On the soundness of attack trees

Maxime Audinot Sophie Pinchinat

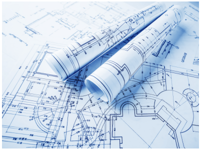
Université de Rennes 1

27 june 2016

Context : Risk analysis

system

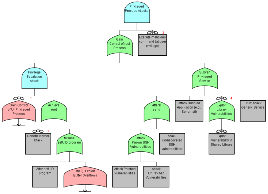
system model



likelihood

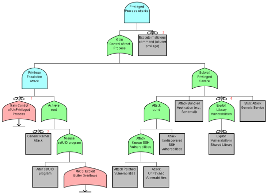
cost

time



attack tree

The attack tree construction



Top-down manual construction

Manual construction is tedious and **error-prone**:

non relevant subgoals, forgotten cases, etc.

Automated validation

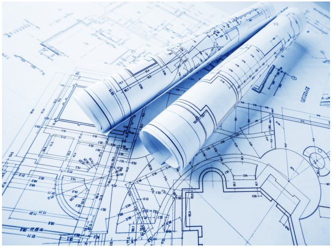
How do we guarantee that this construction is sound?

Plan

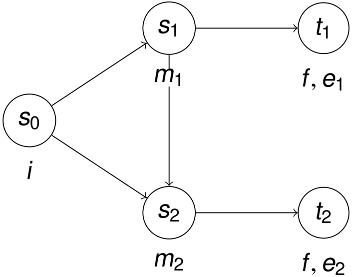
1. Background definitions
2. 3 notions of soundness
   - Admissibility
   - Consistency
   - Completeness
3. Checking Admissibility

Plan

System representation



a domain-specific, high-level specification



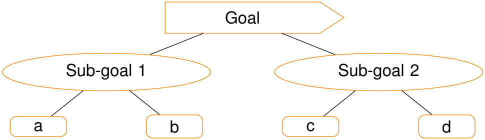
a labeled transition system $\mathcal{S}$

Compilation phase

ATSyRA Attack Tree Synthesis and Risk Analysis

Attack trees

Introduced by Bruce Schneier in 1999.



Attacks:
ac, ad, bc, bd

3 types of internal nodes:

Or	And	Sequential [Jhawar *et al.* , 2015]
$\varovee$	$\varowedge$	$\ogreaterthan$

$$\square \in \{\varovee, \varowedge, \ogreaterthan\}$$

Plan

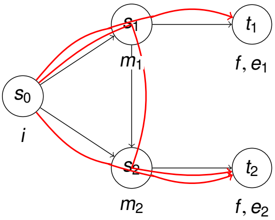
Attack goals

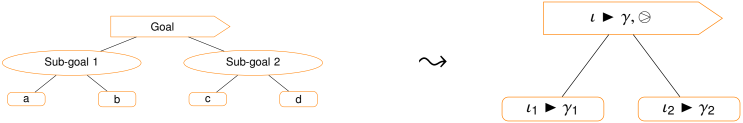
Given by a pair of initial conditions and final conditions:

$$\iota \blacktriangleright \gamma$$

with path semantics $[\iota \blacktriangleright \gamma]_{\mathcal{S}}$:

$[i \blacktriangleright f]_{\mathcal{S}} =$ paths from i to f





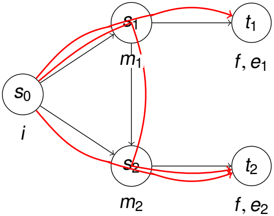
Attack goals

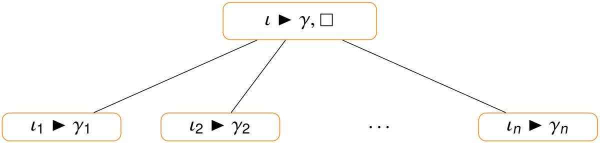
Given by a pair of initial conditions and final conditions:

$$\iota \blacktriangleright \gamma$$

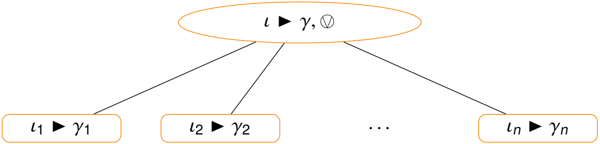
with path semantics $[\iota \blacktriangleright \gamma]_{\mathcal{S}}$:

$[i \blacktriangleright f]_{\mathcal{S}} =$ paths from i to f



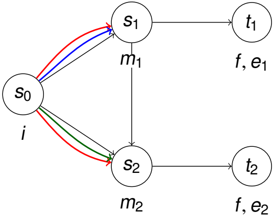


Path semantics for $\ovee$

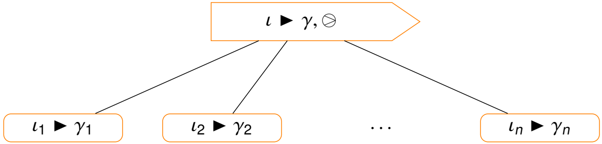


$$[(\iota_1 \blacktriangleright \gamma_1) \ovee (\iota_2 \blacktriangleright \gamma_2) \ovee \ldots (\iota_n \blacktriangleright \gamma_n)]_{\mathcal{S}} = [\iota_1 \blacktriangleright \gamma_1]_{\mathcal{S}} \cup [\iota_2 \blacktriangleright \gamma_2]_{\mathcal{S}} \cup \ldots [\iota_n \blacktriangleright \gamma_n]_{\mathcal{S}}$$

$$[(i \blacktriangleright m_1) \ovee (i \blacktriangleright m_2)]_{\mathcal{S}}$$

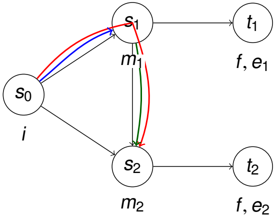


Path semantics for $\ogreaterthan$

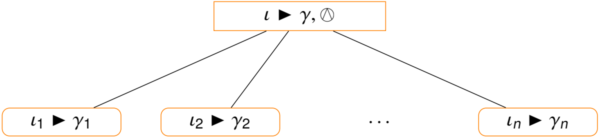


$$[(\iota_1 \blacktriangleright \gamma_1) \ogreaterthan (\iota_2 \blacktriangleright \gamma_2) \ogreaterthan \dots (\iota_n \blacktriangleright \gamma_n)]_{\mathcal{S}} = [\iota_1 \blacktriangleright \gamma_1]_{\mathcal{S}}.[\iota_2 \blacktriangleright \gamma_2]_{\mathcal{S}}. \dots [\iota_n \blacktriangleright \gamma_n]_{\mathcal{S}}$$

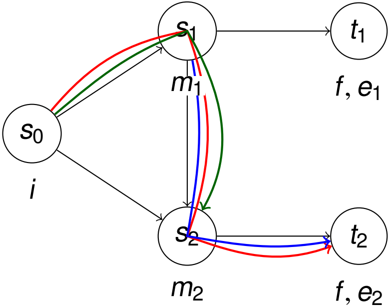
$$[(i \blacktriangleright m_1) \ogreaterthan (m_1 \blacktriangleright m_2)]_{\mathcal{S}}$$



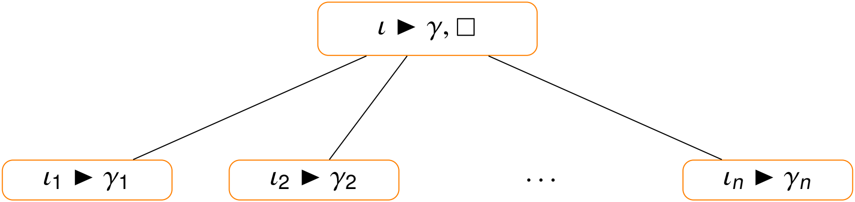
Path semantics for $\owedge$



$[(m_1 \blacktriangleright f) \owedge (i \blacktriangleright m_2)]_{\mathcal{S}}$



Soundness

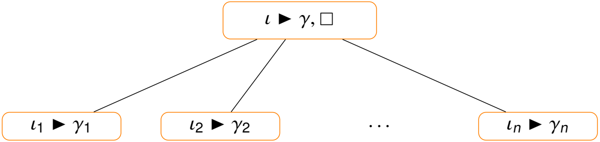


Compare two sets of paths:

$$[(\iota_1 \blacktriangleright \gamma_1) \Box \dots \Box (\iota_n \blacktriangleright \gamma_n)]_{\mathcal{S}} \text{ versus } [\iota \blacktriangleright \gamma]_{\mathcal{S}}$$

in 3 different manners $\rightsquigarrow$ *Admissibility*, *Consistency*, and *Completeness*

Soundness notions



Definition (Admissibility)

$$[(\iota_1 \blacktriangleright \gamma_1) \Box \ldots \Box (\iota_n \blacktriangleright \gamma_n)]_{\mathcal{S}} \cap [\iota \blacktriangleright \gamma]_{\mathcal{S}} \neq \emptyset$$

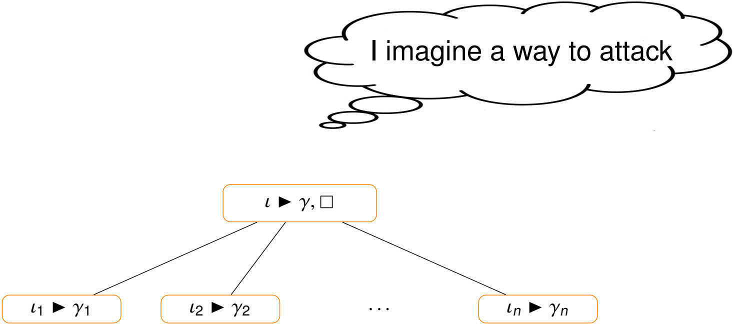
Definition (Consistency)

$$[(\iota_1 \blacktriangleright \gamma_1) \Box \ldots \Box (\iota_n \blacktriangleright \gamma_n)]_{\mathcal{S}} \subseteq [\iota \blacktriangleright \gamma]_{\mathcal{S}}$$

Definition (Completeness)

$$[(\iota_1 \blacktriangleright \gamma_1) \Box \ldots \Box (\iota_n \blacktriangleright \gamma_n)]_{\mathcal{S}} = [\iota \blacktriangleright \gamma]_{\mathcal{S}}$$

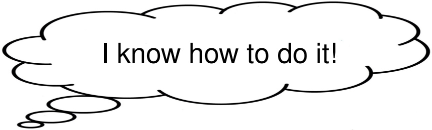
Admissibility

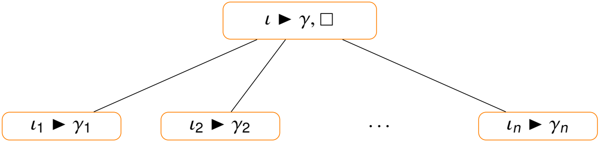


Definition (Admissibility)

$$[(\iota_1 \blacktriangleright \gamma_1) \square \ldots \square (\iota_n \blacktriangleright \gamma_n)]_{\mathcal{S}} \cap [\iota \blacktriangleright \gamma]_{\mathcal{S}} \neq \emptyset$$

Consistency

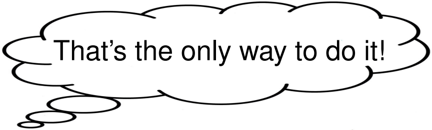


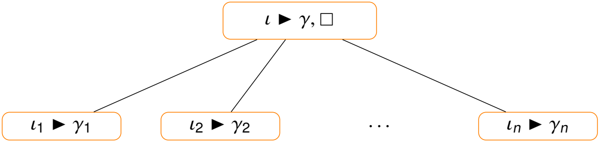


Definition (Consistency)

$$[(\iota_1 \blacktriangleright \gamma_1) \Box \ldots \Box (\iota_n \blacktriangleright \gamma_n)]_{\mathcal{S}} \subseteq [\iota \blacktriangleright \gamma]_{\mathcal{S}}$$

Completeness





Definition (Completeness)

$$[(\iota_1 \blacktriangleright \gamma_1) \Box \ldots \Box (\iota_n \blacktriangleright \gamma_n)]_{\mathcal{S}} = [\iota \blacktriangleright \gamma]_{\mathcal{S}}$$

Plan

The decision problem ADM($\square$)

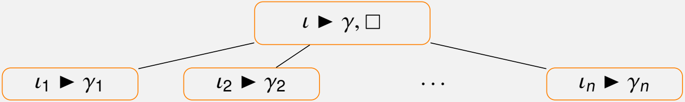
For $\square \in \{\ovee, \ogreaterthan, \owedge\}$

Definition (Admissibility)

$[(\iota_1 \blacktriangleright \gamma_1) \square \ldots \square (\iota_n \blacktriangleright \gamma_n)]_{\mathcal{S}} \cap [\iota \blacktriangleright \gamma]_{\mathcal{S}} \neq \emptyset$

ADM($\square$)

Input:

- 

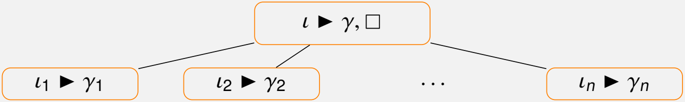
- A labeled transition system $\mathcal{S}$

Output: yes if Admissibilty holds, no otherwise.

Admissibility: computational complexity

ADM($\Box$)

Input:

- 

- labeled transition system $\mathcal{S}$

Output: yes if Admissibilty holds, no otherwise.

Theorem

ADM($\ovee$) and ADM($\circledgtr$) are in P*.*

Theorem

ADM($\owedge$) is in PSPACE*.*

Conclusion & Future work

Conclusion

- 3 notions of soundness: Admissibility, Consistency, and Completeness.
- Deciding admissibility is in P for $\ovee$ and $\ogreaterthan$, and in PSPACE for $\owedge$.

Future work

- Exact complexity of ADM($\owedge$).
- Complexities for consistency and completeness.
- Implementation of the notions in the tool ATSyRA [Pinchinat *et al.* , 2015].
- Extension to system models with quantitative aspects.

Thank you for your attention.

Questions?