Library-based Attack Tree Synthesis

Sébastien Lê Cong, Sophie Pinchinat
Francois Schwarzentruber

Univ Rennes - France

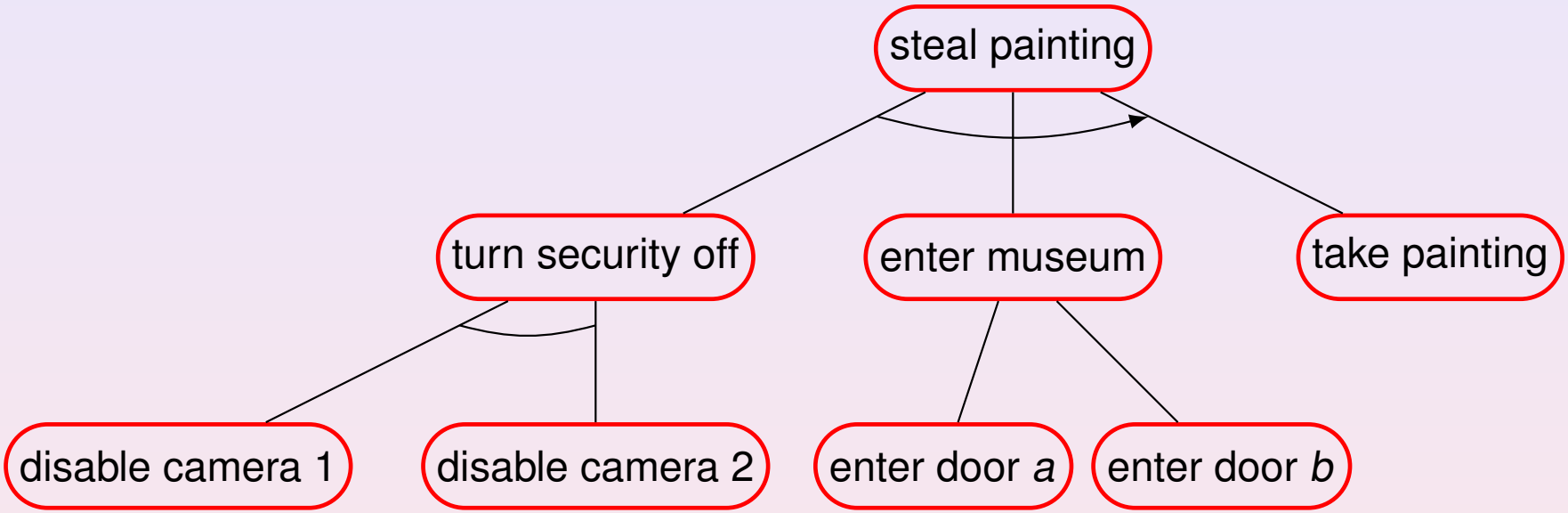
June 22, 2020

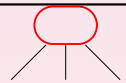
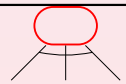
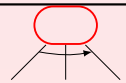
Attack reports are difficult to “parse”

```
09:07:06:213 4288 12376 Start.
09:07:06:215 4288 12376 The minimum supported Office version is 14
09:07:06:216 4288 12376 The host's version is 16.0.8827.2082
09:07:06:216 4288 12376 Creating a new instance of the add-in loader.
09:07:06:216 4288 12376 Loading mscoree.dll
09:07:06:217 4288 12376 Success.
09:07:06:217 4288 12376 Loading the configuration from the system registry.
09:07:06:219 4288 12376 Getting the latest CLR version.
09:07:06:226 4288 12376 The latest CLR version is 'v4.0.30319'.
09:07:06:226 4288 12376 The configuration has been loaded successfully.
09:07:06:226 4288 12376     Runtime version: v4.0.30319.
09:07:06:226 4288 12376     Assembly name: MSIP.Office.PowerPointAddin.
09:07:06:226 4288 12376     Class name: Microsoft.InformationProtection.Office.PowerPo
09:07:06:226 4288 12376     Registry key: CLSID\{C890DC9C-FE43-4418-BD39-D91C547BE49E}
09:07:06:226 4288 12376 Attempting to create a new instance of the managed add-in clas
```

```
2016/11/25 12:38:52:711  Reloading account configuration
2016/11/25 12:41:15:026  Reloading account configuration
2016/11/25 12:41:15:065  Requesting Authentication for Modes: 16382
2016/11/25 12:41:15:065  Modes after account check: 8190
2016/11/25 12:41:15:066  Modes after Keychain check: 8190
2016/11/25 12:41:15:066  Modes after message-only check: 8190
2016/11/25 12:41:15:067  Modes after ignore-missing-values check: 8190
2016/11/25 12:41:16:491  Reloading account configuration
2016/11/25 12:41:17:526  Reloading account configuration
2016/11/25 12:41:47:977  Reloading account configuration
2016/11/25 12:43:10:934  Reloading account configuration
2016/11/25 12:43:10:976  Requesting Authentication for Modes: 16382
2016/11/25 12:43:10:976  Modes after account check: 8190
2016/11/25 12:43:10:978  Modes after Keychain check: 8190
2016/11/25 12:43:10:978  Modes after message-only check: 8190
2016/11/25 12:43:10:979  Modes after ignore-missing-values check: 8190
2016/11/25 12:43:12:409  Reloading account configuration
2016/11/25 12:43:13:463  Reloading account configuration
2016/11/25 12:43:48:278  Reloading account configuration
2016/11/25 12:43:49:441  Reloading account configuration
2016/11/25 12:45:03:348  Reloading account configuration
2016/11/25 15:58:42:135  System is going into sleep mode -> disconnecting ac
2016/11/25 16:00:11:907  System is waking from sleep -> reconnecting sleepin
seconds
2016/11/25 17:24:10:156  System is going into sleep mode -> disconnecting ac
2016/11/25 17:36:29:715  System is waking from sleep -> reconnecting sleepin
seconds
2016/11/25 17:47:06:114  System is going into sleep mode -> disconnecting ac
2016/11/25 21:57:29:286  System is waking from sleep -> reconnecting sleepin
seconds
2016/11/25 22:51:06:101  System is going into sleep mode -> disconnecting ac
2016/11/26 00:20:44:537  Shimo detected a change of network configurations.
2016/11/26 00:20:51:009  Shimo detected a change of network configurations.
2016/11/26 10:48:57:753  Shimo detected a change of network configurations.
```

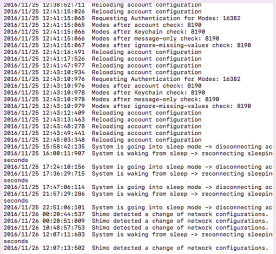
Attack tree as recipe of attack task



leaf		Primitive task
`OR` node		Execute one of the subtasks
`AND` node		Execute subtasks “concurrently”
`SAND` node		Execute subtasks sequentially

Our contribution: library-based attack tree synthesis

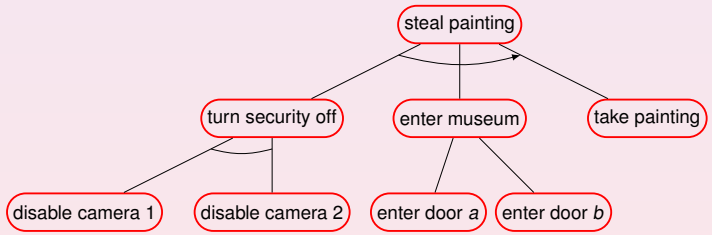
An attack
(e.g. log file)



Synthesis

A library

An attack tree



Outline

Outline

An attack

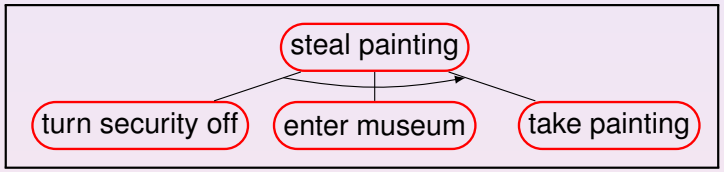
```
2016/11/25 12:38:52:711  Reloading account configuration
2016/11/25 12:41:15:026  Reloading account configuration
2016/11/25 12:41:15:065  Requesting Authentication for Modes: 16382
2016/11/25 12:41:15:065  Modes after account check: 8190
2016/11/25 12:41:15:066  Modes after Keychain check: 8190
2016/11/25 12:41:15:066  Modes after message-only check: 8190
2016/11/25 12:41:15:067  Modes after ignore-missing-values check: 8190
2016/11/25 12:41:16:491  Reloading account configuration
2016/11/25 12:41:17:526  Reloading account configuration
2016/11/25 12:41:47:977  Reloading account configuration
2016/11/25 12:43:10:934  Reloading account configuration
2016/11/25 12:43:10:976  Requesting Authentication for Modes: 16382
2016/11/25 12:43:10:976  Modes after account check: 8190
2016/11/25 12:43:10:978  Modes after Keychain check: 8190
2016/11/25 12:43:10:978  Modes after message-only check: 8190
2016/11/25 12:43:10:979  Modes after ignore-missing-values check: 8190
2016/11/25 12:43:12:409  Reloading account configuration
2016/11/25 12:43:13:463  Reloading account configuration
2016/11/25 12:43:48:278  Reloading account configuration
2016/11/25 12:43:49:441  Reloading account configuration
2016/11/25 12:45:03:348  Reloading account configuration
2016/11/25 15:58:42:135  System is going into sleep mode -> disconnecting ac
2016/11/25 16:00:11:907  System is waking from sleep -> reconnecting sleepin
seconds
2016/11/25 17:24:10:156  System is going into sleep mode -> disconnecting ac
2016/11/25 17:36:29:715  System is waking from sleep -> reconnecting sleepin
seconds
2016/11/25 17:47:06:114  System is going into sleep mode -> disconnecting ac
2016/11/25 21:57:29:286  System is waking from sleep -> reconnecting sleepin
seconds
2016/11/25 22:51:06:101  System is going into sleep mode -> disconnecting ac
2016/11/26 00:20:44:537  Shimo detected a change of network configurations.
2016/11/26 00:20:51:009  Shimo detected a change of network configurations.
2016/11/26 10:48:57:753  Shimo detected a change of network configurations.
2016/11/26 12:07:11:683  System is waking from sleep -> reconnecting sleepin
seconds
2016/11/26 12:07:13:502  Shimo detected a change of network configurations.
```

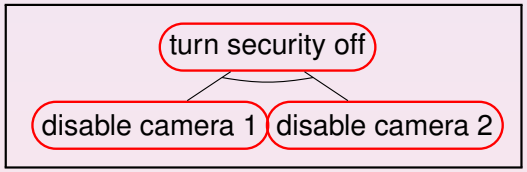
formalized as a trace:

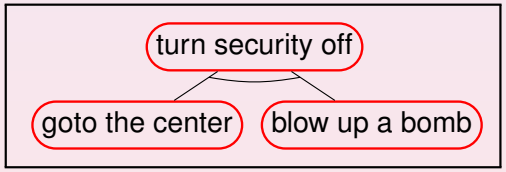
notmonitor1	notmonitor2	∅	frozen1	frozen2 frozen12	enterb frozen12	hasPaint frozen12

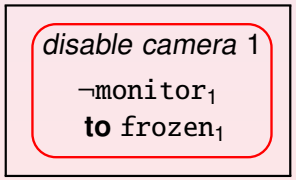
Library

A catalog of known attack patterns

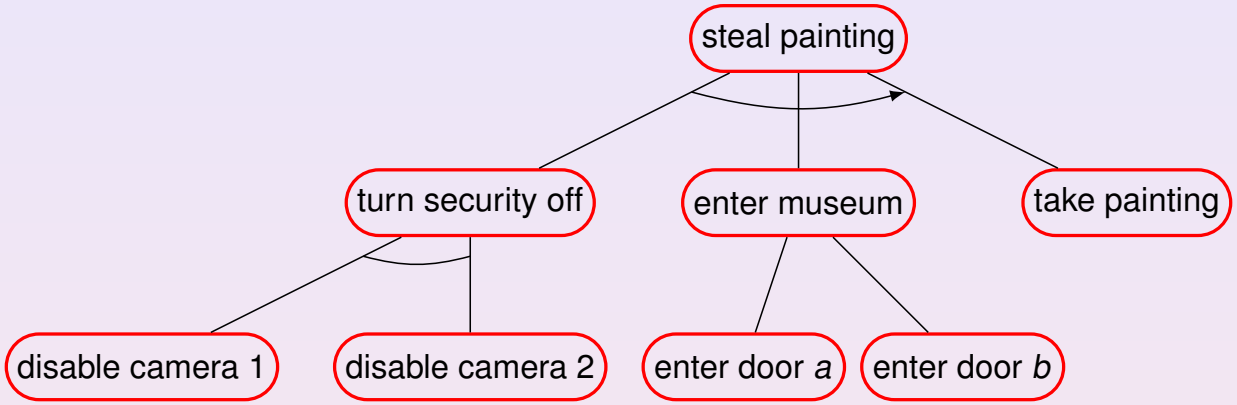
1. 

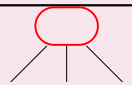
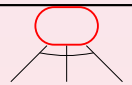
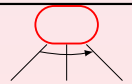
2. 

3. 

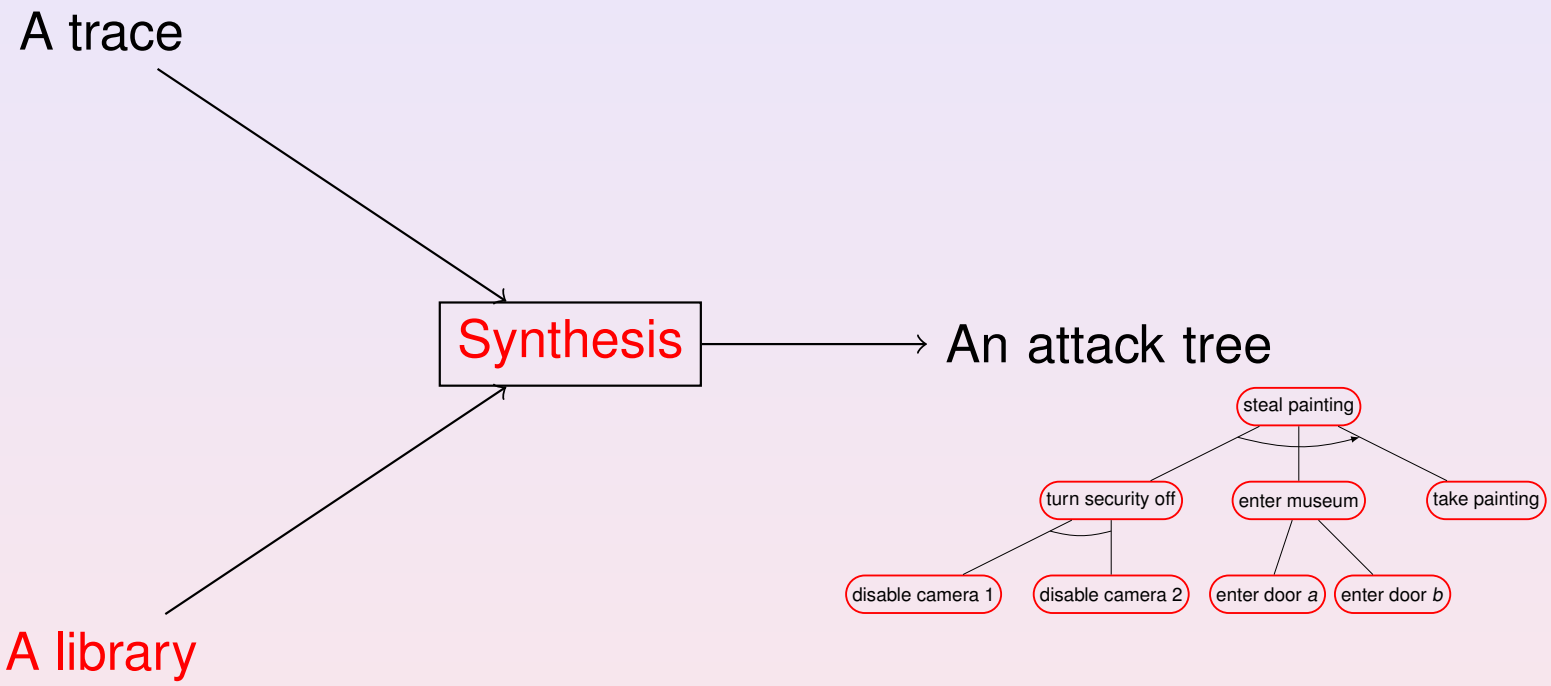
4. 

Semantics of attack trees



attack tree		explains trace *t* if
leaf		*t* achieves primitive task (direct notion)
`OR` node		at least one child tree explains *t*
`AND` node		*t* is a merge of traces explained by child trees
`SAND` node		*t* is a sequence of traces explained by child trees

Library-based attack tree synthesis



Synthesis specifications : build an attack tree that

1. explains the input trace
2. rests upon the input library

Outline

Attack tree synthesis ∼ Parsing

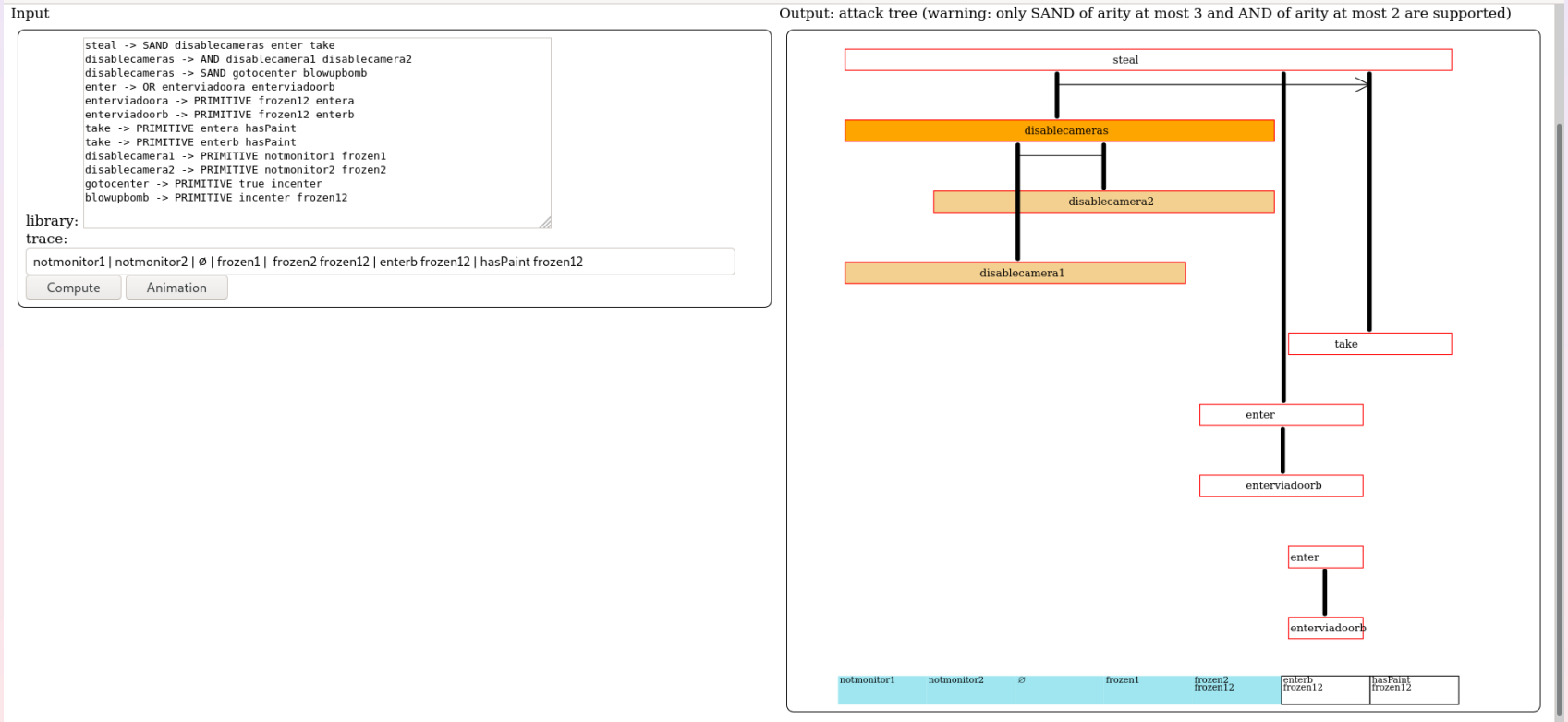
Algorithmic principles

- Trace ∼ Formal word
- Library attack patterns ∼ Grammar rules
- Attack tree ∼ Syntactic tree

Bottom-up approach ∼ Cocke-Younger-Kasami parsing algorithm

Online tool

http://attacktreesynthesis.irisa.fr/



Outline

Theoretical complexity

Theorem

The library-based attack tree synthesis is NP-complete.

- Still, polynomial in the length of the input trace!
- NP-membership: given algorithm
- NP-hardness: reduction from the Packed Interval Coverage, essentially due to `AND` operator.

Theorem

For bounded `AND`-arity libraries, synthesis is in P*.*

Outline

Conclusion

- A formal library-based attack tree synthesis problem
- An algorithm and an online protoype tool
- A complete study of the theoretical complexity
  $\Rightarrow$ Algorithm essentially optimal
- Bounded `AND`-arity in libraries is a realistic assumption

Perspectives

Theoretical:

- More abstract attack patterns: first-order features in rules as in (Jhawar et al. 2018) and (Ivanova et al. 2015)
- Library-based attack tree synthesis for a set of traces

Practical:

- Scalability of the tool, e.g. parsing optimisation techniques
- Bridge the gap with libraries in practice, e.g. MITRE-ATT&CK

Thank you for your attention!