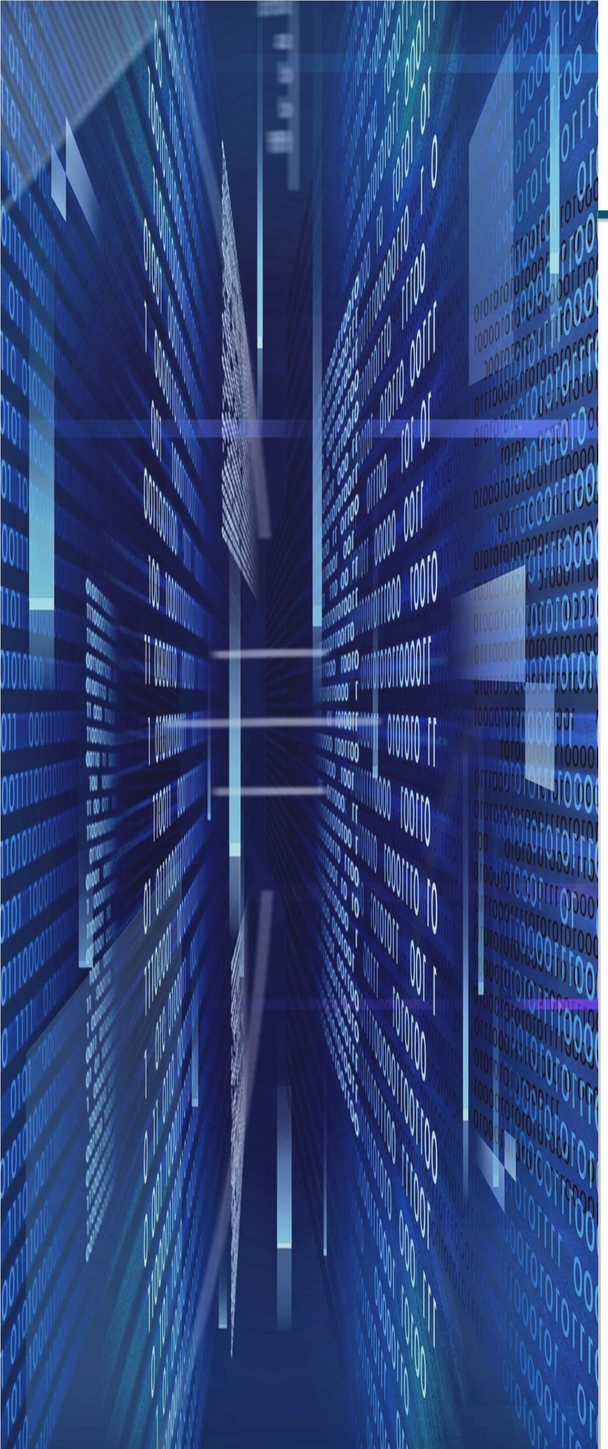
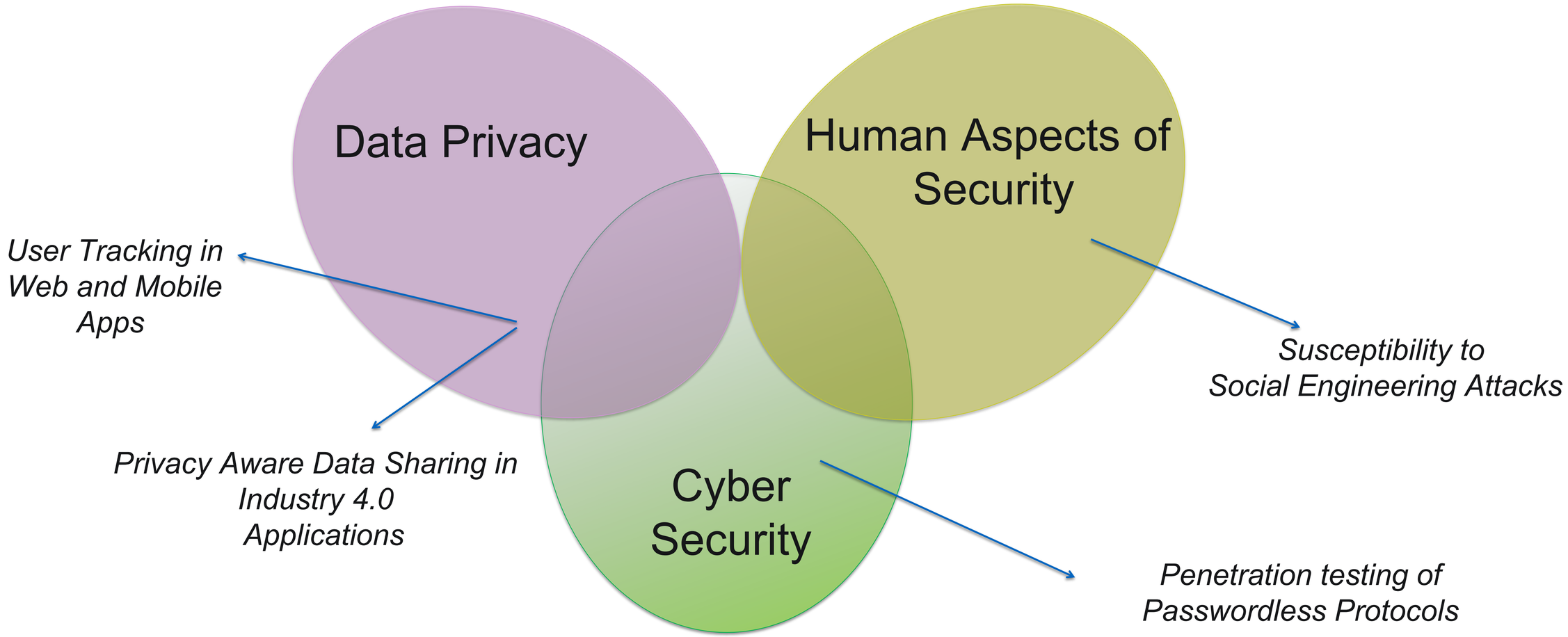


# Cyber security and data protection
# Course Organization

Prof. Federica Paci

# My research


Data Privacy
Human Aspects of Security
Cyber Security
User Tracking in Web and Mobile Apps
Privacy Aware Data Sharing in Industry 4.0 Applications
Susceptibility to Social Engineering Attacks
Penetration testing of Passwordless Protocols

# Learning outcomes

- This course aims to give an overview of **cyber security**. The course will equip students with a clear view of the current cyber security landscape considering not only technical measures and defenses, but also the other subject areas that apply, including legal, management, crime, risk, social and human factors.
- At the end of the course, students will have the necessary knowledge and understanding of:
  - the importance of taking a multi-disciplinary approach to cyber security,
  - the cyber threat landscape, both in terms of recent emergent issues and those issues which recur over time,
  - general principles and strategies that can be applied to systems to make them more robust to attack,
  - and issues surrounding privacy, anonymity and pervasive passive monitoring

# Syllabus

- Cybersecurity and cyber security concepts
- MITRE ATT&ck, Cyberkill chain
- Cyber threat actors, Threat landscape
- Malware and Ransomware Attacks
- Social Engineering Attacks
- Cyberwar and Attacks to Critical Infrastructures
- User Authentication
- Digital Identity Management
- Access Control Models and Mechanism
- Cyber risk management
- NIST Framework, Cyber essentials

- Introduction to Privacy: notions of privacy, privacy threats
- Database privacy: anonymization techniques, differential privacy
- Data protection regulations

# Lectures

- 2 hour on Monday from 13:30 to 15:30
- 3 hours on Friday from 14:30 to 17:30
- Frontal lecture in the classroom
  - The slides will be made available the day before the lecture

# Guest Lectures from Industry

- 25/10/ 2023 Mazars Italia on Social Engineering Attacks
- 4/12/2023 Unicredit on Infrastructure Security
- 11/12/2023 V-Research on Cyber risk assessment

# Labs

- 5 laboratory activities on:
  - Threat intelligence: analysis of a cyber attack's techniques using MITRE ATT&ck matrix
    - Computer
  - Reconnaissance, Exploitation, and Defense Evasion techniques
    - Kali Linux VM and Metasploitable VM
  - Social Engineering Attacks
    - Kali Linux VM and Windows 10 VM
  - Password Attacks
    - Kali Linux VM and Metasploitable VM
  - Persistance and Post-Exploitation techniques
    - Kali Linux VM, Metasploitable VM and Windows 10 VM

# Exam

- Students will be evaluated based on
  - A practical or theoretical project
  - An oral examination on any of the topics taught in the course
- The projects will elaborate on topics taught in the course.
- The project must be done in a group of a maximum of 2 students.
- The students must prepare a written report to present the results of the project.
- During the oral examination, the students will present the project to the teacher, who will ask questions about the project and any of the topics taught during the course.
- At the end of the oral exam, the teacher will propose a final mark.
- The date of the oral examination must be agreed with the teacher during the exam session.

# Practical Project 1

- The goal of this project is to implement a malicious Word document
- The document must include a VBA macro VBA that executes a Powershell command
- The Powershell command must download from differen C2 servers a malware, save the malware on a Windows machine, and execute it.
- The VBA macro code must be obfuscated and the Powershell command must be base 64  encoded.

# Practical Project 2

- The objective of this project is to implement an infostealer for Windows OS.
- The malware must implement the following attack techniques from MITRE Att&ck matrix:
  - Persistence - Create or Modify System Process: Windows Service [T1543.003].
  - Defense Evasion - Impair Defenses ID[T1562.001]
  - Exfiltration - Exfiltrate Data Through Cloud Account -T1537.

# Practical Project 3

- The objective of this project is to analyze the compliance of web sites' privacy policies with the transparency principle imposed by GDPR (articles 12 and 13)

- You will have to analyze the privacy policies of 30 web sites provided by the teacher based on an analysis template that focus on the following aspects of the policies:
  - Content of the policy (article 13)
  - Accessibility (article  12)
  - Clear and plain language (article 12)
  - Policy interface (article12)

# Practical Project 4

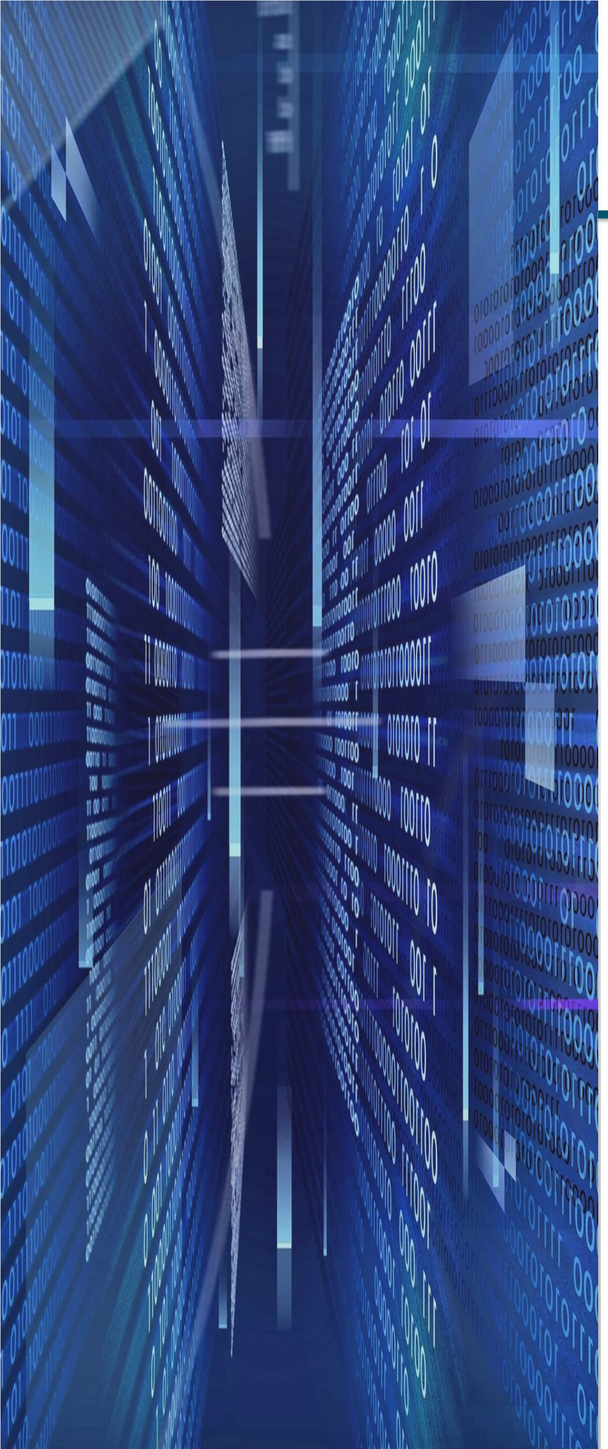
- The objective of this project is to analyze the compliance of websites with the right of access (article 15 of GDPR)

- You will have to analyze the process of requesting access to users' personal data implemented by of 30 websites provided by the teacher based on an analysis template that focuses on the following aspects of access request and response:
  - Requesting access interface
  - Type of user identification
  - Type of response
  - Content of the response
  - Time to return the response
  - Accuracy and format of the returned copy of the data

# How to communicate with me

- **Email:** federicamariafrancesca.paci@univr.it

- **Office hours:** Monday from 15:30 to 17:30
  - Please take appointment via email



# Cyber security and data protection

Prof.Federica Paci

# Lecture Outline

- What is cyber security?
- Key cyber security properties
- Key cyber security concepts

# Learning outcomes

At the end of this session, you should be able to:

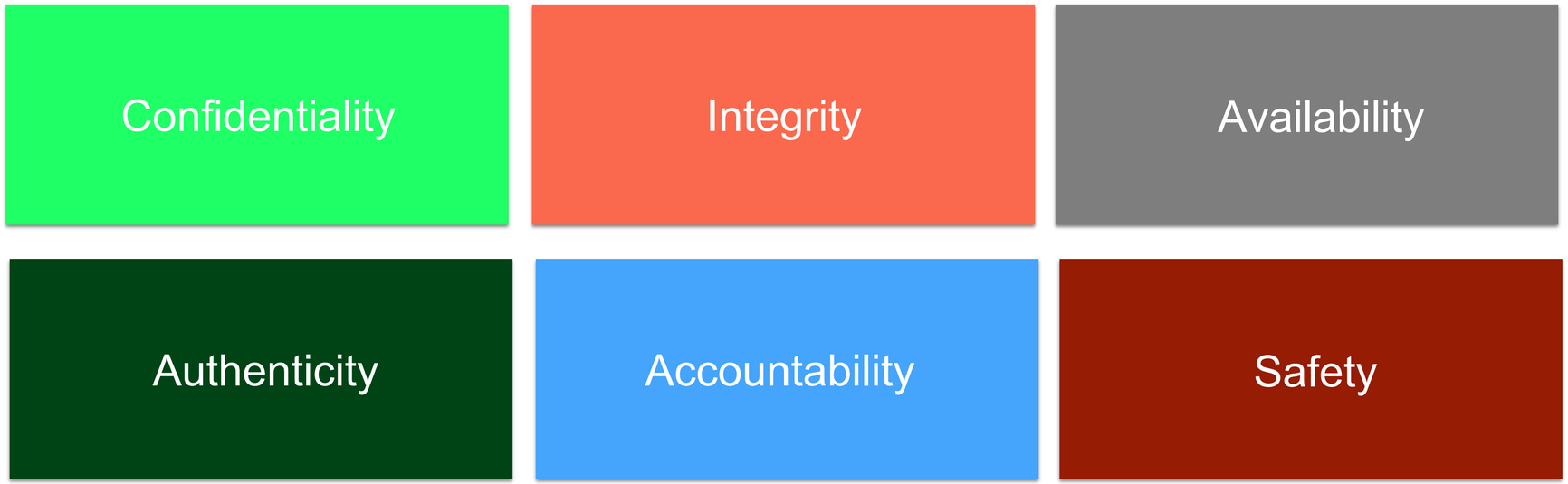
- Define what is cyber security
- Explain key cyber security concepts

# What is cyber security?

Cyber security's core function is to protect the devices we all use (smartphones, laptops, tablets and computers), and the services we access - both online and at work - from unauthorized access, harm or misuse.

It's also about preventing unauthorized access to the vast amounts of personal information we store on these devices, and online

# Elements of Cyber Security



# Cyber security key concepts

## Assets

- Anything that has value to an organization, including, but not limited to, another organization, person, computing device, information technology (IT) system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards).

# Cyber security key concepts

## Vulnerability

- a bug, flaw, weakness, or exposure of an application, system, device, or service that could lead to a failure of confidentiality, integrity, or availability

## Cyber Threat

- any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service

## Attack

- The realization of some specific threat that impacts the confidentiality, integrity, accountability, or availability of a computational resource.

# Cyber security key concepts

**Threat Actor** (synonyms attacker, threat source, threat agent)

- person (or group) seeking to exploit potential vulnerabilities of a system

**Risk**

- the level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.

**Security controls (synonyms safeguards or countermeasures)**

- the management, operational, and technical controls prescribed for a system to protect the confidentiality, integrity, and availability of the system, its components, processes, and data.

# References

NIST Glossary. Available at https://csrc.nist.gov/glossary/