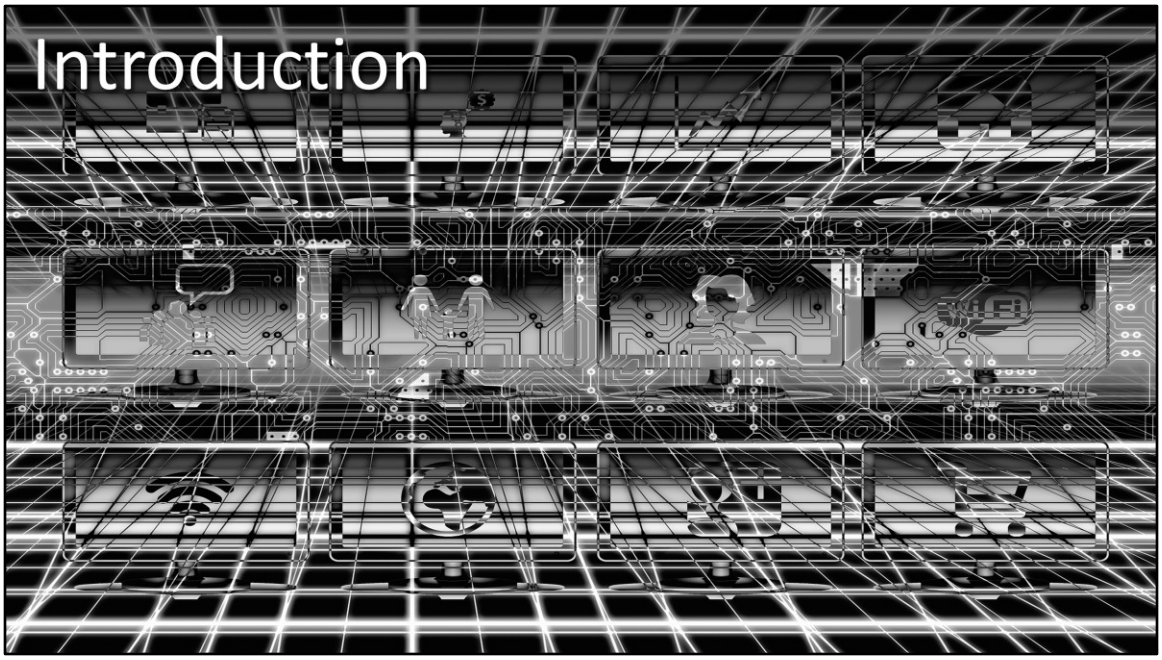
UNIVERSITAT POLITÈCNICA DE VALÈNCIA

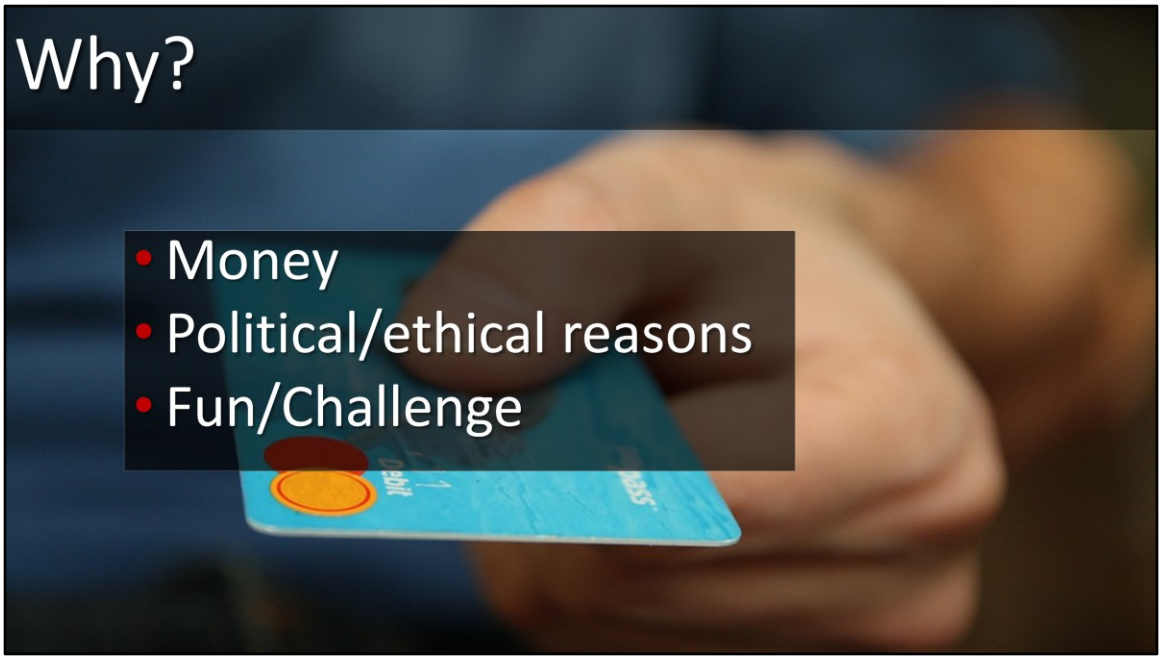
Privacy, security and intellectual property

Computer threats-Hackers

Introduction



In this unit we are going to talk about the threats an IT system faces. We will see why the IT systems are attacked, who attacks them and how they do it.



The first question we are going to answer is why IT systems are attacked.
Nowadays IT systems are involved in many aspects of our lives, and some of these are critical for the smooth functioning of our societies. This means that misusing or disrupting IT systems can have huge potential for making illicit profits or for disturbing the normal functioning of a society.

There are three main reasons for cybercrime:

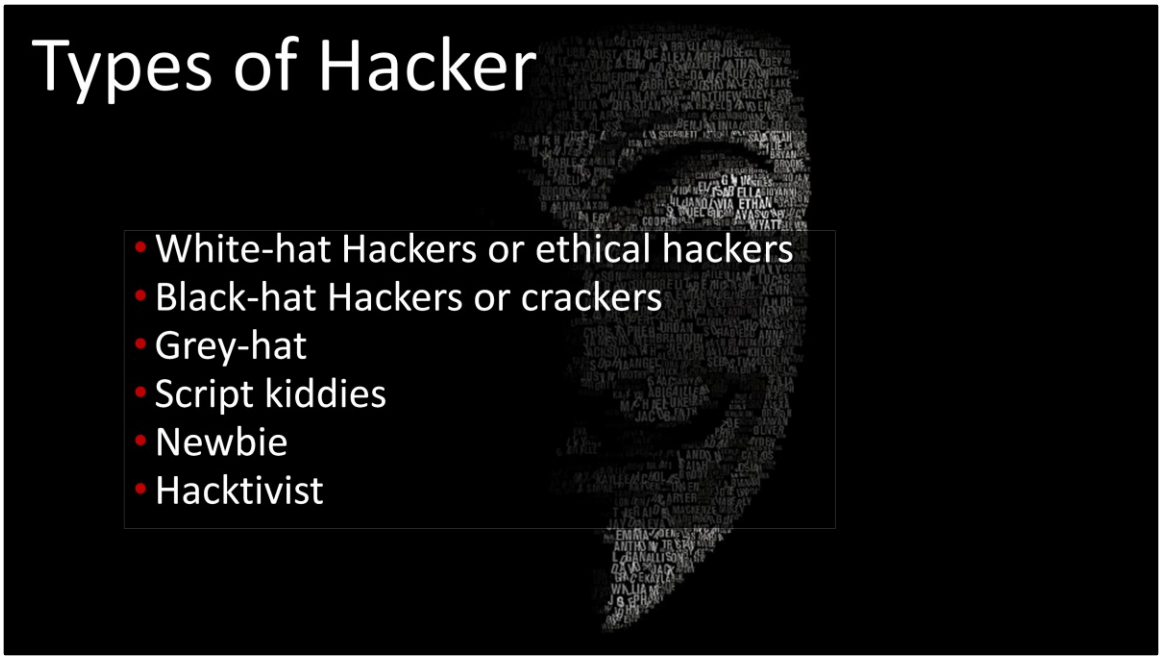
•The first and most important reason is money. In 2014, for example, US companies suffered a loss of more than 800 million US dollars. Identity theft and fraud, stealing trade secrets, extortion, blackmail and other forms of cybercrime can be very lucrative.
•The second are political reasons. Information Systems can be attacked either to disclose some information for ethical reasons, as in the Wikileaks case, to spread a message, to cause political disruption, or even for terrorism, as they manage very critical systems. One example is the Stuxnet computer worm that targeted the Siemens industrial control systems and damaged Iran's uranium enrichment infrastructure.
•And the last one is simply the joy of challenge, the fun of defeating systems created by others.

When speaking about security attacks most people immediately think of an individual sitting in front of his or her computer in a dark room, and the word ‘hacker’ comes to mind. In most cases this is no longer true, as there are big organized criminal groups making huge profits from cybercrime.

‘Hacker’ is a word with several meanings. In computer security, a hacker is someone who focuses on security mechanisms of computer and network systems. It includes those who work strengthening such mechanisms, but it is more often used by the mass media and popular culture to refer to those who seek access despite these security measures. In fact, there is a long standing controversy over how to define the word ‘hacker’. Some computer programmers argue that a person who breaks into computers should be called crackers.

Hackers may be motivated by a multitude of reasons, such as profit, protest, challenge, enjoyment, or their job may involve evaluating network weaknesses to assist in removing them. Most of them operate under a codename.

The term bears strong connotations that are favorable or pejorative, depending on the context.



When using the word 'hacker' to refer to those who break into Information Technology systems without authorization, we should differentiate between several types:

White-hat hackers or ethical hackers They break security for non-malicious reasons. They usually work for the owner of the system trying to find system vulnerabilities.

Black-hat hackers They break into secure networks to destroy, modify, or steal data; and to gain control of them for non-intended uses. Black hat hackers are also referred to as "crackers" within the security industry and by modern programmers. They can work for organized cybercrime gangs or for national intelligence agencies.

Grey-hat A grey hat hacker lies between a black hat and a white hat hacker. A grey hat hacker may surf the Internet and hack into a computer system for the sole purpose of notifying the administrator that their system has a security defect. Even though grey hat hackers may not necessarily perform hacking for their personal gain, unauthorized access to a system can be considered illegal and unethical.

Script kiddies A script kiddie (also known as a skid or skiddie) is an unskilled hacker who breaks into computer systems by using automated tools written by others, frequently scripts created by black-hat hackers, hence the term script. They usually have little understanding of the underlying concept.

Newbie or Neophyte is someone who is new to hacking and has almost no knowledge or experience of the workings of technology and hacking.

Hacktivist A hacktivist is a hacker who utilizes technology to publicize a social, ideological, religious or political message. Hacktivism can be divided into two main groups:

- Cyberterrorism — Activities involving website defacement or denial-of-service attacks; and,
- Freedom of information — Making information that is not public accessible to the public for ethical reasons.

Attribution:

The sources of some of these figures and text are :

- Slide 2 https://pixabay.com/es/equipo-internet-tecnolog%C3%ADa-datos-475555/
- Slide 3 https://pixabay.com/en/money-card-business-credit-card-256319/
- Slide 4 https://pixabay.com/en/binary-binary-code-binary-system-823336/
- Slide 5 https://pixabay.com/en/hack-hacker-elite-hacking-exploits-813290/
- https://en.wikipedia.org/wiki/Hacker_(computer_security)
- http://www.statista.com/markets/424/topic/1065/cyber-crime/