### **MONID**

A Temporal Logic Based Framework for Intrusion Detection

#### Zanolin Lorenzo<sup>1</sup>

<sup>1</sup>DMIF University of Udine

September 2023



## **Table of Contents**



1. Introduction



## **Intrusion Detection**



Intrusion detection means maintaining constant surveillance on a system in order to detect any misuse of these weak areas as soon as feasible so that they can be repaired.

There are three approaches:

- signature-based: aims to identify patterns and match them with known signs of intrusions;
- anomaly-based: can identify new attacks when it detects behavior that differs significantly from previously learned normal behavior;
- hybrid: combines the best of both worlds by looking at patterns and one-off events.

We will present MONID which is a signature-based intrusion detector.

## What is MONID?



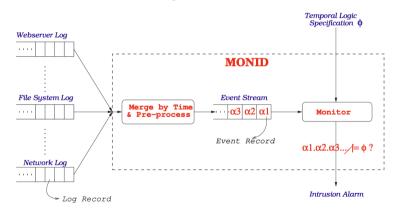
MONID is a prototype which can detect intrusions on a system and operates in both online and offline modes.

#### In order:

- 1. we will use the logic **EAGLE** to define intrusion patterns using temporal logic formula  $\varphi$ ; in this case the monitored formula will be  $\psi = \Box(\neg \varphi)$ .
- 2. MONID will create a stream of events  $\sigma = \alpha_1, \alpha_2, \ldots$  obtained from a merge of the logs by ascending time order;
- 3. a monitor will processes each event  $\alpha_i$  as it happens and updates the monitored formula  $\psi$  to store a relevant summary;
- **4**. an intrusion alarm is triggered if, for any reason,  $\alpha_1, \alpha_2 \dots \not\models \psi$ .

# What is MONID? (cont'd)

The architecture is the following.



Now, let us start from the basics of EAGLE.



## References I

- [1] Howard Barringer et al. "EAGLE can do Efficient LTL Monitoring". In: Fossacs Ortacas. 2003.
- [2] Howard Barringer et al. "Program monitoring with LTL in EAGLE". In: 18th International Parallel and Distributed Processing Symposium, 2004. Proceedings. IEEE. 2004, p. 264.
- [3] Howard Barringer et al. "Rule-based runtime verification". In: Verification, Model Checking, and Abstract Interpretation: 5th International Conference, VMCAI 2004 Venice, Italy, January 11-13, 2004 Proceedings 5. Springer. 2004, pp. 44–57.
- [4] Wei Gao and Thomas H Morris. "On cyber attacks and signature based intrusion detection for modbus based industrial control systems". In: *Journal of Digital Forensics, Security and Law* 9.1 (2014), p. 3.

## References II



- [5] Akash Garg and Prachi Maheshwari. "A hybrid intrusion detection system: A review". In: 2016 10th International Conference on Intelligent Systems and Control (ISCO). IEEE. 2016, pp. 1–5.
- [6] VVRPV Jyothsna, Rama Prasad, and K Munivara Prasad. "A review of anomaly based intrusion detection systems". In: *International Journal of Computer Applications* 28.7 (2011), pp. 26–35.
- [7] Urupoj Kanlayasiri, Surasak Sanguanpong, and Wipa Jaratmanachot. "A rule-based approach for port scanning detection". In: *Proceedings of the 23rd electrical engineering conference, Chiang Mai Thailand*. Citeseer. 2000, pp. 485–488.

## **References III**



- [8] John McHugh. "Testing intrusion detection systems: a critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by lincoln laboratory". In: ACM Transactions on Information and System Security (TISSEC) 3.4 (2000), pp. 262–294.
- [9] Prasad Naldurg, Koushik Sen, and Prasanna Thati. "A temporal logic based framework for intrusion detection". In: Formal Techniques for Networked and Distributed Systems—FORTE 2004: 24th IFIP WG 6.1 International Conference, Madrid Spain, September 27-30, 2004. Proceedings 24. Springer. 2004, pp. 359–376.
- [10] Krerk Piromsopa and Richard J Enbody. "Buffer-overflow protection: the theory". In: 2006 IEEE International Conference on Electro/Information Technology. IEEE. 2006, pp. 454–458.

## **References IV**

[11] Gholam Reza Zargar and Peyman Kabiri. "Identification of effective network features to detect Smurf attacks". In: 2009 IEEE Student Conference on Research and Development (SCOReD). IEEE. 2009, pp. 49–52.

# Thanks for the attention