2023-10-25

Security Policy for the CS2Lab and the "Virtual Sandbox"

In the following, "CS2Lab" refers to the room marked "säklabb" on the 2nd floor of the NOD building, and also to the "Virtual Sandbox" i.e. any virtual computers and networked environments specifically designed to mirror the functionality and purpose of that laboratory. The term "CS2Lab staff" refers to the DSV designated S*äklabb* laboratory coordinator, department employed CS2Lab laboratory assistants and members of the DSV teaching staff who are directly involved in the running of such experiments as the student conducts within the confines of CS2Lab.

The CS2Lab laboratory is for the benefit of students studying on IT security courses at the Dept. of Computer and Systems Sciences (DSV) at Stockholm University. Apart from making specialised tools and software available, the laboratory is an environment wherein students may test some of the kinds of systems, tools and practices that would otherwise be prohibited, for security reasons, in normal network environments. This policy is to be applied at all times when activities that are potentially harmful to others, or can contravene the Network Security Policy of Stockholm University, are conducted within the CS2Lab, or with the aid of its laboratory equipment. When laboratory work that has the potential to be harmful is scheduled by CS2Lab staff, the lab is said to be running in "Sandbox mode" and no laboratory work may be conducted by any persons who do not adhere to this policy.

Wireless networks are not considered to be a part of CS2Lab and are therefore not covered by this policy. It should therefore be clear that the DSV department will not sanction the use of wireless networks for security for security experiments unless that use is clearly in accordance to University rules and Swedish law. Specific student experiments with wireless networks may be explicitly sanctioned by the CS2Lab staff and in such cases the security requirements for such experiments, including whether they should be assumed to be covered by this policy, must be agreed on for each individual experiment.

The Network Security Policy of Stockholm University

Stockholm University sets out rules for students use of IT resources. See:
https://www.su.se/polopoly_fs/1.217168.1420795768!/menu/standard/file/
Regulations%20for%20students%20and%20alumni%20information%20mgmt%20resources.pdf.
The student must be fully conversant with all the University rules, in particular those above that control what activities may be conducted within the CS2Lab, and the student shall strictly adhere to those rules.

With respect to the University rule - *It is not permitted to hide one's identity when using information management resources (such as Internet and email)* – When working in the CS2Lab some exercises may require elements of so-called spoofing attacks. When executing such exercises the student must be sure, and ensure, that the effects of the exercise cannot propagate beyond the CS2Lab environment. Some experiments may involve the use of anonymising software where the effects necessarily will extend beyond the CS2Lab network, into the University network and beyond. In all such cases the students running such experiments must consult with CS2Lab staff a minimum of 48 hours before the experiment is expected to take place, and clearly specify the duration of the experiment. Only with explicit CS2Lab staff approval may any such experiments take place.

With respect to the University rule - *It is not permitted to exploit incorrect configurations, software bugs, or other methods in order to gain additional access or other privileges*. - When executing laboratory exercises that may have elements of such exploits the student must be sure, and ensure, that the effects of the exercise cannot propagate beyond the CS2Lab environment.

Whenever the student is in doubt about the scope of effects that any experiment may have, they may not conduct the experiment without first consulting CS2Lab staff.

Special Restrictions and Responsibilities Applied to the CS2Lab

Physical Access to the CS2Lab

Only students who are reading IT security courses at DSV or otherwise have been given special permission from DSV staff are allowed access to CS2Lab. It is the student's responsibility to ensure that no person who does not have legitimate access privileges (i.e., who does not have key-card access to the physical laboratory or permission to use any associated virtual network) can gain entry to the facilities by enabling them to pass the doors or through careless handling of login credentials.

Restrictions Regarding Effects on Other Parties

The CS2Lab and its resources may only be used for educational purposes and no potentially harmful activities may be directed towards computers other than those within the CS2Lab network, and then only with the explicit prior consent of other users who are the target of such activities.

2023-10-25

Security Incidents

In all laboratory activities students shall take reasonable measures to ensure that no breaches of this policy can occur through careless use of software tools irrespective of whether they are provided on the course or obtained from exterior sources.

Any student that is the cause of, or witness to, incidents that could in any way be suspected of being a breach of this policy, Stockholm University rules, or Swedish law, shall report said incident immediately to the laboratory assistants, to the involved course staff, or to DSV's system personnel (DMC).

Protection of Personal Data

On occasion, when working within the CS2Lab laboratory or Virtual Sandbox, there will be opportunities to eavesdrop information such as network traffic and keystrokes made on other computers. For this reason, students should be vigilant, exercise discretion and even avoid communicating secret information, including passwords used for normal networked services, at any time that this information could be eavesdropped. Consequently, neither should students save passwords on any computer when, for example, a web browser offers the opportunity to do so. This might otherwise invite others to discover and misuse such information.

Students who fail to uphold the terms of this policy will forfeit the privilege of access to the CS2Lab and the Virtual Sandbox. No special provisions will be made in case such forfeiture implies that students will be unable to complete assignments necessary for the completion of their Stockholm University education.