1/3/2022

IO 6: WEBLAB TUTORIAL OF TECHNICAL DESIGN AND IMPLEMENTATION – SECURITY AND COMMUNICATIONS

Co-funded by
the European Union

1. INTRODUCTION

Lab equipment and resources that get exposed to the world through the internet as WebLabs, automatically become vulnerable and may be attacked and/or accessed by malicious users. Therefore, while this issue is usually not taken too seriously by those groups and universities that develop and use WebLabs, it is actually one of the most critical points that need to be addressed. In this sense, the communication channels, protocols and architecture selected to offer the lab services online is of the utmost importance, as it immediately affects the level of security.

This document reviews some of the most typical security threats and the solutions for communications in order to tackle with such risks.

2. COMMON SECURITTY THREATS IN WEBLABS

The following are the most common sources of threats related to WebLabs, and the risks associated to them:

- Equipment (cameras, computers, switches, etc.) use public IPs. When the lab devices use public IPs, they are visible and reachable to anyone. While this is a very handful solution for exposing the lab services and making them accessible, it also carries a huge risk, as any user or bot is able to try to access such devices.
- WebLab services do not use an authentication system. Sometimes, WebLabs are left open, so anyone can access to it. This may be done either by design or by mistake, but in both cases, malicious users may take control of the lab and make a bad use of it, potentially harming the equipment, monopolize it and prevent others from using it or simply, access to cameras that shouldn't be available to everyone at any time.
- Services are not running over HTTPs. Even when an authentication mechanism is in place, if such mechanism does not rely on HTTPs, security is at risk due to the use of unencrypted transport of the credentials. Many WebLab webpages and services still run on HTTP instead of HTTPs, which is far from being ideal.
- Access given to users include full access to the Operating System (OS). Sometimes, WebLabs are based on remote desktop type of connections. When this is the case, the person accessing the WebLab has access to the whole OS. Even if the user in the WebLab computer has limited privileges, which is not always the case, this also poses a great hazard, as users may, for example, send phishing or spam e-mails from remote addresses. Not only that, students sharing the same user in the lab computer may also find files with lab data and results obtained by other students who previously entered the computer, whether these were left there on purpose or accidentally.

The basic recommendations to avoid the above issues are:

- Use private IPs within a VLAN/VPN that is protected and allows you to control who may access which resources within the private network.
- Always use some type of authentication system at the communications protocol level. Using authentication for accessing a webpage is not enough, as users may be able to access the webpage at some point, load a web app and keep it open and running if not security is implemented at the communications protocol level. Such users may even download the app and keep using it whenever they want, without having to log in and authenticate in the webpage never again.
- Always install an SSL certificate to enable the use of HTTPs and encrypted communications.
- Either use a web app that communicates with the WebLab services in a limited way (like the documents 2a, 2b and 3 show) or, if a remote desktop type of access is used: 1) do it through a user in the machine that has been prepared to have very limited privileges and 2), limit the visual access to the remote computer so that only the desktop application that controls the lab equipment is displayed and can be accessed.