More than Zero: Diagnosing unknown attacks using abductive reasoning

Kushal Ramkumar, Wanling Cai, Gavin Doherty, John McCarthy, Bashar Nuseibeh, Liliana Pasquale

1

Unknown attacks are on the rise and pose a major challenge to providing sustainable security

Zero-Day Attacks

Technical Blind Spots

For long lived systems such as smart homes, providing enduring security requires

DETECTION
behavioural anomalies

DIAGNOSIS
violated security requirements

MITIGATION
select security controls

References:

1. Mady Stone. 2022. The More You Know, The More You Know You Don't Know (April 2022). Retrieved September 20, 2022 from https://googleprojectzero.blogspot.com/2022/04/the-more-you-know-more-you-know-you.html
2. Pasquale, L., Ramkumar, K., Cai, W., McCarthy, J., Doherty, G., & Nuseibeh, B. (2023). Sustainable Adaptive Security. arXiv preprint arXiv:2306.04481.

2

Research Objective: to implement a novel technique that **detects** (anomaly detection) and **diagnoses** (abductive reasoning) *unknown attacks* in a smart home

Terminology

- **Diagnosis:** identification of violated security requirement[1] and class of attack of an anomaly
- **Abductive reasoning:** process that maps effect to cause, to generate explanations.

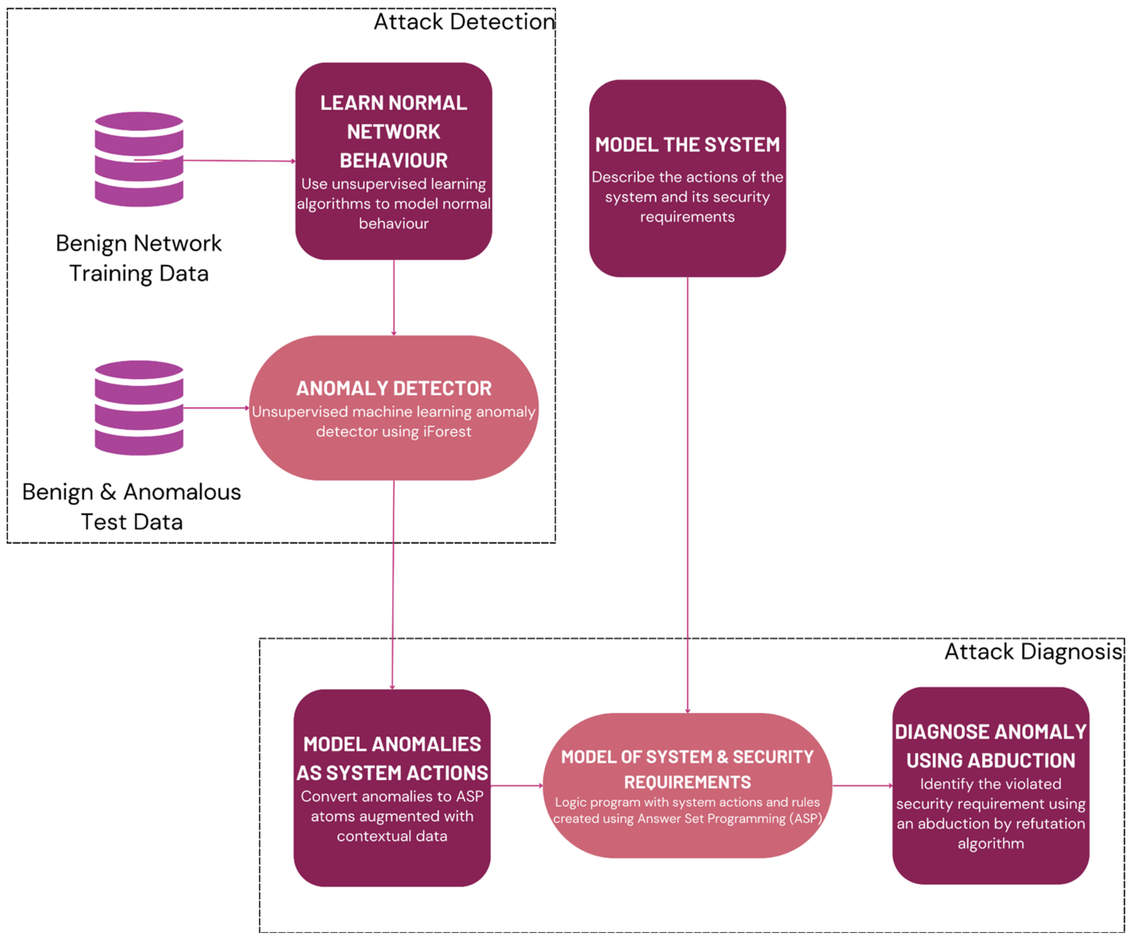
Techniques

- **Answer set programming (ASP):** declarative programming paradigm that identifies violations of the rules that govern a given model
- **Abduction by refutation:** identify which conditions (security requirements) prevent a contradiction (anomaly) from existing

References:

1. Haley, C., Laney, R., Moffett, J., & Nuseibeh, B. (2008). Security requirements engineering: A framework for representation and analysis. IEEE Transactions on Software Engineering, 34(1), 133-153.Chicago
2. Paul, G. (1993). Approaches to abductive reasoning: an overview. *Artificial intelligence review*, *7*(2), 109-152.
3. Kaminski, R., Schaub, T., & Wanko, P. (2017). A tutorial on hybrid answer set solving with clingo. *Reasoning Web. Semantic Interoperability on the Web: 13th International Summer School 2017, London, UK, July 7-11, 2017, Tutorial Lectures 13*, 167-203.
4. Russo, A., Miller, R., Nuseibeh, B., & Kramer, J. (2002). An abductive approach for analysing event-based requirements specifications. In *Logic Programming: 18th International Conference, ICLP 2002 Copenhagen, Denmark, July 29-August 1, 2002 Proceedings 18* (pp. 22-37). Springer Berlin Heidelberg.

3 OUR TECHNIQUE:



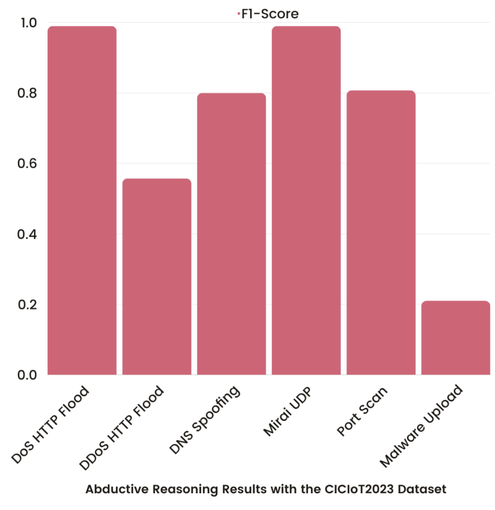
4 EVALUATION:

Datasets: **CICIoT2023** and **IoT-23** contain 18 attacks against 8 real devices

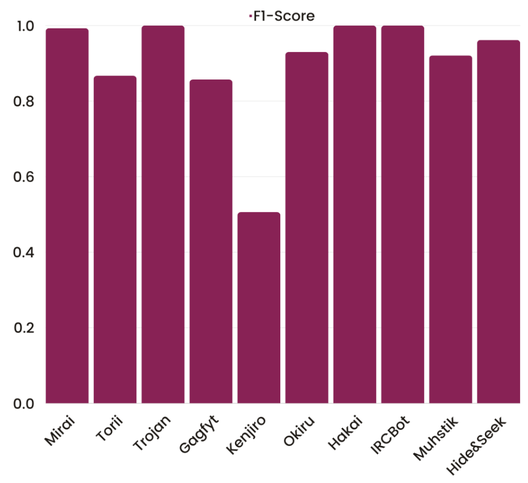
Metric: **F1-score** for a balance of identifying most anomalies (recall) with detecting true anomalies (precision).

Results:

- **Detection:** Anomaly detector shows **f1-score > 0.80**.
- **Diagnosis:** With sufficient *contextual data*, effectively *reduces false positives* of the anomaly detector and *identifies violated security requirements* with an **f1-score > 0.83**.



Abductive Reasoning Results with the CICIoT2023 Dataset



Abductive Reasoning Results with the botnet attacks in the IoT-23 Dataset

Discussion:

- The anomaly detection technique is effective when the benign and malicious data show distinct behaviours (see HTTP Flood and Malware Upload).
- The performance of the diagnosis technique is dependent on the contextual factors provided (see Kenjiro botnet misdiagnosed as DoS instead of DDoS)

HOST INSTITUTION

UNIVERSITY OF LIMERICK
OLLSCOIL LUIMNIGH

PARTNER INSTITUTIONS

Ollscoil na Gaillimhe University of Galway · Maynooth University National University of Ireland Maynooth · Trinity College Dublin, Coláiste na Tríonóide, Baile Átha Cliath, The University of Dublin · University College Dublin, An Coláiste Ollscoile, Baile Átha Cliath · UCC University College Cork, Ireland, Coláiste na hOllscoile Corcaigh · MTU Ollscoil Teicneolaíochta na Mumhan, Munster Technological University · DCU · SETU South East Technological University · Dundalk Institute of Technology, Institiúid Teicneolaíochta Dhún Dealgan · TUS · ATU

FUNDED BY:

Ireland's European Structural and Investment Funds Programmes 2014-2020, Co-funded by the Irish Government and the European Union · European Union, European Regional Development Fund · Science Foundation Ireland sfi For what's next