# Causal Model Extraction from Attack Trees to Attribute Malicious Insider Attacks

**Amjad Ibrahim,** Simon Rehwald, Antoine Scemama,

Florian Andres, Alexander Pretschner

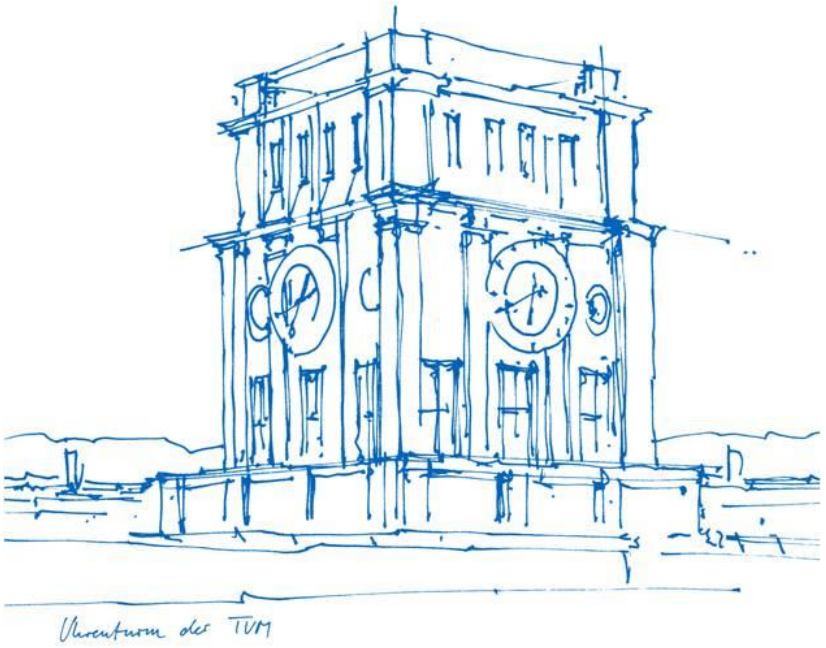
Technische Universität München

Department of Informatics

Chair of Software & Systems Engineering

The Seventh International Workshop on

Graphical Models for Security- **GraMSec 2020**



# Introduction

"Hide it or lose it"!

What Tesla's Spygate Teaches Us About Insider Threats

Forbes Technology Council

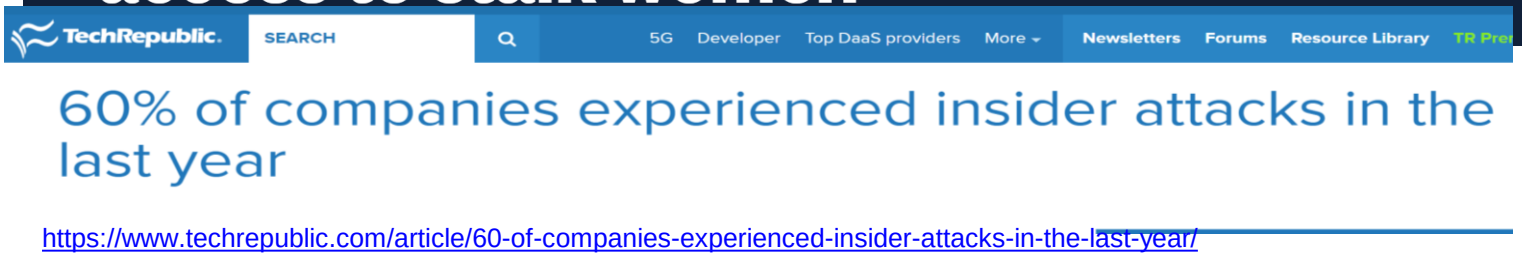
Tom Kemp Forbes Councils Member

Forbes Technology Council COUNCIL POST | Paid Program

Innovation

https://www.forbes.com/sites/forbestechcouncil/2018/07/19/what-teslas-spygate-teaches-us-about-insider-threats/#3ccd1c735afe

Facebook fires engineer who allegedly used access to stalk women



TechRepublic. SEARCH 5G Developer Top DaaS providers More Newsletters Forums Resource Library TR Pre

60% of companies experienced insider attacks in the last year

https://www.techrepublic.com/article/60-of-companies-experienced-insider-attacks-in-the-last-year/

# Introduction

- Mostly non malicious
  - Accountability
    - Attack attribution a deterrent measure
    - Assigning blame
- Accountable system can answer questions regarding the **cause** of some event
  - System monitoring
  - Model-based causality analysis
- In this paper, we propose
  - A methodology to automatically create causal models in the context of insiders from attack trees
  - An open-source tool (ATCM) that implements the approach
  - An evaluation of the efficiency, the validity of the approach, and the electiveness of the model.

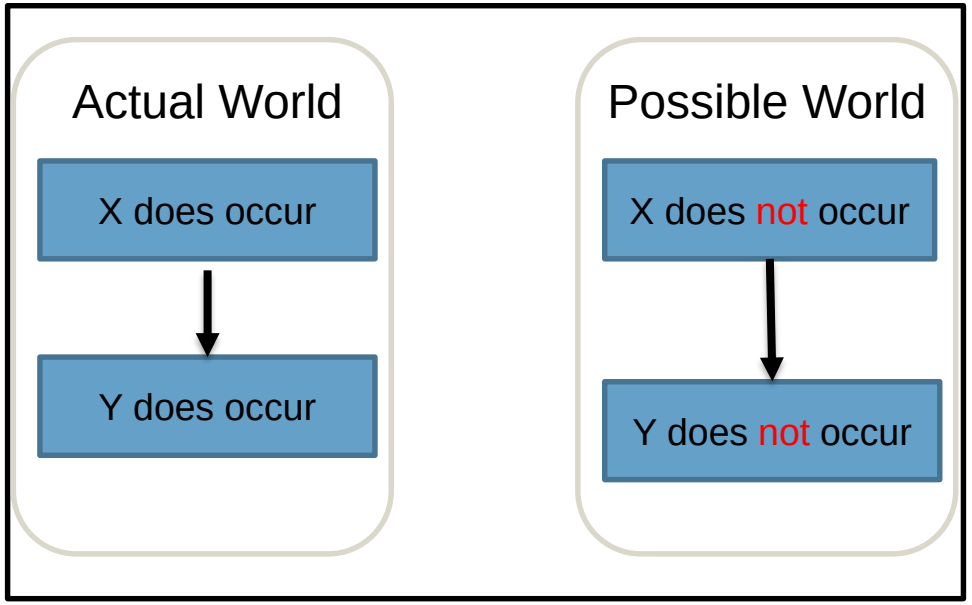
# BACKGROUND

# A Counterfactual Cause is..

"…Or, in other words, where, if the first object had not been, the second never had existed " (Hume 1748 sec. VII).

David Hume

Lewis's Definition of cause:
"X has caused Y" if "Y would not have occurred if it were not for X "
(Lewis 1986)

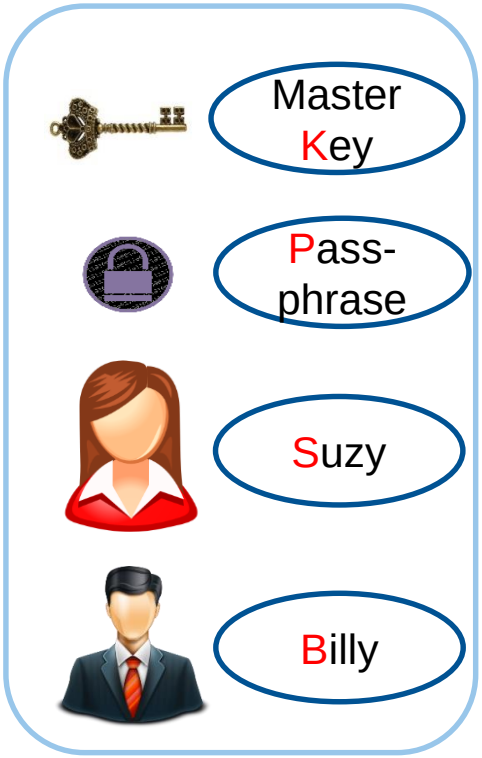


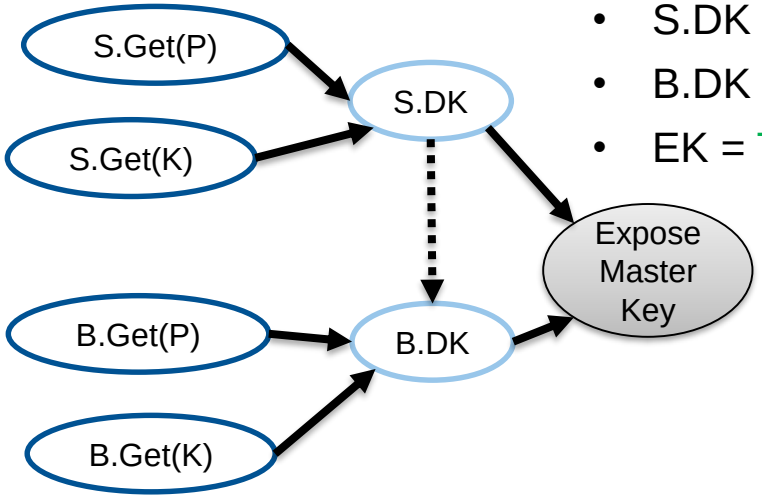
# Halpern and Pearl definition of Actual Causality

- Causal models [Pearl 1996]
  - Structural equations represent mechanisms of the world
  - Variables represent properties of the world
  - Interventions

- Causal Model: M=(U, V, R, **F**) [Halpern and Pearl 2000]
  - **U**: Set of exogenous variables
  - **V:** Set of endogenous variables
  - **R**: Associates with each variable a set of possible values
  - **F**: Associates a function $F_X$ with each $X \in V$
  - Visualization via Causal Networks

# Example




Context

- S.Get(P)/B.Get(P) = T/T
- S.Get(K)/B.Get(K) = T/T
- S.DK = T AND T = T
- B.DK = T AND T AND F = F
- EK = T OR F = T

- S.Get(P)/B.Get(P) = read the passphrase file
- S.Get(K)/B.Get(K) = Suzy/Billy queried the key
- S.DK = S.Get(P) AND S.Get(K) (Suzy decrypts the key)
- B.DK = B.Get(P) AND B.Get(K) AND !S.DK (Billy decrypts)
- EK = S.DK OR B.DK

# Why HP?

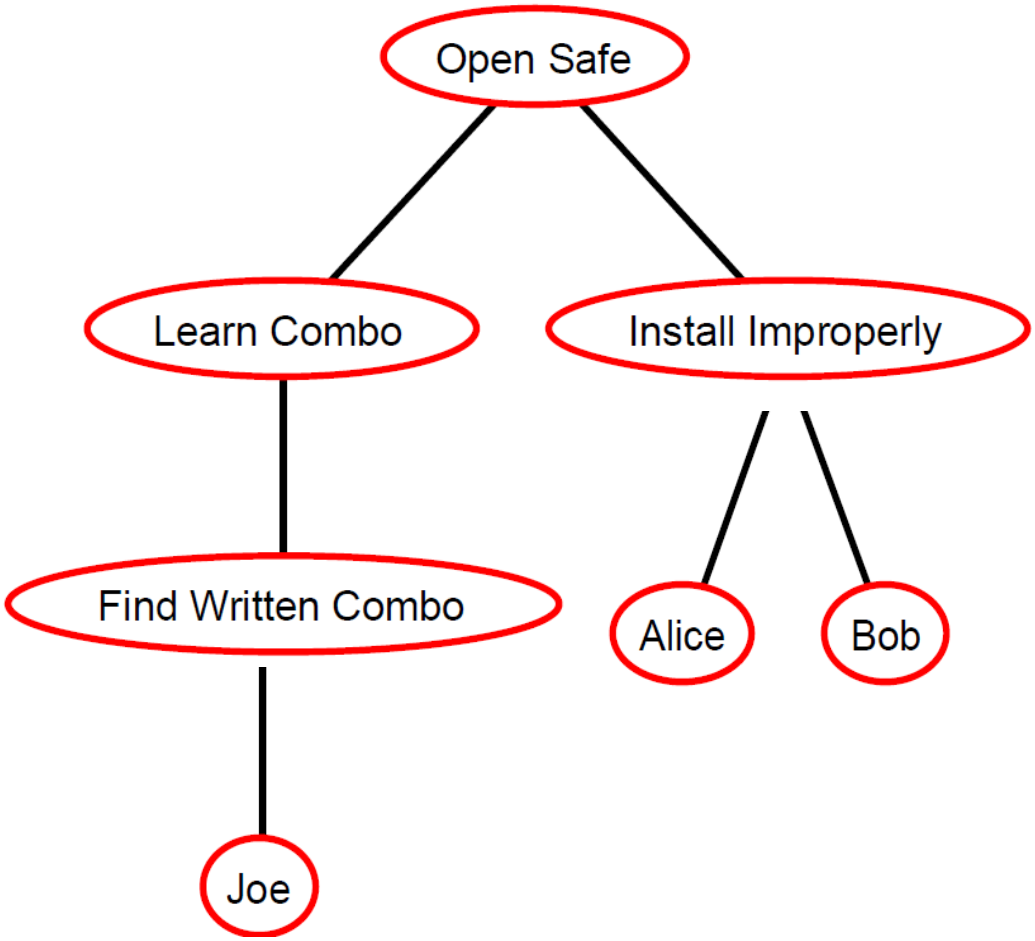
- Preemption
- Irrelevance
- Conjunction and disjunction of events
- Non-occurrence of events

- ”…no right model…” [Halpern 2016]
  - Considerable influence of the model on the result
  - Domain specific

# Sources for models: Attack Trees

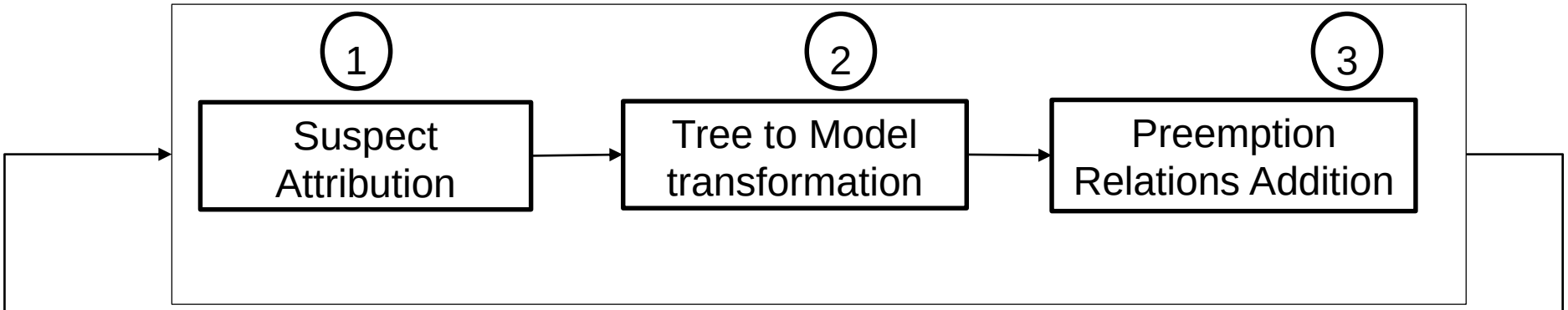
- Describe potential threats and the steps necessary to successfully perform
  - Root node contains the ultimate goal of an attack tree
  - Sub-nodes describe activities that are necessary to accomplish the respective parent activity/goal
  - Formal
  - Graphical

# Attack Trees** ≠ Causal Models

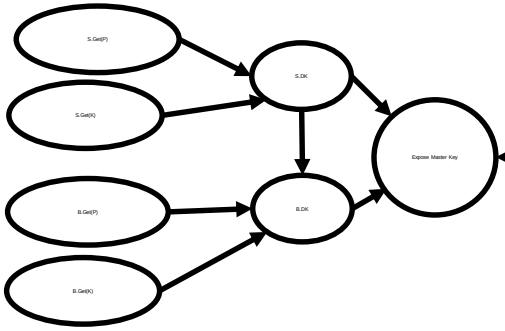



**All the attack trees in this presentation are drawn using ADTool

# Methodology for Causal Modeling







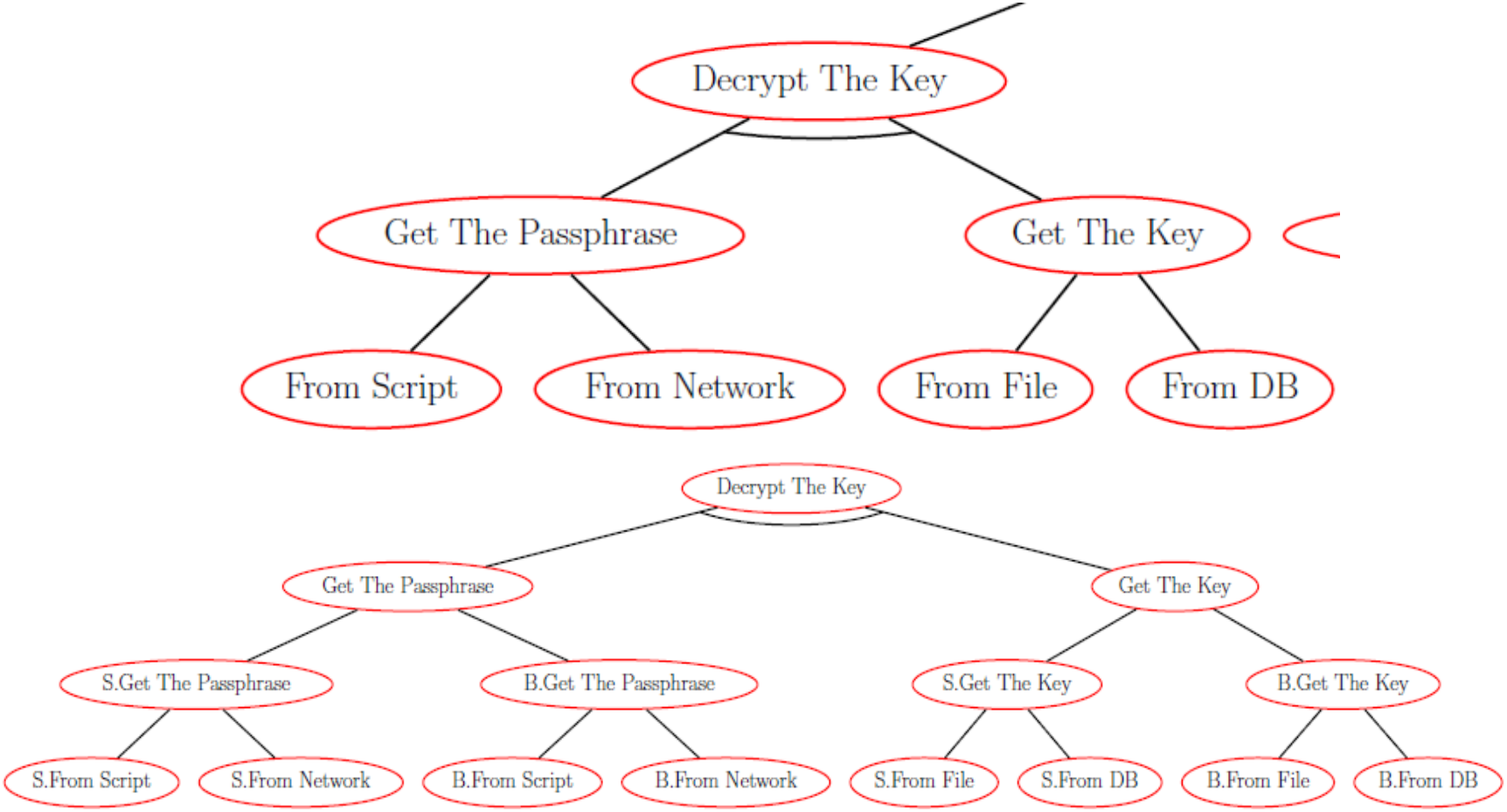
# Suspect Attribution

- Automatically adding instance of roles to a tree
  - Duplicating parts of the tree followed by allotting the new parts to one suspect

**Definition 4.** *A subtree* $\mathcal{B} = (\mathcal{N}, \rightarrow, n_0, [[n]])$ *is attributed with suspects* $\{s_1, s_2, \ldots s_l\}$ *by: 1) Creating a set (size* $l$*) of* $\mathcal{B}$ *duplicates, denoted* $\{\mathcal{B}_1, \mathcal{B}_2 \ldots \mathcal{B}_l\}$*. A duplicate* $\mathcal{B}_i$ *contains the nodes of* $\mathcal{B}$ *with every node renamed with* $i$ *suffix. 2) Constructing a new tree* $\mathcal{AB}$ *with root* $n_0$ *from* $\mathcal{B}$*, then adding the disconnected* $\{\mathcal{B}_1, \mathcal{B}_2 \ldots \mathcal{B}_l\}$*, and connecting their root nodes using an OR function with* $n_0$*.*

- Where do we attribute
  - Trees that model different attack vectors

# Attribution Level



# Adding Roles to Attack trees

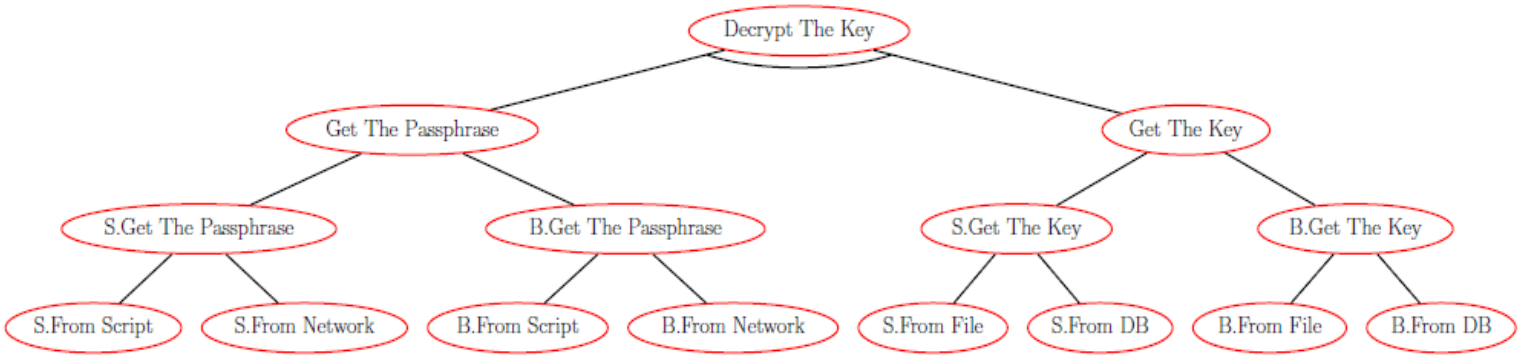
- Depends on the structure and the and the semantics of the branch
- Unfolding after the last AND gate allows considering any possibility of colluding attacks, in some cases it may be unnecessary.

# Tree Transformation

**Definition 6.** ***Attack Tree To Causal Model***

*$AT = (\mathcal{N}, \rightarrow, n_0, [[n]])$ is mapped to a $M = (\mathcal{U}, \mathcal{V}, \mathcal{R}, \mathcal{F})$ i.e. $AT \rightarrowtail M$ as follows*

- *$\mathcal{U} = E(AT)$, where $E(AT)$ returns the leaf nodes of a tree $AT$*
- *$\mathcal{V} = \mathcal{N} \backslash E(AT)$, where $\backslash$ is the difference between two sets.*
- *$\mathcal{R} = \{0, 1\}$.*
- *$\mathcal{F}$ associates with each $X \in \mathcal{V}$ a propositional formula $F_X = [[X]]$, which corresponds to the semantical formula from the AT*

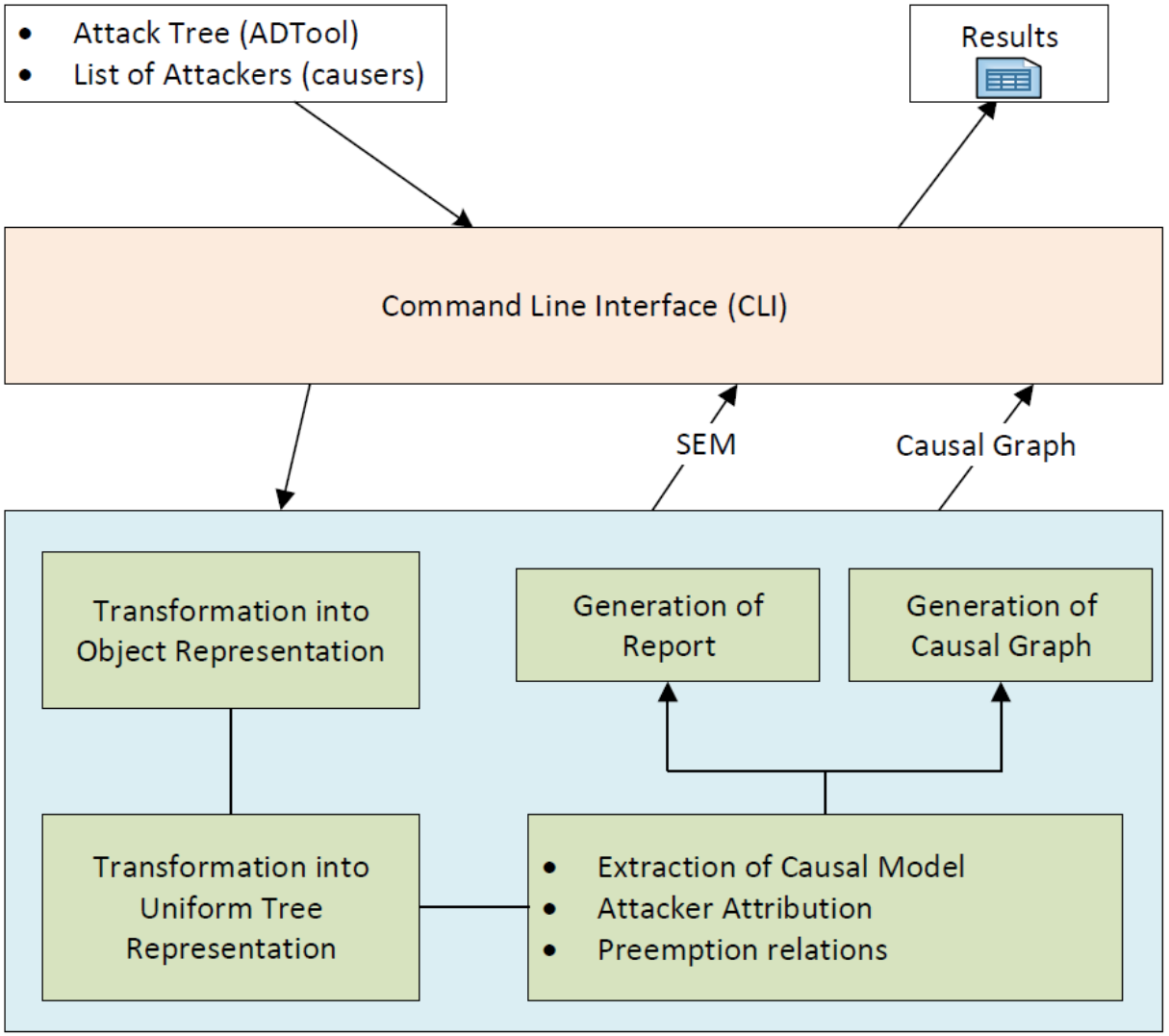


# Adding Preemption Relations

- Preemption relations relate variables about same event for different suspects
  - They represent disparity between suspects
  - Hard to model from different facts
    - Suzy's privileges in a system
    - Billy's criminal record ….
- For automation relate them to metrics of insiders' risk assessment.
  - Suspiciousness metric (SM): aggregates ability to perform an event or willingness attack
  - Calculation is incident-specific: it can be a simple reflection of privileges in the system; it can be a sum of weighted factors
- Location : among attribution variables one level after the attribution level
  - two variables with an edge from the the more suspicious suspect (higher SM) to the less suspicious suspect (in case of equal values the edge is not added).

- Semantically, the preemption relation is represented by a not clause (!X) added to the less suspicious (i.e. smaller value) suspect about the higher suspicious suspect

# Tool Support



# Evaluation

| Class | Use Case | Nodes | # Potential Attackers |
|---|---|---|---|
| HP | $HP_1$ | 3 | 2 |
| | $HP_2$ | 2 | 2 |
| Insider (Industry) | Steal Master Key | 12 | $\{2, 8\}$ |
| Insider (Literature) | $BecomeRootUser_1$ | 8 | $\{2, 8\}$ |
| | $BecomeRootUser_2$ | 11 | $\{2, 8\}$ |
| Artificially Generated | $Artificial_1$ | 255 | $\{2, 8\}$ |
| | $Artificial_2$ | 1017 | $\{2, 8\}$ |
| | $Artificial_3$ | 3057 | $\{2, 8\}$ |

- Efficiency of the process: model expansion and automation
- Validity of the model
- Effectiveness of the model:
  - Threat analysis → Attack Trees → Implement the attacks → Check the logs
  - Formulated queries

# Conclusions

- Problem: insider threat and preventive measures
- Solution: accountability through supporting causal reasoning
  - A methodology that automatically constructs  HP causal models form attack trees
    - Suspect attribution while allowing colluding.
    - Preemption relations.
  - Efficiency of the process, validity and effectiveness of the model
- Future Work
  - Consider more elements of threat models
    - Examples: notions of attack-defense trees, SAND attack trees

# Thanks For Your Attention!

# HP Definition (Informal)

$A\ set\ of\ events\ \vec{X} = \vec{x}$ is an actual cause of $\varphi$ given a model if the following three conditions hold [Halpern 2015]:

**AC1.** $both$ the cause and the effect actually happened

**AC2.** Changing the original values of $\vec{X}$ to a different setting $\overrightarrow{x'}$ while keeping a possibly empty set ($\overrightarrow{W}$) of the remaining variables at their original value, $\varphi$ does not occur anymore.

**AC3.** $\vec{X}$ is minimal; no subset of $\vec{X}$ satisfies conditions AC1 and AC2.

# Example

Context

- S.Get(P)/B.Get(P) = T/T
- S.Get(K)/B.Get(K) = T/T
- S.DK = T AND T = T
- B.DK = T AND T AND F = F
- EK = T OR F = T

Is S.Get(K) a cause?

Set S.Get(K) = F and $\overrightarrow{W}$ = ∅

- S.Get(P)/B.Get(P) = T/T
- S.Get(K)/B.Get(K) = F /T
- S.DK = T AND F = F
- B.DK = T AND T AND T = T
- EK = F OR T = T

$\varphi$ still occurs → AC2

Set S.Get(K) = F and and $\overrightarrow{W}$ = {B.DK}

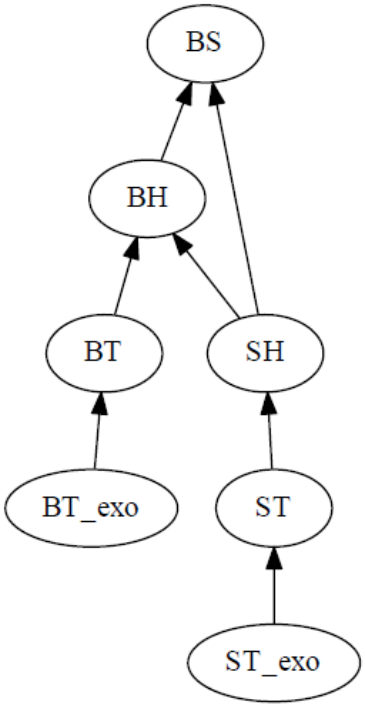
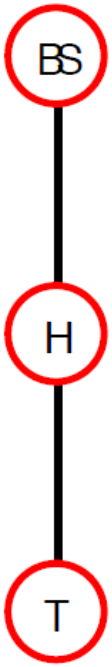
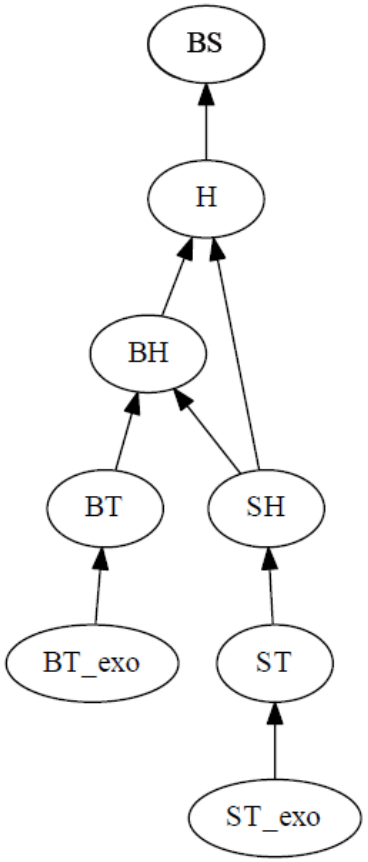
- S.Get(P)/B.Get(P) = T
- S.Get(K)/B.Get(K) = F/T
- S.DK = T AND F = F
- B.DK = ~~T AND T AND T~~ = F
- EK = F OR F = F

$\varphi$ does not occur anymore → AC2

# Evaluation: Efficiency of the extraction

| | | | | 2 Suspects | | | | | | 8 Suspects | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Top | | Middle | | Leafs | | Top | | Middle | | Leafs | |
| **AT** | **n** | **l** | **b** | **n** | **exec(s)** | **n** | **exec(s)** | **n** | **exec(s)** | **n** | **exec(s)** | **n** | **exec(s)** | **n** | **exec(s)** |
| **SMK** | 12 | 5 | 2 | 37 | 0.0002 | 36 | 0.0002 | 36 | 0.0003 | 139 | 0.0004 | 126 | 0.0004 | 108 | 0.0004 |
| **Be.Root1** | 8 | 4 | 1 | 24 | 0.0002 | 25 | 0.0002 | 23 | 0.0002 | 90 | 0.0004 | 91 | 0.0004 | 71 | 0.0004 |
| **Be.Root2** | 11 | 4 | 1 | 32 | 0.0002 | 35 | 0.0002 | 32 | 0.0003 | 122 | 0.0006 | 125 | 0.0006 | 98 | 0.0006 |
| $T_1$ | 255 | 8 | 2 | 767 | 0.0069 | 767 | 0.0117 | 767 | 0.0512 | 3059 | 0.0283 | 2879 | 0.0460 | 2303 | 0.1925 |
| $T_2$ | 1017 | 8 | 8 | 3065 | 0.0354 | 3065 | 0.1133 | 3065 | 0.7473 | 12233 | 0.1380 | 11513 | 0.4610 | 9209 | 2.99 |
| $T_3$ | 3057 | 8 | 16 | 6129 | 0.0939 | 6129 | 0.4084 | 6129 | 2.94 | 24465 | 0.3700 | 23025 | 1.65 | 18417 | 11.97 |

# Validity of the Models

| Example | HP Model | Attack Tree | Our Model |
|---|---|---|---|
| Rock-Throwing |  |  |  |