The Serial Model of Attack trees

Aivo Jürgenson, Margus Niitsoo, Jan Willemson

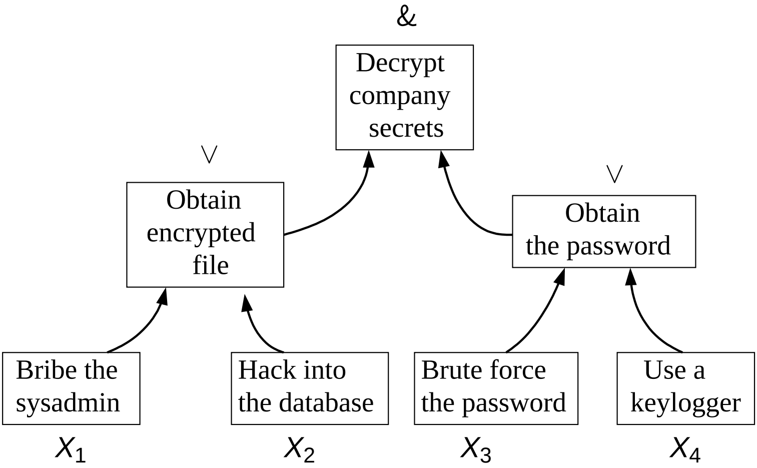
Cybernetica AS, University of Tartu

Theory Days, oct. 2-4, 2009

Attack trees

- Model for adversary behavior in attacking a system
- One central root goal
- Recursively down into subattacks
  - & nodes - all subattacks need to succeed
  - $\vee$ nodes - one of the subattacks needs to succeed
- Can be used to estimate many different parameters

Attack tree - Example



History

- Used since the 70-es for failiure and threat analysis
- Made famous by Bruce Schreiner in ’99
- Buldas, Laud, Priisalu, Saarepera, Willemson - ’06
  - Financial analysis
  - Gains of root threat g
  - Two parameters – expenses e_i and success probability p_i.
  - Attacks made in parallel

Computation in Buldas et al Model

- Computation proceeds from leaves to the root
  - Add the costs in and node
  - Take the cheapest choice in the or-node
- Just like in all the previous models with other parameters

Computation in Buldas et al Model

- Computation proceeds from leaves to the root
  - Add the costs in and node
  - Take the cheapest choice in the or-node
- Just like in all the previous models with other parameters
- Semantically complete nonsense

Work of Jürgenson and Willemson

- Proved BLPSW06 was nonsense
- Parallel model with sensible semantics
    - A small loss of computational efficiency...

Work of Jürgenson and Willemson

- Proved BLPSW06 was nonsense
- Parallel model with sensible semantics
  - A small loss of computational efficiency...
  - $O(n) \longrightarrow O(2^n)$

Work of Jürgenson and Willemson

- Proved BLPSW06 was nonsense
- Parallel model with sensible semantics
  - A small loss of computational efficiency...
  - $O(n) \longrightarrow O(2^n)$
  - Small trees can still be analyzed
  - Aivo is working on optimization and an approximate solver

Work of Jürgenson and Willemson

- Proved BLPSW06 was nonsense
- Parallel model with sensible semantics
  - A small loss of computational efficiency...
  - $O(n) \longrightarrow O(2^n)$
  - Small trees can still be analyzed
  - Aivo is working on optimization and an approximate solver
- However - not good enough!

The Serial Model of Willemson

- New intuition:
  - Attacks take place one after the other
  - Adversary sees the past outcomes
  - Can skip an attack if it does not help
- Linear computation time

The Serial Model of Willemson

- New intuition:
  - Attacks take place one after the other
  - Adversary sees the past outcomes
  - Can skip an attack if it does not help
- Linear computation time
  - In a bizarre model where an attack is always performed if it can influence the final outcome (irrespective of the cost)

The Serial Model of Willemson

- New intuition:
  - Attacks take place one after the other
  - Adversary sees the past outcomes
  - Can skip an attack if it does not help
- Linear computation time
  - In a bizarre model where an attack is always performed if it can influence the final outcome (irrespective of the cost)
- a "dirty hack" – consider subsets of attacks

The Serial Model of Willemson

- New intuition:
    - Attacks take place one after the other
    - Adversary sees the past outcomes
    - Can skip an attack if it does not help
- Linear computation time
    - In a bizarre model where an attack is always performed if it can influence the final outcome (irrespective of the cost)
- a "dirty hack" – consider subsets of attacks
- "Modeling cost-sensitive terrorist behavior"

Our new model

- Similar:
  - Fix an order of attacks
  - At each point the past results are known
- Different:
  - Separate descisions possible for each history
  - Optimize for maximal expected outcome

Our new model

- Similar:
  - Fix an order of attacks
  - At each point the past results are known
- Different:
  - Separate descisions possible for each history
  - Optimize for maximal expected outcome
- Basically - the classic model of economic decision theory!
  - Less likely to be flawed

Computability

- Base model: Decision tree
  - Greedy back-to-front optimization in time linear in tree size

Computability

- Base model: Decision tree
  - Greedy back-to-front optimization in time linear in tree size
  - Trees are exponential sized

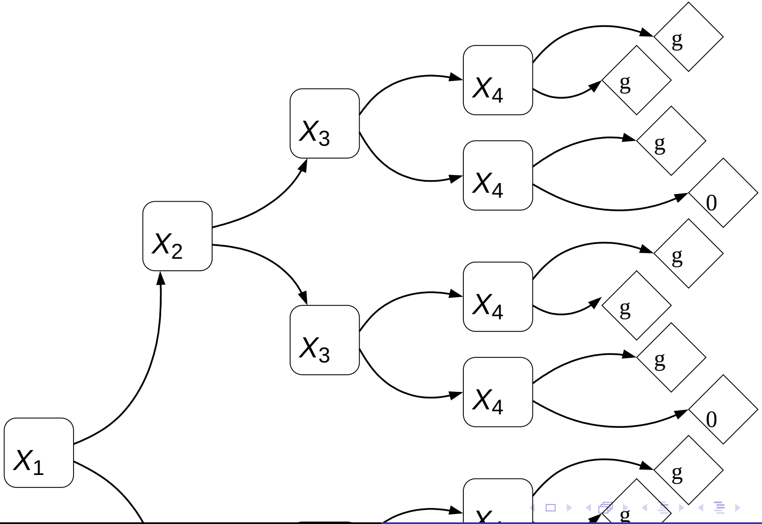
Computability

- Base model: Decision tree
  - Greedy back-to-front optimization in time linear in tree size
  - Trees are exponential sized
  - Decisions can be identical
  - We can combine them

Computability

- Base model: Decision tree
  - Greedy back-to-front optimization in time linear in tree size
  - Trees are exponential sized
  - Decisions can be identical
  - We can combine them
  - Size of the problem is greatly reduced

Decision tree - Example



Computability

- Base model: Decision tree
  - Greedy back-to-front optimization in time linear in tree size

Computability

- Base model: Decision tree
  - Greedy back-to-front optimization in time linear in tree size
  - Trees are exponential sized

Computability

- Base model: Decision tree
  - Greedy back-to-front optimization in time linear in tree size
  - Trees are exponential sized
  - Decisions can be identical
  - We can combine them

Computability

- Base model: Decision tree
  - Greedy back-to-front optimization in time linear in tree size
  - Trees are exponential sized
  - Decisions can be identical
  - We can combine them
  - Size of the problem is greatly reduced

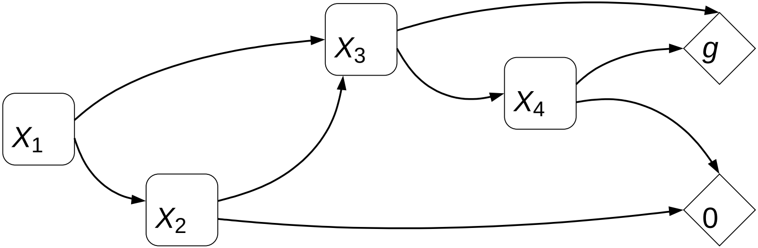
Computability

- Base model: Decision tree
  - Greedy back-to-front optimization in time linear in tree size
  - Trees are exponential sized
  - Decisions can be identical
  - We can combine them
  - Size of the problem is greatly reduced
- Final model: Binary Decision Diagrams

Computability

- Base model: Decision tree
  - Greedy back-to-front optimization in time linear in tree size
  - Trees are exponential sized
  - Decisions can be identical
  - We can combine them
  - Size of the problem is greatly reduced
- Final model: Binary Decision Diagrams
  - Structurally, anyways

Binary Decision Diagrams



Mixed Blessings

- For each tree there are 2^{n-1} orders with BDD is of size n

Mixed Blessings

- For each tree there are 2^{n-1} orders with BDD is of size n
- There are orders with exponential complexity

Mixed Blessings

- For each tree there are 2^{n-1} orders with BDD is of size n
- There are orders with exponential complexity
- Real life more likely to imply orders of the first kind

Mixed Blessings

- For each tree there are 2^{n-1} orders with BDD is of size n
- There are orders with exponential complexity
- Real life more likely to imply orders of the first kind
- Orders of the second kind can be strictly better

Implications

- The model is strictly better than the previous serial model

Implications

- The model is strictly better than the previous serial model
- Strictly better outcome than parallel model
  - For any order – we can use the "good" order with $O(n)$ complexity
  - Can be used as an upper bound for that case as well

Future perspectives

- The model can be extended in many ways
  - Intermediate payments
  - Recurring subattacks
  - Continuous decisions (bribe)

Future perspectives

- The model can be extended in many ways
  - Intermediate payments
  - Recurring subattacks
  - Continuous decisions (bribe)
- Finding a good attack order

Future perspectives

- The model can be extended in many ways
  - Intermediate payments
  - Recurring subattacks
  - Continuous decisions (bribe)
- Finding a good attack order
- Sensitivity analysis for parameters e_i and p_i

Future perspectives

- The model can be extended in many ways
  - Intermediate payments
  - Recurring subattacks
  - Continuous decisions (bribe)
- Finding a good attack order
- Sensitivity analysis for parameters e_i and p_i
- Analysis of how to best strenghten the system

Thank you!

Questions? Comments?