VÍDEO intypedia004en

LESSON 4: INTRODUCTION TO NETWORK SECURITY

AUTHOR: Justo Carracedo Gallardo

Technical University of Madrid, Spain

BOB

Hello friends, welcome to Intypedia. During the past weeks I have been studying a very interesting topic: security in computer networks, a complex subject with many nuances that affects a great number of users and companies. In this lesson, Alice and I will immerse ourselves in this fascinating subject. Please, join us!

SCENE 1: COMPUTER NETWORKS. DEFINITIONS

ALICE

For many years, mankind has overcome time and space obstacles by creating communication mechanisms of great precision. In today's 21st century world, the use of mobile telephones and the Internet are clear examples of these achievements. But the end user isn't always aware of the complexity of these technologies and the inconveniences that may arise from an inappropriate use...

To understand these technologies it is important to have a basic knowledge of the workings of telecommunication networks and, in this specific case, computer networks and how they communicate.

BOB

A computer network is basically a group of systems interconnected by a medium that transmits data --for example, cables the transmit signals or waves that travel through the air-- allowing information, resources and services to be shared, in order to provide an added value to the final entities that use them.

ALICE

Advanced students would ask themselves how the computer networks operate, wouldn't they?

BOB

Yes, Alice. The initial answer can be found in the existence of network protocols. A protocol is a strict group of rules that defines the syntax and the semantics of communication. In other words, it defines what can and cannot be done in that communication. Interconnection elements --like routers, for example-- are needed to connect the systems and for the correct functioning of the network protocols.

Thanks to all of this, Internet can exist; a worldwide communications network formed by the interconnection of thousands of networks, and, therefore, the interconnection of millions of computers.

ALICE

I have a question... Is it necessary to know all those protocols to communicate through a computer network?

BOB

When it comes to technology, the best thing is to exclude the end user from the technological complexities. For example, essential elements needed for reading e-mails or surfing the Internet like the TCP/IP or the DNS protocols, don't have to be known in depth by the end users.

It is very common, nowadays, to hear about information systems and ICT; Information and Communications Technologies that allow the use and transmission of great amounts of data to cover a specific need. Luckily, a great part of this complexity is hidden to the end user. Nevertheless, the use of information systems implies a number of risks that have to be taken into account, many of which derive from the lack of knowledge by the end user of the technology.

We will now go on to analyse this matter in detail.

SCENE 2: RISKS AND PROTECTION OF COMPUTER NETWORKS

BOB

Computer networks are used for communication between individual people as well as for communication in business, banking, government, military, administrations and other entities. Great amounts of information --often sensitive information-- travels through these networks, so there is a real risk that non-authorized people may try to access this information illegally.

ALICE

But cryptography solves that problem, doesn't it? As far as I know, cryptography is the base for many secure network protocols that protect information.

BOB

Well, let's see, Alice. Computer networks present many vulnerabilities, so they need protection. In this way, the definition of network security is "the group of techniques that try to minimize the vulnerability of the systems or the problems derived from processing the information contained within." The aim is to make it more expensive to break security measures than the value of what is being protected.

Security mechanisms are designed with this idea in mind and are used to build secure protocols able to provide security services. In other words, security mechanisms are the "shields" that protect the communication between users against the attacks, thanks to security services.

Security mechanisms are mainly based on cryptographic techniques, which are, therefore, the foundations of security services. As you can see, security services are more than just a specific cryptographic technique.

The seven most significant security services are: entity authentication, data confidentiality, data integrity, access control, non-repudiation, availability and anonymity.

The definition of security services is very important because there are many attacks to minimize. The most common ones being: attacks to the identity of entities (interception and impersonation), attacks to information (revelation, forwarding, manipulation and data repudiation) and attacks to services (denial of service and appropriation).

ALICE

I have a question regarding the attacks to services: why would anyone be interested in interrupting the access to a service or taking it over, like for example, taking control over an end user's computer?

BOB

That is very easy to explain. Today it is as important to protect the information as it is to protect the systems and services that allow them to access the information.

Attackers now try to compromise computers because they can be used for many things, like hiding the track of illegal activities, sending non-wanted e-mails --SPAM for example-- or using their connection to the Internet to send massive requests to try and saturate Internet services --for example to make a website crash. These attacks are called DoS (denial of service).

It is common to speak about the creation of botnets. A botnet is a network of compromised computers --usually controlled by one or more persons using a control panel-- that benefits from the computational capacity and the Internet connection of these computers to carry out illegal activities like the ones mentioned previously. There is usually an important economic component in these types of attacks, so organized crime has professionalized in this area.

In addition to this, there are computers and networks that manage information and processes which are very important for a country. Examples of this are the networks that manage critical infrastructures like power stations, dams, transports, etcetera. As you can imagine, the malfunction of these infrastructures would cause serious consequences.

In future lessons we will see in detail this complex topic, known as Critical Infrastructure Protection.

SCENE 3: LEARNING ABOUT YOUR ENEMY

ALICE

I've had an idea. If we knew more about the attackers, we could create network protocols that are more secure.

BOB

Exactly. That's what researchers have been focusing on during the past years due to an increase of professionalized attacks to computer networks. Some solutions, such as honeynets or honeypots, are an example of this awareness.

When it comes to define the danger levels of an attacker, you've probably heard of the terms "hacker" or "cracker" before.

ALICE

Sure... And as far as I know, a hacker is someone who enjoys learning about computer systems and networks, getting access to them without permission to do so, in order to show off his or her skills. But a cracker's attack implies turning upside down the security measures of a computer system or network to obtain some type of benefit, usually a financial gain.

BOB

Well... that is a good start. In the information technologies industry it is common to tag everything, sometimes incorrectly. The truth is that there are people with great knowledge of the protocols and technologies sustaining computer networks. Sometimes, this knowledge, along with hard work and skills, allows these people to discover bugs that can push technology forward, but other times it is used to fulfil economic, moral, political or military interests. To be fair, attackers can't be classified just as good or bad; there is a lot of grey area.

ALICE

Are there other ways to classify the attackers?

BOB

Several, in fact... An interesting classification is to group attackers by their knowledge instead of their final interests or consequences in the system. According to this classification, we can find attackers that try to maximise the results with the minimum effort. The security measures that will be explained in upcoming lessons are useful to avoid or minimise these attacks.

Other types of attackers, the most dangerous ones, are those who aim at a specific target. In these cases, not only technical knowledge is important, but also the time and money invested by both parties to protect and attack the system or network.

Today it is fairly common for attackers to aim at corporations' systems and for the attacks to use in-house employees, since they have a good knowledge of the communication infrastructure.

ALICE

That's very interesting... But I suppose a company or a person can't invest all their money to protect its computers and networks, right?

BOB

Certainly. Your question leads us to another topic: risk management. The investment in security has to be proportional to the value of the assets or the information that is being protected. Clear rules for action have to be set in order to analyse potential threats, the impact of an attack, etcetera. We will cover this subject in future lessons.

SCENE 4: PROTECTING YOUR NETWORK

ALICE

Based on what I've seen, it isn't easy to protect a computer network and the information it contains.

BOB

That's the idea. An administrator should protect and take care of all the points subject to an attack because an attacker can take advantage of one single non-protected point to perform an attack and continue privilege escalation in the network or the computer to achieve his objective.

Complete security doesn't exist, since there will always be a way to break a security measure. Nevertheless, we mustn't forget that today's digital security measures offer a much higher protection than the ones used in the real world, for example when sharing paper documents.

ALICE

It is said that, when talking about computer security, humans are the weakest link... So, I can imagine where the attacks focus on.

BOB

You're right. Usually, the easiest way to enter a computer network, steal information or fake an identity is manipulating, misleading or coercing people. This is related with what is known as "social engineering", which consists of manipulating people into performing actions for your gain.

The solution to this problem is teaching computer security awareness and establishing clear security policies, for example to prevent a user from telling a system's password to a stranger on the telephone.

In future lessons we will talk about public key certificates and existing security infrastructures based on trusted security authorities. These help users to protect themselves against the many risks and attacks that may take place within the computer networks.

We will also have time to analyse the different types of attacks in greater depth and new concepts such as firewalls, IDS, logs, sniffers and more.

But that will have to be another day.

BOB

Bye and take care out there!

ALICE

See you!

Script adapted from original. Dr. Justo Carracedo Gallardo. Technical University of Madrid. Madrid, Spain, February 2011

http://www.intypedia.com

http://twitter.com/intypedia