פרויקט באבטחת מידע 236349

מחשב גישור מעל מערכת הפעלה בטוחה

מנחה: ד"ר איתן קוך [etankoch@gmail.com](mailto:etankoch@gmail.com)

1. **רקע**

מחשב גישור – Cross Domain Guard נועד להפריד בין סביבות בעלות רמות סודיות שונות (למשל סודי לעומת בלמ"ס), וסביבות בעלות רמות אמינות שונות (אינטרנט לעומת סביבה מאובטחת).

מחשב גישור צריך להיות בעל רמת חסינות גבוהה מאד כדי שיהיה עמיד בפני תקיפות סייבר מצד הסביבות ביניהן הוא מפריד. כפועל יוצא מכך מחשב הגישור צריך להתבסס על מערכת הפעלה מאובטחת, וכן להיות כתוב בעצמו בצורה מאובטחת.

במקרה של סביבות ברמות סודיות שונות, מחשב הגישור צריך לוודא שמידע ברמת סיווג גבוהה לא יעבור לסביבה בעלת רמת סיווג נמוכה יותר. במקרה של סביבות ברמות אמינות שונות, מחשב הגישור צריך לוודא שהסביבה ברמת אמינות גבוהה לא תותקף ע"י הסביבה ברמת אמינות נמוכה יותר.

לצורך זה מחשב הגישור צריך לסנן את **תוכן** ההודעות המועברות בין הסביבות השונות. הסינון מתבצע על פי חוקי סינון קשיחים הקובעים את מבנה ההודעות, קצב ההודעות, גודלן, תלות בסדר ההודעות, פורמט השדות השונים המרכיבים כל הודעה, תחומי ערכים של כל שדה, וכו'.

יודגש שמחשב גישור שונה מ-FW רגיל בכך שהוא חוסם או מרשה מעבר על פי רמות סיווג של תוכן החבילות והתוכן עצמו. כלומר, בעוד ש-FW רגיל בוחן את החבילות המועברות **ברמה התקשורתית**, לדוגמה כתובת IP, פורט, שברור, פרוטוקולי תקשורת וכו', מחשב הגישור מתייחס בעיקר **לתוכן** **ההודעות ברמה האפליקטיבית**, ואמור למנוע העברת מידע מסווג או קוד עוין. מחשב גישור מתייחס לפרוטוקול הודעות מצומצם ואפליקטיבי בלבד – בדר”כ פרוטוקול ייעודי בעל מבנה מוגדר וקבוע. דוגמאות לפרוטוקולים כאלה כוללות למשל תקשורת 1553 (רשתות של מטוסים להן יש פרוטוקול תקשורת ומבנה הודעות פשוטים וחוזרים על עצמם בחבילות מוגבלות בגודלן בכמה עשרות בתים), CAN bus (רשתות פנימיות של מכוניות שמוגבלות במקורן לשמונה בתים בכל חבילה), וגם פרוטוקולים אפליקטיביים מסוימים שרצים מעל TCP/IP.

מחשב הגישור מורכב משלוש מחיצות, A, B, C, כאשר מחיצה A קולטת את ההודעות מסביבה אחת ומעבירה אותן אך ורק למחיצה B, אשר מפעילה על ההודעות את חוקי הסינון ואם הן עומדות בחוקים, אזי הן מועברות למחיצה C ומשם, ורק משם, מועברות לסביבה השנייה. יודגש שמחשב הגישור בנוי כך שלא ניתן לעקוף את מחיצה B, כלומר A אינה יכולה לתקשר ישירות עם C אלא רק עם B, וגם B יכולה להעביר הודעות אך ורק ל-C (במקרה של הודעות הזורמות בכיוון הפוך, ניתן להגדיר מחיצות A’, B’, C’, אך לא נידרש לכך במסגרת הפרויקט).

1. **מטרה**

מטרת הפרויקט היא כפולה: האחת, לבנות מחשב גישור שירוץ מעל מערכת הפעלה מאובטחת QUBES, המורצת מעל הייפרוויזור מאובטח XEN (הן QUBES והן XEN רצים בסביבת אינטל, ויש להתקינם במחשב PC במעבדה לאחר פירמוט הדיסק הקשיח). והשנייה, לנסות לבחון איך ניתן לעקוף את מנגנוני ההגנה של מחשב הגישור, ולהעביר מידע מצד לצד למרות קיומם.

1. **מטלות הפרויקט**
   1. לימוד נושא מחשב גישור, מערכת הפעלה QUBES והיפרוייזור XEN, כולל המנגנונים המאפשרים תקשורת מוגבלת בין המחיצות השונות.
   2. אפיון ותיכון: תוכנה של מחשב גישור שירוץ מעל מערכת ההפעלה וההיפרוייזור הנ"ל, תוכנה להגדרת קובץ החוקים של ההודעות המותרות בין הסביבות ביניהן מגשר המחשב, תוכנה לחילול הודעות שתועברנה בין הסביבות דרך מחשב הגישור.
   3. ניסיון לעקוף את מנגנוני QUBES האוכפים תקשורת בלעדית בין A ל-B ובין B ל-C, ולאפשר תקשורת בערוצים סמויים בין מחיצות A ו-C.
   4. קידוד תוכנת מחשב הגישור כולל וידוא חסינות התוכנה והתשתית. קידוד תוכנה לקביעת החוקים לעיל, קידוד תוכנה לחילול הודעות שתועברנה בין הסביבות.
   5. חיפוש דרכים לביצוע ערוצים סמויים, קידוד ערוצים סמויים.
   6. בדיקות, הדגמת הפרויקט.
   7. וכמובן כל שאר חובות הקורס (מצגות, דו”ח סיום, וכו’).
2. **הערכת המימוש של הפרויקט** תתבצע בין השאר על פי הפרמטרים הבאים:
   1. מימוש מחשב הגישור
   2. מידת ההבנה והעומק של מנגנוני מערכת ההפעלה והשימוש בהם, בפרט במימוש מחשב הגישור.
   3. מידת המורכבות של מנגנוני הסינון כתלות בפרוטוקול האפליקטיבי שיבחר/יוגדר.
   4. הצלחה במימוש ערוץ סמוי כמוסבר לעיל, ומגוון ועומק הרעיונות שנוסו לשם כך.

זאת בנוסף לפרמטרי ההערכה הרגילים של הקורס.