סמינר במדעי המחשב – 236802
סמסטר חורף תש"פ

סמינר באימות אוטומטי עבור תכונות אבטחה

מרצה: דר' יקיר ויזל
יום ג' 1430-1630

דרישות קדם:
לוגיקה ומבוא לאימות תוכנה או ניסיון בתחום (באישור המרצה).

סילבוס:
הסמינר יעסוק באלגוריתמים ושיטות לאימות פורמלי עם דגש על אימות של תכונות אבטחה. הנושאים יכללו: אימות פורמלי מבוסס SAT ו-SMT, אימות של הייפר-תכונות (hyper-properties), אלגוריתמים סטטיים ודינמיים לזיהוי של side-channel attacks ועוד.

דרישות הקורס:
- נוכחות חובה.
- קריאה והצגה של מאמר אקדמי (או שניים).
- השתתפות פעולה בדיון בנושא שמוצג ונידון בהרצאה

רשימת ספרות (חלקית):

1. D. Basin, S. Mödersheim, L. Viganò - OFMC: A symbolic model checker for security protocols.
2. A. Armando and L. Compagna - SAT-based model-checking for security protocols analysis
3. B. Blanchet - Automatic Verification of Security Protocols in the Symbolic Model: The Verifier ProVerif
4. T. Terauchi, A. Aiken - Secure Information Flow as a Safety Problem.
5. W Yang, Y. Vizel, P. Subramanyan, A. Gupta, S. Malik - Lazy Self-composition for Security Verification
6. Clarkson and Schneider – Hyperproperties.
7. M. Backes, B Kopf, A Rybalchenko - Automatic Discovery and Quantification of Information Leaks.
8. JB. Almeida, M. Barbosa, G. Barthe, F. Dupressoir, M. Emmi - Verifying Constant-Time Implementations
9. R. Shemer, A. Gurfinkel, S. Shoham, and Y. Vizel - Property Directed Self Composition
10. E. Schwartz, T. Avgerinos, and D. Brumley - All You Ever Wanted to Know about Dynamic Taint Analysis and Forward Symbolic Execution (but Might Have Been Afraid to Ask).
11. R. Bloem, S. Jacobs, Y. Vizel - Efficient Information-Flow Verification under Speculative Execution
12. T. Antonopoulos, P. Gazzillo, M. Hicks, E. Koskinen, T. Terauchi, and S. Wei. - Decomposition instead of self-composition for proving the absence of timing channels
13. M. Sousa and I. Dillig. Cartesian Hoare Logic for verifying k-safety properties.
14. G. Barthe, J. M. Crespo, and C. Kunz. Relational verification using product programs.
15. J. Chen, Y. Feng, and I. Dillig. Precise detection of side-channel vulnerabilities using quantitative cartesian hoare logic.
16. M. G. Kang, S. McCamant, P. Poosankam, and D. Song. DTA++: Dynamic Taint Analysis with Targeted Control-Flow Propagatio
17. A. Farzan, A. Vandikas - Reductions for Automated Hypersafety Verification