Abduction as Diagnostic Tool in Computer Security

Martin Homola and Júlia Pukancová

Comenius University in Bratislava, Mlynská dolina, 84248 Bratislava, Slovakia

Abduction [3] is a type of inference, where we have model of some situation or system and we observe some effects that are not supported by this model deductively – abduction looks for hypothetical explanations that can be added to the model in order for the observation to be supported.

To borrow a brief example from a medical domain, assume condition $C1$ causes symptom $S1$ and condition $C2$ causes symptoms $S1$ and $S2$. If we observe $S1$ in a patient, then both $C1$ and $C2$ are plausible explanations for the observation. If, in addition, we observe $S2$, then the explanations narrow down to $C2$.

The model can be of anything, say medical conditions and symptoms [5], manufacturing system [2], or a scene from a sporting event observed by a computer vision software [4].

Abduction offers a flexible framework suitable for diagnosing complex models where there are overlapping symptoms of different conditions, and where one condition may be symptom of another, and so on. Abduction may guarantee to find minimal (or weakest) diagnoses and thus avoid hypothesizing more than it is required [1, 5] which is useful in most application scenarios.

In this presentation we will provide typical examples of abduction applications and we will discuss its possible applications in the area of computer security.

Acknowledgents. This work was partially supported by projects ORBIS, funded by Slovak SRDA agency under contract No APVV-19-0220, KATO, funded by Slovak VEGA agency under contract No 1/0778/18, and by TAILOR, funded by EU Horizon 2020 research and innovation programme under GA No 952215.

References

1. Elsenbroich, C., Kutz, O., Sattler, U.: A case for abductive reasoning over ontologies. In: Proceedings of the OWLED*06 Workshop on OWL: Experiences and Directions, Athens, GA, US. CEUR-WS, vol. 216 (2006)
2. Hubauer, T., Legat, C., Seitz, C.: Empowering adaptive manufacturing with interactive diagnostics: A multi-agent approach. In: Advances on Practical Applications of Agents and Multiagent Systems – 9th International Conference on Practical Applications of Agents and Multiagent Systems, PAAMS 2011, Salamanca, Spain. pp. 47–56 (2011)
3. Peirce, C.S.: Illustrations of the logic of science VI: Deduction, induction, and hypothesis. Popular Science Monthly **13**, 470–482 (1878)

4. Petasis, G., Möller, R., Karkaletsis, V.: BOEMIE: Reasoning-based information extraction. In: Proceedings of the 1st Workshop on Natural Language Processing and Automated Reasoning co-located with 12th International Conference on Logic Programming and Nonmonotonic Reasoning (LPNMR 2013), A Corunna, Spain. pp. 60–75 (2013)
5. Pukancová, J., Homola, M.: Abductive reasoning with description logics: Use case in medical diagnosis. In: Proceedings of the 28th International Workshop on Description Logics (DL 2015), Athens, Greece. CEUR-WS, vol. 1350 (2015)