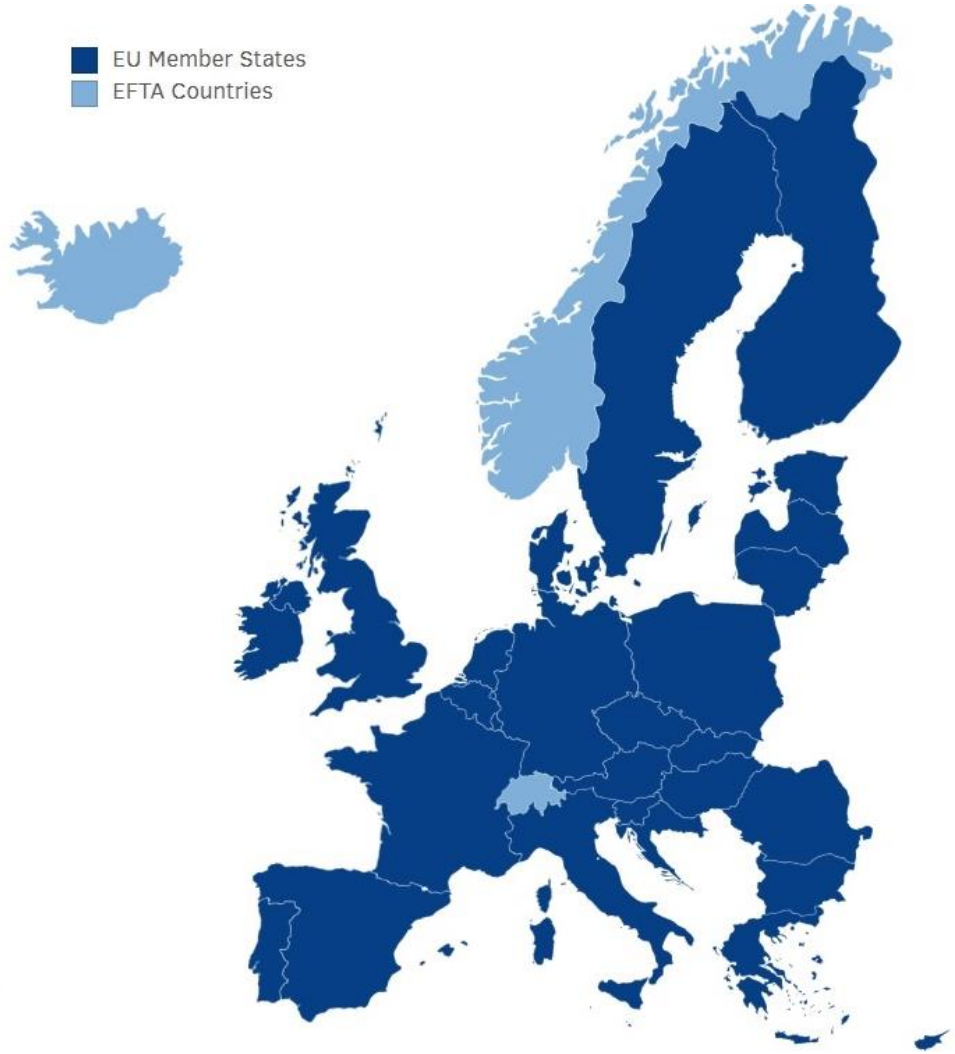
Warm-up Questions

In this module we will be looking at cyber vulnerabilities and threats in the cyberspace, how they allow cyber attacks to succeed, and what the role of cyber security is.

- What is the cyberspace?
  - Information systems (hardware, software and associated infrastructure), the data on them, and the services they provide
- What is a cyber vulnerability?
  - Weakness or loophole in the cyberspace
- What is a cyber attack?
  - Malicious attempts to damage, disrupt or gain unauthorised access to resources in the cyberspace, by exploiting one or more cyber/human vulnerabilities
- What is cyber security?
  - It refers to the protection of the cyberspace from unauthorised access, harm or misuse

The Wider Context

- ENISA: European Union Agency for Cybersecurity (https://www.enisa.europa.eu)
  - NCSS: **National Cyber Security Strategies**
    - main documents of nation states to set strategic principles, guidelines, objectives and measures to mitigate risk associated with cyber security
    - Each member state defined its own national cyber security strategy



UK National Cyber Security Strategy 2016-2021

UK National Cyber Security Strategy 2016-2021

- Objectives
  1. Address cyber crime
  2. Citizen's awareness
  3. Critical Information Infrastructure Protection
  4. Engage in international cooperation
  5. Establish a public-private partnership
  6. Establish an incident response capability
  7. Establish an institutionalised form of cooperation between public agencies
  8. Establish baseline security requirements
  9. Establish incident reporting mechanisms
  10. Foster R&D
  11. Organise cyber security exercises
  12. Strengthen training and educational programmes

The National Cyber Security Centre (NCSC)

UNIVERSITY OF Southampton

- Launched on 1 October 2016 and based in central London
- The NCSC was set up to help protect our critical services from cyber attacks, manage major incidents, and improve the underlying security of the UK Internet through technological improvement and advice to citizens and organisations
- NCSC objectives
  - Understand CS and distils this knowledge into practical guidance
  - Respond to CS incidents to reduce the harm they cause to organisations and wider UK
  - Use industry and academic expertise to nurture the UK's cyber security capability
  - Reduce risks to the UK by securing public and private sector networks

What businesses and industry can do

- Report cyber incidents
  - Action Fraud
  - NCSC
- Sharing knowledge and expertise
  - CiSP is a joint industry and government initiative set up to exchange cyber threat information in real time, in a secure, confidential and dynamic environment, increasing situational awareness and reducing the impact on UK business
- Manage risks
  - NIST 800-30, ISO 27005
- Adopt Cyber Security Guidance
  - Cyber Security Essentials
  - Guidance for SMEs
  - 10 Steps to Cyber Security

What Academia can do

- Academic Centres of Excellence in Cyber Security Research
  - 14 universities have been accredited. Southampton is one of them!!

- Certified Master Degrees
  - MSc in Cyber Security
  - MEng in Computer Science with Cyber Security

- Doctoral studentships

What citizens can do

- Britons urged to take cyber security as seriously as home security

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Cats from https://business.currys.co.uk

Recap

- Don’t panic about labs!
- For non-CS students: attend tutorials!

- Cyber security is about protecting the cyberspace from cyber attacks

- Protecting the cyberspace requires a nation-wide strategy to cyber security and collaboration from government, industry, academia and individual citizens.

Resources

- UK National Cyber Security Strategy 2016-2021 https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021
- National Cyber Security Centre https://www.ncsc.gov.uk
- ActionFraud https://www.actionfraud.police.uk/