Quantitative Attack Tree Analysis: Stochastic Bounds and Numerical Analysis

Nihal Pekergin, LACL, Université Paris Est-Créteil

with collaboration Sovanna Tan (LACL, UPEC)
Jean-Michel Fourneau (DAVID, UVSQ)

Motivation

- Efficient numerical analysis of temporal properties of Attack Trees
- Inputs: discrete probability distributions (times to success of Basic Attacks) *typically obtained from measurements*
- Algorithms on discrete distributions
- Output: distribution of the time that the attack of the whole system would be successful
- Problem: the size of the distributions may increase after each operation which may be high time consuming
- Answer: using the strong stochastic ordering $\leq_{st}$ to obtain a bound of the results with a smaller size

Attack Trees (AT)

- non state-space models to illustrate graphically attack scenarios
- similar to fault trees in reliability (safety)

  cross-fertilization between safety and security engineering have been stated by many authors in the literature
- leaves : Basic Attacks (BA)
- internal nodes : logical operators

  AND : both inputs must be TRUE

  OR : at least one input must be TRUE
- static ATs are extended to dynamical ATs

Dynamical Attack Trees

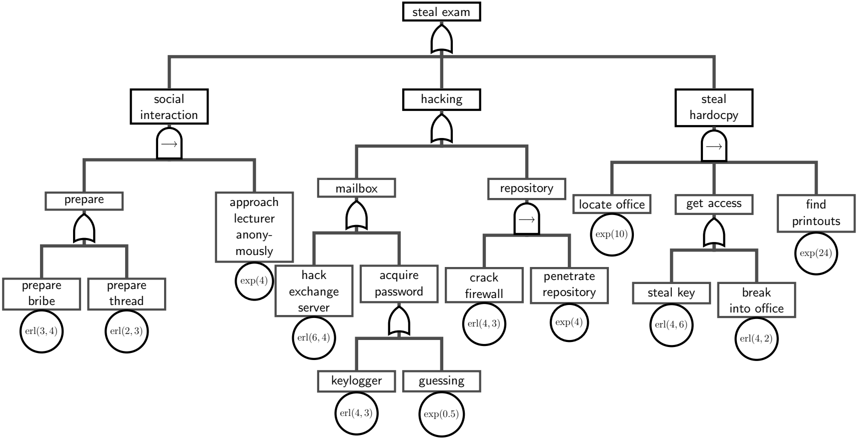
- input distributions : associated to the leaves represent the time that input becomes TRUE

  success time of the underlying BA

- gates: AND, OR, SEQ (sequential dependencies)
- output distribution of a gate: attack (compromising) time for the subsystem having the gate as root
- output distribution at the root of the AT : attack time for the whole system

  the temporal success probabilities of the attack scenario defined by the AT

Attack Tree *Steal Exam*



Logical gates

- input distributions are any discrete distribution
  efficient algorithms
- input distributions are mutually independent
- X_i discrete random variable of size $l_i, \;\; i = 1, 2$
- $AND(X_1, X_2) = max(X_1, X_2)$
  $\Pr(O = a) = \Pr(X_1 = a) \times \Pr(X_2 < a) + \Pr(X_2 = a) \times \Pr(X_1 < a) + \Pr(X_1 = a) \times \Pr(X_2 = a)$
- $OR(X_1, X_2) = min(X_1, X_2)$
  $Pr(O = a) = \Pr(X_1 = a) \times \Pr(X_2 > a) + \Pr(X_2 = a) \times \Pr(X_1 > a) + \Pr(X_1 = a) \times \Pr(X_2 = a)$
- $SEQ(X_1, X_2) = X_1 + X_2 \; (convolution)$
  $\Pr(O = a) = \sum_k \Pr(X_1 = k) \times \Pr(X_2 = a - k)$

Complexities

- AND and OR gates:
  - **Max size:** $l_1 + l_2 - 1$.
  - **Algorithm :** If sorted $\Theta(l), \quad l = max(l_1, l_2)$
    $\Theta(l \times \log l)$
- SEQ gate
  - **Max size:** $l_1 \times l_2 - 1$.
  - **Algorithm :**
    Naive approach $\Theta(l_1 \times l_2)$
    Discrete Fast Fourier $\Theta(l \times \log l)$

Due to the successive application of these operations, distribution sizes increase so the time complexity

Bounding distributions

$\leq_{st}$ order between random variables:

$$X \leq_{st} Y \quad \Leftrightarrow \quad \mathrm{E}[f(X)] \leq \mathrm{E}[f(Y)]$$

for all increasing function f, when the expectations E exist

first-order stochastic dominance in the economics literature

- *If* $X \leq_{st} Y$, *then* $\mathrm{E}[X] \leq \mathrm{E}[Y]$
- $\Pr(X \leq a) \geq \Pr(Y \leq a) \ \ \forall a$
- $\Pr(X > a) \leq \Pr(Y > a) \ \ \forall a$

Example:

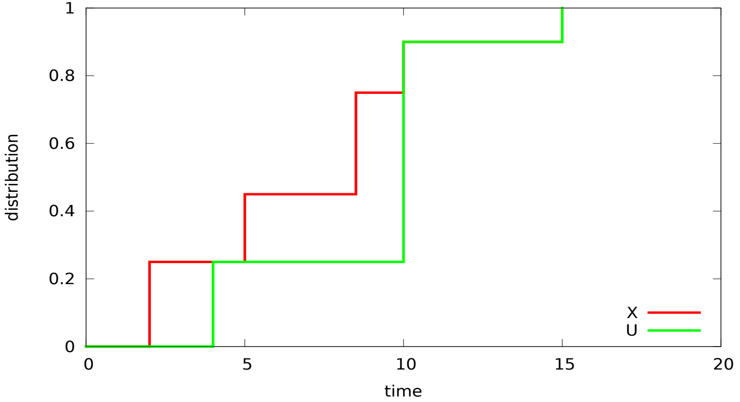
Let X be the time at which a basic attack (a leaf in the AT) would be successful.

$\mathcal{V}_X$	2	5	8.5	10	15
$\mathcal{P}_X$	0.25	0.2	0.3	0.15	0.1

Let U be the upper bound

$\mathcal{V}_U$	4	10	15
$\mathcal{P}_U$	0.25	0.65	0.1

X and U cumulative distributions



Attack success probabilities

The probability that the attack associated with the random variable X would be successful at time t:

$$\sum_{\{i|\mathcal{V}_X[i]\leq t\}} \mathcal{P}_X[i]$$

If $X \leq_{st} U$, then $\forall t$, the success probability before or at time t for the attack associated with X is greater than that of U.

Monotonicity of gates

AND, OR, SEQ are monotone:

increase of inputs $\rightarrow$ *increase of output*

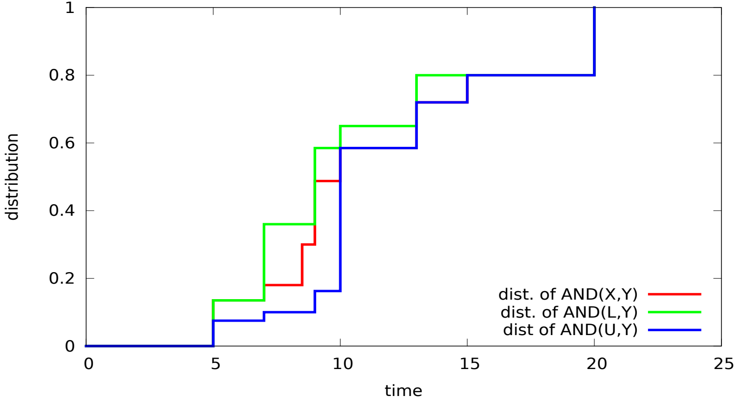
$\mathcal{V}_Y \| 5$	7	9	13	20
$\mathcal{P}_Y \| 0.3$	0.1	0.25	0.15	0.2

$\mathcal{V}_L \| 2$	7	10
$\mathcal{P}_L \| 0.45$	0.45	0.1

Monotonicity of AND *gate:*

$$AND(L,Y) \leq_{st} AND(X,Y) \leq_{st} AND(U,Y)$$

Monotonicity of AND gate



Sizes: $AND(U,Y) = 7$, $AND(L,Y) = 6$ $AND(X,Y) = 8$

Success probabilities for $t = 7$:

$AND(U,Y) = 0.1$, $AND(X,Y)$ =0.18, $AND(L,Y)$ =0.36

Algorithm

Require: AT: A
input distributions for the leaves: $\mathcal{D}$
max number of bins of a distribution : $n \in \mathbb{N}$

Ensure: Output distribution at the root of A.

```
Label the gates using the topological order from bottom-up.
for all gates g in the ascending order of the labels do
    Evaluate the output distribution of gate g
    If the size of the output distribution is larger than n,
    reduce its size to n.
end for
```

Bounding Algorithms

- Trade-off between the accuracy of results and the complexity
- optimal bounding distributions with respect to an increasing positive reward
  high complexity: $\Theta(N^2 n)$,
  N: the size of the original distribution and
  n : the size of the bounding distribution
- greedy algorithm with complexity $\Theta(N \log N)$
- naive approach $\Theta(N)$.

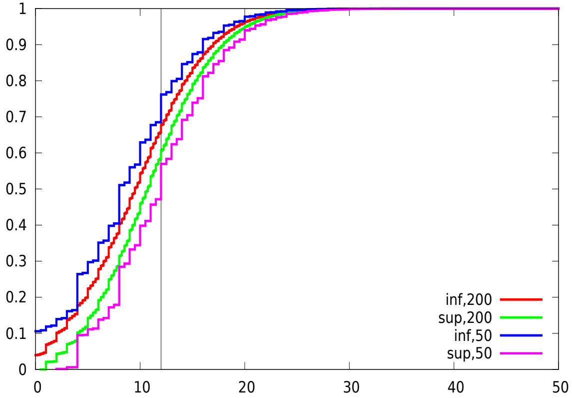
Usefulness of the bounding approach

- Reduced-size bounding distributions $\rightarrow$ decrease the algorithmic complexity

- Difficulty to estimate temporal behaviors of basic attacks. Bounds in the context of the uncertainty are useful

- Checking constraints:
  - output distributions: $d_L \leq_{st} d \leq_{st} d_U$
  - success probabilities for a fixed t: $p_U \leq p \leq p_L$
    - if $p_L < threshold$, then the constraint is satisfied
    - if $p_U \geq threshold$, then the constraint is not satisfied
    - otherwise, the bounds must be refined (the number of bins must be increased)

Output distribution for *Steal Exam*



$t = 12$

- 50 bins : $0.57 \leq p \leq 0.76$
- 200 bins: $0.606 \leq p \leq 0.677$

Conclusions

- The quantitative analysis of attack trees are very useful to highlight the impact of the potential countermeasures that can be taken to reinforce the security of the system
- Due to the stochastic monotonicity properties of the AND, OR, SEQ gates, the upper and lower discrete, reduced-size, bounding distributions can be efficiently derived
- Bounds are relevant when the quantitative evaluation is done to check security constraints
- Trade-off between the accuracy and the time complexity