COMSM0102 Systems & Software Security Coursework

Joseph Hallett and Sana Belguith

November 7, 2024

Part A—Unit Specific Coursework Details

Unit Number: COMSM0102

Unit Name: Systems & Software Security

Unit Director: Sana Belguith

Assignment Name: Systems & Software Security Coursework

Assignment Weighting: 30%

Assignment Description:

This coursework is for unit COMSM0102 Systems & Software Security Coursework. It will be released on *Friday 8th November* and must be submitted by *Friday 29th November* at 1pm at the very latest. The intention is that you submit by 12pm and keep the last hour as an emergency reserve for technical problems.

In case of problems with your submission, you must e-mail coms-info@bristol.ac.uk before the 1pm final deadline to avoid your work being counted as late. You must submit the coursework on the Blackboard page for the assessment unit COMSM0102 (not the teaching unit COMSM0049). On the assessment unit, go to the menu item *"Assessment, Submission and Feedback"* and follow the instructions there.

If you have any questions, please write your question in the Teams channel and we will answer it as quickly as possible. You are recommended to do this work in groups of 3 students, but you may work individually if you prefer. We will consider the group size when we mark your work. A marking scheme for this coursework is included on the last page of this document

Introduction

This project validates the whole unit, there is no other assessment. It represents a significant investment of time and effort that should mostly take place during Week 8, 9 and 10. We encourage you to form groups of 3 students, however you can undertake this coursework individually if you prefer. You will need as part of the project to submit: your code, a video demo and a final write up.

We expect every member of a group to participate fully in the project. You are free to organise as you wish, but your personal contribution will be evaluated and need to be demonstrated (see below). We are expecting you to work together and to collaborate effectively. If you have any concern about your group dynamic or you are struggling to form a group, do contact us via e-mail and we will be able to help.

If you decide to undertake this coursework individually, we will take into consideration that you are working alone and we will reflect that in the marking scheme.

Deliverables

Project demonstration (group, graded 30%) You will demonstrate that your solution works and demonstrate your project. Your project should be coming with a `README`. You will follow the `README` instructions and demonstrate that you obtain the results presented in your report and that you can reproduce the evaluation. The video should be *no longer than 10 minutes*.

PS: Please use appropriate compression settings while processing your demonstration videos as Blackboard will not allow videos larger than 100MB to be uploaded. README

Final write up (group, graded 70%) You should submit a report of roughly 5 pages (excluding references and appendice). Your report should contain a minimum of six academic citations. We suggest the following structure:

- Introduction
- Background
- Design & Implementation
- Evaluation
- Conclusion

Please use figures to illustrate your points (as appropriate).

In addition in the appendix you should:

1. Discuss how well you met your project's objective. If you did not implement everything you planned this does not mean that you will fail (or get a bad grade). You should discuss why it could not be done (e.g. technical challenges, change of direction, alternative approach taken, sickness of one of the group members etc.).

2. Your individual contribution to the project as a score (e.g., in a group of three if you all worked equally 33% each) and list your individual contributions. You need to all agree on this section.

You are all expected to participate in the technical aspects as well as the writing. We will take into consideration the complexity of your work as well as your individual contributions when deciding your individual grades. Our intent is to ensure that no one is penalized if one (or several) of the students want to work above and beyond expectations. We will only *improve* individual grades, we won't award any grades below the report grade.

Project

In the labs we have been generating exploits using *return oriented programming (ROP)*. For this coursework takes the lab to the next step by generating such exploits automatically. In particular:

1. We assume a stack overflow based vulnerability that overwrites the saved return address. You are supposed to automatically find the input (string) length that is sufficient to overwrite the saved return address (in the lab, you did so by doing manual analysis to find that you needed 44 bytes of junk data before starting to overwrite the saved return address).
2. In the lab, we were generating a ROP chain thatused to setup:

   `execve("/tmp//nc","-lnp","5678","-tte","\bin//sh", NULL)`

   In this courswork, we need to automatically generate the exploit which takes arbitrary command line for execve and on a successful exploit, you should get that program (argument to `execve`) launched. (look at the code of the ROPGadget tool)
3. You need to make sure that the exploit works for any chosen .data address (remember, no null bytes!).
4. Rather than forming a ROP of step 2 above (i.e. arbitrary arguments to execve), generate a ROP based exploit for a given arbitrary shellcode (see: Transforming Malicious Code to ROP Gadgets for Antivirus Evasion)

Support provided to students during coursework period

Joseph and Sana are both available to answer questions on Teams or by email, we also set up Q&A sessions-check your timetables.

Submission Details

Both final writeup and project demonstration to be submitted in Blackboard: Systems and Software Security (with Coursework) 2024 → Assessment, submission and feedback Project → Systems and Software Security Coursework

Marking Criteria

Project Demonstration Marking Scheme (30%)

Weight	Category	Comment
10%	Technical Clarity	You will explain clearly how to run your project. Technical terminology should be used appropriately. You should assume an educated audience of your peers and explain terminologies and concepts specific to your project. It should be clear how that relates to the evaluation section of your report.
20%	Instructions Clarity	The instructions contained in your `README` should be simple to follow and lead to the results presented in your report. You need to demonstrate this, by following the instructions step by step in your video. We invite you to start from a "clean" environment.

Report Marking Scheme (70%)

Weight	Category	Comment
10%	Presentation	You should use the provided latex template properly. Reference should be appropriately formatted. We expect the presentation standard to be on par with the reading material seen during lectures.
20%	Literature Review	You will identify the relevant academic literature, show understanding of the papers you have selected and cite them appropriately. It should be clear how they relate to your work. You are expected to explore beyond the papers assigned as reading material.
20%	Design & Implementation	You should describe your implementation at an appropriate level of abstraction (refer to the reading material seen during teaching). You should clearly describe any technical challenges you faced and articulate the design decisions you made and why you believe they were appropriate. This should be understandable by an audience of your peers.
20%	Evaluation	You should evaluate how well the outcome of your work addresses your objectives. You should use quantitative (e.g. measuring performance overhead of a security mechanism) or qualitative (e.g. critical discussion of the security guarantees of a mechanism) as appropriate to your project. You are strongly encouraged to draw from evaluations found in the literature to design yours (reference this clearly when this is the case).

Part B—Universal Coursework Details

Deadline

The deadline for submission of all optional unit assignments is 13:00 on Friday 29th November. Students should submit all required materials to the *"Assessment, submission and feedback"* section of Blackboard—it is essential that this is done on the Blackboard page related to the *"With Coursework"* variant of the unit.

Time commitment

You are expected to work on both of your optional unit courseworks in the 3-week coursework period as if it were a working week in a regular job—that is 5 days a week for no more than 8 hours a day. The effort spent on the assignment for each unit should be approximately equal, being roughly equivalent to 1.5 working weeks each. It is up to you how you distribute your time and workload between the two units within those constraints.

You are strongly advised NOT to try and work excessive hours during the coursework period: this is more likely to make your health worse than to make your marks better. If you need further pastoral/mental health support, please talk to your personal tutor, a senior tutor, or the university wellbeing service.

Academic Offences

Academic offences (including submission of work that is not your own, falsification of data/evidence or the use of materials without appropriate referencing) are all taken very seriously by the University. Suspected offences will be dealt with in accordance with the University's policies and procedures. If an academic offence is suspected in your work, you will be asked to attend an interview with senior members of the school, where you will be given the opportunity to defend your work. The plagiarism panel are able to apply a range of penalties, depending the severity of the offence. These include: requirement to resubmit work, capping of grades and the award of no mark for an element of assessment.

Extenuating circumstances

If the completion of your assignment has been significantly disrupted by serious health conditions, personal problems, periods of quarantine, or other similar issues, you may be able to apply for consideration of extenuating circumstances (in accordance with the normal university policy and processes). Students should apply for consideration of extenuating circumstances as soon as possible when the problem occurs, using the extenuating circumstances form.

You should note however that extensions are not possible for optional unit assignments. If your application for extenuating circumstances is successful, it is most likely that you will be required to retake the assessment of the unit at the next available opportunity.