דרייברים על קצה המזלג

מי נגד מי ולמה

מה זה בכלל דרייבר

- קוד, כמו כל תוכנה אחרת שקיימת בעולם
- רץ במרחב של מערכת ההפעלה, הkernel (ring 0)
- יודע לקשר בין חומרה לתוכנה
  - לפעמים אין קשר ישיר, אל הדרייבר הוא חלק מstack של בקשה בין תוכנה לחומרה
- יש גם דרייברים שלא קשורים לחומרה (software drivers)

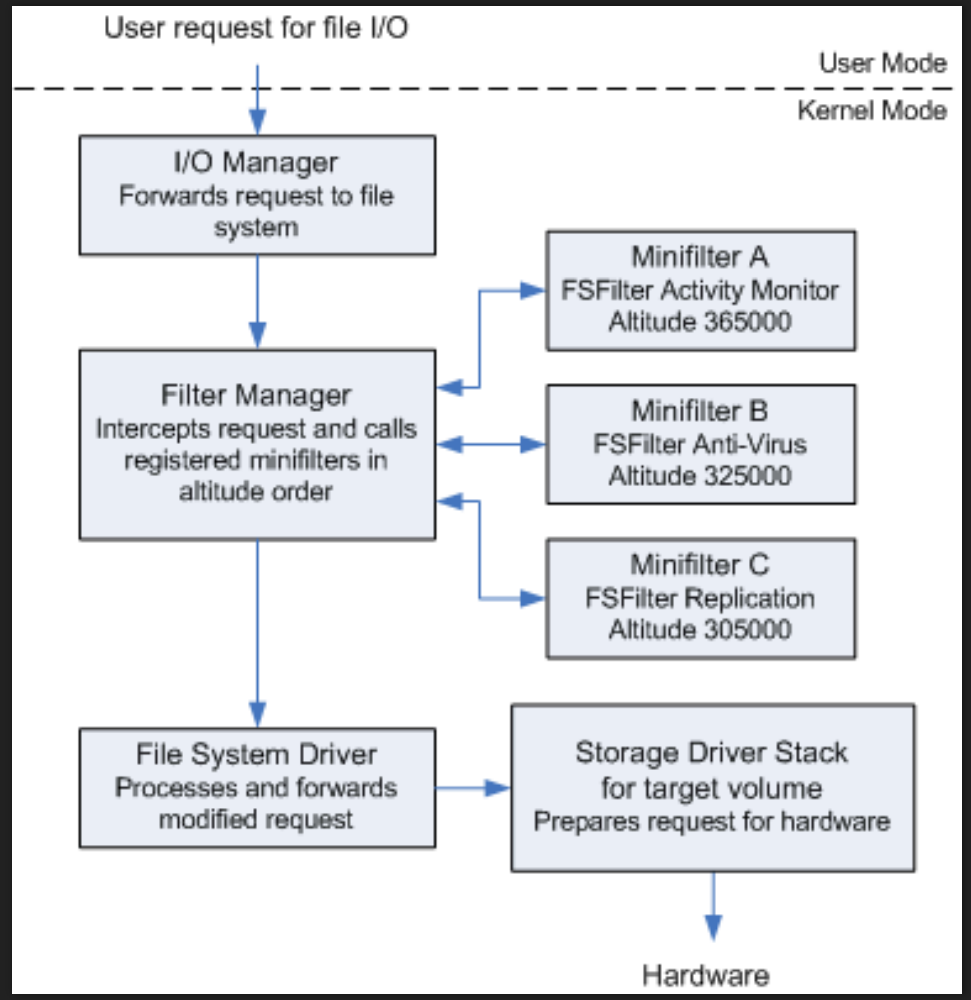
מה אפשר לעשות בדרייברים

1. לנטר על פעולות על קבצים
2. לנטר על פעולות registry
3. לנטר על יצירת processים
4. להסניף ולהוציא פקטות
5. הכל

למה לא לעשות הכל בדרייבר

- מותר לנו לעשות הכל אבל
  - מערכת ההפעלה לא מגנה עלינו מלעשות טעויות ולהרוס לעצמנו את המחשב
  - מערכת ההפעלה לא מגנה עלינו מטעיוות ולכן אנחנו יכולים לגרום לBSOD
  - אם אנחנו מספיק מוכשרים אפשר לגרום לו לקרוס בכל פעם שהוא עולה וככה להרוס לעצמנו את המחשב

עבודה עם קבצים בדרייבר



עבודה עם קבצים בדרייבר

- בקשה של המשתמש
- קוד של מערכת ההפעלה שמבין שמדובר בפעולת I/O
- ממשק של Filter Manager – מנהל את כל הmini filters שיודעים לבצע פעולות על קבצים
  - מעביר את הבקשה דרך הmini filters הרלוונטים
- המשך בקשה לדרייבר שקשור לחומרה

איך mini-filter עובד?

כותבים דרייבר שמייצג אובייקט של mini filter

1. מגדירים לו על אילו פונקציות הוא פועל
2. רושמים אותו לfilter manager
3. מתחילים לפלטר

איך mini-filter עובד?

הmini-filter יכול לפעול על כל פעולת קבצים שניתן לדמיין.

רישום לפעולה הוא למעשה רישום של callback שיקרא כאשר פעולה על קובץ מתבעצת.

הcallback יכול לשנות את המידע/ לחסום את הפעולה/ להעביר אותה הלאה וכו'.

נקודות חשובות לפיתוח דרייברים

- תמיד **אבל תמיד** לבדוק על מכונה וירטואלית
  - לא היינו רוצים לדפוק לעצמנו את המחשב ☹
- מומלץ להיות מחוברים עם kernel debugger
  - באג בדרייבר = קריסה של המחשב. להיות מחוברים עם kernel debugger עוזר לנו לתפוס את הבאג רגע לפני שהמחשב קורס.
- גם printים תמיד עוזרים
  - משתמשים בפונקצייה DbgPrint בדרייברים
- קוראים מלא באינטרנט

מה נעשה היום

נכתוב את הMini-filter הראשון שלנו!

ברגע שהוא יזהה שמישהו רוצה לפתוח קובץ שקוראים לו virus.exe הוא יחסום את הבקשה של המשתמש!