Attack Trees
Models and Computation

Jan Willemsen, Aivo Jürgenson, Margus Niitsoo
Cybernetica, Estonia
http://www.cybernetica.eu/

January 19th, 2010
University of Luxembourg
An Attack Tree

Obtain Administrator Privileges

OR

Access System Console

OR

Enter Computer Center

Corrupt Operator

Guess Password

Look Over Sys. Admin Shoulder

Trojan Horse SA Account

Corrupt Sys. Admin

Obtain Administrator Password

OR

Obtain Access System Console

OR

Guessable Password

Encounter

Obtain File

Unattended Guest
An Attack RDAG

Introduction

Models of Attack Trees

Computational Semantics
Brief History

Hierarchical approach to security evaluation:

- Fault trees (Vesely, Goldberg, Roberts, Haasl, 1981)
- Threat logic trees (Weiss, 1991)
- Attack trees (Schneier, 1999)
- Foundations of Attack Trees (Mauw & Oostdijk, 2005)
- Multi-parameter attack trees (Buldas et al., 2006)
Our Papers

- Jürgenson, Willemsen, Processing Multi-parameter Attacktrees with Estimated Parameter Values, IWSEC 2007
- Jürgenson, Willemsen, Serial Model for Attack Tree Computations, ICISC 2009
- Jürgenson, Willemsen, On Fast and Approximate Attack Tree Computations, submitted to ISPEC 2010
- Niitsoo, Finding the Optimal Behavior for Adaptive Attack trees, submitted to ????
From Qualitative to Quantitative Analysis

Once an attack tree is complete, one can . . .

- . . . use it for qualitative description of attack scenarios
- An Attack Tree for the Border Gateway Protocol, IETF draft, 2004
Once an attack tree is complete, one can . . .

- . . . use it for qualitative description of attack scenarios
  - An Attack Tree for the Border Gateway Protocol, IETF draft, 2004
- . . . analyze some property of the attacks (cost, feasibility, skill level required, etc.)
  - Schneier, 1999
  - Mauw & Oostdijk, 2005
From Qualitative to Quantitative Analysis

Once an attack tree is complete, one can . . .

• . . . use it for qualitative description of attack scenarios
  • An Attack Tree for the Border Gateway Protocol, IETF draft, 2004
• . . . analyze some property of the attacks (cost, feasibility, skill level required, etc.)
  • Schneier, 1999
  • Mauw&Oostdijk, 2005
• . . . try to find the attack most profitable for the attacker
  • Buldas et al., 2006
Rational Attacker Paradigm

In order to find the best attack, we must assume some kind of rationality of the attacker

- The original model of Buldas et al. assumes that the attacker is a fully rational utility maximizer
Rational Attacker Paradigm

In order to find the best attack, we must assume some kind of rationality of the attacker

- The original model of Buldas et al. assumes that the attacker is a fully rational utility maximizer
- Jürgenson & Willemson, 2009, builds on another framework:
  - The attacker tries to
    - first, maximize success probability
    - second, achieve the best possible outcome
  - Hence, a certain form of irrational behavior is obtained
  - This is the first known treatment of irrational attacks using quantitative methods
Rational Attacker Paradigm

In order to find the best attack, we must assume some kind of rationality of the attacker

- The original model of Buldas et al. assumes that the attacker is a fully rational utility maximizer
- Jürgenson & Willemson, 2009, builds on another framework:
  - The attacker tries to
    - first, maximize success probability
    - second, achieve the best possible outcome
  - Hence, a certain form of irrational behavior is obtained
    - This is the first known treatment of irrational attacks using quantitative methods
- Niitsoo, 2010, has shown how to apply classical decision theory to attack tree computations
Parallel vs. Serial Approach

- Virtually all the present models of attack trees disregard the possible order of elementary attacks
  - Schneier, 1999
  - Mauw & Oostdijk, 2005
  - Buldas et al., 2006
- This restriction is unrealistic
  - The attacker can use the knowledge concerning success/failure of some elementary attacks to decide, which attacks to skip or try next
  - Intuitively, this will allow the attacker to avoid hopeless branches, thus reducing the potential penalties and increasing the expected outcome
Flavors of the Serial Model

- Blocking vs. non-blocking
  - In practice, there exist elementary attacks, failed attempt of which blocks the execution of the whole tree, e.g. due to imprisonment of the attacker
Flavors of the Serial Model

• Blocking vs. non-blocking
  • In practice, there exist elementary attacks, failed attempt of which blocks the execution of the whole tree, e.g. due to imprisonment of the attacker

• Fully adaptive vs. semi-adaptive
  • In reality, the attacker can freely choose the order of the next elementary attacks based on the results of already tried ones
  • From theoretical viewpoint, this gives a superexponential explosion
  • Hence, for an intermediate step we may limit ourselves to the model, where the attacker
    • Fixes the order of the elementary attacks in advance
    • Is only allowed to skip some of them or stop attacking altogether
The Attack Game (Buldas et al., 2006)

Attack preparation costs
The Attack Game (Buldas et al., 2006)

- **Attack preparation costs**
- Preventive security broken?
  - yes: $\mathcal{p}$
  - no: $(1 - \mathcal{p})$

Outcome = \(-\)Cost \(-\)Penalties

- yes: Gains from the attack $p$
  - yes: $\mathcal{p}$
    - yes: (1 - $\mathcal{p}$) no
  - no: $q$
    - yes: $\mathcal{p}$
      - yes: $\mathcal{p}$
        - yes: (1 - $\mathcal{p}$) no
      - no: $q$
        - yes: $\mathcal{p}$
          - yes: (1 - $\mathcal{p}$) no
          - no: $q$
            - yes: $\mathcal{p}$
              - yes: (1 - $\mathcal{p}$) no
              - no: $q$
                - yes: $\mathcal{p}$
                  - yes: (1 - $\mathcal{p}$) no
                  - no: $q$
                    - yes: $\mathcal{p}$
                      - yes: (1 - $\mathcal{p}$) no
                      - no: $q$
                        - yes: $\mathcal{p}$
                          - yes: (1 - $\mathcal{p}$) no
                          - no: $q$
                            - yes: $\mathcal{p}$
                              - yes: (1 - $\mathcal{p}$) no
                              - no: $q$
                                - yes: $\mathcal{p}$
                                  - yes: (1 - $\mathcal{p}$) no
                                  - no: $q$
                                    - yes: $\mathcal{p}$
                                      - yes: (1 - $\mathcal{p}$) no
                                      - no: $q$
                                        - yes: $\mathcal{p}$
                                          - yes: (1 - $\mathcal{p}$) no
                                          - no: $q$
                                            - yes: $\mathcal{p}$
                                              - yes: (1 - $\mathcal{p}$) no
                                              - no: $q$
                                                - yes: $\mathcal{p}$
                                                  - yes: (1 - $\mathcal{p}$) no
                                                  - no: $q$
                                                    - yes: $\mathcal{p}$
                                                      - yes: (1 - $\mathcal{p}$) no
                                                      - no: $q$
                                                        - yes: $\mathcal{p}$
                                                          - yes: (1 - $\mathcal{p}$) no
                                                          - no: $q$
                                                            - yes: $\mathcal{p}$
                                                              - yes: (1 - $\mathcal{p}$) no
                                                              - no: $q$
                                                                - yes: $\mathcal{p}$
                                                                  - yes: (1 - $\mathcal{p}$) no
                                                                  - no: $q$
                                                                    - yes: $\mathcal{p}$
                                                                      - yes: (1 - $\mathcal{p}$) no
                                                                      - no: $q$
                                                                        - yes: $\mathcal{p}$
                                                                          - yes: (1 - $\mathcal{p}$) no
                                                                          - no: $q$
                                                                            - yes: $\mathcal{p}$
                                                                              - yes: (1 - $\mathcal{p}$) no
                                                                              - no: $q$
                                                                                - yes: $\mathcal{p}$
                                                                                  - yes: (1 - $\mathcal{p}$) no
                                                                                  - no: $q$
                                                                                      - yes: $\mathcal{p}$
                                                                                        - yes: (1 - $\mathcal{p}$) no
                                                                                        - no: $q$
                                                                                           - yes: $\mathcal{p}$
                                                                                            - yes: (1 - $\mathcal{p}$) no
                                                                                            - no: $q$
                                                                                               - yes: $\mathcal{p}$
                                                                                                - yes: (1 - $\mathcal{p}$) no
                                                                                                - no: $q$
                                                                                                      - yes: $\mathcal{p}$
                                                                                                             - yes: (1 - $\mathcal{p}$) no
                                                                                                             - no: $q$
                                                                                                               - yes: $\mathcal{p}$
                                                                                                                  - yes: (1 - $\mathcal{p}$) no
                                                                                                                  - no: $q$
                                                                                                                    - yes: $\mathcal{p}$
                                                                                                                        - yes: (1 - $\mathcal{p}$) no
                                                                                                                        - no: $q$
                                                                                                                          - yes: $\mathcal{p}$
                                                                                                                             - yes: (1 - $\mathcal{p}$) no
                                                                                                                             - no: $q$
                                                                                                                               - yes: $\mathcal{p}$
                                                                                                                                  - yes: (1 - $\mathcal{p}$) no
                                                                                                                                  - no: $q$
                                                                                                                                    - yes: $\mathcal{p}$
                                                                                                                                        - yes: (1 - $\mathcal{p}$) no
                                                                                                                                        - no: $q$
                                                                                                                                          - yes: $\mathcal{p}$
                                                                                                                                             - yes: (1 - $\mathcal{p}$) no
                                                                                                                                             - no: $q$
                                                                                                                                                - yes: $\mathcal{p}$
                                                                                                                                                     - yes: (1 - $\mathcal{p}$) no
                                                                                                                                                     - no: $q$
                                                                                                                                                    - yes: $\mathcal{p}$
                                                                                                                                                                     - yes: (1 - $\mathcal{p}$) no
                                                                                                                                                                     - no: $q$
                                                                                                                                                    - no: $q$
                                                                                                                                                    - yes: $\mathcal{p}$
                                                                                                                                                    - yes: (1 - $\mathcal{p}$) no
                                                                                                                                                    - no: $q$
                                                                                                                                                    - no: $q$
                                                                                                                                                    - yes: $\mathcal{p}$
                                                                                                                                                    - yes: (1 - $\mathcal{p}$) no
                                                                                                                                                    - no: $q$
                                                                                                                                                    - no: $q$
                                                                                                                                                    - yes: $\mathcal{p}$
                                                                                                                                                    - yes: (1 - $\mathcal{p}$) no
                                                                                                                                                    - no: $q$
                                                                                                                                                    - no: $q$
                                                                                                                                                    - yes: $\mathcal{p}$
                                                                                                                                                    - yes: (1 - $\mathcal{p}$) no
                                                                                                                                                    - no: $q$
                                                                                                                                                    - no: $q$
                                                                                                                                                    - yes: $\mathcal{p}$
                                                                                                                                                    - yes: (1 - $\mathcal{p}$) no
                                                                                                                                                    - no: $q$
                                                                                                                                                    - no: $q$
                                                                                                                                                    - yes: $\mathcal{p}$
                                                                                                                                                    - yes: (1 - $\mathcal{p}$) no
                                                                                                                                                    - no: $q$
                                                                                                                                                    - no: $q$
                                                                                                                                                    - yes: $\mathcal{p}$
                                                                                                                                                    - yes: (1 - $\mathcal{p}$) no
                                                                                                                                                    - no: $q$
                                                                                                                                                    - no: $q$
                                                                                                                                                    - yes: $\mathcal{p}$
                                                                                                                                                    - yes: (1 - $\mathcal{p}$) no
                                                                                                                                                    - no: $q$
                                                                                                                                                    - no: $q$
                                                                                                                                                    - yes: $\mathcal{p}$
                                                                                                                                                    - yes: (1 - $\mathcal{p}$) no
                                                                                                                                                    - no: $q$
                                                                                                                                                    - no: $q$
                                                                                                                                                    - yes: $\mathcal{p}$
                                                                                                                                                    - yes: (1 - $\mathcal{p}$) no
                                                                                                                                                    - no: $q$
                                                                                                                                                    - no: $q$
                                                                                                                                                    - yes: $\mathcal{p}$
                                                                                                                                                    - yes: (1 - $\mathcal{p}$) no
                                                                                                                                                    - no: $q$
                                                                                                                                                    - no: $q$
                                                                                                                                                    - yes: $\mathcal{p}$
                                                                                                                                                    - yes: (1 - $\mathcal{p}$) no
                                                                                                                                                    - no: $q$
                                                                                                                                                    - no: $q$
                                                                                                                                                    - yes: $\mathcal{p}$
                                                                                                                                                    - yes: (1 - $\mathcal{p}$) no
                                                                                                                                                    - no: $q$
                                                                                                                                                    - no: $q$
                                                                                                                                                    - yes: $\mathcal{p}$
                                                                                                                                                    - yes: (1 - $\mathcal{p}$) no
                                                                                                                                                    - no: $q$
                                                                                                                                                    - no: $q$
                                                                                                                                                    - yes: $\mathcal{p}$
                                                                                                                                                    - yes: (1 - $\mathcal{p}$) no
                                                                                                                                                    - no: $q$
                                                                                                                                                    - no: $q$
                                                                                                                                                    - yes: $\mathcal{p}$
                                                                                                                                                    - yes: (1 - $\mathcal{p}$) no
                                                                                                                                                    - no: $q$
                                                                                                                                                    - no: $q$
                                                                                                                                                    - yes: $\mathcal{p}$
                                                                                                                                                    - yes: (1 - $\mathcal{p}$) no
                                                                                                                                                    - no: $q$
                                                                                                                                                    - no: $q$
                                                                                                                                                    - yes: $\mathcal{p}$
                                                                                                                                                    - yes: (1 - $\mathcal{p}$) no
                                                                                                                                                    - no: $q$
                                                                                                                                                    - no: $q$
                                                                                                                                                    - yes: $\mathcal{p}$
                                                                                                                                                    - yes: (1 - $\mathcal{p}$) no
                                                                                                                                                    - no: $q$
                                                                                                                                                    - no: $q$
The Attack Game (Buldas et al., 2006)

- Attack preparation costs
- Preventive security broken? (yes) Gains from the attack
- Preventive security broken? (no) $\frac{1 - p}{(1 - p)}$

- Attacker caught? yes
- Penalty paid $q$
- Outcome = $-\text{Cost} - \text{Penalties}$

- Attacker caught? no
- Penalty paid $q$
- Gains from the attack $\frac{1}{(1 - q)}$
- Outcome = $-\text{Cost} + \text{Gains} + \text{Penalties}$
The Attack Game (Buldas et al., 2006)

- **Attack preparation costs**
- **Preventive security broken?**
  - yes $p$
  - no $(1 - p)$
- **Gains from the attack**
  - yes $p$
- **Attacker caught?**
  - yes $q^-$
  - no $(1 - q^-)$
  - no $(1 - q^+)$

Outcome: $-\text{Cost} - \text{Penalties}$
The Attack Game (Buldas et al., 2006)

- **Attack preparation costs**
- **Preventive security broken?**
  - yes: Gains from the attack
  - no: (1 − p)
- **Penalties**
  - yes: Attacker caught?
    - yes: Penalties
    - no: (1 − q−)
  - no: (1 − q+)
- **Penalties**
  - yes: Attacker caught?
    - yes: Penalties
    - no: (1 − q+)

Outcome = −Cost − Penalties

Outcome = −Cost + Gains − Penalties

(1 − q−)

(1 − q+)

no

no

no
The Attack Game (Buldas et al., 2006)

- **Attack preparation costs**
- **Preventive security broken?**
  - yes
  - $(1 - p)$
  - no

- **Penalties**
  - paid
  - yes
  - $(1 - q^-)$
  - no

- **Outcome**
  - $\neg\text{Cost} - \text{Penalties}^-$

- **Attacker caught?**
  - yes
  - $q^-$
  - no

- **Outcome**
  - $\neg\text{Cost}$

- **Gains from the attack**
  - yes
  - $p$ (Gains from the attack)
  - no

- **Penalties**
  - paid
  - yes
  - $q^+$
  - no

- **Outcome**
  - $\neg\text{Cost} + \text{Gains}$

- **Attacker caught?**
  - yes
  - $q^+$
  - no

- **Outcome**
  - $\neg\text{Cost} + \text{Gains} - \text{Penalties}^+$
Multi-parameter Attack Trees (Buldas et al., 2006)

- **Gains** – value gained from the successful attack
- **Cost** \(i\) – cost of the elementary attack, \(p_i\) – success probability
- \(\pi_i^- = q^- \cdot \text{Penalty}^-\) – expected penalty, unsuccessful attack
- \(\pi_i^+ = q^+ \cdot \text{Penalty}^+\) – expected penalty, successful attack

\[\text{Outcome}_i = p_i \cdot \text{Gains} - \text{Cost}_i - p_i \cdot \pi_i^+ - (1 - p_i) \cdot \pi_i^-\]
Multi-parameter Attack Trees (Buldas et al., 2006)

- **Gains** – value gained from the successful attack
- **Cost**\(_i\) – cost of the elementary attack, \(p_i\) – success probability
- \(\pi_i^- = q^- \cdot \text{Penalty}^-\) – expected penalty, unsuccessful attack
- \(\pi_i^+ = q^+ \cdot \text{Penalty}^+\) – expected penalty, successful attack

\[
\text{Outcome}_i = p_i \cdot \text{Gains} - \text{Cost}_i - p_i \cdot \pi_i^+ - (1 - p_i) \cdot \pi_i^-
\]

For an OR-node:

\[
(\text{Cost}, p, \pi^+, \pi^-) = \begin{cases} 
(\text{Cost}_1, p_1, \pi_1^+, \pi_1^-), & \text{if Outcome}_1 > \text{Outcome}_2 \\
(\text{Cost}_2, p_2, \pi_2^+, \pi_2^-), & \text{if Outcome}_1 \leq \text{Outcome}_2
\end{cases}
\]
Multi-parameter Attack Trees (Buldas et al., 2006)

- **Gains** – value gained from the successful attack
- **Cost**$_i$ – cost of the elementary attack, $p_i$ – success probability
- $\pi_i^- = q^- \cdot \text{Penalty}^-$ – expected penalty, unsuccessful attack
- $\pi_i^+ = q^+ \cdot \text{Penalty}^+$ – expected penalty, successful attack

$$\text{Outcome}_i = p_i \cdot \text{Gains} - \text{Cost}_i - p_i \cdot \pi_i^+ - (1 - p_i) \cdot \pi_i^-$$

For an OR-node:

$$(\text{Cost}, p, \pi^+, \pi^-) = \begin{cases} (\text{Cost}_1, p_1, \pi_1^+, \pi_1^-), & \text{if } \text{Outcome}_1 > \text{Outcome}_2 \\ (\text{Cost}_2, p_2, \pi_2^+, \pi_2^-), & \text{if } \text{Outcome}_1 \leq \text{Outcome}_2 \end{cases}$$

For an AND-node:

$$\text{Cost} = \text{Cost}_1 + \text{Cost}_2, \quad p = p_1 \cdot p_2, \quad \pi^+ = \pi_1^+ + \pi_2^+,$$

$$\pi^- = \frac{p_1(1 - p_2)(\pi_1^+ + \pi_2^-) + (1 - p_1)p_2(\pi_1^- + \pi_2^+)}{1 - p_1p_2} + \frac{(1 - p_1)(1 - p_2)(\pi_1^- + \pi_2^-)}{1 - p_1p_2}$$
Buldas et al., 2006: pros and cons

Pros:

- The semantics uses several intuitively relevant parameters
- The semantics is very fast, works by one tree traversal in time $O(n)$
Buldas et al., 2006: pros and cons

Pros:

• The semantics uses several intuitively relevant parameters
• The semantics is very fast, works by one tree traversal in time $O(n)$

Cons:

• In each OR-node, \textbf{Outcome} needs to be computed, which needs \textbf{Gains} for each OR-node, but \textbf{Gains} only has a meaning globally
• The model (as most of the other previous models) assumes that exactly one descendant is picked in an OR-node
• The model is inconsistent with Mauw&Oostdijk 2005
Jürgenson & Willemsen, 2008

\( \mathcal{F} \) — Boolean formula corresponding to the attack tree
\( \mathcal{X} \) — set of elementary attacks
\( \sigma \) — attack suite, satisfying the root node of the attack tree
Jürgenson & Willemsen, 2008

$\mathcal{F}$ — Boolean formula corresponding to the attack tree
$\mathcal{X}$ — set of elementary attacks
$\sigma$ — attack suite, satisfying the root node of the attack tree

$$\textbf{Outcome} = \max_{\sigma} \{ \textbf{Outcome}_\sigma : \sigma \subseteq \mathcal{X}, \mathcal{F}(\sigma := \text{true}) = \text{true} \}$$

$$\text{Outcome}_\sigma = p_\sigma \cdot \text{Gains} - \sum_{X_i \in \sigma} \text{Expenses}_i$$

$$\text{Expenses}_i = \text{Cost}_i + p_i \cdot \pi_i^+ + (1 - p_i) \cdot \pi_i^-$$

$$p_\sigma = \sum_{\rho \subseteq \sigma} \prod_{X_i \in \rho} p_i \prod_{X_j \in \sigma \setminus \rho} (1 - p_j)$$

$$\mathcal{F}(\rho := \text{true}) = \text{true}$$
Implementation & Results

- Implemented in Perl programming language, using terribly inefficient data structures
- $p_\sigma$ can be computed in linear time
  - Going through potentially all the subsets of $X$ still remains exponential, of course
- Using a modified DPLL algorithm for finding all such attack suites, which satisfy the attack tree
- Theorem: We don’t need to consider AND nodes, where some child node is not satisfied
Implementation & Results

- Implemented in Perl programming language, using terribly inefficient data structures
- \( p_\sigma \) can be computed in linear time
  - Going through potentially all the subsets of \( \mathcal{X} \) still remains exponential, of course
- Using a modified DPLL algorithm for finding all such attack suites, which satisfy the attack tree
- Theorem: We don’t need to consider AND nodes, where some child node is not satisfied

- **Outcome**\(^{\text{JW08}} \geq \text{Outcome}^{\text{B+06}}\)
- If \( T_1 \equiv T_2 \) then \( \text{Outcome}(T_1) = \text{Outcome}(T_2) \)
Performance test results showing the average running times and the standard deviation of the running times of the algorithm depending on the number of leaves are displayed in Figure 2. Note that the time scale is logarithmic. The times are measured together with the conversion of the attack tree formula to the conjunctive normal form. In Figure 2, we have included the trees with only up to 19 leaves, since the number of larger trees generated was not sufficient to produce statistically meaningful results. The number of the generated trees by the number of leaves is given later in Figure 3.

6. Generate the value of Gains as an integer chosen uniformly from the interval \([0, 1000000]\). Thus, the generated trees may in theory have up to 2^7 leaves. That particular size limit for the trees was chosen because the running time for larger trees was already too long for significant amount of tests.

Figure 2. Performance test results

![Performance graph](image)
Comparison with Buldas et al., 2006

Theorem 2 implies that the exact attack tree computations introduced in the current paper always yield at least the same outcome compared to [10]. Thus, the potential use of the routine of [10] is rather limited, because it only allows us to get a lower estimate of the attacker's expected outcome, whereas the upper limit would be of much higher interest. We can still say that if the tree computations of [10] show that the system is insufficiently protected (i.e. \( \sigma' > 0 \)), the exact computations would yield a similar result (\( \sigma > 0 \)). Following the proof of Theorem 2, we can also see that the semantics of [10] is actually not too special. Any routine that selects just one child of every OR-node when analysing the tree would essentially give a similar under-estimation of the attacker's expected outcome.

Together with the performance experiments described in Section 4.2, we also compared the outcome attack suites produced by the routines of the current paper and [10] (the implementation of the computations of [10] was kindly provided by Alexander Andrusenko [15]). The results are depicted in Figure 3.

Figure 3. Precision of the computational routine of Buldas et al. [10]

- Number of trees
- Found the same attack suite
Jürgenson & Willemsen, 2010

Reimplementation of Jürgenson & Willemsen, 2008

- C++ instead of Perl
- Removing unnecessary DPLL overhead (e.g. transformation to CNF)
- Bit vectors instead of classes representing sets of subsets
- Catching true&false as soon as it occurs
- Implementing better strategies for choosing undefined literals
  - Most-AND and Weighted-AND
  - Heuristic complexity of the resulting algorithm: $O(1.71^n)$
    - The best #SAT-solver works in time $O(1.6423^n)$
- Fast approximation using a custom genetic algorithm
  - At least 89% accuracy within 2 seconds for the trees with less than 30 leaves
Comparing Strategies

Fig. 1. Performance test results

Average running time in seconds, logarithmic scale

Number of leaves in the tree

- random strategy
- weighted-2-AND strategy
- weighted-0.5-AND strategy
- weighted-1-AND strategy

$O(1.71^n)$

The average complexity estimations for all strategies were the following:
- Random strategy – $O(1.90n)$
In this paper we reviewed the method proposed by Jürgenson and Willemson for computing the exact outcome of a multi-parameter attack tree [14]. We proposed and implemented several optimizations and this allowed us to move the horizon of computability from the trees having 20 leaves (as in [14]) to the trees with roughly 30 leaves.

However, computing the exact outcome of an attack tree is an inherently exponential problem, hence mere optimizations on the implementation level are rather limited. Thus we also considered an approximation technique based on genetic programming. This approach turned out to be very successful, allowing us to reach 89% of confidence within 2 seconds of computation for the trees having up to 29 leaves.

When running a genetic approximation algorithm, we are essentially computing a lower bound to the attacker's expected outcome. Still, an upper bound (showing that the attacker can not achieve more than some amount) would be much more interesting in practice. Hence, the problem...
Introduction of the serial model

- Semi-adaptive, non-blocking case, i.e.
  - The attacker fixes the order of the elementary attacks in advance
  - He is allowed to skip the elementary attacks that have become useless
  - No failure blocks the entire execution

Jürgenson & Willemsen, 2009
Attacker’s Choices

- Decrypt company secrets
- Obtain encrypted file
  - Bribe sysadmin
  - Hack system
- Obtain the password
  - Steal backup
  - Install keylogger

$\Rightarrow t$
Outcome in the Serial Model (I)

The expected outcome of the attack based on permutation $\alpha$ is

$$\text{Outcome}_\alpha = p_\alpha \cdot \text{Gains} - \sum_{X_i \in \mathcal{X}} p_{\alpha,i} \cdot \text{Expenses}_i,$$

where $p_\alpha$ is the success probability of the primary threat and $p_{\alpha,i}$ denotes the probability that the node $X_i$
Outcome in the Serial Model (I)

The expected outcome of the attack based on permutation $\alpha$ is

\[
\text{Outcome}_{\alpha} = p_\alpha \cdot \text{Gains} - \sum_{X_i \in \mathcal{X}} p_{\alpha,i} \cdot \text{Expenses}_i,
\]

where $p_\alpha$ is the success probability of the primary threat and $p_{\alpha,i}$ denotes the probability that the node $X_i$.

**Theorem**

Let $\mathcal{F}_1$ and $\mathcal{F}_2$ be two monotone Boolean formulae such that $\mathcal{F}_1 \equiv \mathcal{F}_2$, and let $\text{Outcome}^1_{\alpha}$ and $\text{Outcome}^2_{\alpha}$ be the expected outcomes obtained running the algorithm on the corresponding formulae using the leaf set permutation $\alpha$. Then

\[
\text{Outcome}^1_{\alpha} = \text{Outcome}^2_{\alpha}.
\]
Outcome in the Serial Model (II)

Theorem

We have

\[ \text{Outcome}_{\text{JW09}} \geq \text{Outcome}_{\text{JW08}}. \]

If for all the elementary attacks \( X_i \) \((i = 1, \ldots, n)\) one also has \( \text{Expenses}_i > 0 \), then strict inequality holds in the above inequality.
Outcome in the Serial Model (II)

Theorem
We have

$$\text{Outcome}_{JW09} \geq \text{Outcome}_{JW08}.$$

If for all the elementary attacks $X_i$ ($i = 1, \ldots, n$) one also has $\text{Expenses}_i > 0$, then strict inequality holds in the above inequality.

• The naïve algorithm for computing the attacker’s outcome is average-case exponential in the number of leaves $n$
• We propose an efficient algorithm with complexity $O(n^2)$
  • Recall, need only the quantities $p_\alpha$ and $p_{\alpha,i}$
The Algorithm

\[ t = 0 \]
\[ f = 1 - p_2 \]
\[ u = p_2 \]

\[ t = p_1 \]
\[ f = 0 \]
\[ u = 1 - p_1 \]

\[ t = p_2 \]
\[ f = 1 - p_2 \]
\[ u = 0 \]

\[ t = 0 \]
\[ f = 0 \]
\[ u = 0 \]

\[ t = 0 \]
\[ f = 0 \]
\[ u = 1 \]

\[ p_{\alpha,3} = (1 - p_1) \cdot (1 - (1 - p_2)) \]
Sequential model revised

- Jürgenson & Willemsen, 2009, builds on another framework:
  - The attacker tries to
    - first, maximize success probability
    - second, achieve the best possible outcome
  - Hence, a certain form of irrational behavior is obtained
Sequential model revised

- Jürgenson & Willemsen, 2009, builds on another framework:
  - The attacker tries to
    - first, maximize success probability
    - second, achieve the best possible outcome
  - Hence, a certain form of irrational behavior is obtained
- Niitsoo, 2010 analyzes the rational case
  - Builds on classical decision theory
  - Attacks can be skipped if they are too expensive
  - Otherwise same as JW09
    - Order of attacks fixed before the attack
    - Full information about the past
Sequential model computation

- Decision tree optimization algorithm
  - Decision trees usually exponential in general
- Attack trees provide for a simple structure
  - We do not optimize Trees but BDD-s
- Non-crossing orders optimized in $O(n)$ time.
  - Modeling goal-oriented behavior
  - Optimal non-crossing order for JW10 can be found in $O(n \lg n)$ time (Niitsoo, 2010)
Fully rational model

- **Pros:**
  - Fully rational behavior (easy to justify)
  - Optimal subset found automatically
  - Highest expected utility of all models to date
  - Efficient $O(n)$ computation for some orders
  - Highly extensible:
    - Blocking case (even partial blocking)
    - Bribes and uncertainty
    - Intermediate payments

- **Cons:**
  - Computation exponential for some orders
  - Still only semi-adaptive
  - Conventional