Adversarial Formal Semantics of Attack Trees and Related Problems

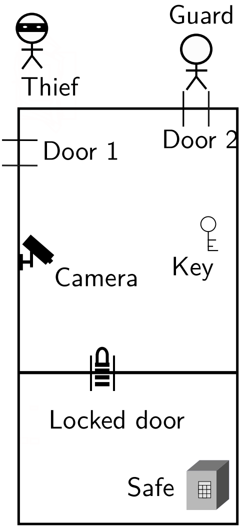
Thomas Brihaye, Sophie Pinchinat, **Alexandre Terefenko**

Université de Mons
Université de Rennes

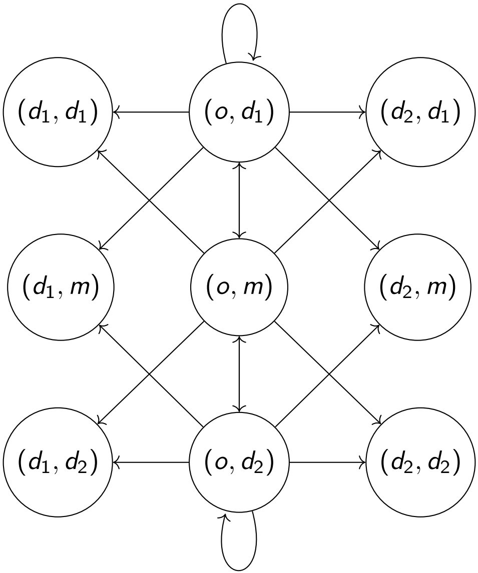
July 4, 2023

Situation

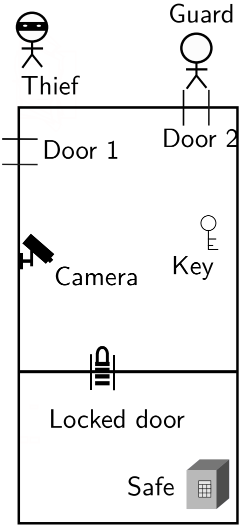
A thief wants to steal some document in a safe of a building without being seen.

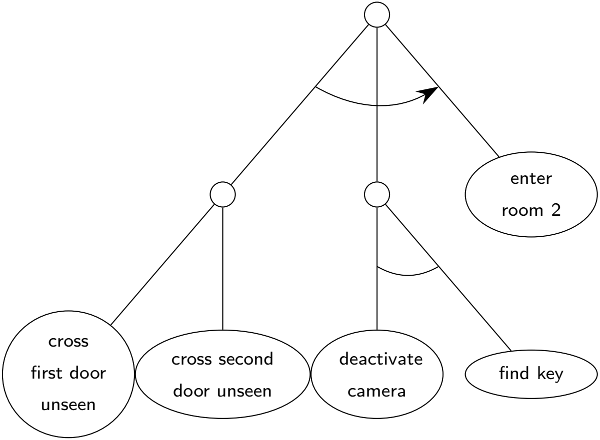


The entrance in the building



An example of an attack tree



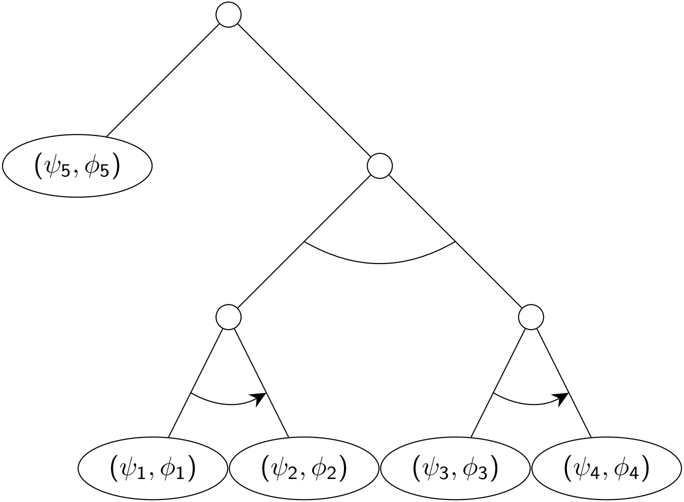


Related work

- **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 Willemson, *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.

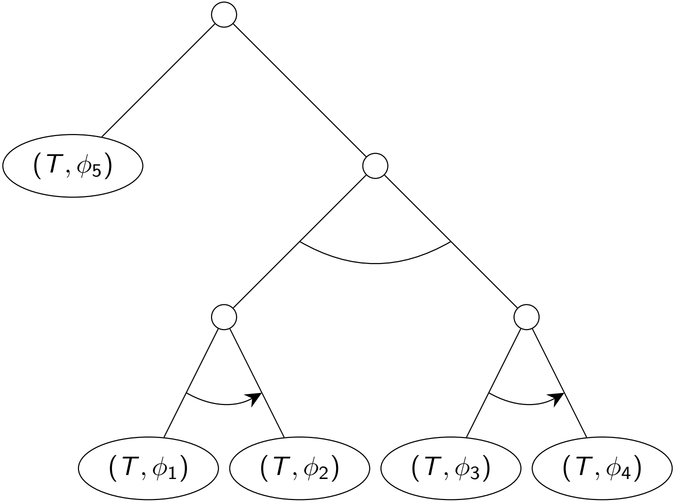
Survey: Wideł, W., Audinot, M., Fila, B., Pinchinat, S. (2019). *Beyond 2014: Formal Methods for Attack Tree–based Security Modeling.* ACM Computing Surveys (CSUR), 52(4), 1-36.

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



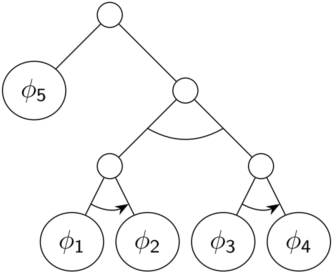
Maxime Audinot, Sophie Pinchinat, and Barbara Kordy, *Is my attack tree correct ?*, European Symposium on Research in Computer Security, Springer, 2017, pp. 83-102.

Syntax of an attack tree (no precondition)

Definition

An *attack tree* τ is:

- a Boolean formula ϕ over a set of proposition *Prop*,
- an expression $OP(\tau_1, ..., \tau_n)$ where $OP \in \{OR, AND \text{ and } SAND\}$ and $\tau_1, ..., \tau_n$ are attack trees.



Path semantics

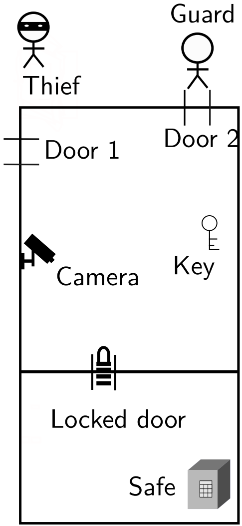
Let $\mathcal{S} = (S, \rightarrow, val)$ be a transition system with $val : S \rightarrow PROP$ a valuation function. We denote $\Pi(\mathcal{S})$ the set of all paths over $\mathcal{S}$.

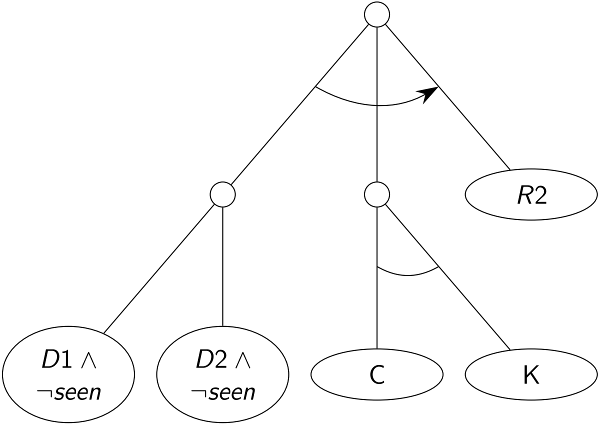
Definition

$Paths(\tau)_{\mathcal{S}}$ is inductively defined as follow:

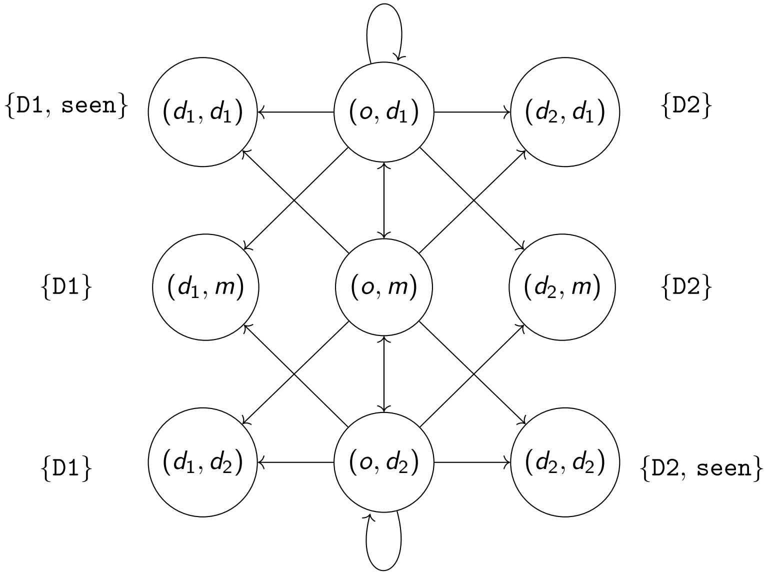
- $Paths(\phi)_{\mathcal{S}} = \{s_0 s_1 ... s_n \in \Pi(\mathcal{S}) | s_n \models \phi\}$,
- For $Paths(OR(\tau_1, ..., \tau_n))_{\mathcal{S}}$, we use the **union** of the semantics,
- For $Paths(SAND(\tau_1, ..., \tau_n))_{\mathcal{S}}$, we use the **synchronised concatenation** of the semantics,
- For $Paths(AND(\tau_1, ..., \tau_n))_{\mathcal{S}}$, we use the **merge** of the semantics.

Example: path semantics





The entrance in the building

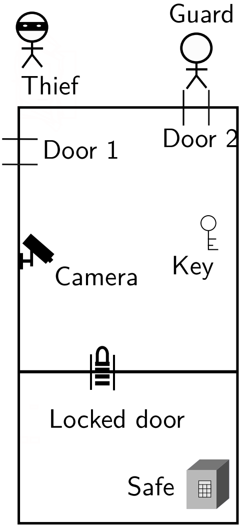


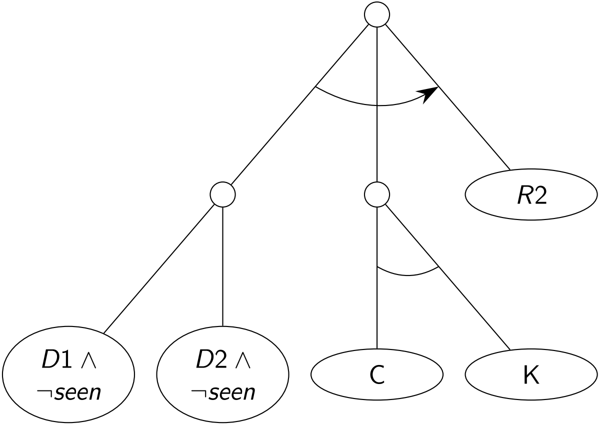
Intuition for a strategy semantics

Paths semantics	**Strategy semantics**
Transition system	Game arena
Paths	Strategies
$Paths(\phi) = \{s_0 \ldots s_n \in \Pi(\mathcal{S}) \mid s_n \models \phi\}$	$Strat(\phi)$ winning strategies for the reachability game defined by ϕ

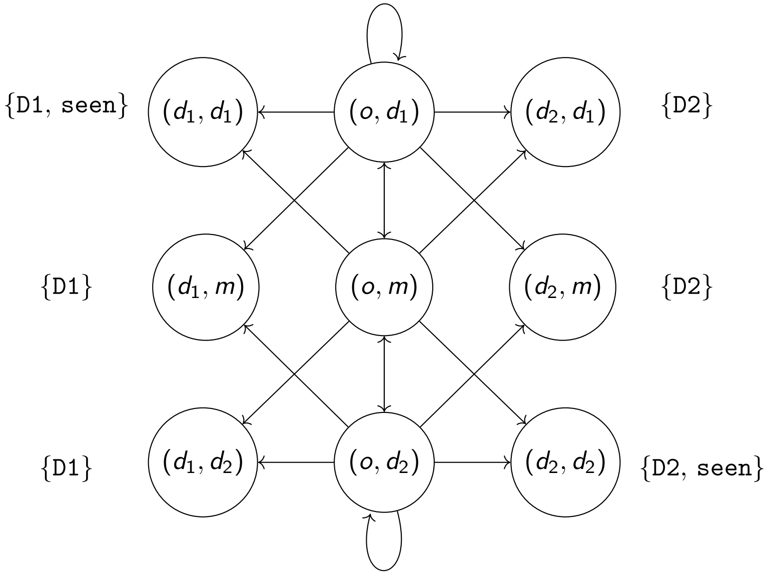
For an attack tree τ, $Strat(\tau)$ denotes all winning attacking strategies.

Example: strategy semantics





Problems with a compositional semantics



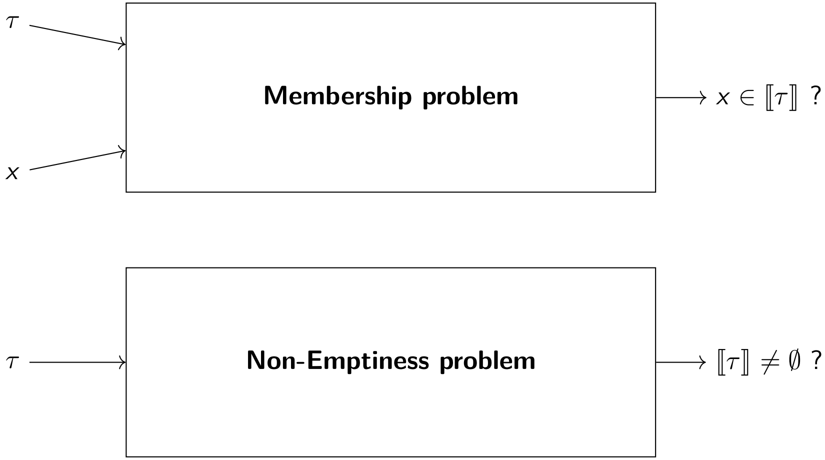
Strategy semantics

Definition

The strategy semantics of an attack tree τ is the set of all trees σ respecting the two following conditions:

- σ denotes a strategy
- every branch of σ is a path in $\mathit{Paths}(\tau)$

Considered decision problems



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

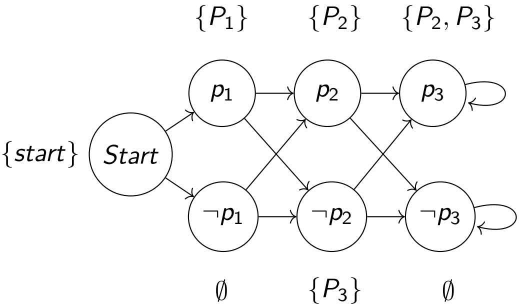
	Paths semantics	Strategy semantics
Membership Problem	P	
Non-Emptiness Problem	NP-complete[2]	

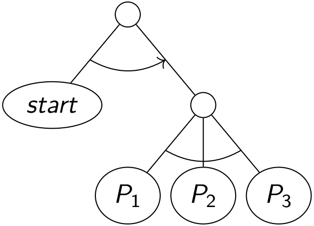
[2] Maxime Audinot, Sophie Pinchinat, and Barbara Kordy, *Is my attack tree correct ?*, European Symposium on Research in Computer Security, Springer, 2017, pp. 83-102.

Results summary

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

Hardness: $\exists x_1 \exists x_2 \exists x_3, x_1 \wedge (x_2 \vee x_3) \wedge (\neg x_2 \vee x_3)$





Results summary

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

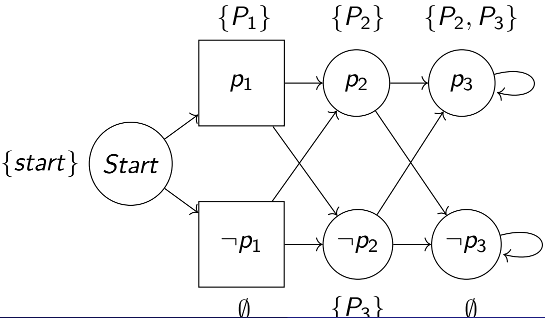
Membership:

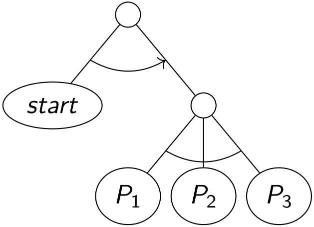
- Semantics non-empty $\implies$ existence of not too long strategies
- construct an alternating Turing machine:
  - Guess a play π (AP)
  - check whether $\pi \in \mathit{Paths}(\tau)$

Results summary

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

Hardness: $\exists x_1 \forall x_2 \exists x_3, x_1 \wedge (x_2 \vee x_3) \wedge (\neg x_2 \vee x_3)$





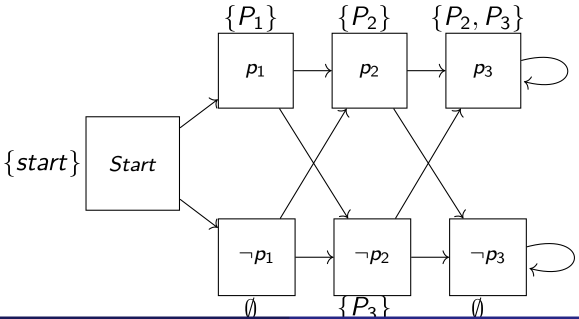
Results summary

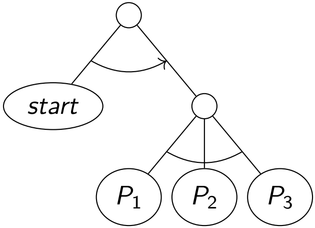
	Paths semantics	Strategy semantics
Membership Problem	P	coNP-complete
Non-Emptiness Problem	NP-complete	PSPACE-complete

Results summary

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

Hardness: $\forall x_1 \forall x_2 \forall x_3, x_1 \wedge (x_2 \vee x_3) \wedge (\neg x_2 \vee x_3)$





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