Chair of Security in Information Technology
TUM Department of Electrical and Computer Engineering
Technical University of Munich

Seminar

Solving Reverse Engineering Issues with Graph Theory Solutions?

Gate-level netlist reverse engineering is basically graph analysis. The single gates and wires of a netlist can be interpreted as a graph structure. During sequential reverse engineering, this graph is analyzed in order to identify and extract the control logic. For this purpose, the first analysis step is the classification of state and data flip-flops in this gate-level netlist graph. To solve this classification problem, a number of different methods are already developed and investigated. One promising method (RELIC), which is proposed by T. Meade et. al., determines similarity scores which represent the similarities between flip-flop input structures. Based on the results, the flip-flops are classified.

This seminar work should first give a general overview of already existing graph node similarity score algorithms. In a second step, it should analyze and discuss which of these could be used as alternatives to the similarity score algorithm of RELIC.

References

- Zager, L. A., & Verghese, G. C. (2008). Graph similarity scoring and matching. Applied mathematics letters, 21(1), 86-94.
- Meade, T., Jin, Y., Tehranipoor, M., & Zhang, S. (2016, May). Gate-level netlist reverse engineering for hardware security: Control logic register identification. In Circuits and Systems (ISCAS), 2016 IEEE International Symposium on (pp. 1334-1337). IEEE.

Contact

Request Topic

Advisors

Michaela Brunner