COMP6015- Principals of Secure Operating Systems
Coursework: Security of an OS- File System Security
Semester 2- 2022-23

Learning outcome

(This exercise assesses LO (Learning Outcome) 1 and 3)
LO 1: Demonstrate a thorough understanding of the fundamentals of OS design, including process/thread, file, IO, and memory management.

LO 3: Critically evaluate the security, reliability, and protection in a given OS configuration. Use the results of the evaluation to produce recommendations for hardening the system.

Task

Pick one of the two current major commercial OSes (Windows or macOS) and write a report on its security features with respect to File System. Focus especially on recent changes made to enhance security within the OS and the effects these have on application developers.
Note that a certain amount of original research will be required for this, and your report will go far beyond what is covered in the lecture notes.

Your report must be formally written and include citations to demonstrate fact-checking. Your primary reference should be the *developer documentation* for each OS. Both Microsoft and Apple make this freely available online. Advertisements or other marketing documents, or press statements, are not acceptable sources; nor is Wikipedia. Because the documentation for both OSes is freely available, it is not necessary to choose the OS you use, although familiarity with the OS you choose will be helpful.

Remember to consider low-level security of features within the OS such as related built-in encryption techniques/tools (e.g., File Vault in macOS).

In the end, briefly compare the listed techniques/tools with similar techniques in an alternative OS.

Deliverable, word limit, and deadline

This exercise is worth 40% of the total marks for the module.

Your report covers

1) A high-level **description** of the security features of an OS file system (15% of the assessment component mark).

2) A detailed description of how your selected **OS support**s and provides the listed security features. This should be based on the official documents and includes the timeline that tells from which version the mentioned features were added to the selected OS (30%).

3) A **comparison** of the listed features in your selected OS with an alternative OS (15%).

4) The **effects** that the listed security features have **on** application **developers** (20%).

5) A **conclusion** section that includes recommendations for improving the security of OS File Systems and personal reflection(15%).

6) **References** (using Harvard or Numerical style of referencing) and proper citation(5%).

Submission

- Submit your final report via Moodle by 3rd March 2023, 5:00 PM.
- Your report must be at most 1500 words (excluding references).
- Reports longer than 10% of the word limit will be penalised; the extra words will not be marked.
- Marks and feedback will be available on Moodle 3 weeks after submission.
- This coursework is an individual piece of work. The University rules concerning plagiarism, syndication and cheating apply.
- Version Control: You'll need to use a version control platform that records your report development history i.e., GitHub. Your report will include the link to your GitHub repository. If you use any other repository, you must justify this in your report Appendices. Reports without a valid version control history will not be acceptable.

Marking rubric

Weighting	Section	Mark distribution					
		0	**1 to <40**	**40 to <50**	**50 to <60**	**60 to <70**	**70 to 100**
15%	Description: A description of the security features of an OS file system.	Not presented	Inadequately addressed: Poor quality content; incomplete /irrelevant.	Satisfactory: Provides some overview of the report and it covers some related security features, but it is incomplete.	Acceptable: Provides some overview of the report and it covers almost half of the essential security features, but it is incomplete.	Very good: Provides a very good overview of the report and it covers most of the essential features, but it could be more brief/relevant/complete.	Excellent: Provides an excellent overview of the report and it covers all the essential features, concise, and brief.
30%	OS Support: A description of how your selected OS supports the listed security features. This should be based on the official documents and includes the timeline that tells from which version the mentioned features were added to the selected OS.			Satisfactory: A general description of how the selected OS supports the listed features, but lacks an acceptable timeline, referencing, and citations.	Acceptable: Good description of how the selected OS supports the listed features with an acceptable timeline, referencing, and citations.	Very good: Good description of how the selected OS supports the listed features with a good presentation of timeline, referencing, and citations.	Excellent: Excellent description of how the selected OS supports the listed features with a great presentation of timeline, referencing, and citations.
15%	Comparison: A comparison of the listed features in your selected OS with an alternative OS.			Satisfactory: A general comparison of some of the listed features in the selected OS with an alternative OS.	Acceptable: An acceptable comparison of some of the listed features in the selected OS with an alternative OS.	Good: A good comparison of most of the listed features in the selected OS with an alternative OS.	Excellent: An excellent comparison of almost all the listed features in the selected OS with an alternative OS.

20%	Effects on developers: The effects that the listed security features have on application developers.			Acceptable: An acceptable description of some of the effects that the listed security features have on application developers.	Acceptable: An acceptable description of some of the effects that the listed security features have on application developers.	Good: A good description of some of the effects that the listed security features have on application developers.	Acceptable: An acceptable description of some of the effects that the listed security features have on application developers.
15%	Conclusion: A conclusion section that includes recommendations for improving the security of OS File Systems			Satisfactory: A general conclusion section with no valid recommendations for improving the security of OS File Systems.	Acceptable: An acceptable conclusion section with one or two recommendations for improving the security of OS File Systems.	Good: A good conclusion section with some recommendations for improving the security of OS File Systems.	Excellent: An excellent conclusion section with some important/essential recommendations for improving the security of OS File Systems.
5**%**	.References (using Harvard or Numerical style of referencing)			Satisfactory: A list of some related references provided.	Acceptable: An acceptable list of some related valid references provided, which some cited inside the report.	Good: A good list of some related valid references provided, which some cited inside the report.	Excellent: An excellent well-structured reference list containing valid resources/scholars, which all were cited inside the report.