

# 50239 - סייבר למערכות זמן אמת Cyber for real time systems

אופן הוראה: שיעור ותרגול  
שעות שבועיות: 4  
נקודות זכות: 3.5  
דרישות קדם: 50224 מערכות הפעלה זמן אמת במקביל

## מטרת הקורס:

הכרת הטכנולוגיות הנפוצות להתקפות סייבר למערכות זמן אמת (tampering) של שינויי קוד והגנות כנגד שינויים בקוד (anti-tampering). במסגרת הקורס נתמקד בארכיטקטורת אינטל ונלמד את קווי ההגנה המרכזיים נגד התקפות סייבר של מערכות זמן אמת בארכיטקטורות אחרות.

## הנושאים שיילמדו בקורס:

1. טמפרינג. מטרות יעדים. סוגים של גישה למכונה, ניתוח סיכונים, ניהול סיכונים
2. מבוא לאסמבלר
3. שיטות "טמפרינג" בקוד: הנדסה אחורה (REVERSE ENGINEERING), הזרקת קוד והשתלת קוד.
4. intel TXT TCG API gTPM trusted computin
5. פיתוח בסביבות אנטי טמפרינג
6. ARM Trustzone
7. התקפות ערוץ צד (side channel attacks)
8. אסמבלר מתקדם
9. בהנתן זמן : נושאים מודרניים. הגנה באמצעות וירטואליזציה סביבת מיקרוסופט ברומיום אינטל SGX ואחרים.

## ספר לימוד:

Practical Reverse Engineering: x Bruce Dang, Alexandre Gazet, Elias Bachaalany, Sebastien Josse

Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation 2014 ISBN 1118787315

## חומר עזר :

1. Reversing: Secrets of Reverse Engineering
2. Intel system programming  
<http://www.intel.com/content/dam/www/public/us/en/documents/manuals/64-ia-32-architectures-software-developer-system-programming-manual-325384.pdf>