נושאים מתקדמים באבטחת מידע
אבטחת מחשבים
נושאים מתקדמים 7 - 236607
סמסטר אביב תשע"ח

שם המרצה: דר' שרה ביתן

היקף הקורס: שעות הרצאה: שתיים, שעות תרגול: אחת

דרישות קדם: מערכות הפעלה

מטרות הקורס:

1. הצגת חולשות ותקיפות על מ"ה עדכניות
2. הצגת עקרונות אבטחת מידע דוגמת מזעור זכויות, הפרדת רשויות, הפרדה ובידוד
3. הצגת מנגנוני Sandboxing בחומרה ובתוכנה
4. הצגת פתרונות "סביבת מחשוב אמינה" (TEE) משולבי חומרה תוכנה

מרכיבי הציון: 70% ציון בחינה. 30% ציון תרגילים. כל עבודות הבית שוות במשקלן.

סילבוס:

1. מבוא
   - הגדרת גבולות גזרה
   - מודל האיום
2. חולשות, התקפות ועקרונות הגנה
   - דוגמאות של חולשות
   - PE: Privileges elevation
3. ניתוח סיכונים ושטח פני ההתקפה
4. בקרת גישה
   - שיטות בקרת גישה: DAC, MAC, RBAC
   - בקרת גישה מבוססת שיקול דעת (DAC):

- בקרת גישה ב-Linux וב-Windows, Linux Capabilities
- בקרת גישה כפויה (MAC)
- LSM – Linux Security Module
- SeLinux

5. אבטחה ב-Android
   - מודל האבטחה של Android
   - בידוד והפרדה ב-Android
   - Dalvik, Android name spaces
   - הרשאות ב-Android
   - ה-Manifest
   - Android Binder ו-MAC
   - Rooting
6. הפרדה ובידוד:
   - וירטואליזציה - Hypervisors, containers
   - תמיכה בחומרה: AMD-V, Intel VT, ARM
   - Blue Pill malware
   - Separation Kernel
7. סביבת מחשוב (Trusted Execution Environment):
   - TC: Trusted Computing & TPM
   - Intel TXT
   - Intel SGX (Software Guard Extensions)
   - AMD SME, SVE

ביבליוגרפיה :

- Android Security Internals: An In-Depth Guide to Android's Security Architecture by Nikolay Elenkov, October 2014, 432 pp, No Scratch Press.
- Android Hacker's Handbook 1st Edition, by Joshua J. Drake, et al. John Wiley & Sons, 2014
- The Flask Security Architecture: System Support for Diverse Security Policies, Ray Spencer et al. USENIX Security 1999.
- Linux Security Modules - General Security Support for the Linux Kernel, Chris Wright et al. USENIX Security 2002.
- Implementing SELinux as a Linux Security Module, Stephan Smalley et al. 2006.
- Trustworthy Execution on Mobile Devices: What security properties can my mobile platform give me? Amit Vasudevan et al. CMU technical report, 2011
- Flicker: An Execution Infrastructure for TCB minimization, Jonathan M. McCune et al. The European Conference on Computer Systems (EuroSys), April 2008.
- Intel SGX Explained, Victor Costan and Srinivas Devadas, *Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology*