Rational Choice of Security Measures via Multi-Parameter Attack Trees

CRITIS'06
August 30 – September 2, 2006, Samos Island, Greece

Ahto Buldas, Peeter Laud, Jaan Priisalu, Märt Saarepera, Jan Willemson

Motivation

- It is a complicated task to evaluate whether (IT-)infrastructure of a company is protected

Motivation

- It is a complicated task to evaluate whether (IT-)infrastructure of a company is protected
  - sufficiently (i.e. achieving a satisfactory level), and

Motivation

- It is a complicated task to evaluate whether (IT-)infrastructure of a company is protected
  - sufficiently (i.e. achieving a satisfactory level), and
  - reasonably (i.e. not spending too much)

Motivation

- It is a complicated task to evaluate whether (IT-)infrastructure of a company is protected
  - sufficiently (i.e. achieving a satisfactory level), and
  - reasonably (i.e. not spending too much)
- Even if the losses associated with vulnerability exploits can be estimated, the corresponding probabilities are very difficult to evaluate

Motivation

- It is a complicated task to evaluate whether (IT-)infrastructure of a company is protected
  - sufficiently (i.e. achieving a satisfactory level), and
  - reasonably (i.e. not spending too much)
- Even if the losses associated with vulnerability exploits can be estimated, the corresponding probabilities are very difficult to evaluate
- This is especially true for targeted, company-specific attacks, since the required statistics does not exist or is difficult to get

Rational Attackers and Attack Trees

- Luckily, targeted attacks are mostly *rational*, i.e. the attackers

Rational Attackers and Attack Trees

- Luckily, targeted attacks are mostly *rational*, i.e. the attackers
    - attack only if the attack is profitable, and

Rational Attackers and Attack Trees

- Luckily, targeted attacks are mostly *rational*, i.e. the attackers
  - attack only if the attack is profitable, and
  - choose the attack with the highest outcome

Rational Attackers and Attack Trees

- Luckily, targeted attacks are mostly *rational*, i.e. the attackers
  - attack only if the attack is profitable, and
  - choose the attack with the highest outcome
- From now on, this paper assumes rational attacks

Rational Attackers and Attack Trees

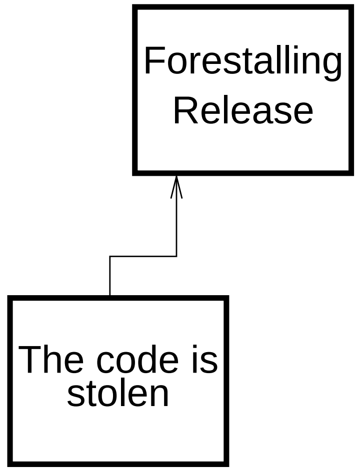
- Luckily, targeted attacks are mostly *rational*, i.e. the attackers
  - attack only if the attack is profitable, and
  - choose the attack with the highest outcome
- From now on, this paper assumes rational attacks
- Such attacks can be modelled using gradual refinement starting from primary threats and breaking them down to elementary attacks

Rational Attackers and Attack Trees

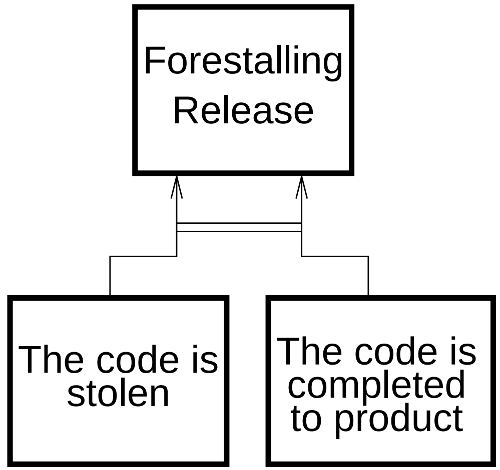
- Luckily, targeted attacks are mostly *rational*, i.e. the attackers
  - attack only if the attack is profitable, and
  - choose the attack with the highest outcome
- From now on, this paper assumes rational attacks
- Such attacks can be modelled using gradual refinement starting from primary threats and breaking them down to elementary attacks
- As a result, we obtain an *attack tree*

An Attack Tree

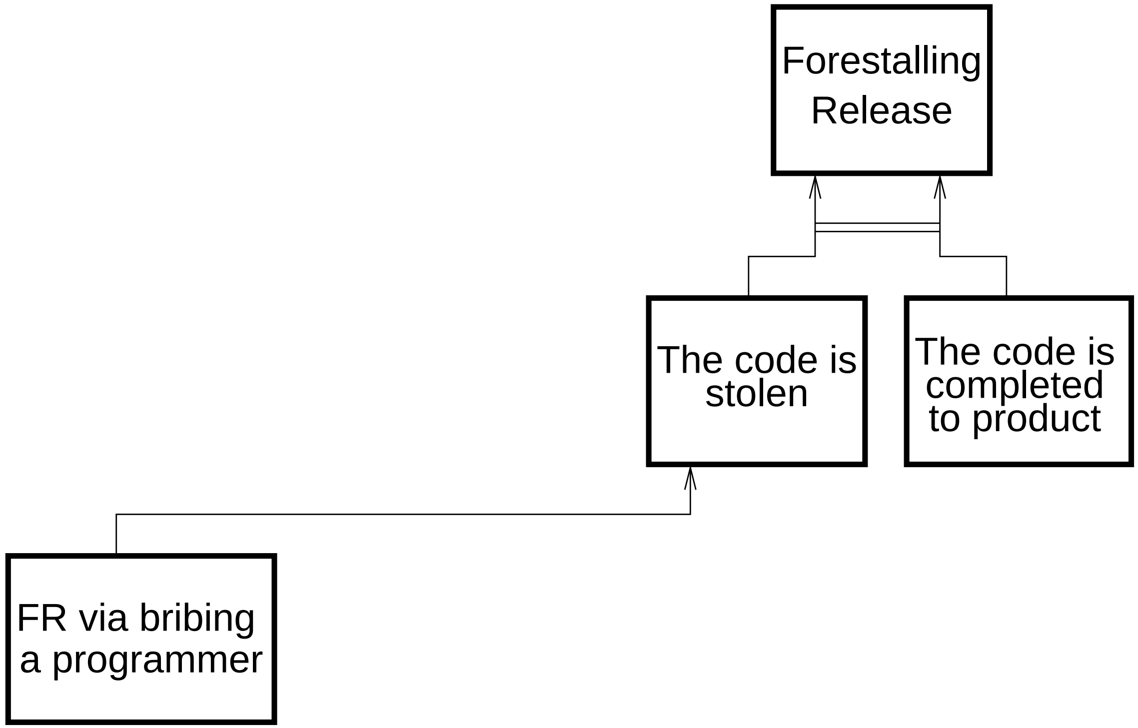
An Attack Tree



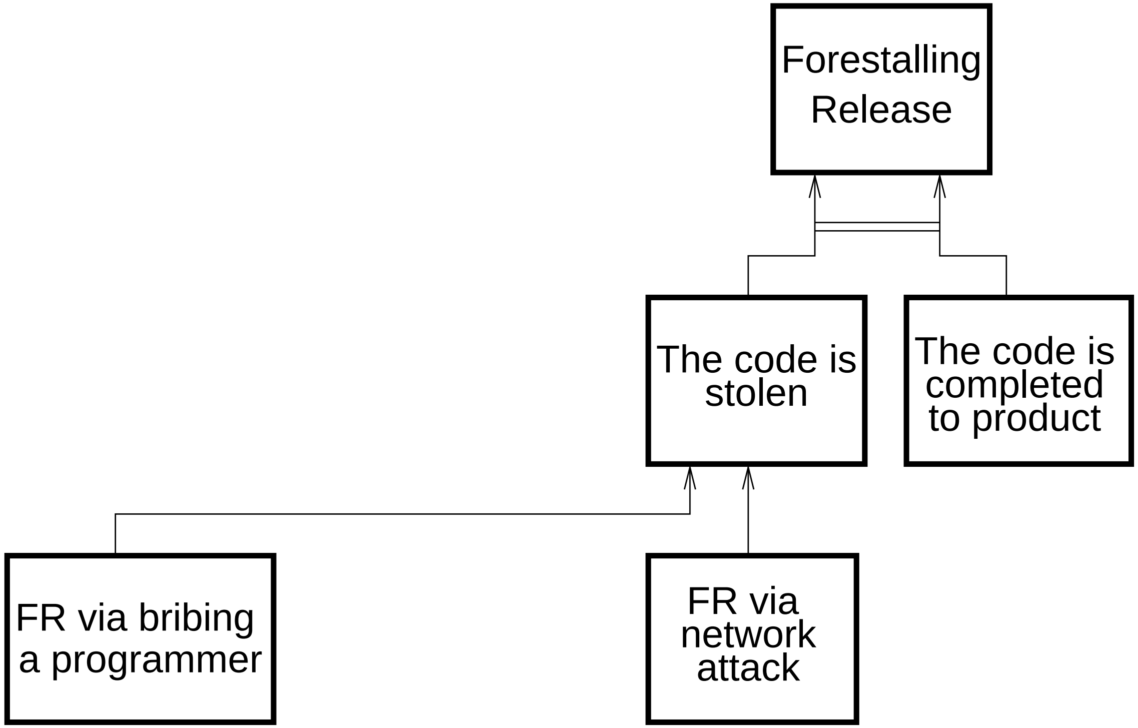
An Attack Tree



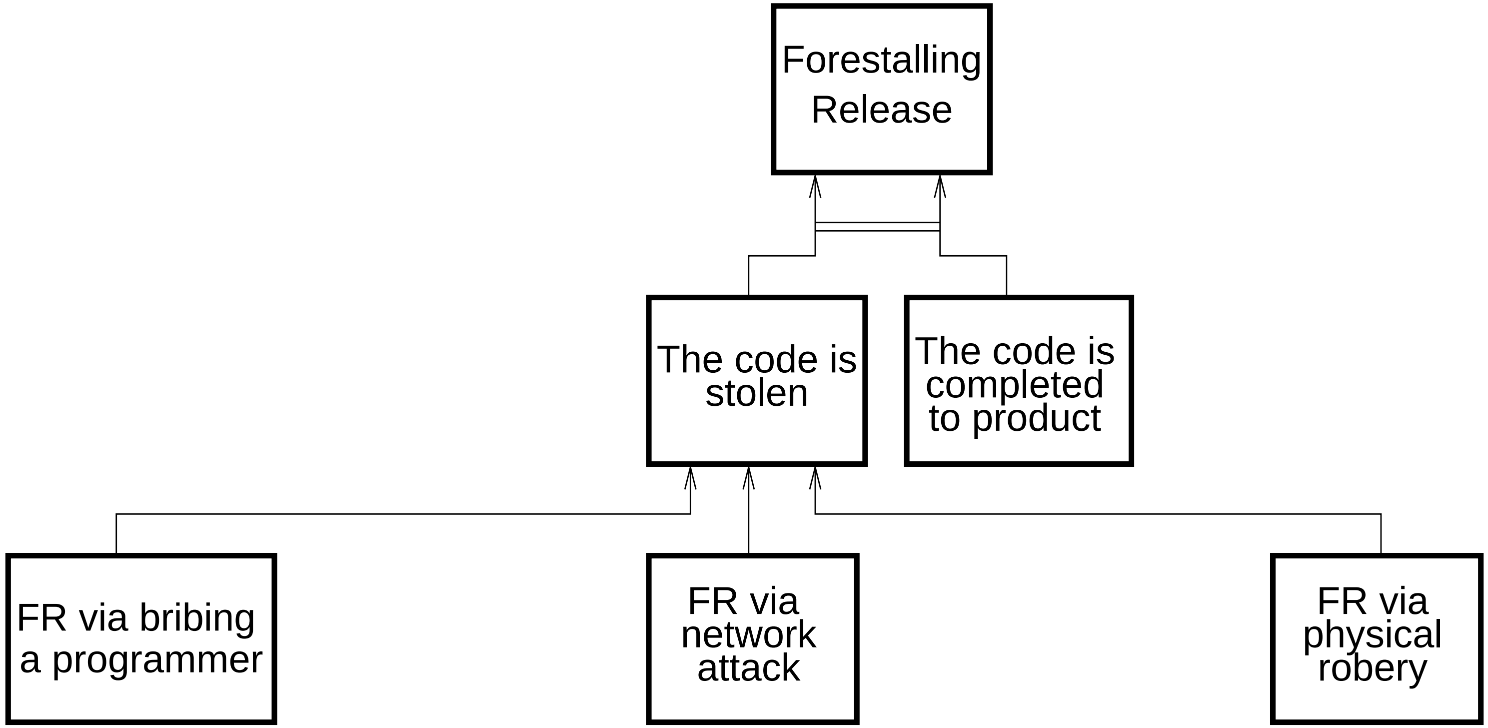
An Attack Tree



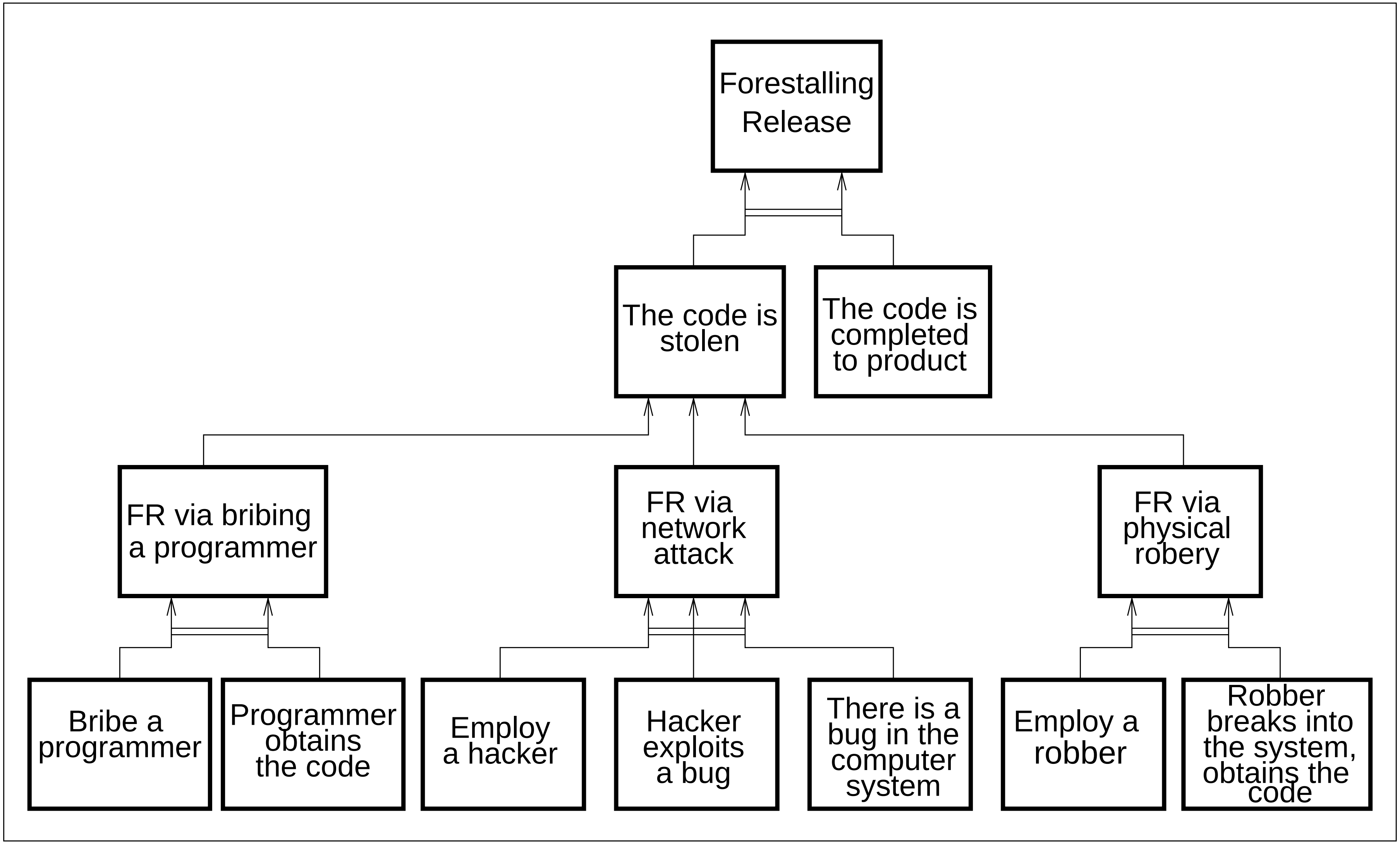
An Attack Tree



An Attack Tree



An Attack Tree



Parametrizing the Attack Tree

- When modelling the attack, we need to

Parametrizing the Attack Tree

- When modelling the attack, we need to
  - set some parameter values to the leaves of the tree

Parametrizing the Attack Tree

- When modelling the attack, we need to
  - set some parameter values to the leaves of the tree
  - define computation rules for parameter propagation

Parametrizing the Attack Tree

- When modelling the attack, we need to
  - set some parameter values to the leaves of the tree
  - define computation rules for parameter propagation
- In this paper we will consider the following parameters:

Parametrizing the Attack Tree

- When modelling the attack, we need to
  - set some parameter values to the leaves of the tree
  - define computation rules for parameter propagation
- In this paper we will consider the following parameters:
  - Gains – the gains of the attacker if attack succeeds

Parametrizing the Attack Tree

- When modelling the attack, we need to
  - set some parameter values to the leaves of the tree
  - define computation rules for parameter propagation
- In this paper we will consider the following parameters:
  - Gains – the gains of the attacker if attack succeeds
  - Costs – the cost of the attack

Parametrizing the Attack Tree

- When modelling the attack, we need to
  - set some parameter values to the leaves of the tree
  - define computation rules for parameter propagation
- In this paper we will consider the following parameters:
  - Gains – the gains of the attacker if attack succeeds
  - Costs – the cost of the attack
  - p – the success probability of the attack

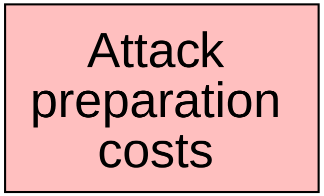
Parametrizing the Attack Tree

- When modelling the attack, we need to
  - set some parameter values to the leaves of the tree
  - define computation rules for parameter propagation
- In this paper we will consider the following parameters:
  - Gains – the gains of the attacker if attack succeeds
  - Costs – the cost of the attack
  - p – the success probability of the attack
  - q, Penalties – the probability of getting caught and penalties (if the attack was successful)

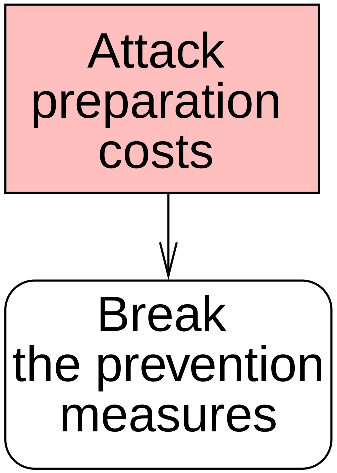
Parametrizing the Attack Tree

- When modelling the attack, we need to
  - set some parameter values to the leaves of the tree
  - define computation rules for parameter propagation
- In this paper we will consider the following parameters:
  - Gains – the gains of the attacker if attack succeeds
  - Costs – the cost of the attack
  - p – the success probability of the attack
  - q, Penalties – the probability of getting caught and penalties (if the attack was successful)
  - q_-, Penalties$_-$ – the probability of getting caught and penalties (if the attack was unsuccessful)

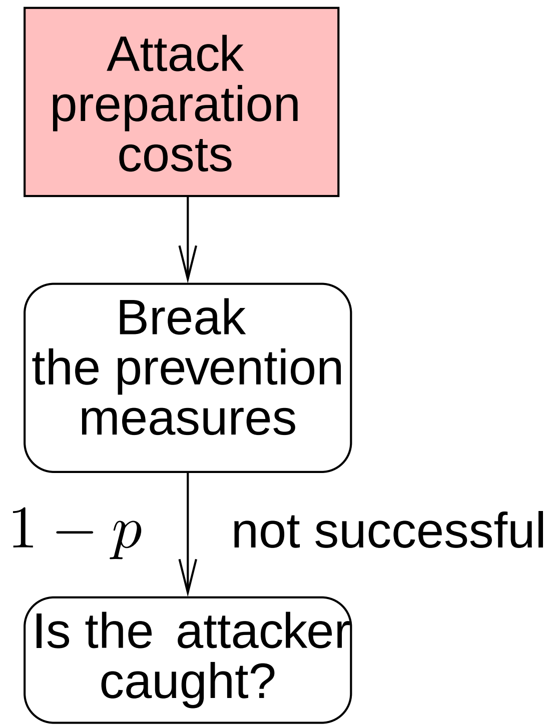
The Attack Game



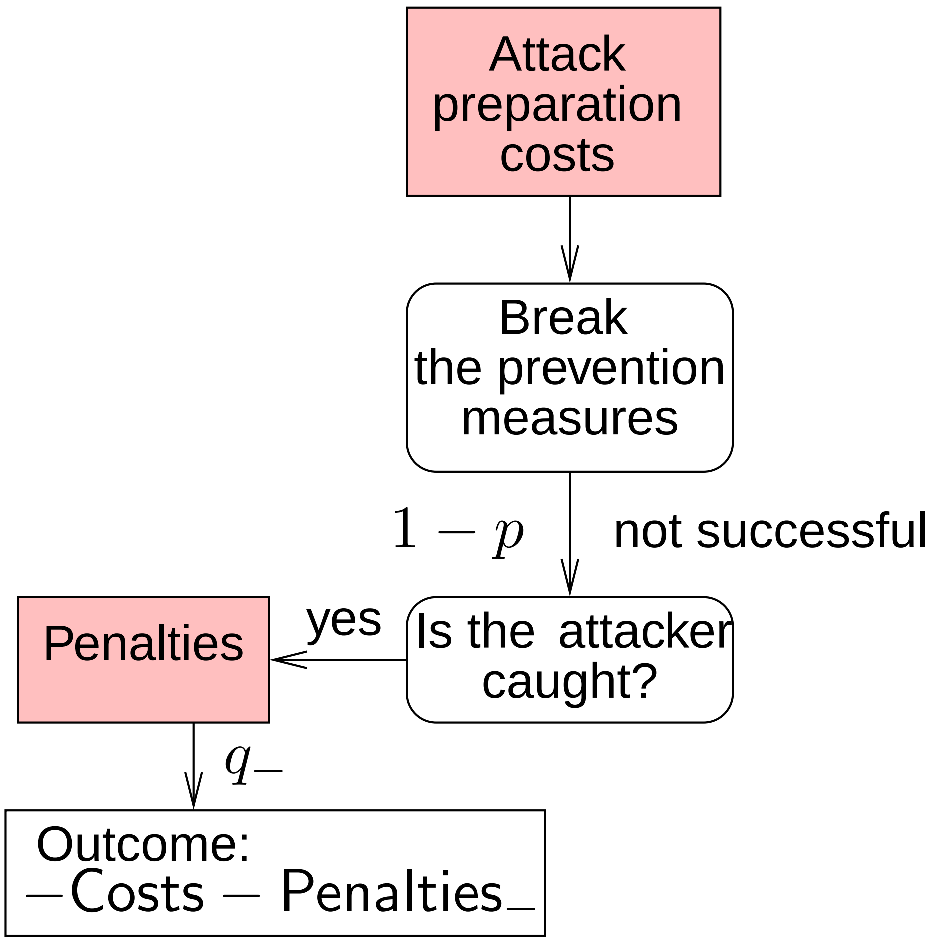
The Attack Game



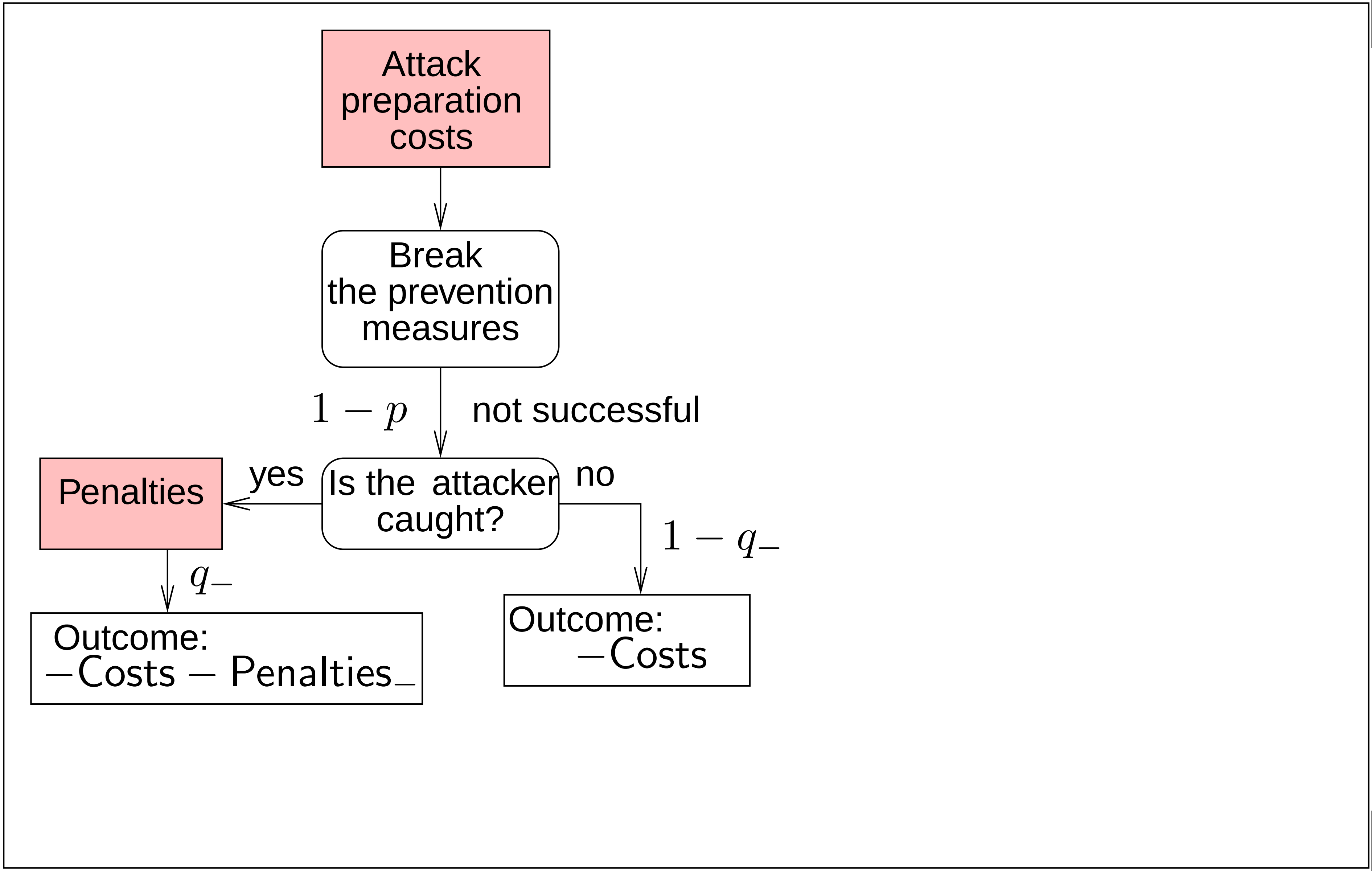
The Attack Game



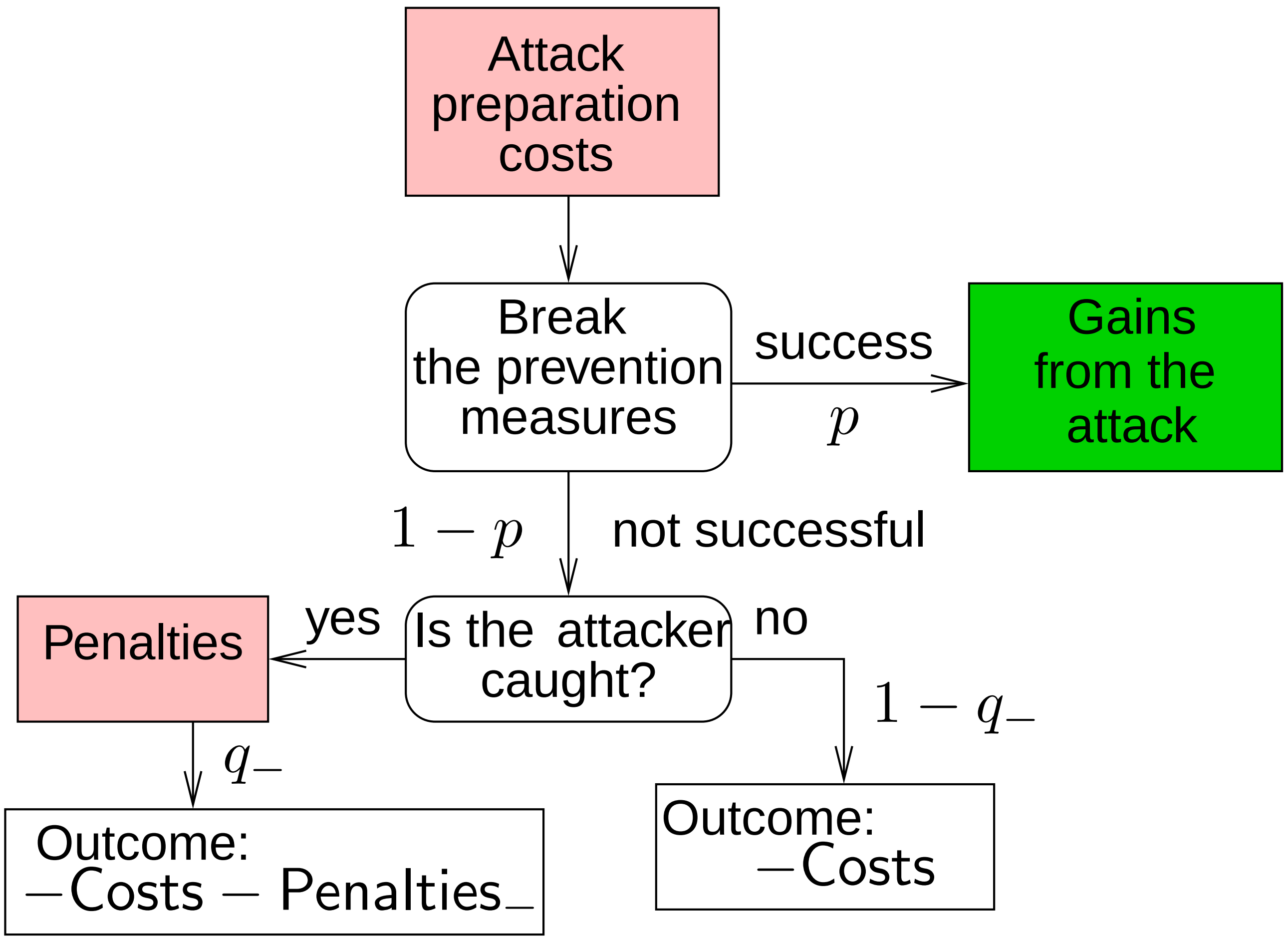
The Attack Game



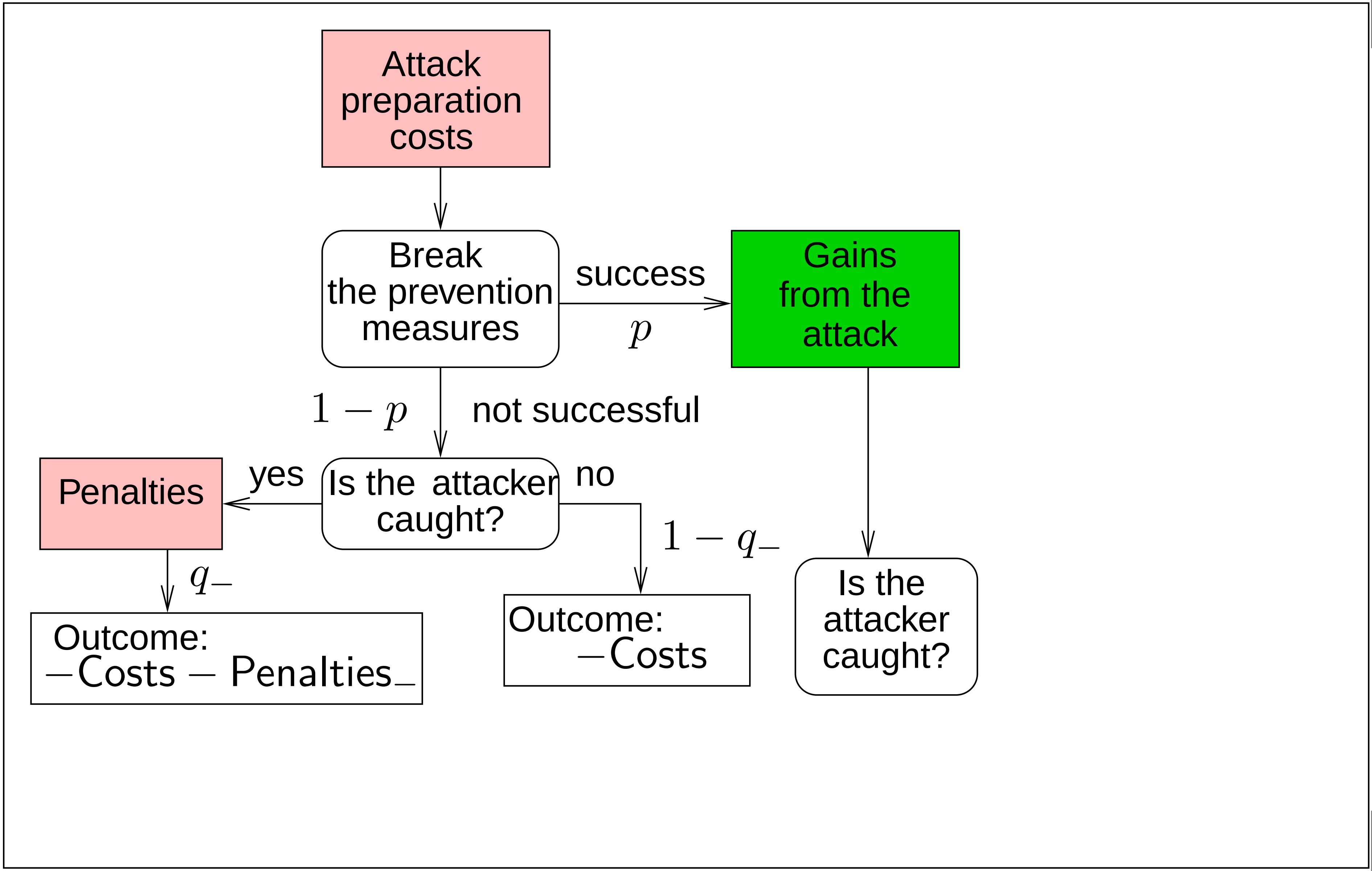
The Attack Game



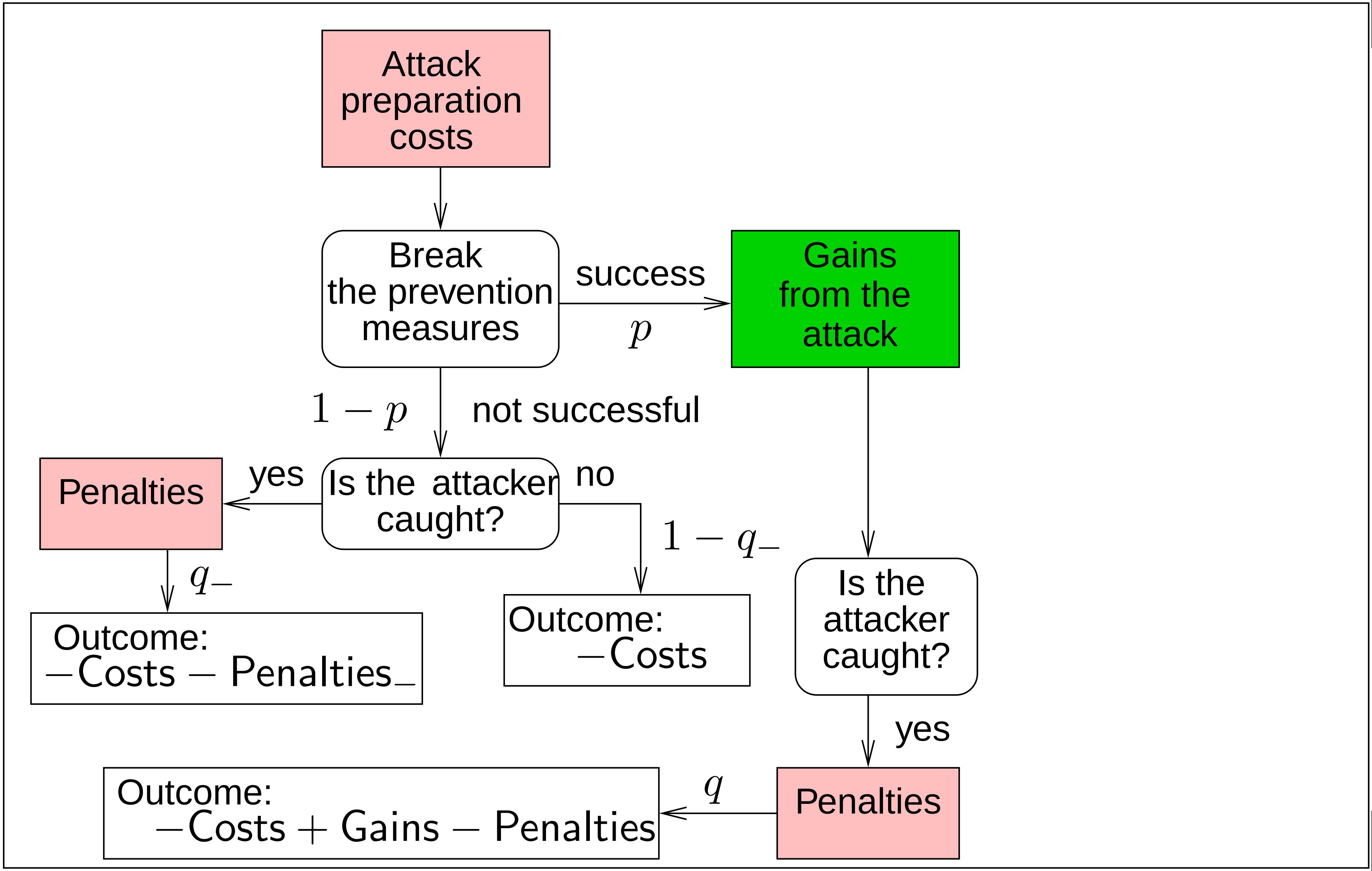
The Attack Game



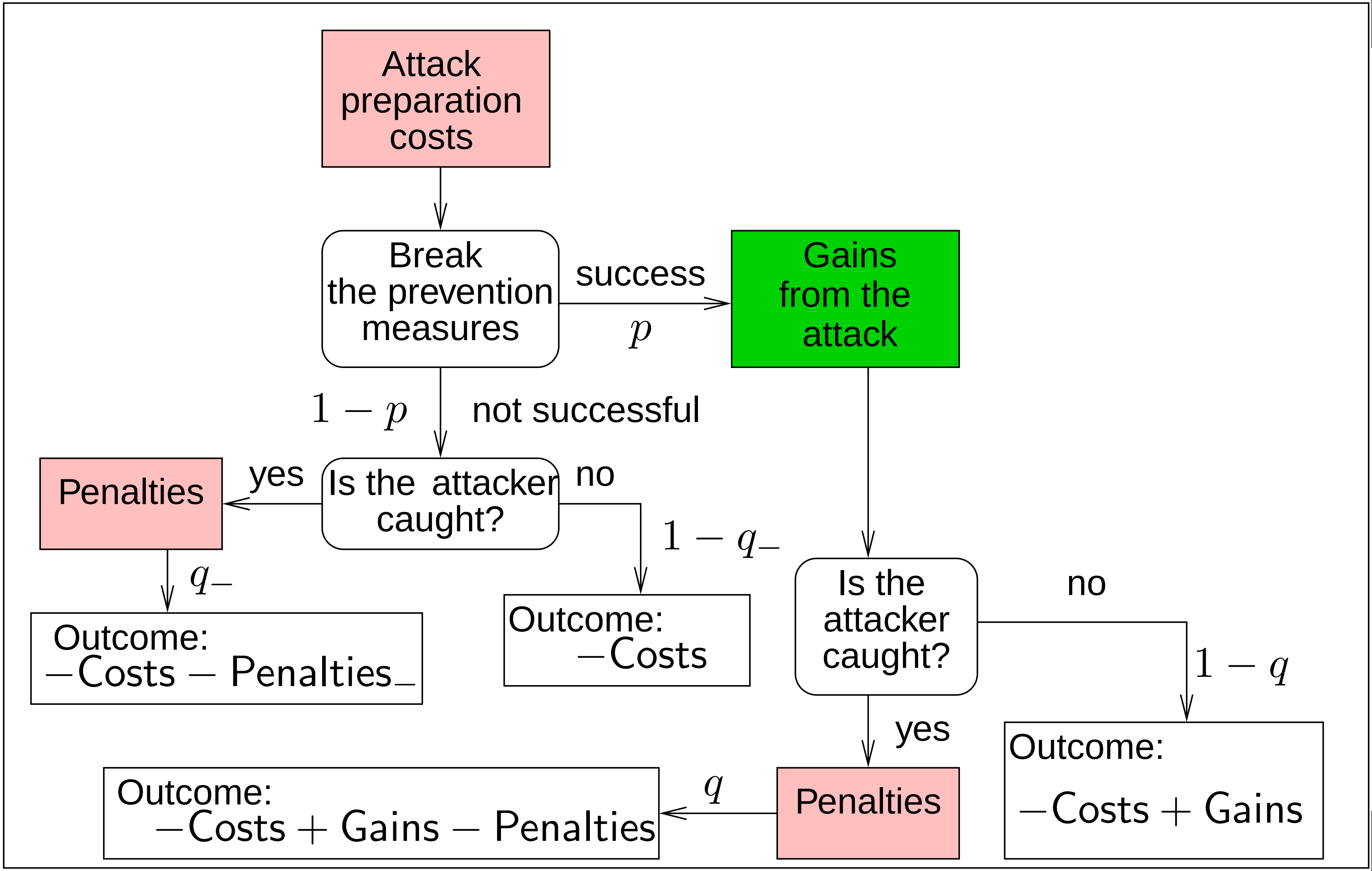
The Attack Game



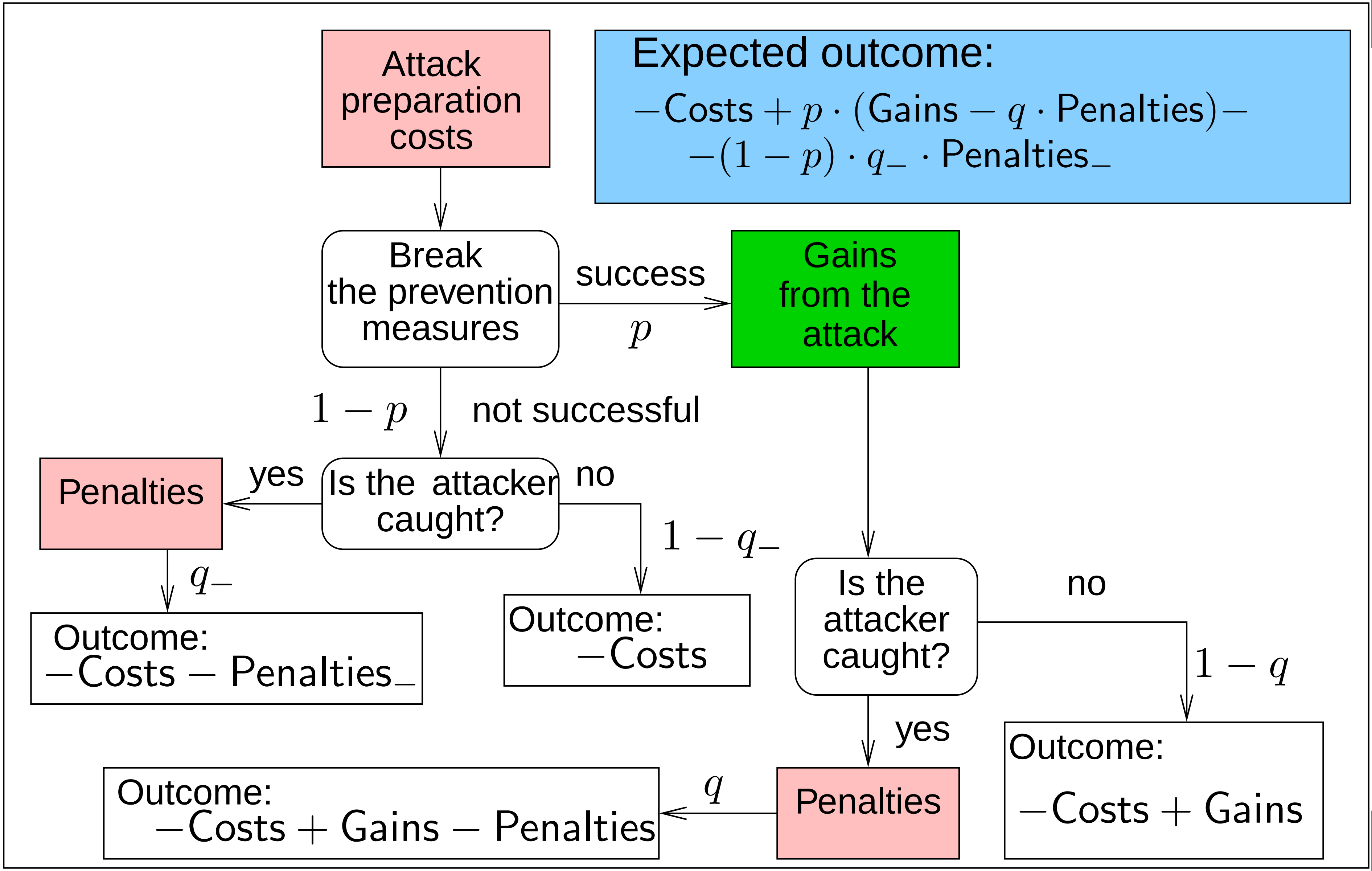
The Attack Game



The Attack Game



The Attack Game



Tree Computations (I)

- Denoting $\pi = q \cdot \mathsf{Penalties}$ and $\pi_- = q_- \cdot \mathsf{Penalties}_-$, we set the parameters $(\mathsf{Costs}, p, \pi, \pi_-)$ for every leaf node. Then we have

$$\mathsf{Outcome} = -\mathsf{Costs}_1 + p \cdot \mathsf{Gains} - p \cdot \pi - (1-p) \cdot \pi_-$$

- For an OR-node with child nodes with parameters $(\mathsf{Costs}_1, p_1, \pi_1, \pi_{1-})$ and $(\mathsf{Costs}_2, p_2, \pi_2, \pi_{2-})$ the parameters $(\mathsf{Costs}, p, \pi, \pi_-)$ are computed as:

$$(\mathsf{Costs}, p, \pi, \pi_-) =$$

$$\begin{cases} (\mathsf{Costs}_1, p_1, \pi_1, \pi_{1-}), & \text{if } \mathsf{Outcome}_1 > \mathsf{Outcome}_2 \\ (\mathsf{Costs}_2, p_2, \pi_2, \pi_{2-}), & \text{if } \mathsf{Outcome}_1 \leq \mathsf{Outcome}_2 \end{cases}$$

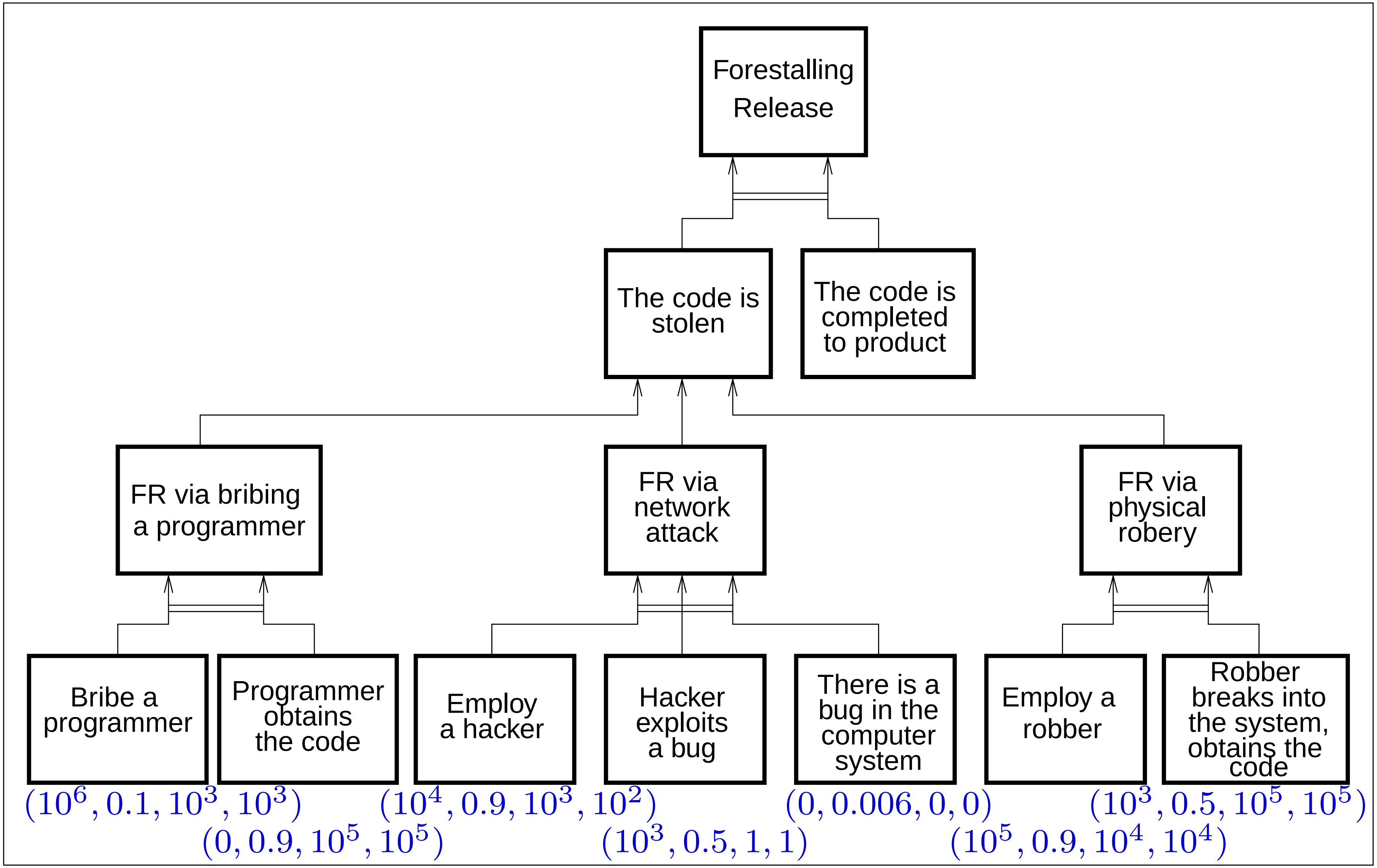
Tree Computations (II)

- For a AND-node with child nodes with parameters $(\mathsf{Costs}_1, p_1, \pi_1, \pi_{1-})$ and $(\mathsf{Costs}_2, p_2, \pi_2, \pi_{2-})$ the parameters $(\mathsf{Costs}, p, \pi, \pi_-)$ are computed as follows:

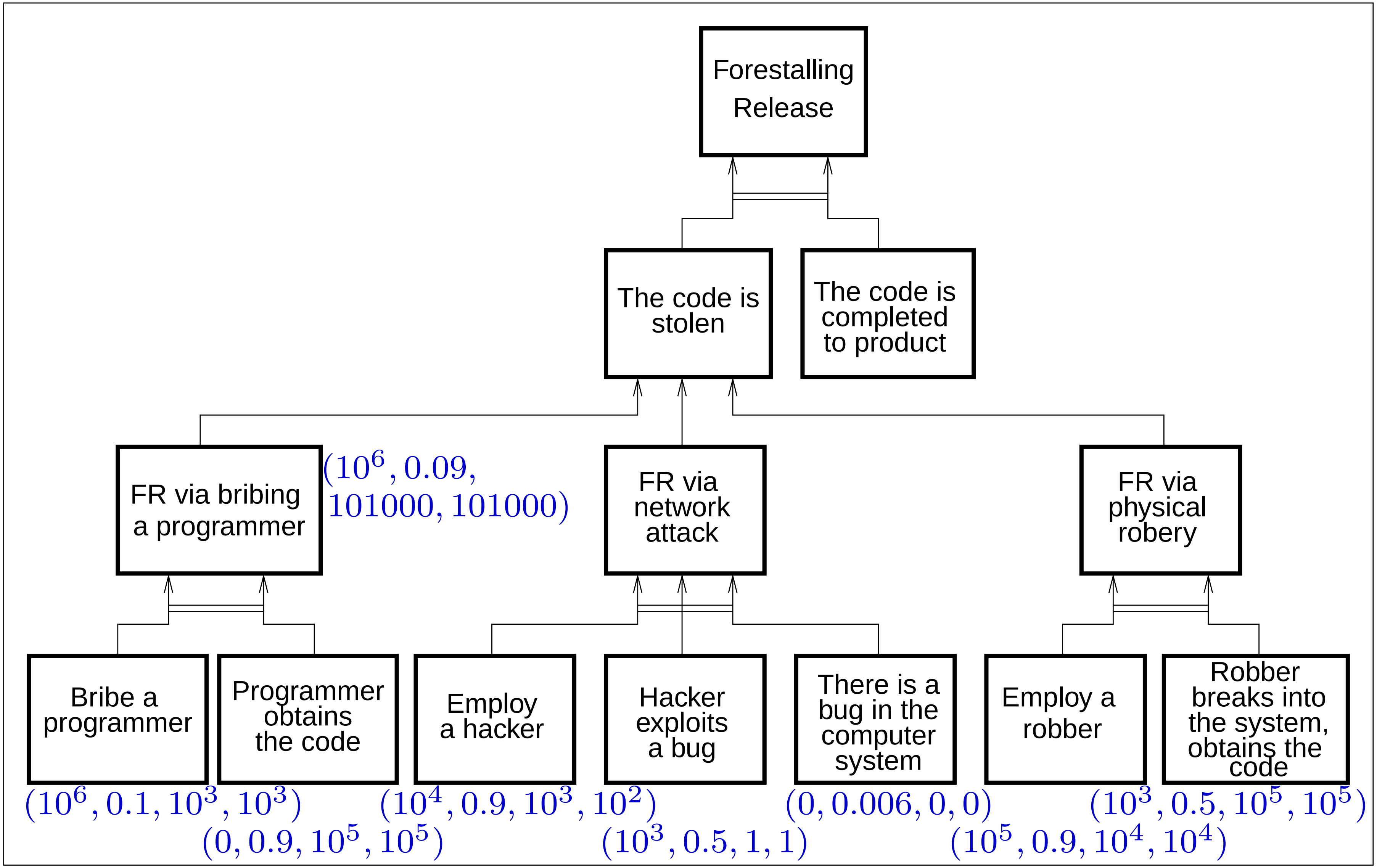
$$\begin{aligned}
\mathsf{Costs} &= \mathsf{Costs}_1 + \mathsf{Costs}_2 \\
p &= p_1 \cdot p_2 \\
\pi &= \pi_1 + \pi_2 \\
\pi_- &= \frac{p_1(1-p_2)(\pi_1+\pi_{2-}) + (1-p_1)p_2(\pi_{1-}+\pi_2)}{1-p_1p_2} + \\
&\quad \frac{(1-p_1)(1-p_2)(\pi_{1-}+\pi_{2-})}{1-p_1p_2}
\end{aligned}$$

- The last formula represents the average penalty of an attacker, assuming that at least one of the two child-attacks was not successful

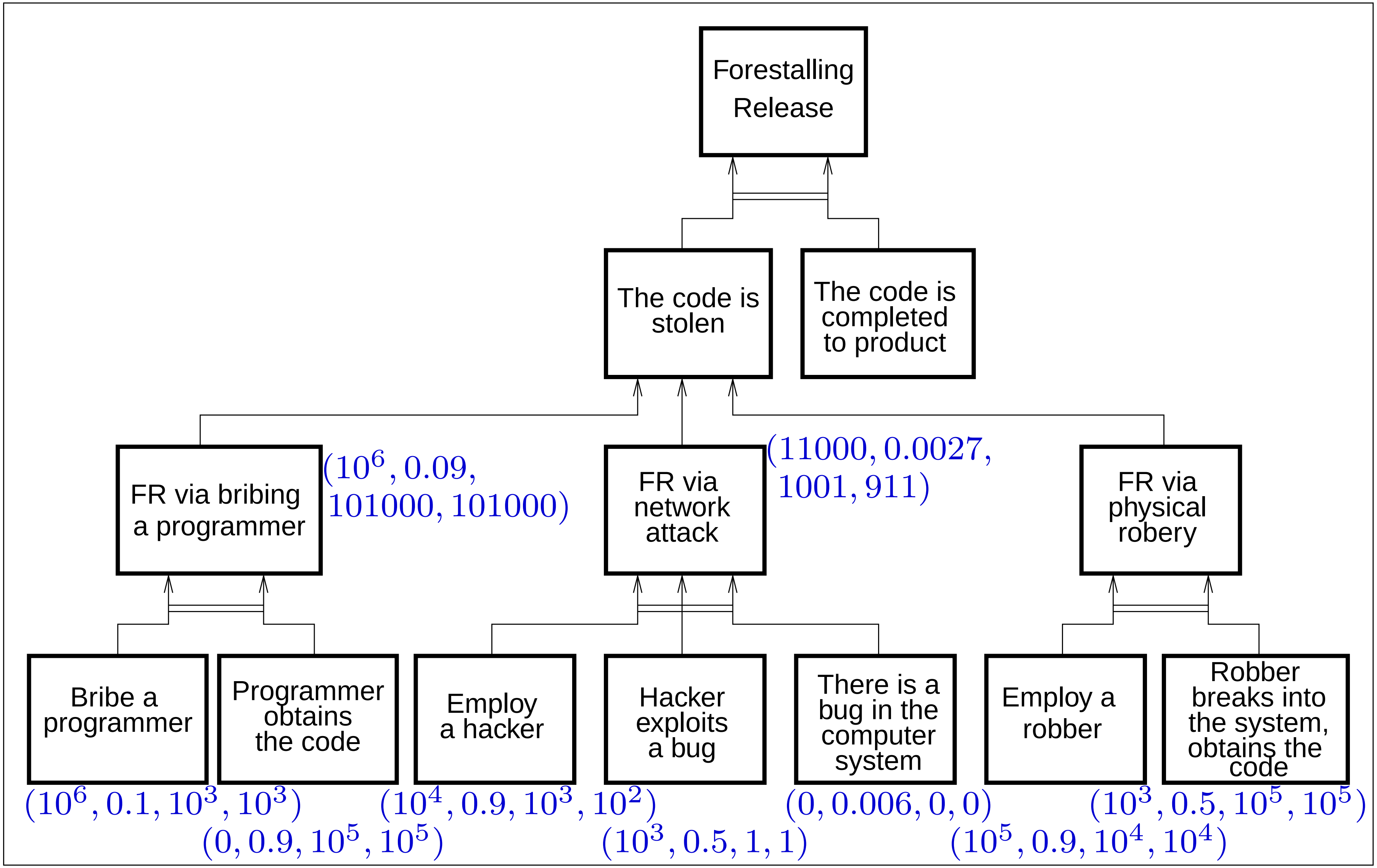
Tree Computations: Example



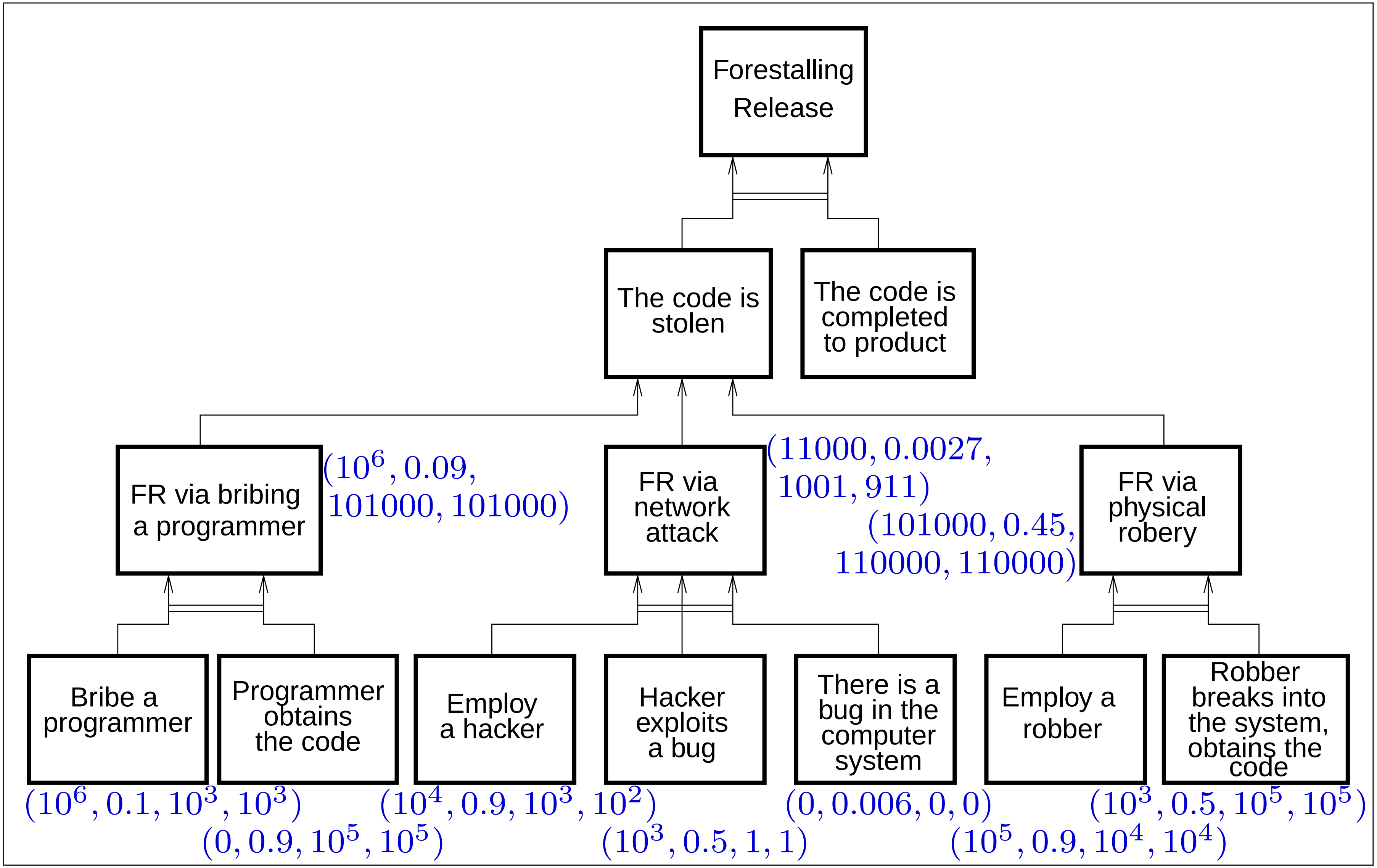
Tree Computations: Example



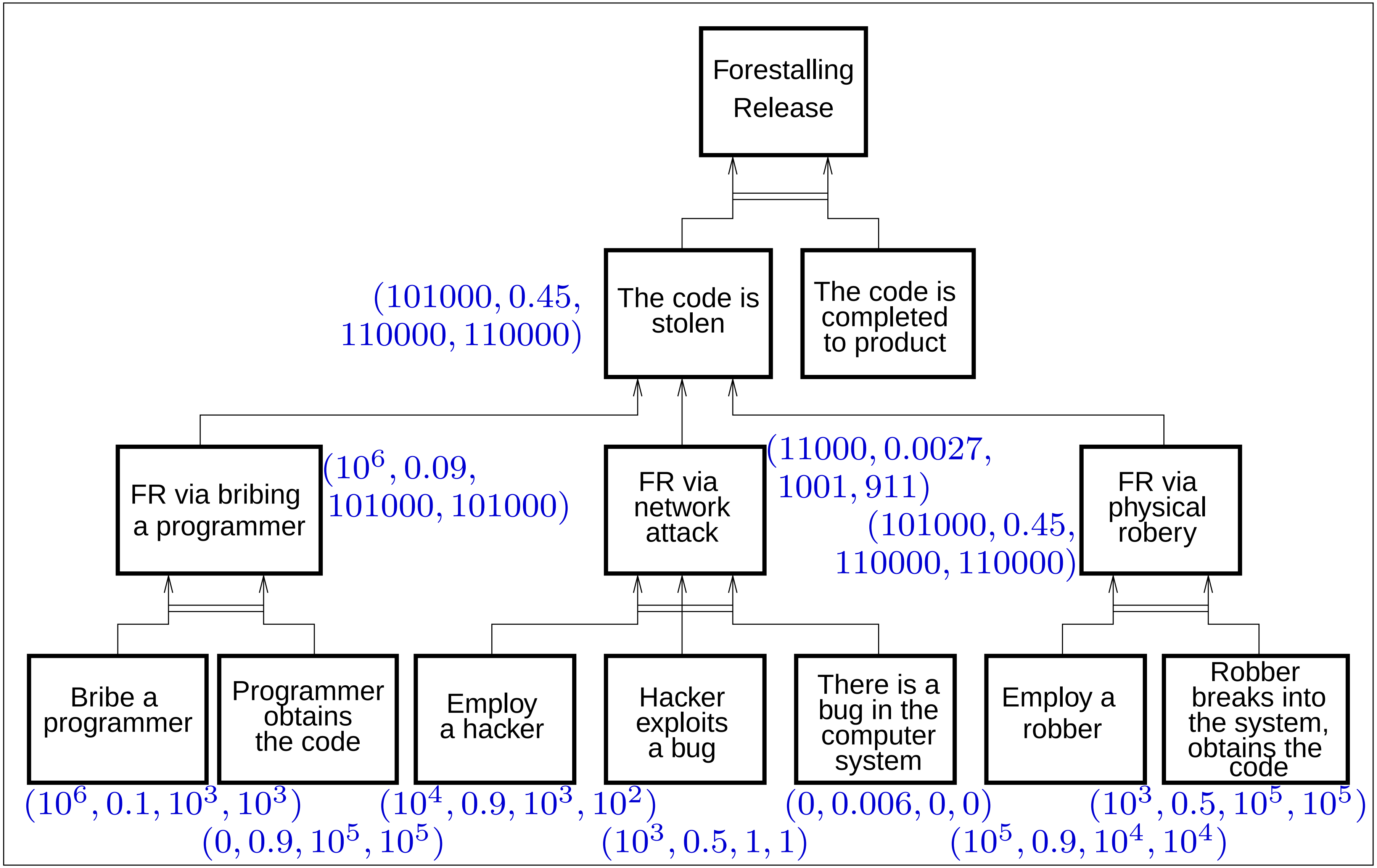
Tree Computations: Example



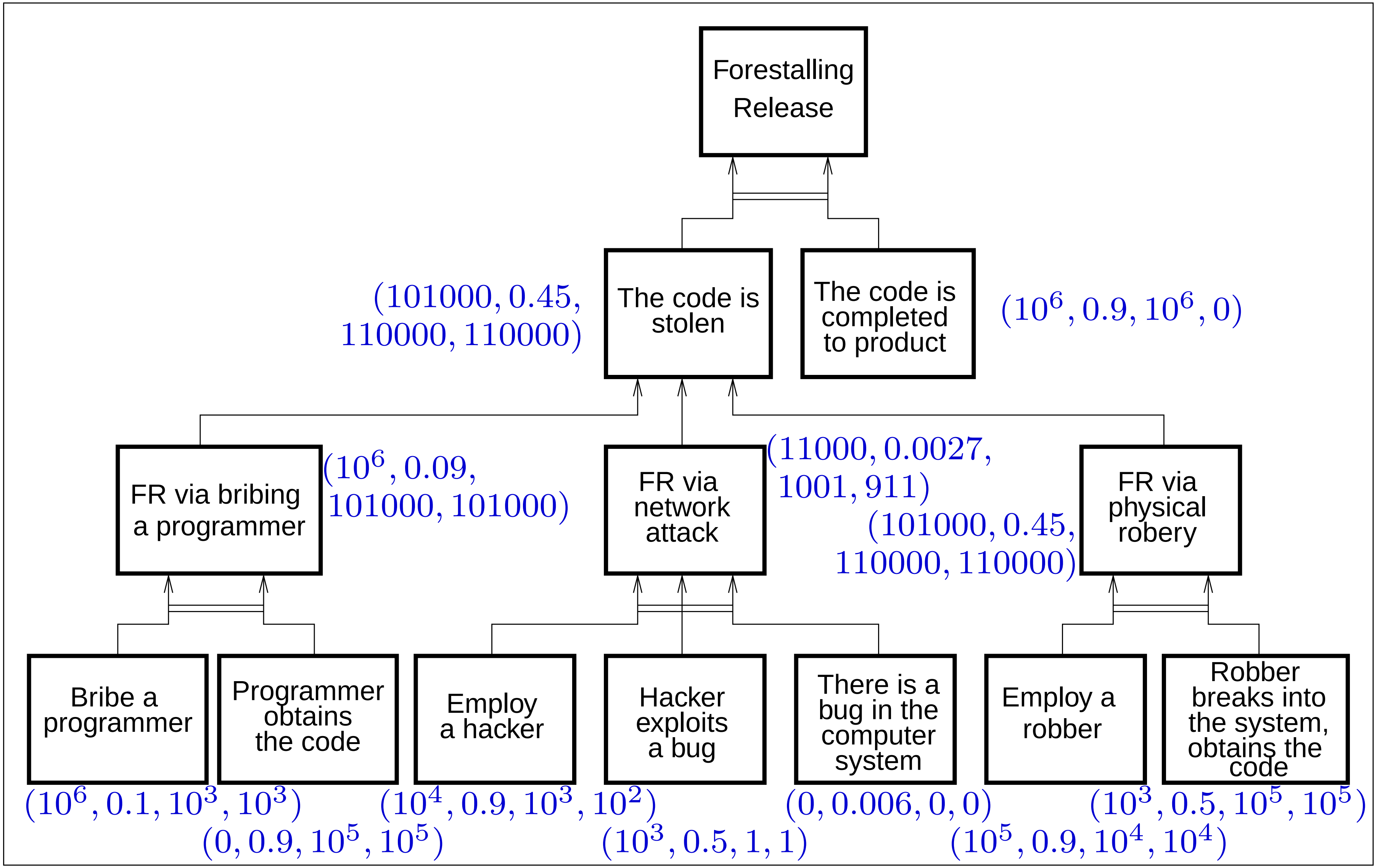
Tree Computations: Example



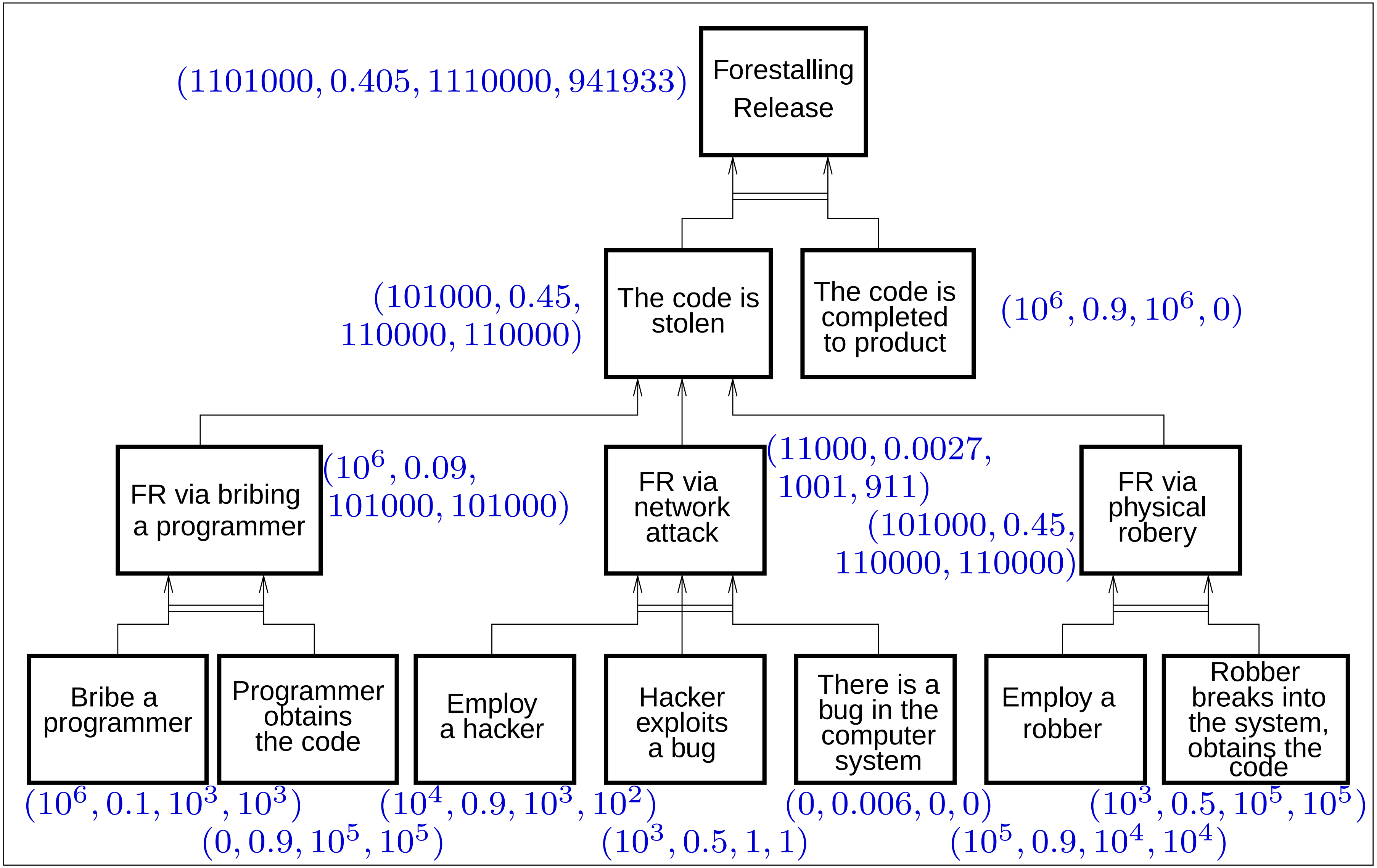
Tree Computations: Example



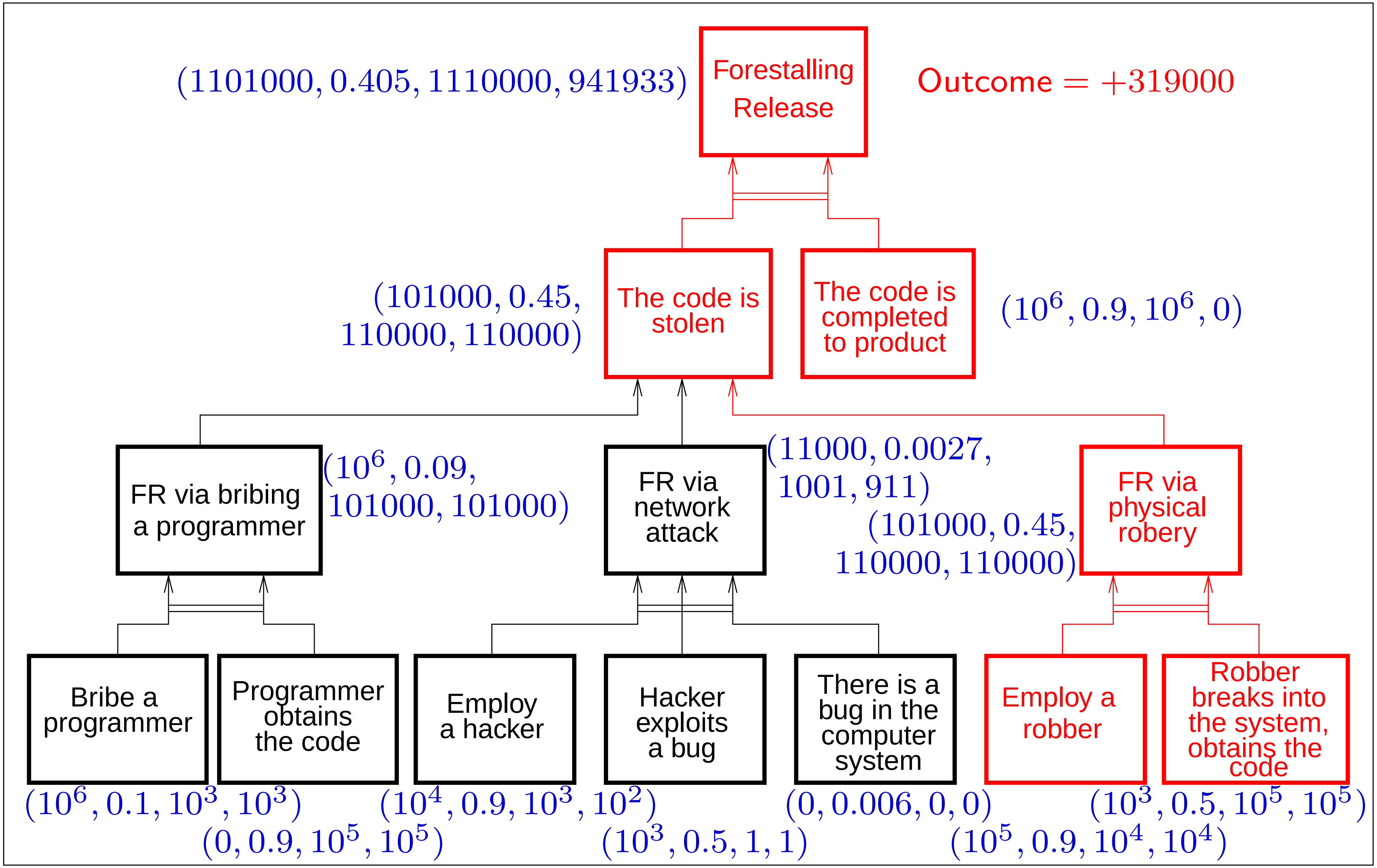
Tree Computations: Example



Tree Computations: Example



Tree Computations: Example



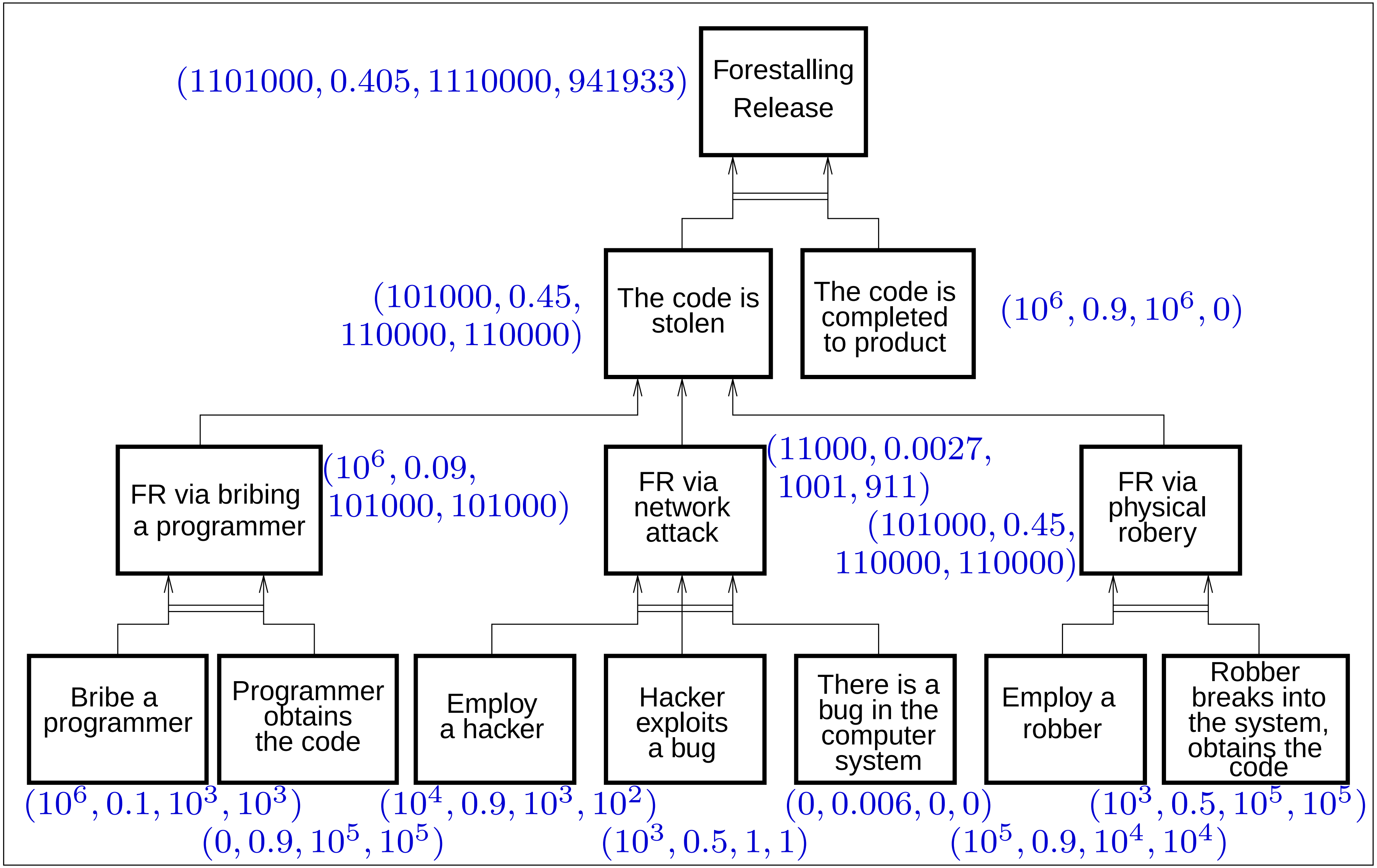
Security Measures

- Let $\mathcal{T}$ denote the set of all *primary threats* and let $\mathcal{M}$ denote some set of security measures
- Let $\mathsf{Loss}[\mathfrak{T}]$ and $\mathsf{Loss}[\mathfrak{T} \mid \mathcal{M}]$ denote the losses of the company without and with the measures, respectively
- Let $\mathsf{Outcome}[\mathcal{T} \mid \mathcal{M}]$ denote the outcome of the game when measures $\mathcal{M}$ are applied
- The set $\mathcal{M}$ of measures is *sufficient (against rational attacks)* if for all primary threats $\mathcal{T} \in \mathfrak{T}$ we have $\mathsf{Outcome}[\mathcal{T} \mid \mathcal{M}] \leq 0$, or equivalently, $\mathsf{Loss}[\mathfrak{T} \mid \mathcal{M}] = 0$
- The set $\mathcal{M}$ of measures is *adequate* (worth its cost) if $\mathsf{Loss}[\mathfrak{T}] - \mathsf{Loss}[\mathfrak{T} \mid \mathcal{M}] > \mathsf{Cost}[\mathcal{M}]$

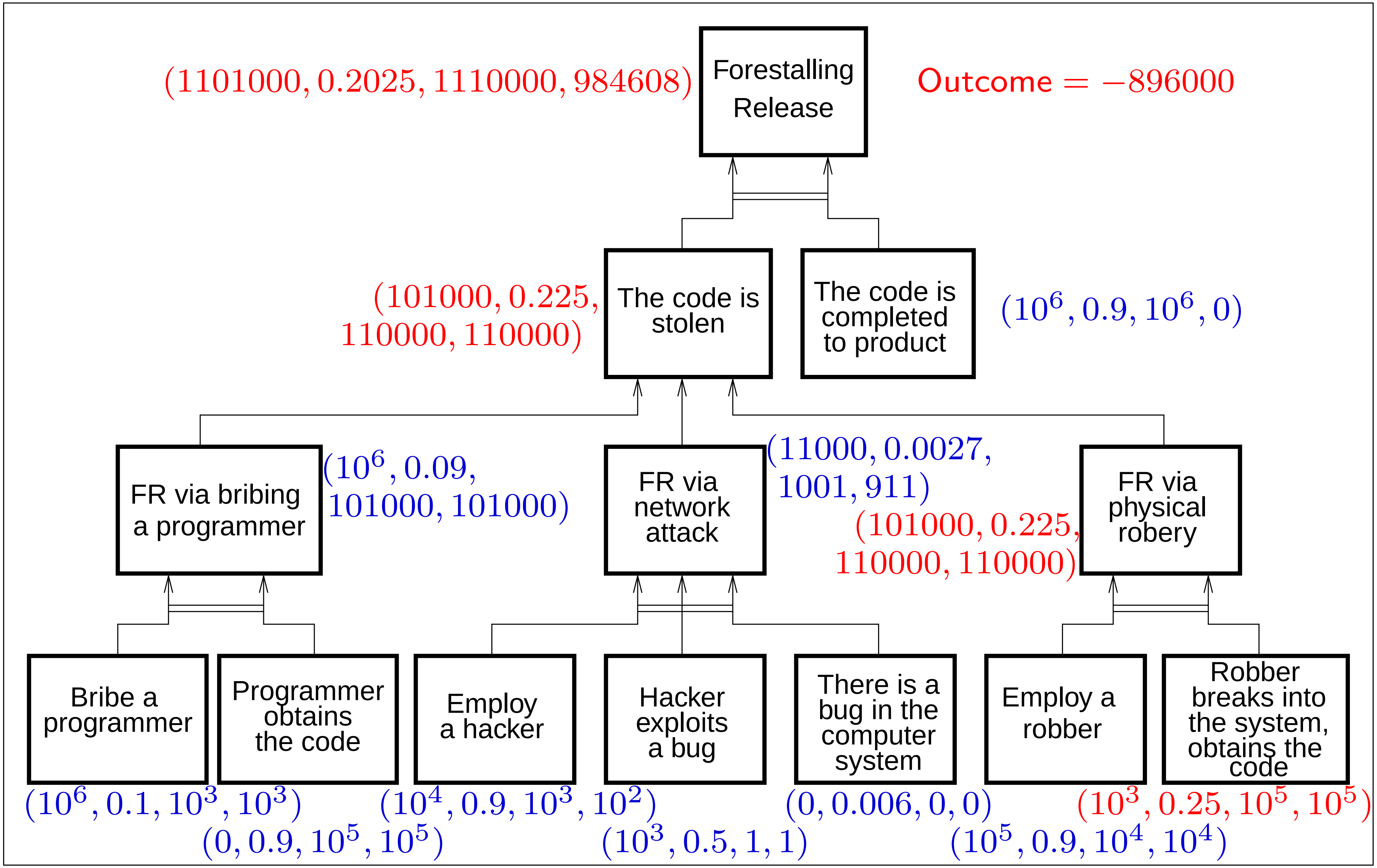
Example continued

- Let us consider two potential sets of security measures:
  - The set $\mathcal{M}_X$ with price $\mathsf{Cost}[\mathcal{M}_X] = \$2,000,000$ reducing the probability of break-in from 0.5 to 0.25
  - The set $\mathcal{M}_Y$ with price $\mathsf{Cost}[\mathcal{M}_Y] = \$1,000,000$ increasing the detection probabilities (hence also the parameters π and π_-) twice
- Provided both sets are adequate, are they also sufficient?

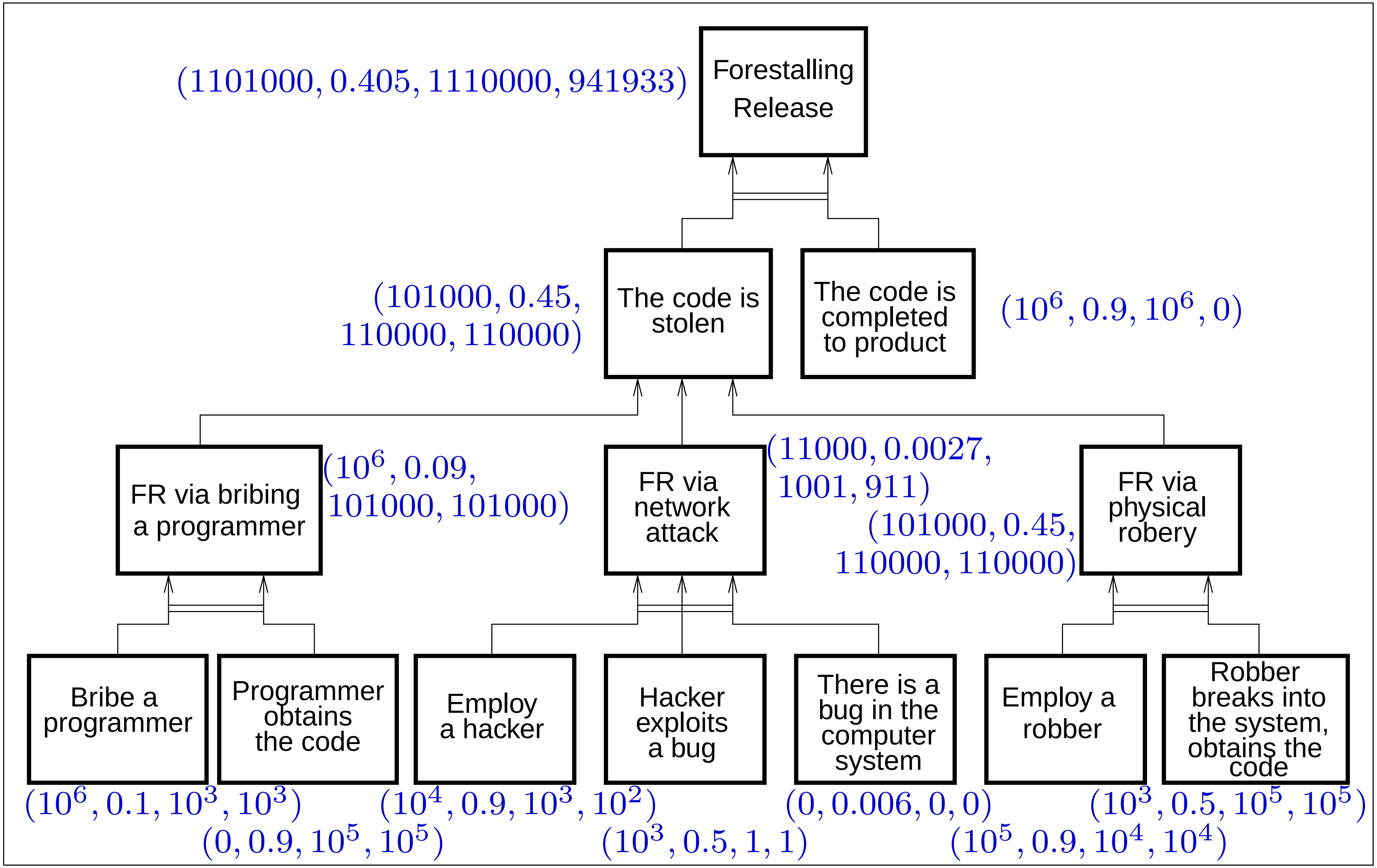
Example: Set $\mathcal{M}_X$



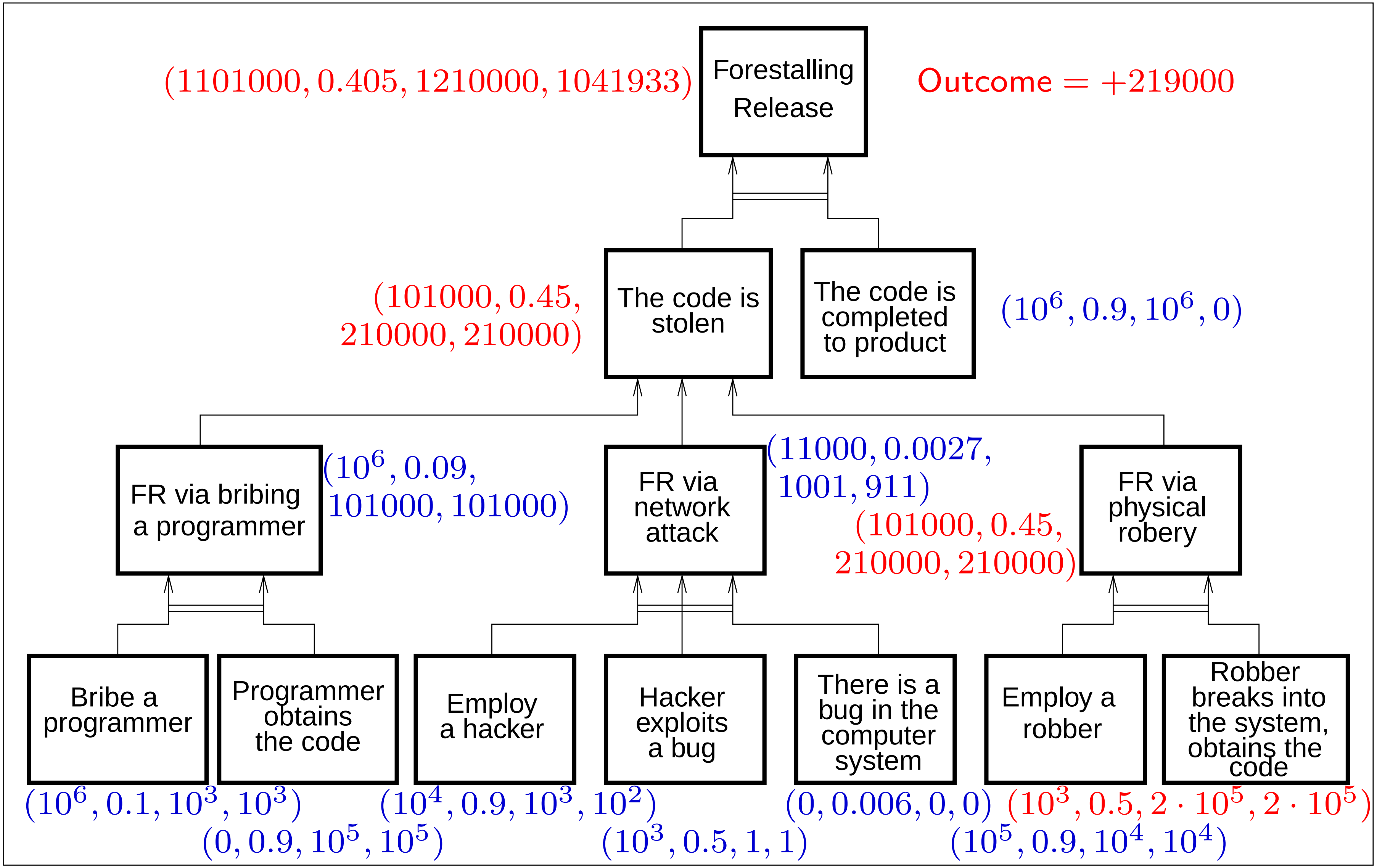
Example: Set $\mathcal{M}_X$



Example: Set $\mathcal{M}_Y$



Example: Set $\mathcal{M}_Y$



Conclusions

- Our contributions:
  - We have considered multi-parameter attack trees with interdependent parameters
  - We have shown how such trees can be used to make security decisions against rational attackers
- Problems to study further:
  - Gains is a global parameter, making the computations in OR-nodes imprecise
  - Dependencies between different child nodes

Thank You!

Questions?