Forside IDATG2202 august 2024

Institutt for informasjonssikkerhet og kommunikasjonsteknologi

Eksamensoppgave i IDATG2202 - Operativsystemer, virtualisering og sikkerhet

Eksamensdato: 06.08.2024

Eksamenstid (fra-til): 09:00 - 12:00

Hjelpemiddelkode/Tillatte hjelpemidler: **D**: Ingen trykte eller håndskrevne hjelpemidler tillatt. Bestemt, enkel kalkulator tillatt.

Faglig kontakt under eksamen: Erik Hjelmås

Tlf.: 93034446

Faglig kontakt møter i eksamenslokalet: Nei.

ANNEN INFORMASJON:

Skaff deg overblikk over oppgavesettet før du begynner på besvarelsen din.

Les oppgavene nøye, gjør dine egne antagelser og presiser i besvarelsen hvilke forutsetninger du har lagt til grunn i tolkning/avgrensing av oppgaven. Faglig kontaktperson kontaktes kun dersom det er direkte feil eller mangler i oppgavesettet. Henvend deg til en eksamensvakt hvis du mistenker feil og mangler. Noter spørsmålet ditt på forhånd.

Ingen håndtegninger: Denne eksamenen tillater ikke bruk av håndtegninger. Har du likevel fått utdelt skanne-ark, er dette en feil. **Arkene vil ikke bli akseptert for innlevering, og de vil derfor heller ikke sendes til sensur**.

Varslinger: Hvis det oppstår behov for å gi beskjeder til kandidatene underveis i eksamen (f.eks. ved feil i oppgavesettet), vil dette bli gjort via varslinger i Inspera. Et varsel vil dukke opp som en dialogboks på skjermen. Du kan finne igjen varselet ved å klikke på bjella øverst til høyre.

Trekk fra/avbrutt eksamen: Blir du syk under eksamen, eller av andre grunner ønsker å levere blankt/avbryte eksamen, gå til “hamburgermenyen” i øvre høyre hjørne og velg «Lever blankt». Dette kan ikke angres selv om prøven fremdeles er åpen.

Tilgang til besvarelse: Etter eksamen finner du besvarelsen din i arkivet i Inspera. Merk at det kan ta én virkedag før eventuelle håndtegninger vil være tilgjengelige i arkivet.

Språk: Alle oppgavetekster er på engelsk, men du står fritt til å svare på norsk eller engelsk eller "blanding".

Negative poeng/minuspoeng: Ingen oppgaver kan føre til minuspoeng totalt på den respektive oppgaven, men noen av flervalgsoppgavene kan ha minuspoeng internt i oppgaven for å unngå at man "helgarderer". *Dette står da tydelig presistert i oppgaveteksten for de respektive oppgavene.*

Lykke til!

NYNORSK VERSJON:

Institutt for informasjonssikkerhet og kommunikasjonsteknologi

Eksamensoppgåve i IDATG2202 - Operativsystemer, virtualisering og sikkerhet

Eksamensdato: 06.08.2024

Eksamenstid (frå-til): 09:00 - 12:00

Hjelpemiddelkode/Tillatne hjelpemiddel: **D**: Ingen trykte eller handskrevne hjelpemidler tillate. Bestemt, enkel kalkulator tillat.

Fagleg kontakt under eksamen: Erik Hjelmås

Tlf.: 93034446

Fagleg kontakt kjem til eksamenslokalet: Nei.

ANNA INFORMASJON:

Skaff deg eit overblikk over oppgåvesettet før du byrjar å svare på oppgåvene.

Les oppgåvene nøye, gjer deg opp dine eigne meiningar og presiser i svara dine kva for føresetnadar du har lagt til grunn i tolking/avgrensing av oppgåva. Fagleg kontaktperson kontaktast berre dersom du meiner det er direkte feil eller manglar i oppgåvesettet. Vend deg til ei eksamensvakt om du meiner det er feil eller manglar. Noter spørsmålet ditt på førehand.

Ingen handteikningar: Denne eksamenen tillèt ikkje bruk av handteikningar. Om du likevel har fått utdelt skanne-ark, er dette en feil. **Arka vil ikkje bli akseptert for innlevering, og dei vil difor heller ikkje sendast til sensur**.

Varslingar: Dersom det oppstår behov for å gje beskjedar til kandidatane medan eksamen er i gang (f.eks. ved feil i oppgåvesettet), vil dette bli gjort via varslingar i Inspera. Eit varsel vil dukke opp som en dialogboks på skjermen i Inspera. Du kan finne att varselet ved å klikke på bjølla i øvre høgre hjørne på skjermen.

Trekk frå/avbroten eksamen: Blir du sjuk under eksamen, eller av andre grunnar ynskjer å levere blankt/avbryte eksamen, gå til “hamburgermenyen” i øvre høgre hjørne og vel «Lever blankt». Dette kan ikkje angrast sjølv om prøven framleis er open.

Tilgang til svara dine: Etter eksamen finn du svara dine i arkivet i Inspera. Merk at det kan ta ein vyrkedag før eventuelle handteikningar vert tilgjengelege i arkivet.

Språk: Alle oppgåvetekstar er på engelsk, men du står fritt til å svare på norsk eller engelsk eller "blanda".

Negative poeng/minuspoeng: Ingen oppgåver kan føre til minuspoeng totalt på dei respektive oppgåva, men nokon av flervalgsoppgavene kan ha minuspoeng internt i oppgåva for å unngå at ein "heilgarderer". *Dette står då tydeleg presistert i oppgåveteksten for dei respektive oppgåvene*.

Lykke til!

1 Merknader

Bokmål:
Dette tekstfeltet kan du benytte om du i løpet av eksamen finner det nødvendig å legge inn egne kommentarer eller presiseringer vedrørende enkelte oppgaver. Husk å merke tydelig hvilken/hvilke oppgaver det er snakk om. (Feltet er ikke poenggivende i seg selv.)

Nynorsk:
Dette tekstfeltet kan du nytte om du i løpet av eksamen finn det nødvendig å leggje inn eigne kommentarar eller presiseringar vedkomande enkelte oppgåver. Hugs å merke tydeleg kva/korleis oppgåver det er snakk om. (Feltet er ikkje poenggjevande i seg sjølv.)

Dine merknader

Format

Words: 0

Maks poeng: 0

2 introproc.os (2%)

What best describes the main function of an operating system?
Velg ett alternativ:

- Boot the system and hand over control of the keyboard and mouse to user programs
- Manage system resources and provide a set of services to user programs
- Allow user programs to manage system resources directly
- Allow user programs to directly control the CPU

Maks poeng: 2

3 hwreview.interrupt (2%)

The CPU is interrupted in all of the following situations *except:*
Velg ett alternativ:

- A direct memory access (DMA) transfer has completed.
- A read from memory has finished.
- An I/O-device has finished processing a request.
- A periodic hardware timer resumes the kernel.

Maks poeng: 2

4 hwreview.register (2%)

Which register is used when addressing/referencing local variables in memory?
Velg ett alternativ:

- ESP/RSP
- EBP/RBP
- EFLAG/RFLAG
- EBX/RBX
- EAX/RAX
- EIP/RIP

Maks poeng: 2

5 syscalls.def (2%)

A system call is performed when
Velg ett alternativ:

- an instruction divide a number with zero.
- a new device in the system is assigned a new name.
- the operating system requests a service from a process.
- a process asks the operating system to do I/O.

Maks poeng: 2

6 scheduling.theory (2%)

Which of the following scheduling algorithm may suffer from *convoy effect*?
Velg ett alternativ:

- RR
- FCFS
- MLFQ
- SJF

Maks poeng: 2

7 scheduling.theory (2%)

Which of the following scheduling algorithms gives the minimum average turaround time for a given set of processes?
Velg ett alternativ:

- STCF/PSJF/SRTN/SRTF
- FCFS
- MLFQ
- RR

Maks poeng: 2

8 threads.terminology (2%)

When the result/output of a multithreaded program depend on the scheduling of the threads (the result/output is "non-deterministic") this is called:

Velg ett alternativ:

- mutual exclusion
- buffer overflow
- critical section
- ✓ race condition

Maks poeng: 2

9 io.ssd (2%)

What is a key challenge with Solid State Drives (SSD)?

Velg ett alternativ:

- ✓ you cannot overwrite data without erasing first
- the flash translation layer (the controller) needs to update the inode whenever a file changes
- using RAM as cache is not as efficient when the backend storage is SSD
- larger blocks of random writes are slow

Maks poeng: 2

10 fscore.rootdir (2%)

Which of the following paths correctly specifies the root directory of a Linux file system?
Velg ett alternativ:

- /sys
- /root
- /
- /home/root

Maks poeng: 2

11 fscore.consistency (2%)

What happens during a check of "file system consistancy"?
Velg ett alternativ

- No directories should have more than 512 files.
- Whether the same file is present in more than one directory in the file system.
- If all files use at least one data block.
- Whether blocks registered as available are actually in use or not.

Maks poeng: 2

12 fscore.links (2%)

Which ONE of the following statements about hard and symbolic links is true?

Velg ett alternativ:

- Hard links are limited to entries within the same filesystem; symbolic links can refer to entries within other filesystems.
- Hard links can refer to files or directories; symbolic links can only refer to files.
- Creating a hard link adds a new inode to the filesystem; creating a symbolic link does not add a new inode to the filesystem
- Hard links cannot be deleted; symbolic links can be deleted.

Maks poeng: 2

13 virt.cpuhw (2%)

The problem on X86 before 2005 with 17 sensitive instructions not being a part of the privileged instructions was solved by introducing hardware support for virtualization. What was changed in hardware?

Velg ett alternativ

- The NX-bit was added to each page table entry
- Duplication of all registers on each CPU core (hyperthreading)
- A new "higher level kernel mode" called VMX root mode.
- A third bit in the FLAG register

Maks poeng: 2

14 virt.cpuhw (2%)

When an application does simple system calls, why does a virtual machine perform almost like a native machine when there is hardware support for virtualization on the CPU?

Velg ett alternativ

- Because the MMU does not use shadow page tables.
- Because TLB (Translation Lookaside Buffer) is filled directly from the shadow page tables.
- Because all interrupts (system calls, hardware interrupt, exceptions) goes directly to the hypervisor
- Because all interrupts (system calls, hardware interrupt, exceptions) goes directly to the guest operating system

Maks poeng: 2

15 ossec.design (2%)

Which of the following is one of Saltzer and Schroeders design principles from 1975?

Velg ett alternativ:

- Economy of mechanism: Keep the design as simple and small as possible
- Accountability: Trace the actions of users and processes to identify the sources of errors or malicious activities.
- Protected accounts: Passwords should follow complex password policies (composition and length)
- Confidentiality: Protect the secrecy of the information stored and processed.

Maks poeng: 2

16 ossec.accesstoken (2%)

Which one of the following is present in an Access Token on Windows?
Velg ett alternativ:

- Privileges
- Inode
- Security Descriptors
- Discretionary Access Control List

Maks poeng: 2

17 semaph.sync (4%)

If we want to output to be

```
parent: begin
child
parent: end
```

What should the value of X be in the following code?

```
sem_t s;

void *child(void *arg) {
    printf("child\n");
    sem_post(&s); // signal here: child is done
    return NULL;
}

int main(int argc, char *argv[]) {
    sem_init(&s, 0, X); // what should X be?
    printf("parent: begin\n");
    pthread_t c;
    Pthread_create(&c, NULL, child, NULL);
    sem_wait(&s); // wait here for child
    printf("parent: end\n");
    return 0;
}
```

Velg ett alternativ:

- -1
- 0
- 1
- 01
- 10
- Y
- X

Maks poeng: 4

18 addrspace.vaspace (3%)

The virtual address space is split into:
Velg ett alternativ

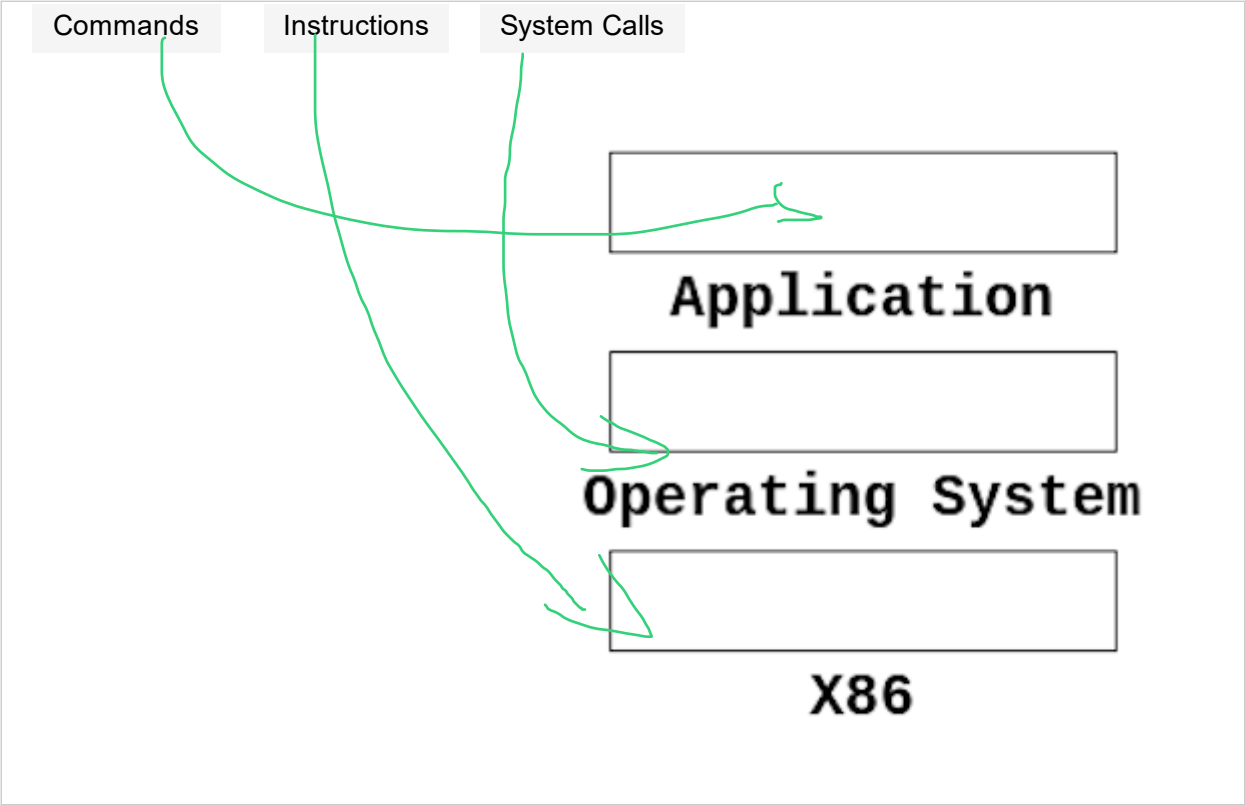
- Partitions
- Memory Management Units
- Segments
- Pages
- Translation Lookaside Buffers
- Swaps
- Tracks
- Frames

Maks poeng: 3

19 introproc.layers (3%)

Move (drag-and-drop) the texts "Commands", "Instructions" and "System Calls" to their correct box.

Velg ett alternativ:



Maks poeng: 3

20 hwreview.stackframe (10%)

How are the registers ESP/RSP and EBP/RBP used to keep control of a function's stack frame? What happens to these registers when a program enters a function ("makes a function call")?

Skriv ditt svar her...

Format

E/RSP - stack pointer points to the top of the stack in the function call (variables, arguments etc)
E/RBP - base pointer points to the base of the stack

Words: 0

Maks poeng: 10

21 syscalls.fork (5%)

Explain in as much detail as possible the situation that occurs in a machine where you execute the program code:

```
01  main() {
02     while (1) {
03      fork();
04     }
05  }
```

Skriv ditt svar her...

Format

Fork bomb - will fork processes forever and the program will crash after a few seconds of running because it will use too much memory. (Interrupt of Execption)

Words: 0

Maks poeng: 5

22 syscalls.fork (10%)

Write a C-program using fork(). You do not have to include header files, just write the main()-function.

1. (4%) The child process should print “mysil”; the parent process should print “solan”.
2. (2%) Make sure that the child process always prints first using a system call.
3. (2%) Suggest an alternative way of getting the child process to print first using some kind of "simple hack". This method does not have to work all the time.
4. (2%) Assuming the program is called kjell.c, write down the command line you would use for compiling this to an executable file called kjell. Include the option for showing all warnings.

Skriv ditt svar her

```
int main(int argc, char** argv) {
  pid_t rc = fork();                          gcc -Wall kjell.c -o kjell
  if (rc == 0) {
    printf("mysil");
  }
  else {
    wait(NULL);
    prinft("solan");
  }
    return 0;

}
```

Maks poeng: 10

23 addrspace.paging (10%)

Assume 12-bit logical/virtual addresses, page size 512B and the slightly simplified page table

```
  +-----+---+
7 | 111 | 1 |
6 | 101 | 1 |
5 | 000 | 0 |
4 | 011 | 1 |
3 | 000 | 0 |
2 | 000 | 0 |
1 | 010 | 1 |
0 | 001 | 1 |
  +-----+---+
```

Explain how the logical/virtual address 1101 1011 1010 is translated to a physical address.

Skriv ditt svar her

Format

Offset = 2^9 = 512B
VPN = 2^3 = 0110 = 6 -> 101 1101 1101 10

Words: 0

Maks poeng: 10

24 threads.sync (5%)

If **i=7** is a global variable and two threads T1 and T2 are running in parallel without synchronization mechanisms and T1 does **i++** (once) and T2 does **i--** (once) what are the possible final values of **i**? Justify your answer.

Skriv ditt svar her...

Format

6,7,8

Words: 0

Maks poeng: 5

25 semaph.sync (10%)

Explain what the problem(s) is/are with the following proposed solution to the Producer-Consumer problem:

```
semaphore mutex = 1;
semaphore empty = N;
semaphore full = 0;
int buffer[N];
void producer() {
   int item;
   while(TRUE) {
      item = produce_item();
      down(mutex);
      down(empty);
      insert_item(item,buffer);
      up(full);
      up(mutex);
   }
}
void consumer() {
   int item;
   while(TRUE) {
      down(mutex);
      down(full);
      item = remove_item(buffer);
      up(empty);
      up(mutex);
   }
}
```

1 - call to the produce_item function should be inside the mutex as well.
2 - what if one of the consumer is the first to down the mutex? Then deadlock will inventively occur since it's then waiting for full to become >= 1.
3.

Skriv ditt svar her

Format

Words: 0

Maks poeng: 10

26 fscore.discuss (5%)

Discuss advantages and disadvantages with small vs large block sizes in file systems.

Skriv ditt svar her...

Format

Large block size, internal fragmentation , but data is in one place making it easier to access/read.
Small block size, invernt advantages/disadvantages of large block size, also will cause more metadata.

Words: 0

Maks poeng: 5

27 fscore.codesample (5%)

What is the problem with the following code?

```
if (access(filename, W_OK) == 0){
     if ((fd = open(filename, O_WRONLY)) == NULL){
          perror(filename);
          return(0);
     }
     /* now write to the file */
```

Skriv ditt svar her

Format

Time of check vs time of use - between the if's, something could happen and change the filename thus, a race condition could occur affected by other processes/threads.

Words: 0

Maks poeng: 5