Master project in Information Security at the University of Luxembourg

Title: Performing risk assessment by solving known problems in graph theory

The Security and Trust of Software Systems group, led by Prof. Dr. Sjouke Mauw, is looking for outstanding master students who want to develop their master thesis within our group.

Project description

Attack trees, popularized by Bruce Schneier [5], are a widely used graphical modeling language in risk assessment. The root of an attack tree represents the attacker goal, and its children are either different ways to achieve the attack (in disjunctive form) or necessary steps to satisfy the attacker goal (in conjunctive form). Considering each root's child a goal itself, the attack tree can be further developed up to any desired level of granularity.

As a visual mean, attack trees are simple and intuitive enough to attract security practitioners. As a risk analysis tool, on the other hand, attack trees have been provided with powerful quantification methods that can determine a huge variety of security-related attributes, such as probability, cost, and impact of an attack. Nevertheless, most of these quantification methods have the limitation that they are tightened to the tree structure, which abstracts away from details necessary to compute other type of security-related attributes.

Casi in point, we may ask for the minimum number of edges we need to remove from an attack tree in such a way that attacks of low-skilled attackers are unfeasible while attacks of high-skilled attackers remain feasible. We can intuitively interpret a solution to this problem as the smallest set of countermeasures required to avoid attacks from, for example, script kiddies. It is apparent that such a problem cannot be solved in a bottom-up approach is the one intuitively sketched by Bruce Schneier [5].

General goal. In this project we will investigate the impact of different problems in graph theory on the analysis of attack trees. For example, the maximum-weightsum problem [4], the partial constraint satisfaction problem [2], and the quadratic $0-1$ knapsack problem [3]. All these problems are efficiently solvable in SP graphs, i.e., they can be solved on the semantical representation of attack trees [1]. We will use our findings to analyze the security of different cases studies within the European FP7 project TREsPASS.

Contact Information

For further inquiries please contact:

- Prof. Dr. Sjouke Mauw (`sjouke.mauw@uni.lu`) or
- Dr. Rolando Trujillo (`rolando.trujillo@uni.lu`)

References

[1] Ravi Jhawar, Barbara Kordy, Sjouke Mauw, Sasa Radomirovic, and Rolando Trujillo-Rasua. Attack trees with sequential conjunction. In *ICT Systems Security and Privacy Protection - 30th IFIP TC 11 International Conference, SEC 2015, Hamburg, Germany, May 26-28, 2015, Proceedings*, pages 339–353, 2015.

[2] Arie M.C.A. Koster, C.P.M. van Hoesel, and A.W.J. Kolen. Solving partial constraint satisfaction problems with tree decomposition. *Networks*, 40(3):170–180, 2002. http://dx.doi.org/10.1002/net.10046.

[3] David J. Rader Jr. and Gerhard J. Woeginger. The quadratic 0-1 knapsack problem with series-parallel support. *Oper. Res. Lett.*, 30(3):159–166, June 2002.

[4] Isao Sasano, Zhenjiang Hu, Masato Takeichi, and Mizuhito Ogawa. Make it practical: A generic linear-time algorithm for solving maximum-weightsum problems. In *Proceedings of the Fifth ACM SIGPLAN International Conference on Functional Programming*, ICFP '00, pages 137–149, New York, NY, USA, 2000. ACM.

[5] Bruce Schneier. Attack Trees: Modeling Security Threats. *Dr. Dobb's Journal of Software Tools*, 24(12):21–29, 1999.