Text, logo

Description automatically generated **San Francisco Bay University**

**CE521 - Real-time Systems and Programming**

**Homework Assignment #1**

**Due day: 2/13/2022**

**Student ID:19590**

**Instruction:**

1. **Push the answer sheet to Github**
2. **Overdue homework submission could not be accepted.**
3. **Takes academic honesty and integrity seriously (Zero Tolerance of Cheating & Plagiarism)**
4. Keeping in mind the various definitions of operating system, consider whether the operating system should include applications such as web browsers and mail programs. Argue both that it should and that it should not, and support your answers

2Chapter 1 Introduction

1.4 Keeping in mind the various definitions of operating system, consider

Answer:

* If the application is embedded within the operating system, it is likely to be better able to take advantage of features in the kernel and therefore have performance advantages over an application that runs outside of the kernel.
* Arguments against embedding applications within the operating system typically dominate however: 1) the applications are not part of an operating system, 2) any performance benefits of running within the kernel are offset by security vulnerabilities and 3) it leads to a bloated operating system.

1. How does the distinction between kernel mode and user mode function as a rudimentary form of protection (security) system?

* The distinction between kernel mode and user mode provides a rudimentary form of protection in the following manner. Certain instructions could be executed only when the CPU is in kernel mode.
* Similarly, hardware devices could be accessed only when the program is executing in kernel mode. Control over when interrupts could be enabled, or disabled is also possible only when the CPU is in kernel mode.
* Consequently, the CPU has very limited capability when executing in user mode, thereby enforcing protection of critical resources.

1. In a multiprogramming and time-sharing environment, several users share the system simultaneously. This situation can result in various security problems.
   1. What are two such problems?

* One user can read the private data of another user - privacy.
* One user can corrupt the private data of another user - integrity.
* One user can prevent another user from getting anything done - denial of service.
  1. Can we ensure the same degree of security in a time-shared machine as in a dedicated machine? Explain your answer.
* If we can ensure that the operating system prevents any sharing of data between users, either for reading or writing, and fairly shares the computer, then we can achieve the same level of security.
* However, we can never be sure that our software doesn't have bugs, so we can never be sure that we prevent all sharing of data and fairly allocate computer resources.

1. Describe a mechanism for enforcing memory protection to prevent a program from modifying the memory associated with other programs.

* The processor could keep track of what locations are associated with each process and
* limit access to locations that are outside of a program’s extent. Information regarding the extent of a program’s memory could be maintained by using base and limits registers and by performing a check for every memory access.

1. Describe some of the challenges of designing operating systems for mobile devices compared with designing operating systems for traditional PCs.

* Besides a core kernel, middleware must be designed in mobile operating systems to support a set of software frameworks that provide additional services to application developers.
* Different from using a physical keyboard and mouse, mobile devices need to feature a touch screen and let user interact with the system by pressing and swiping fingers across the screen.
* Mobile operating system must balance the performance with the battery life.
* Mobile operating system must have a good support for external peripheral devices like GPS, HDMI which is essential for mobile devices.
* Mobile operating system must consider the limited resources since the mobile devices is much smaller compared with PC.
* The mobile devices are more and more related to people's privacy, so the security of the operating system for the mobile devices counts even more than the traditional PCs and harder to prevent malicious code and access.

the operating system for the mobile devices counts even more than the traditional

PCs and harder to prevent malicious code an