Computer Security (CM2025)

Course Notes

Felipe Balbi

October 12, 2020

Contents

Week 1

Key Concepts

- Understand the central goals and aspects of computer security.
- Understand and explain the differences between a range of malware types.
- Identify key examples of malware and their historical significance.

Reading: Ethics in information security

Read the following article:

Ethics in information security, IEEE Security & Privacy, vol.15 May/June 2017, pp.3–4.

You should also familiarise yourselves with the ACM ethics guidelines.

Defining computer security

With the advent of the Internet, computer security became a very important field of research.

Computer Security is the *protection of computer-related assets against danger, loss or loss of control of something valuable.*

Security has three main goals:

Prevention The safeguarding of assets from threats;

Detection Systems that alert if malicious activity is, or is about to, take place;

Reactiion Definition of procedures that enables us to deal with an attack.

Security can also be split into three main components:

Policy deals with confidentiality, integrity and availability of data;

Threat Model assumptions about those involved with malicious activity;

Mechanism The SW/HW used to make sure the policies are enforced using the assumptions made during Threat Modelling.

There are five important terms that need to be defined:

Attack activities harmful to computer systems, data, software, and hardware;

Risk the possibility of damage or loss of digital assets in case of an attack;

Zero-day (vulnerability) a vulnerability used by an attacker before its discovery by the developer of the SW;

Exploit SW used to take advantage of a bug or vulnerability;

Hacker Subdivided into three groups

- **White Hats** Find vulnerabilities with a goal of fixing them before its discovery by an attacker. They work under the permission of the owner of the computer system being attacked;
- **Black Hats** Try to penetrate the system to gain unauthorized access. Often, their motivation is harm operations or steal sensitive operations;
- **Gray Hats** They fall somewhere in-between White Hats and Black Hats and work with varying combinations of good and bad intentions.

Types of malicious software 1

Malware is a piece of softwarte designed to disrupt, damange and destroy an information system. There are many types of malwares, some of which are discussed in the following subsections

Viruses

They self-replicate by inserting themselves into other files, programs, documents, etc. Can spread through emails, USB sticks and downloads from unknown sources.

The *Creeper* is considered to be one of the first computer viruses. Developed in 1971, it infected computers connected to the ARPANET, the internet prototype.

Another early virus was the *Elk Cloner*. Written by a high-school student to infect Apple II computers using floppy disks in 1982. Every 50th time the computer booted, it would display a poem written by the hacker.

Not all viruses are harmless. The *I Love You* virus in 2000 caused around $10 billion worth of damages by affecting nearly 10% of all computers around the globe.

Worms

They can replicate without attaching themselves to existing software. The *Stuxnet* is a well-known worm, considered to be one of the most destructive worms ever created. It was designed to attack Programmable Logic Controllers by Siemes.

PLC devices are used for the automation of processes in machinery. In this case, it targetted centrifuges in Iranian nuclear power plants and altered the speed of the machine, causing it to tear itself apart.

It's estimated that *Stuxnet* destroyed 20% of Iranian's nuclear power plant centrifuges.

Adware

These display advertisements on your screen during browsing or online shopping. Possibly the most visible form of malware one can encounter. Its main purpose is to collect user data.

Trojans

Trojans are named after the famous ancient Greek tale of the invasion of the city of Troy by the Greek during the Trojan War.

After trying and failing several times to get access to the city, the Greeks came up witha plan where squatter soldiers would hide in the joint wooden status of a horse presented as a gift.

During the night, after entiring the city within the horse, the Greeks broke out of the horse to attack the city.

Trojans have a similar way of working: they hide themselves inside an application or program data and spread based on specific user action.

Spyware

Designed to spy on the target machine or the user, it collects information and sends it back to the hacker for further use or for sale on the dark web.

The *Dark Hotel* spyware is one famous case which used Hotel Wi-Fi to target the personal systems of government officials, business tycoons and political leaders to extract sensitive information.

Types of malicious software 2