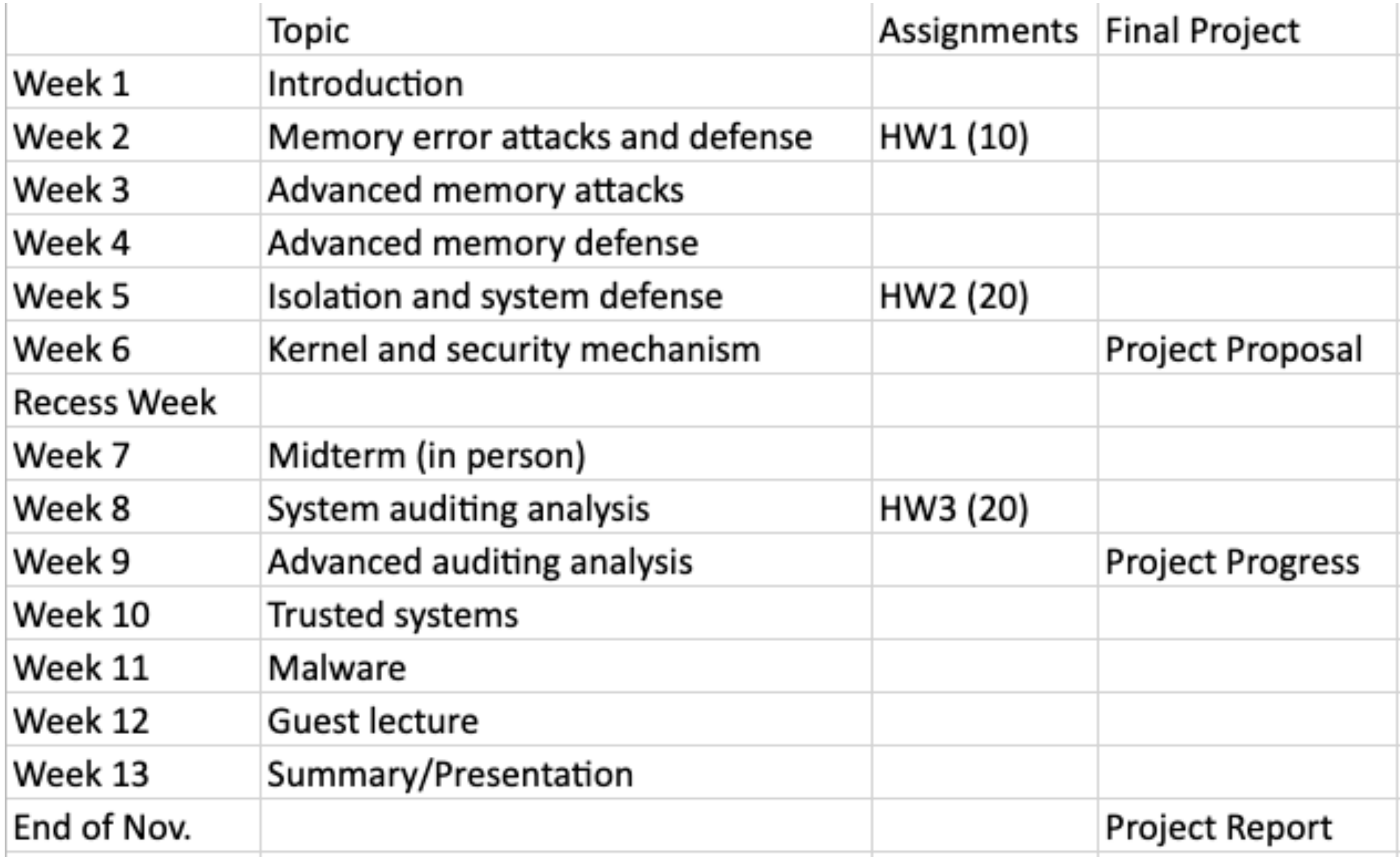
CS5231: Systems Security

Syllabus and Project

Syllabus

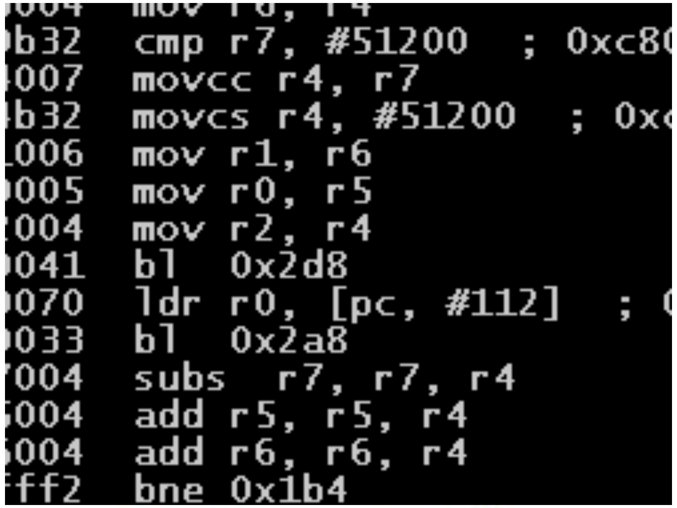


	Topic	Assignments	Final Project
Week 1	Introduction		
Week 2	Memory error attacks and defense	HW1 (10)	
Week 3	Advanced memory attacks		
Week 4	Advanced memory defense		
Week 5	Isolation and system defense	HW2 (20)	
Week 6	Kernel and security mechanism		Project Proposal
Recess Week			
Week 7	Midterm (in person)		
Week 8	System auditing analysis	HW3 (20)	
Week 9	Advanced auditing analysis		Project Progress
Week 10	Trusted systems		
Week 11	Malware		
Week 12	Guest lecture		
Week 13	Summary/Presentation		
End of Nov.			Project Report

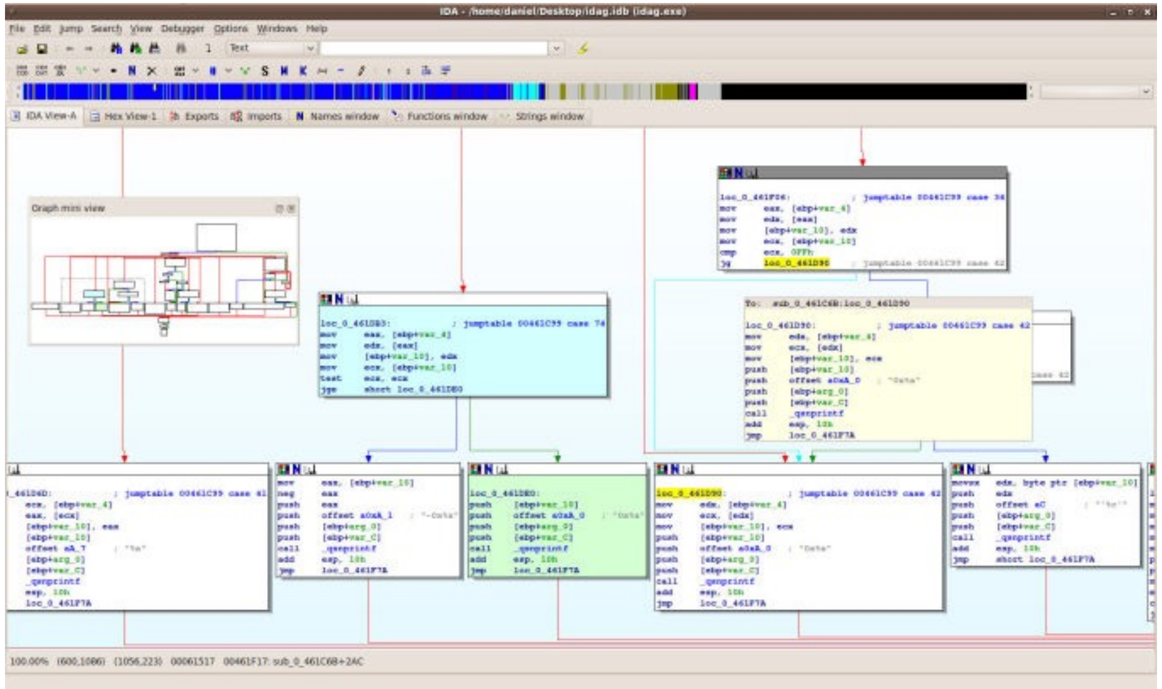
Project Goal and Supports

- Project goal
  - Drive your ***deep*** understanding into a ***complex*** system.
- Teams
- TA support: cs5231ta@googlegroups.com

Binary



```
004  mov r0, r4
b32  cmp r7, #51200   ; 0xc8
007  movcc r4, r7
b32  movcs r4, #51200   ; 0x
006  mov r1, r6
005  mov r0, r5
004  mov r2, r4
041  bl  0x2d8
070  ldr r0, [pc, #112]   ;
033  bl  0x2a8
004  subs  r7, r7, r4
004  add r5, r5, r4
004  add r6, r6, r4
ff2  bne 0x1b4
```

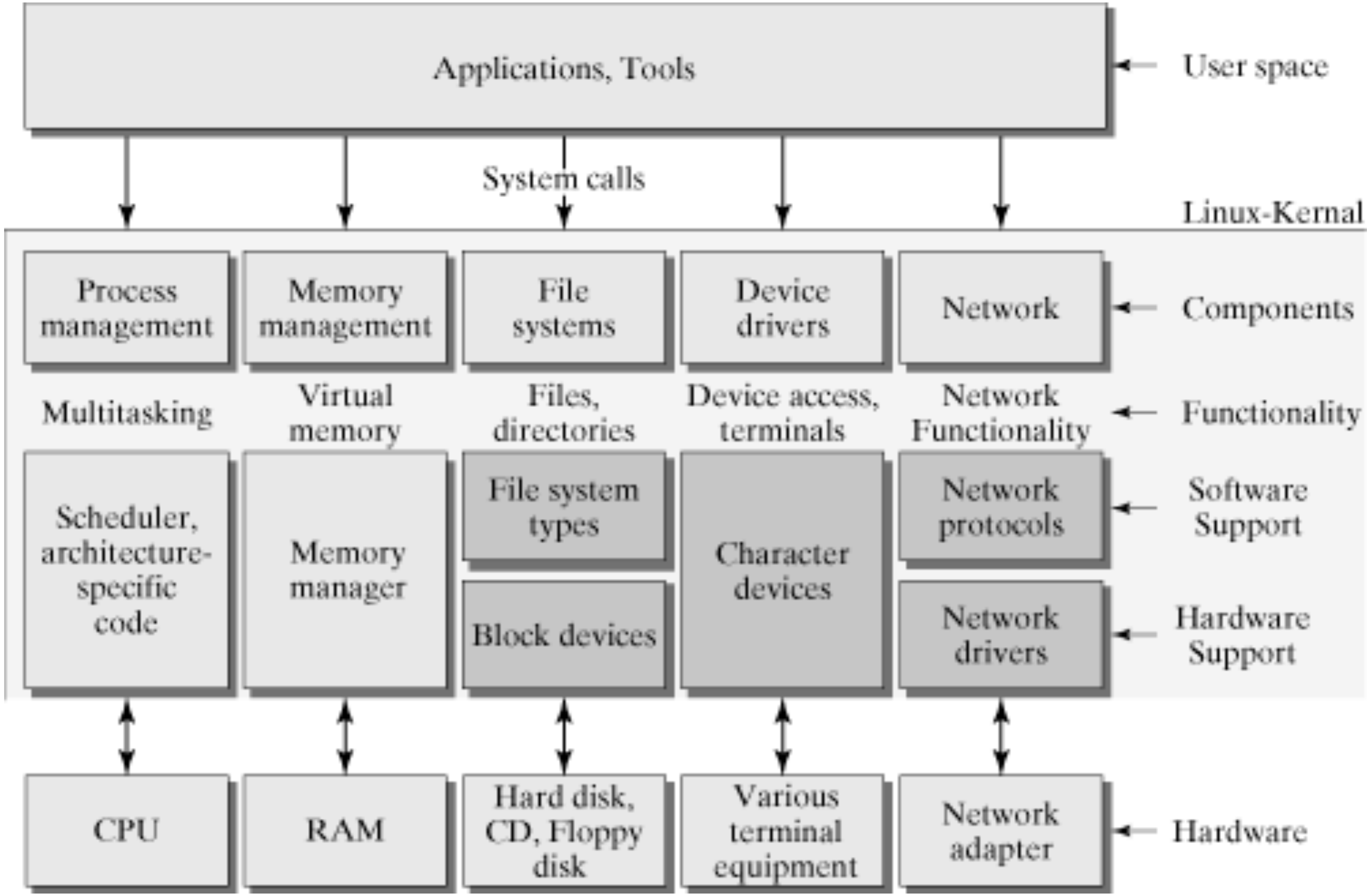

IDA - /home/daniel/Desktop/idag.idb (idag.exe)
File Edit Jump Search View Debugger Options Windows Help
Text
IDA View-A
Hex View-1
Exports
Imports
Names window
Functions window
Strings window
Graph mini view
100.00% (600,1086) (1056,223) 00061517 00461F17: sub_0_461C6B+2AC

Direction 1: Trace-based Exploit Detection

Memory-error Exploit Diagnosis

- Used by security analyst to diagnose vulnerabilities such as buffer overflow
  - The location of buffer overflow is unknown
  - The binary program being exploited and the exploit is known
- Basic workflow
  - Run the binary along with the exploit
  - Record the trace of the whole process of execution
  - Analyze the instruction trace based on the knowledge of attack patterns
    - abnormal register content change
    - abnormal execution path
- Supporting TA: Mingyuan

Linux Kernel



Direction 2: System Auditing Analysis

- Run malicious programs in a monitored environment
- Intercept important system behaviors
  - File access
  - Network connections
  - System calls
  - Other access attempts
- Analyze the recorded behaviors
  - Behavior sequence that looks malicious
  - Building provenance graphs
- Supporting TA: Chuqi

Project Timeline

- Project proposal (Mid-September)
    - Team formed, topic decided (what do you want to understand)
    - Comfortable with initial system setup
- Project progress report (Mid-October)
    - Initial understand into the system w.r.t. the security problem
    - Adjusting directions
- Final report and presentation (End of November)
    - Impressive understanding and your solution
- Optional after-semester activity
    - Short summary of your finding into your CV