exec

ד"ר כרמי מרימוביץ

אפריל 25, 2017

שימו לב שבדרך־כלל צריך לתקן את מימוש **fork** כאשר משנים את **exec**.

1. מרחב הכתובות שרואה תהליך כרגע מתחיל בכתובת אפס.

   הדגימו שאפשר לקרוא ולכתוב מכתובת אפס של התהליך.

   המצב הנוכחי גורם לכך שבאג (שימוש ב־NULL) לא גורר תעופה מיידית. שנו את מודל הכתובות של תהליך כך שהוא יתחיל מכתובת 4096. שימו לב:

   (א) יש לשנות את פקודת הלינק (ld) של התוכניות.

   (ב) יש לשנות את הרוטינות שבודקות חוקיות ארגומנטים לקריאות מערכת.

   (ג) הדגימו שפנייה לכתובת אפס של התהליך גורמת לתעופה.

2. (א) כרגע מחסנית התהליך מופרדת משטח הקוד/נתונים על־ידי ה־guard page. שנו את מיקום המחסנית לסוף טווח הכתובות החוקי של שטח המשתמש. בשיטה זו אין צורך ב־guard page. הוסיפו את השדה szsp למבנה proc. שדה זה יכיל את הכתובת החוקית הנמוכה ביותר עבור המחסנית. שימו לב שיש להתאים את רוטינות בדיקת הארגומנטים כי מודל התהליך החדש כולל שני תחומי כתובות חוקיים.

   (ב) (קשה) הגדילו את המחסנית באופן דינמי כאשר יש גישה לדף הצמוד ישר מתחת למחסנית.