MONID

A Temporal Logic Based Framework for Intrusion Detection

Zanolin Lorenzo[1]

[1]DMIF
University of Udine

September 2023

UNIVERSITÀ
DEGLI STUDI
DI UDINE
hic sunt futura

Table of Contents

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? I

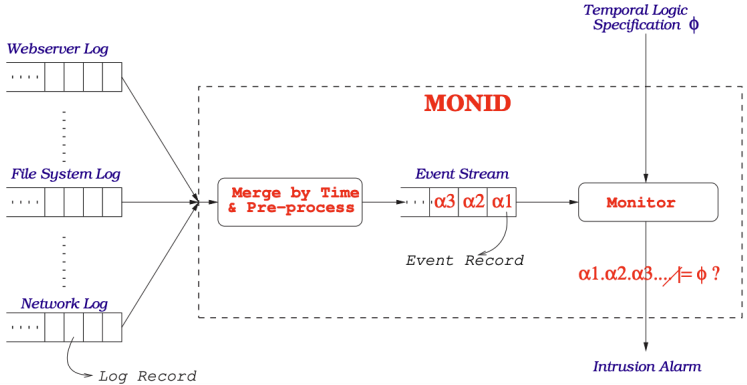
MONID is a prototype which can detect intrusions on a system and operates in both online and offline modes.

In order:

1. we will use the logic **EAGLE** to define intrusion patterns using temporal logic formula φ; 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 α_i as it happens and updates the monitored formula ψ to store a relevant summary;
4. an intrusion alarm is triggered if, for any reason, $\alpha_1, \alpha_2 \ldots \not\models \psi$.

What is MONID? II

The architecture is the following.



Assumptions

Two assumptions must be made:

1. There is a finite sequence of events called $\sigma = \alpha_1, \ldots, \alpha_n$ that is a merge of the system registered logs organized by ascending time. The structure of an event record α_i is the following:

   $$\texttt{LoginLogoutEvent}\{userId : \underline{\text{string}},\ action : \underline{\text{int}},\ time : \underline{\text{double}}\}$$

   An example of event could be:
   $\{userId : \text{"}\texttt{Lori}\text{"},\ action : \texttt{login},\ time : 20\}$
2. For each attack, there is a formula ψ which specifies the absence of it.

Now let us start on the basics of EAGLE.

EAGLE, a Temporal Monitoring Logic

Basics I

EAGLE offers a succinct but powerful set of primitives, supporting recursive parameterized equations with a minimal/maximal fix-point semantics together with three temporal operators: next-time ($\bigcirc$), previous-time ($\odot$), and concatenation ($\cdot$).

As a result, rules in EAGLE give us the power to create specific temporal operators as well as to bind and modify data. This property turns out to be crucial for succinctly expressing executions of attack-safe systems.

EAGLE operates with *finite trace* semantics, meaning it checks formula satisfaction only at the end of a trace. However, in intrusion detection where event sequences can be infinite, the goal is to trigger an alarm as soon as a property is violated, thus MONID continuously checks the formula's satisfaction status after each event.

Basics II

Let us start with an example.

Example 1

We want to express the property "*Whenever there is a login by any user x, then eventually the user x logs out*". In EAGLE we can do it with the following rules:

$$\underline{\textit{min}}\ \texttt{EvLogout}(\underline{\textit{string}}\ k) = (action = \texttt{logout} \wedge userId = k) \vee \bigcirc \texttt{EvLogout}(k)$$
$$\underline{\textit{mon}}\ M_2 = ((action = \texttt{login}) \rightarrow \texttt{EvLogout}(userId))$$

Once the rules are created, the monitor will evaluate and update the monitored formula M_2. A possibile trace $\sigma = \alpha_1, \alpha_2$, where:

$\alpha_1 = \{userId : \text{"}\texttt{Lori}\text{"},\ action : \texttt{login},\ time : 17.0\}$
$\alpha_2 = \{userId : \text{"}\texttt{Lori}\text{"},\ action : \texttt{logout},\ time : 150.0\}$

satisfies M_2.

Syntax I

Each specification S is made up of an observer part O and a declaration part D.

$$
\begin{aligned}
S &::= D\,O \\
D &::= R^* \\
O &::= M^* \\
R &::= \{\underline{\text{max}} \mid \underline{\text{min}}\}\ N(T_1\ x_1, \ldots, T_n\ x_n) = F \\
M &::= \underline{\text{mon}}\ N = F \\
T &::= \underline{\text{Form}} \mid \text{primitive type} \\
F &::= \text{expression} \mid \underline{\text{true}} \mid \underline{\text{false}} \mid \neg F \mid F_1 \wedge F_2 \mid F_1 \vee F_2 \mid \\
&\quad F_1 \rightarrow F_2 \mid \bigcirc F \mid \odot F \mid F_1 \cdot F_2 \mid N(F_1, \ldots, F_n) \mid x_i
\end{aligned}
$$

Let us focus on some details.

Syntax II

Definitions can start with different keywords:

- mon: specifies the EAGLE formulas to be monitored and cannot have a recursive definition; as already told, these kind of rules will evolve as new events appear.
- max: defines *safety properties* (nothing bad ever happens) and have a maximal interpretation.
- min: defines *liveness properties* (something good eventually happens) and have a minimal interpretation.

Note.
The difference between maximal and minimal interpretation becomes important only when we are evaluating the at the boundaries of a trace; max rules evaluates at true at initial and final istants, while min rules evaluates at false.

Semantics I

The semantics of the logic is defined in terms of the *satisfaction* relation $\models$ which defines whether a finite execution trace σ satisfies the specification $\varphi = D\,O$.

Given a trace σ and a specification $D\,O$, satisfaction is defined as follows:

$$\sigma \models D\,O \text{ iff } \forall(\underline{\text{mon}}\ N = F) \in O.\ \sigma, 1 \models_D\ F$$

In other words, a trace satisfies a specification if it fulfills each monitored formula (mon) when monitoring from position 1, which is the initial state.

In the following slide we will present the definition of the satisfaction relation $\models_D \subseteq (Trace \times \mathbb{N}) \times \underline{\text{Form}}$ for a set of rule definitions D.

Semantics II

$\sigma, i \models_D \ expression$ iff $1 \leq i \leq |\sigma|$ and $evaluate(expression, \sigma(i)) = true$

$\sigma, i \models_D \ \underline{\text{true}}$

$\sigma, i \not\models_D \ \underline{\text{false}}$

$\sigma, i \models_D \neg F$ iff $\sigma, i \not\models_D F$

$\sigma, i \models_D F_1 \wedge F_2$ iff $\sigma, i \models_D F_1$ and $\sigma, i \models_D F_2$

$\sigma, i \models_D F_1 \vee F_2$ iff $\sigma, i \models_D F_1$ or $\sigma, i \models_D F_2$

$\sigma, i \models_D F_1 \rightarrow F_2$ iff $\sigma, i \models_D F_1$ implies $\sigma, i \models_D F_2$

$\sigma, i \models_D \bigcirc F$ iff $i \leq |\sigma|$ and $\sigma, i+1 \models_D F$

$\sigma, i \models_D \odot F$ iff $1 \leq i$ and $\sigma, i-1 \models_D F$

$\sigma, i \models_D F_1 \cdot F_2$ iff $\exists j$ s.t. $i \leq j \leq |\sigma|+1$ and $\sigma^{[1,j-1]}, i \models_D F_1$ and $\sigma^{[j,|\sigma|]}, 1 \models_D F_2$

$\sigma, i \models_D N(\overline{F}, \overline{P})$ iff
- if $1 \leq i \leq |\sigma|$ then:
  - $\sigma, i \models_D F[\overline{f} \mapsto \overline{F}, \overline{p} \mapsto \ evaluate(\overline{P}, \sigma(i))]$
  - where $(N(\underline{\text{Form}}\ \overline{f}, \text{T}\ p) = F) \in D$
- otherwise, if $i = 0$ or $i = |\sigma| + 1$ then:
  - rule N is defined as $\underline{\text{max}}$ in D

Evaluation algorithm I

As we can see, a function called $evaluate$ emerges; there are additional functions as well. Let us list them.

- $evaluate$: Form $\times$ State. This function is used to evolve at every event the monitored formulas.
- $update$: Form $\times$ State $\rightarrow$ Form. This function is used by $evaluate$ to pre-evaluate a formula if it is guarded by the previous operator $\odot$
- $value$: Form $\rightarrow \{\text{true}, \text{false}\}$. This function returns true if and only if $\sigma, |\sigma| + 1 \models F$ (or $\sigma, 0 \models F$), and returns false otherwise.

Note.
Formally, a formula $F' = evaluate(F, \alpha_i)$ is created when a formula F is evaluated at an event $\alpha_i = \sigma(i)$ and has the condition that $\sigma, i \models F$ if and only if $\sigma, i + 1 \models F'$. With F being the evolved formula, we compute the boolean function $value(F)$ at the conclusion of the trace.

Evaluation algorithm II

More details are in the paper; let us introduce an example.

Example 2

Given the following rules

$$\underline{\textit{max}}\ \texttt{Always}(\underline{\textit{Form}}\ F) = F \wedge \bigcirc \texttt{Always}(F)$$
$$\underline{\textit{min}}\ \texttt{EvTimedLogout}(\underline{\textit{string}}\ k, \underline{\textit{double}}\ t, \underline{\textit{double}}\ \delta) = (\textit{time} - t \leq \delta) \wedge ((action = \texttt{logout} \wedge userId = k) \vee \bigcirc \texttt{EvTimedLogout}(k, t, \delta))$$
$$\underline{\textit{mon}}\ M_3 = \texttt{Always}((action = \texttt{login}) \rightarrow \texttt{EvTimedLogout}(userId, time, 100))$$

and a trace $\sigma = \alpha_1, \alpha_2$ *, where*

$$\alpha_1 = \{userId : \text{"}\texttt{Lori}\text{"},\ action : \texttt{login},\ time : 17.0\}$$
$$\alpha_2 = \{userId : \text{"}\texttt{Lori}\text{"},\ action : \texttt{logout},\ time : 150.0\}.$$

M_3 *gets modified, at first step, in*

$$evaluate(M_3, \alpha_1) = \texttt{EvTimedLogout}(\text{"}\texttt{Lori}\text{"}, 17.0, 100) \wedge \texttt{Always}((action = \texttt{login}) \rightarrow \texttt{EvTimedLogout}(userId, time, 100)).$$

Relationship with LTL+P

We can define both **Future Time LTL** and **Past Time LTL** operators. As example, let us show the future ones.

$$\underline{\min}\ \texttt{Next}(\underline{\text{Form}}\ F) = \bigcirc F$$
$$\underline{\max}\ \texttt{Always}(\underline{\text{Form}}\ F) = F \wedge \bigcirc \texttt{Always}(F)$$
$$\underline{\min}\ \texttt{Eventually}(\underline{\text{Form}}\ F) = F \vee \bigcirc \texttt{Eventually}(F)$$
$$\underline{\min}\ \texttt{Until}(\underline{\text{Form}}\ F_1, \underline{\text{Form}}\ F_2) = F_2 \vee (F_1 \wedge \bigcirc \texttt{Until}(F_1, F_2))$$

By combining the definitions for the future and past time LTL as defined above, we obtain a temporal logic over the future, present and past, in which one can freely intermix the future and past time modalities;
thus, we can state that EAGLE is expressive at least as LTL+P.

Attacks detection

Smurf Attacks

A *smurf attack* is a DDoS attack targeting computer networks by sending large volumes of ICMP echo request packets to a broadcast address. The attacker spoofs the source IP address to make it appear as originating from the victim's IP address, causing all devices to respond with ICMP echo replies.

In this example we will use *tcpdump* to obtain the logs from the network interface; the formula that describes the absence of the attack is the following:

$$\underline{\text{max}}\ \texttt{SmurfAttack}() = (type = \text{"ICMP"}) \wedge isBroadcast(ip)$$
$$\underline{\text{mon}}\ \texttt{SmurfSafety} = \texttt{Always}(\neg\ \texttt{SmurfAttack}())$$

where *isBroadcast*() checks whether the source's IP address is a broadcast ip, i.e. all the host bits are set to 1.

Cookie-stealing Attacks

A *cookie* is a technique used by web application servers to track client-specific session data; these tools are automatically included in client requests. When a malicious user uses an old cookie provided to a different IP address to take over a session, it is considered an attack.

At this point we need to look at web-server log; the formula that describes the absence of the attack is the following:

$$\underline{\text{min}}\ \texttt{Hijack}(\underline{\text{string}}\ c, \underline{\text{string}}\ i) = ((name = c) \wedge \neg(ip = i)) \vee \odot\, \texttt{Hijack}(c, i)$$

$$\underline{\text{mon}}\ \texttt{CookieSafe} = \texttt{Always}(\neg\texttt{Hijack}(name, ip))$$

where a single cookie is identified from c and it can be associated only at a single ip.

Multi-domain Buffer Overflows attacks

A *buffer overflow* attack uses memory manipulation to overflow a buffer, modifying an address to point to malicious code. Data from network and web server access logs are analyzed to determine when the attack occurred and if no matching log record is found within a timeout, the attack is successful. To capture this scenario we use the following formulas:

$$\begin{aligned}
&\underline{\text{min}}\ \texttt{EventuallyClosed}(\underline{\text{long}}\ t, \underline{\text{long}}\ d, \underline{\text{string}}\ i1, \underline{\text{string}}\ i2) = (time - t < d) \\
&\quad \wedge ((ip1 = i1 \wedge ip2 = i2 \wedge log = web \wedge type = closed) \\
&\quad\ \vee \bigcirc \texttt{EventuallyClosed}(t, d, i1, i2)) \\
&\underline{\text{mon}}\ \texttt{BufferSafe} = \ \texttt{Always}((log = network \wedge type = binary) \\
&\quad \rightarrow \texttt{EventuallyClosed}(time, 100, ip1, ip2))
\end{aligned}$$

where a session, identified by $(ip1, ip2)$, must end within 100 seconds if there is a $binary$ access.

Password guessing attacks

If the system accepts telnet connections for remote login, an attacker can easily compromise a user's password by guessing multiple passwords for a specific user name. We can detect with the following:

$$
\begin{aligned}
&\underline{\text{max}}\ \texttt{Failure}() = (type = login) \wedge \neg success \\
&\underline{\text{max}}\ \texttt{Guess}(\underline{\text{string}}\ i) = (ip = i) \wedge \texttt{Failure}() \\
&\underline{\text{max}}\ \texttt{Counter}(\underline{\text{long}}\ t, \underline{\text{long}}\ d, \underline{\text{int}}\ c, \underline{\text{string}}\ i, \underline{\text{int}}\ C) = (time - t < d) \\
&\qquad \rightarrow ((\texttt{Guess}(i) \rightarrow (c \leq C \wedge \bigcirc \texttt{Counter}(t, d, c+1, i, C))) \\
&\qquad \wedge (\neg \texttt{Guess}(i) \rightarrow \texttt{Counter}(t, d, c, i, C))) \\
&\underline{\text{mon}}\ \texttt{PassGuessSafe} = \ \texttt{Always}(\texttt{Failure}() \rightarrow \texttt{Counter}(time, 300, 1, ip, 3))
\end{aligned}
$$

where an attacks is detected if a password has been incorrectly guessed for 3 times within 300 seconds.

Port Scanning attacks

Port scanning is a method used to identify exploitable communication channels in networks; it involves probing network ports and keeping useful information for attacks. The victim machine suspect port scans as malicious when the counter of reached ports exceeds a specific threshold. The formulas are the following:

$$\underline{\text{max}}\ \texttt{NewPort}(\underline{\text{string}}\ i1, \underline{\text{string}}\ i2, \underline{\text{Set}}\ S) = (i1 = ip1) \wedge (i2 = ip2) \wedge (port \notin S)$$

$$\underline{\text{max}}\ \texttt{Counter}(\underline{\text{long}}\ t, \underline{\text{long}}\ d, \underline{\text{int}}\ c, \underline{\text{string}}\ i1, \underline{\text{string}}\ i2, \underline{\text{Set}}\ S, \underline{\text{int}}\ C) = (time - t < d)$$
$$\rightarrow ((\texttt{NewPort}(i1, i2, S) \rightarrow (c \leq C \wedge \bigcirc\texttt{Counter}(t, d, c + 1, i1, i2, S \cup \{port\}, C)))$$
$$\wedge (\neg\texttt{NewPort}(i1, i2, S) \rightarrow \texttt{Counter}(t, d, c, i1, i2, S, C)))$$

$$\underline{\text{mon}}\ \texttt{PortScanSafe} = \texttt{Always}(\texttt{Counter}(time, 100, 1, ip1, ip2, \{port\}, 10))$$

where we checks if the number of port scans between $ip1, ip2$ does not exceed a threshold of 10 within 100 seconds.

Performances

MONID was evaluated against smurf, port-sweep, and password-guessing attacks using DARPA Intrusion Detection Evaluation dataset in offline mode, detecting 5 password-guess attacks and 2 port-sweep attacks.

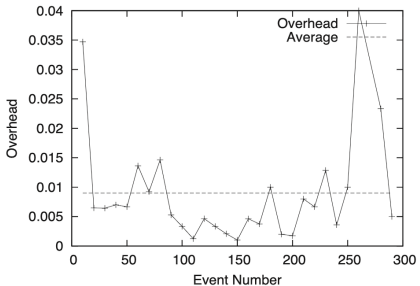


Figure 1: Performances overhead of Port-Sweep attacks.

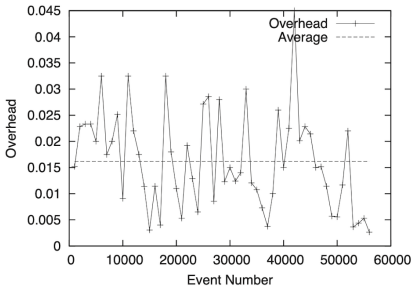


Figure 2: Performances overhead of Password-Guessing attacks.

Conclusions

Conclusions

In conclusion:

- We have introduced the MONID framework and explained how it works.
- We then proceeded introducing a new temporal logic named EAGLE, which serves as the foundation for the MONID framework.
- We have presented some example of formulas which aims at recognize some attacks patterns.

Due to the little overhead involved in the computation and the great performances of MONID when utilized offline, we can state that this method should still be useful in theory today.

Attacks nowadays become more and more complex but once a pattern is found, we can represent it with 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