שם: שמואל ביסברג

ממ"ן 12 שאלה 1

א.

בסרטון מתואר מנגנון ה- GCS - Guarded Control Stack. מנגנון זה מאפשר להפריד את כתובות החזרה של מחסנית הקריאות למידע האחר שנימצא על הBCB. ובנוסף, המנגנון בודק שהכתובת חזרה זהה לכתובת שחוזרים אליה בפועל.

למנגנון זה מספר יתרונות.

1. GCS מגן מפני תקיפות המבוססות על שינוי ערך החזרה של התוכנית (ROP)
2. מאפשר Profiling קל ומהיר יותר בזה שהכתובות לא מכילות את כל המידע של הBCB אלא רק כתובות חזרה.

ב.

מנגנון זה משתייך לכלים של Control Flow Integrity באופן פרטני דומה מאוד לShadow Stack באופן הפעולה שלו.

אך בניגוד לShadow Stack מנגנון זה הוא מוחל בזמן קומפילציה ולא פיצר של חומרה ובכך מובטח שתמיד נריץ את התוכנית באופן בטוח.

ג.

מנגנון זה הוא שינוי של פעולות המכונה ומתאפשר על ידי flag (mbranch-protection=standard) בזמן קומפילציה.

להלן דוגמא עם GCC:

$ gcc -o main.c main -mbranch-protection=standard