Unix Access Control

Variant 0

Recall that RUID stands for "Real User ID", EUID stands for "Effective User ID", and SUID stands for "Saved User ID"; recall also that programs can change their EUID (in restricted ways) by making the seteuid system call.

Suppose that a Unix directory contains the following files with permissions set as shown.
Assume that all SetGID and Sticky bits are turned off.

File Description			*Permissions*			
Filename	*Owner*	*Group*	*SetUID*	*Owner*	*Group*	*Other*
bin.txt	13	13	-	rw-	-w-	---
log.txt	50	50	-	rw-	r--	r--
ron.txt	50	87	-	---	rw-	r--
sys.txt	42	87	-	---	rw-	rw-
rnd.txt	42	42	-	rw-	r--	---
mic.txt	13	87	y	r--	---	rw-
notepad	42	50	-	--x	--x	---
sysutil	0	13	y	--x	--x	---

Assume that user 42 is in groups 42, 87, and 13.
Assume that user 50 is only in group 50.

a. Consider a process running with **RUID=42, EUID=42, and SUID=42**. Assuming no process changes any of the file permissions, which of these files could it **read**?

c. Suppose a process running with **RUID=50, EUID=50, and SUID=50** calls the exec system call to run the program notepad. Assuming no process changes any of the file permissions, which of these files could that instance of **notepad read**?