DEI
DEPARTAMENTO
DE ENGENHARIA INFORMÁTICA
TÉCNICO LISBOA

2019/20

NETWORK AND COMPUTER SECURITY (SIRS)
PROJECT OVERVIEW

PUBLICATION DATE: 2019-10-10

LATEST REVISION: 2019-10-10

This document describes the organization of the project for the Network and Computer Security / Segurança Informática em Redes e Sistemas (SIRS) course.

For any questions regarding this document, please contact:

meic-sirs@disciplinas.tecnico.ulisboa.pt

1 INTRODUCTION

The SIRS (Network and Computer Security) course requires a practical project dealing with security solutions. This whole process is organized in 10 sequential stages, as shown in following figure. The document concludes with a summary table, with all the deadlines.

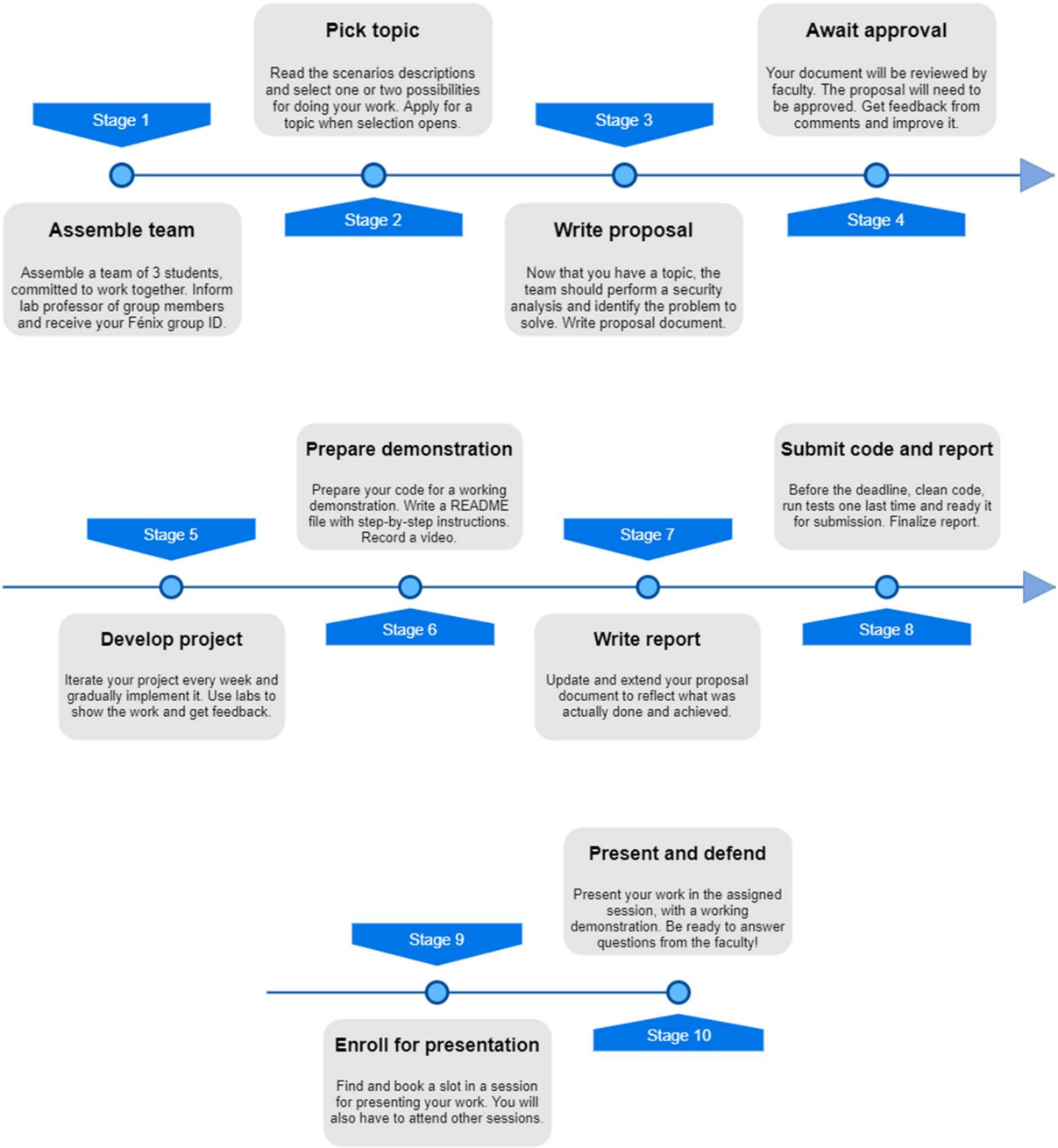

Figura 1 – Project stages.

2 STAGES

Each stage is described in the following sections.

2.1 ASSEMBLE TEAM

Assemble a team of 3 students, committed to work together. Inform the lab professor of the group members.

2.2 PICK TOPIC

The topics for the project are described in another document, which will be posted on the web site.

Read the scenarios descriptions and select one or two possibilities for doing your work. Apply for a topic when the selection page opens.

On the form, select the preferred topic for your group. This is done by adding your group identifier in one of the grey cells below the project topic in the selection table that will appear in the topic selection link.

DO NOT overwrite already occupied slots. Changes to the file are monitored and dishonest behavior will be subject to penalties.

Consider more than one topic, as there are a limited vacancies per project topic that will be assigned on a first-come-first-served basis.

Identify your group as CXX, where C is replaced by A(lameda) or T(aguspark) and XX is replaced by the two digits of your group number, as assigned by Fénix. For example, group 22 of Taguspark is T22 and group 7 of Alameda is A07.

The topic selection will open and close during the week stated in the last page of this document.

The official topic selection list will be posted after the process is concluded, to confirm the topic assigned to each group.

2.3 WRITE PROPOSAL

After having a topic assigned, your group should prepare a proposal document. The project proposal should describe the problem and the proposed solution.

The planned project will need to have, at least:

- The deployment of separate (virtual) machines, with network isolation;
- a secure communication tunnel (e.g. TLS, SSH) using correct configuration;
- the design and deployment of one channel using a custom security protocol.

The proposal should describe three versions of the work: basic, intermediate and advanced. The basic is the bare minimum security functionality. The intermediate version includes the most important security mechanisms. The advanced version addresses a wider range of attacks. As an analogy, the basic version should correspond with a 10/20 values project, the intermediate 15/20 and the advanced 20/20.

Please bring a draft of the proposal to lab session of the week to present it and receive feedback.

The proposal document must be submitted on that same week, before 20:00 of the day following the lab schedule.

Document requirements

- PDF format.
- Mandatory file name "CXX_WWW_HHMM_L_proposal.pdf" (where C is A for Alameda, T for Tagus, XX is the Fenix group number with two digits, WWW is the weekday of the lab shift – Mon, Tue, Wed, Thu, Fri – HHMM is the time – Hours and Minutes – and L is the lab room number).
- Report cover: Project title. Headed by course name, group campus, group number. In the next row: group members sorted by ascending student number. For each student, include the number, name and professional photo. You are encouraged to include a picture of the group members together.
- Report body: The font should be no smaller than 11pt, with standard line and character spacing.
- Limit 4 pages (excluding cover).
- Pages should be numbered (preferably with a label like "Page X of Y").
- The use of diagrams (such as UML) is recommended for clear and concise communication.

Document structure (mandatory)

I. Problem (Given the chosen scenario, where is security necessary? What is the main problem being solved? Use around 200 words)
   a. Requirements (Which security requirements were identified for the solution? Present as a list)
   b. Trust assumptions (Be explicit about trust relationships. Who will be fully trusted, partially trusted, or untrusted)

II. Proposed solution (overview with diagram and explanation with around 200 words or less)
   a. Deployment (describe distinct machines and how they will be interconnected)
   b. Secure channel(s) to configure (identify communication entities; existing library/tool to use; what keys will exist and how will they be distributed)
   c. Secure protocol(s) to develop (identify communication entities; language to use for implementation; what keys will exist and how will they be distributed)

III. Plan
   a. Versions (Describe basic, intermediate and advanced versions of the work and when are they expected to be achieved)
   b. Effort commitments (table containing one row per week until the submission date; and one column per group member with expected activities for the given week; some cells may be left blank because of work in other courses)

IV. References (tools, libraries, etc. that will be used in the project. State if each tool has been found/installed/tested at the time of proposal)

2.4 AWAIT APPROVAL

The proposal document will need to be approved by the course faculty. **The decision is communicated during the week following the proposal submission.**

2.5 DEVELOP PROJECT

Develop basic, intermediate and advanced versions over the project weeks.

Attend the lab sessions to present your ongoing development and receive early feedback from the professor. A security project that receives regular feedback is very likely to be more robust (and better graded).

2.6 PREPARE DEMONSTRATION

Once your team achieves the intermediate version of the work, start preparing the demonstration.

Write a README file with step-by-step instructions on how to run your project. Record screenshots, screencasts or similar of your project in action.

2.7 WRITE REPORT

The project final report should describe the problem and the implemented solution, along with a presentation of results.

Update and extend your proposal document to reflect what was actually done and achieved.

Document requirements

- PDF format.
- Mandatory file name "CXX_WWW_HHMM_L_report.pdf" (where C is A for Alameda, T for Tagus, and XX is the Fenix group number with two digits, WWW is the weekday of the lab shift, HHMM is the time, L is the lab room number).
- Report cover: Headed by course name, campus, group number. Followed by group members sorted by ascending student number. For each student, include the number, name, IST email and a professional photo. Project title. You are encouraged to include a picture of the group members together, during the project implementation.
- Report body: The font should be no smaller than 11pt, with standard line and character spacing.
- Limit of 5 pages (excluding cover), plus 2 pages of Annexes if necessary for reference materials.
- Pages must be numbered (preferably with a label like "Page X of Y").

Document structure (mandatory)

Same as the proposal, with the following differences:

- Replace *Plan* with **Results**: state what was actually achieved, with mention of strengths and weaknesses, and justification of implementation choices.
- All sections must be revised and updated

2.8 SUBMIT CODE AND REPORT

Before the final deadline of the project, as stated in the last page of this document, submit an archive with all the developed code and resources, and the report document. **The code archive and the report are submitted separately on the Fénix system.**

Code archive requirements

- ZIP format - without compiled code, only source and build scripts
- The mandatory file name is "CXX_WWW_HHMM_L_solution.zip" (where C is A for Alameda, T for Tagus, and XX is the Fenix group number with two digits, WWW is the weekday of the lab shift, HHMM is the time, L is the lab room number)
- README file, describing the required platform (e.g. Linux 64-bit, Ubuntu 18.04.1 LTS, Java 8u181) and setup instructions;
- All configuration files and scripts required to configure the solution on the specified platform;
- All developed source code;
- Existing tests and example files.

The project final report should describe the problem and the implemented solution, along with a presentation of results.

Update and extend your proposal document to reflect what was actually done and achieved.

2.9 ENROLL FOR PRESENTATION

The project presentations will occur on the dates following the submission deadline.

The link to make a reservation of the slot for the presentation will be made available during the final days of the project.

Each group should reserve a presentation slot using an electronic form. Groups should register in their respective campus, preferably in the laboratory they are enrolled to. To register, it is enough to add "CXX" in one of the white cells (free slots), where C is A for Alameda, T for Tagus, and XX is the Fenix group number with two digits. DO NOT overwrite already occupied slots. Changes to the file are monitored and dishonest behavior will be subject to penalties.

2.10 PRESENT AND DEFEND

Each group will have to attend at least two presentation sessions: the one where they will present and an additional one, to learn from the presentations and discussions of other groups.

The presentations will be organized as follows:

- 8 minutes for presentation of the work done, supported by slides, with a mandatory 2 minute live demo (also prepare a backup video, just in case there is a technical problem);
- 7 minutes for questions and answers.

It is highly recommended that each presentation includes:

- a slide with the general an architecture;
- a slide with the key distribution and management mechanism, if appropriate;
- a slide with the general protocol/architecture.

Each group member must participate and talk in the presentation, and be prepared to answer individual questions.

If necessary, a more detailed discussion will be scheduled with each group.

After the presentation, submit the slides with the link to the video in Fénix.

Presentation archive requirements

- ZIP format.
- The mandatory file name is "CXX_WWW_HHMM_L_presentation.zip" (where C is A for Alameda, T for Tagus, and XX is the Fenix group number with two digits, WWW is the weekday of the lab shift, HHMM is the time, L is the lab room number).
- Presentation in PDF and also in source format (e.g. PowerPoint).
- Text file containing link(s) to download video and screenshots of the solution. The links must be valid for one month, at least. The video can also be published in YouTube or a similar platform.

Grading

The project grade will take into account:

- Report (20%),
- Presentation (20%),
- Security design/rational (40%),
- Security implementation (40%).

3 DEADLINE CALENDAR

The relevant dates for the project are shown in the following calendar (all dates in **2019**).

Stage	**Deadline**
1 – Assemble team	On the labs, before Friday, October 11th
2 – Pick topic	Opens: Wednesday, October 16th **Closes: 20:00 on Friday, October 18th**
3 – Write proposal	**Submit before 20:00 of the day after your lab session**, i.e.: Lab on Monday, submit until Tuesday, October 22nd Lab on Tuesday, submit until Wednesday, October 23rd Lab on Thursday, submit until Friday, October 25th Lab on Friday, submit until Saturday, October 26th
4 – Await approval	Week of October 28th to November 1st
5 – Develop project	During the weeks of November 4th, November 11th, November 18th, November 25th, December 2nd, articulated with other coursework.
6 – Prepare demonstration	Start preparing once you have the intermediate version of the work. Suggested week: November 25th
7 – Write report	Update as you complete basic, intermediate and advanced versions. Final revision: week of December 9th
8 – Submit code and report	**17:00 on Wednesday, December 11th**
9 – Enroll for presentation	Opens: Tuesday, December 10th **Closes: 20:00 on Wednesday, December 11th**
10 – Present and defend	Sessions start Thursday, December 12th and are expected to end on Friday, December 20th **Submit slides and other presentation materials** **before 20:00 of the day after your presentation session.**

IMPORTANT: keep track of the course **web site** for updates and online forms:

https://fenix.tecnico.ulisboa.pt/disciplinas/SIRS7/2019-2020/1-semestre

We wish you the best of luck in this technical venture!
Make the most of it and ask for our feedback as much as possible.

~ The SIRS Faculty