Adversarial Formal Semantics of Attack Trees and Related Problems

Thomas Brihaye, Sophie Pinchinat, Alexandre Terefenko

Université de Mons
Université de Rennes

July 4, 2023
Introduction

- The attack tree model
- Related work

Semantics for attack tree

Results on decision problems
A thief wants to steal some document in a safe of a building without being seen.
The entrance in the building
An example of an attack tree

- Thief
- Guard
- Door 1
- Door 2
- Camera
- Key
- Locked door
- Safe

The attack tree model

Locked door
Camera
Key

Terefenko
Adversarial Formal Semantics of Attack Trees and Related Problems
July 4, 2023
Related work

- **Different syntax of attack trees:**
  1. Sjouke Mauw and Martijn Oostdijk, *Foundations of attack trees*, International Conference on Information Security and Cryptology, Springer, 2005, pp. 186–198.
  2. Maxime Audinot, Sophie Pinchinat, and Barbara Kordy, *Is my attack tree correct?*, European Symposium on Research in Computer Security, Springer, 2017, pp. 83–102.
  3. Aivo Jürgenson and Jan Willemsen, *Computing exact outcomes of multiparameter attack trees*, OTM Confederated International Conferences "On the Move to Meaningful Internet Systems", Springer, 2008, pp. 1036-1051.

- **Different semantics for attack trees:**
  1. Sophie Pinchinat, Barbara Fila, Florence Wacheux, and Yann ThierryMieg, *Attack trees: a notion of missing attacks*, International Workshop on Graphical Models for Security, Springer, 2019, pp. 23-49.
  2. Maxime Audinot, Sophie Pinchinat, and Barbara Kordy, *Is my attack tree correct?*, European Symposium on Research in Computer Security, Springer, 2017, pp. 83-102.
  3. Ross Horne, Sjouke Mauw, and Alwen Tiu, *Semantics for specialising attack trees based on linear logic*, Fundamenta Informaticae 153 (2017), no. 1-2, 57-86.

**Survey:** Wideł, W., Audinot, M., Fila, B., Pinchinat, S. (2019). *Beyond 2014: Formal Methods for Attack Tree–based Security Modeling*. ACM Computing Surveys (CSUR), 52(4), 1-36.
1 Introduction

2 Semantics for attack tree
   - Syntax
   - Path semantics
   - Strategy semantics

3 Results on decision problems
Syntax of an attack tree

Maxime Audinot, Sophie Pinchinat, and Barbara Kordy, *Is my attack tree correct?*, European Symposium on Research in Computer Security, Springer, 2017, pp. 83-102.
Syntax of an attack tree

Maxime Audinot, Sophie Pinchinat, and Barbara Kordy, *Is my attack tree correct?*, European Symposium on Research in Computer Security, Springer, 2017, pp. 83-102.
Syntax of an attack tree (no precondition)

Definition

An attack tree $\tau$ is:

- a Boolean formula $\phi$ over a set of proposition $Prop$,
- an expression $OP(\tau_1, \ldots, \tau_n)$ where $OP \in \{OR, AND \text{ and } SAND\}$ and $\tau_1, \ldots, \tau_n$ are attack trees.
Let $S = (S, \rightarrow, val)$ be a transition system with $val : S \rightarrow PROP$ a valuation function. We denote $\Pi(S)$ the set of all paths over $S$.

**Definition**

$Paths(\tau)_S$ is inductively defined as follow:

- $Paths(\phi)_S = \{s_0s_1...s_n \in \Pi(S) | s_n \models \phi\}$,
- For $Paths(OR(\tau_1, ..., \tau_n))_S$, we use the **union** of the semantics,
- For $Paths(SAND(\tau_1, ..., \tau_n))_S$, we use the **synchronised concatenation** of the semantics,
- For $Paths(AND(\tau_1, ..., \tau_n))_S$, we use the **merge** of the semantics.
Example: path semantics

Semantics for attack tree

Path semantics

Locked door

Door 1

Door 2

Guard

Camera

Key

Thief

Safe

$D_1 \land \neg \text{seen}$

$D_2 \land \neg \text{seen}$

$R_2$

$C$

$K$

Terefenko
Adversarial Formal Semantics of Attack Trees and Related Problems
July 4, 2023
The entrance in the building

\[
\begin{align*}
\{D1, seen\} & \quad (d_1, d_1) \quad (o, d_1) \quad (d_2, d_1) \quad \{D2\} \\
\{D1\} & \quad (d_1, m) \quad (o, m) \quad (d_2, m) \quad \{D2\} \\
\{D1\} & \quad (d_1, d_2) \quad (o, d_2) \quad (d_2, d_2) \quad \{D2, seen\}
\end{align*}
\]
## Intuition for a strategy semantics

| Paths semantics | Strategy semantics |
|-----------------|--------------------|
| Transition system | Game arena |
| Paths | Strategies |

\[
Paths(\phi) = \{s_0 \ldots s_n \in \Pi(S)|s_n \models \phi\}
\]

\[
Strat(\phi) \text{ winning strategies for the reachability game defined by } \phi
\]

For an attack tree \(\tau\), \(Strat(\tau)\) denotes all winning attacking strategies.
Example: strategy semantics

Semantics for attack tree
Strategy semantics

Locked door
Door 1
Door 2
Camera
Key
Thief
Guard

Safe

$D_1 \land \neg \text{seen}$
$D_2 \land \neg \text{seen}$
$R_2$
$C$
$K$

Terefenko
Adversarial Formal Semantics of Attack Trees and Related Problems
July 4, 2023
15 / 25
Problems with a compositional semantics

\begin{align*}
\{D1, \text{seen}\} & \quad (d_1, d_1) & \quad (o, d_1) & \quad (d_2, d_1) & \quad \{D2\} \\
\{D1\} & \quad (d_1, m) & \quad (o, m) & \quad (d_2, m) & \quad \{D2\} \\
\{D1\} & \quad (d_1, d_2) & \quad (o, d_2) & \quad (d_2, d_2) & \quad \{D2, \text{seen}\}
\end{align*}
Definition

The strategy semantics of an attack tree $\tau$ is the set of all trees $\sigma$ respecting the two following conditions:

- $\sigma$ denotes a strategy
- every branch of $\sigma$ is a path in $\text{Paths}(\tau)$
1. Introduction

2. Semantics for attack tree

3. Results on decision problems
Considered decision problems

Membership problem

\[ x \in \llbracket \tau \rrbracket \ ? \]

Non-Emptiness problem

\[ [\tau] \neq \emptyset \ ? \]
### Results summary

|                        | Paths semantics | Strategy semantics |
|------------------------|-----------------|--------------------|
| Membership Problem     |                 |                    |
| Non-Emptiness Problem  |                 |                    |

- NP-complete if preconditions for leaves.\(^1\)

---

\(^1\)Maxime Audinot, Sophie Pinchinat, and Barbara Kordy, *Is my attack tree correct?*, European Symposium on Research in Computer Security, Springer, 2017, pp. 83-102.
## Results summary

| Paths semantics | Strategy semantics |
|-----------------|-------------------|
| Membership Problem | P                  |
| Non-Emptiness Problem |              |

- NP-complete if preconditions for leaves.\(^1\)
- Without preconditions: a backward induction over the input path can solve the problem in polynomial time.

---

\(^1\)Maxime Audinot, Sophie Pinchinat, and Barbara Kordy, *Is my attack tree correct?*, European Symposium on Research in Computer Security, Springer, 2017, pp. 83-102.
## Results summary

|                         | Paths semantics | Strategy semantics |
|-------------------------|-----------------|--------------------|
| Membership Problem      | \( P \)         |                    |
| Non-Emptyness Problem   | \( \text{NP-complete}^2 \) |                  |

---

\(^2\)Maxime Audinot, Sophie Pinchinat, and Barbara Kordy, *Is my attack tree correct?*, European Symposium on Research in Computer Security, Springer, 2017, pp. 83-102.
Results summary

|                              | Paths semantics | Strategy semantics |
|------------------------------|-----------------|--------------------|
| Membership Problem           | P               |                    |
| Non-Emptiness Problem        | NP-complete     |                    |

**Hardness:** \( \exists x_1 \exists x_2 \exists x_3, x_1 \land (x_2 \lor x_3) \land (\neg x_2 \lor x_3) \)

\[
\{ P_1 \} \quad \{ P_2 \} \quad \{ P_2, P_3 \}
\]

Diagram of a decision problem with paths and strategies.
Results summary

|                           | Paths semantics | Strategy semantics |
|---------------------------|-----------------|--------------------|
| Membership Problem        | P               | \text{PSPACE-complete} |
| Non-Emptiness Problem     | NP-complete     | \text{PSPACE-complete} |

Membership:

- Semantics non-empty $\implies$ existence of not too long strategies
- construct an alternating Turing machine:
  - Guess a play $\pi$ (AP)
  - check whether $\pi \in \text{Paths}(\tau)$
### Results on decision problems

#### Results summary

|                          | Paths semantics | Strategy semantics |
|--------------------------|-----------------|-------------------|
| Membership Problem       | $P$             |                   |
| Non-Emptiness Problem    | NP-complete     | PSPACE-complete   |

**Hardness:** $\exists x_1 \forall x_2 \exists x_3, x_1 \land (x_2 \lor x_3) \land (\neg x_2 \lor x_3)$
### Results summary

| Paths semantics | Strategy semantics |
|-----------------|--------------------|
| **Membership Problem** | P                  | \textsc{coNP}-complete |
| **Non-Emptiness Problem** | \textsc{NP}-complete | \textsc{PSPACE}-complete |
Results on decision problems

Results summary

|                        | Paths semantics | Strategy semantics |
|------------------------|-----------------|-------------------|
| Membership Problem     | P               | coNP-complete     |
| Non-Emptyness Problem  | NP-complete     | PSPACE-complete   |

Hardness: \( \forall x_1 \forall x_2 \forall x_3, x_1 \land (x_2 \lor x_3) \land (\neg x_2 \lor x_3) \)
### Results summary

|                      | Paths semantics | Strategy semantics |
|----------------------|-----------------|--------------------|
| Membership Problem   | P               | coNP-complete      |
| Non-Emptiness Problem| NP-complete     | PSPACE-complete    |

**In conclusion**
Bibliography

- Wideł, W., Audinot, M., Fila, B., Pinchinat, S. (2019). Beyond 2014: Formal Methods for Attack Tree–based Security Modeling. ACM Computing Surveys (CSUR), 52(4), 1-36.

- Sjouke Mauw and Martijn Oostdijk, Foundations of attack trees, International Conference on Information Security and Cryptology, Springer, 2005, pp. 186–198.

- Maxime Audinot, Sophie Pinchinat, and Barbara Kordy, Is my attack tree correct?, European Symposium on Research in Computer Security, Springer, 2017, pp. 83–102.

- Aivo Jürgenson and Jan Willemson, Computing exact outcomes of multiparameter attack trees, OTM Confederated International Conferences “On the Move to Meaningful Internet Systems”, Springer, 2008, pp. 1036-1051.

- Sophie Pinchinat, Barbara Fila, Florence Wacheux, and Yann ThierryMieg, Attack trees: a notion of missing attacks, International Workshop on Graphical Models for Security, Springer, 2019, pp. 23-49.

- Ross Horne, Sjouke Mauw, and Alwen Tiu, Semantics for specialising attack trees based on linear logic, Fundamenta Informaticae 153 (2017), no. 1-2, 57-86.

- Hopcroft, J. E., Motwani, R., Ullman, J. D. (2001). Introduction to automata theory, languages, and computation. Acm Sigact News, 32(1), 60-65.

- Paul, S., Ramanujam, R., Simon, S. (2015). Automata and compositional strategies in extensive form games. In Models of Strategic Reasoning (pp. 174-201). Springer, Berlin, Heidelberg.