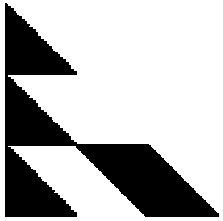
Attack Trees

Bruce Schneier

Counterpane Systems
101 East Minnehaha Parkway, Minneapolis, MN 55419
Phone: (612) 823 1098; Fax: (612) 823-1590
schneier@counterpane.com
http://www.counterpane.com

SANS Network Security 99
New Orleans, LA
8 October 1999



COUNTERPANE

Needs for Threat Modeling

- Understand what the attack goals are.
- Understand who the attackers are.
- Understand what attacks are likely to occur.
- Understand the security assumptions of a system.
- Understand where to best spend a security budget.

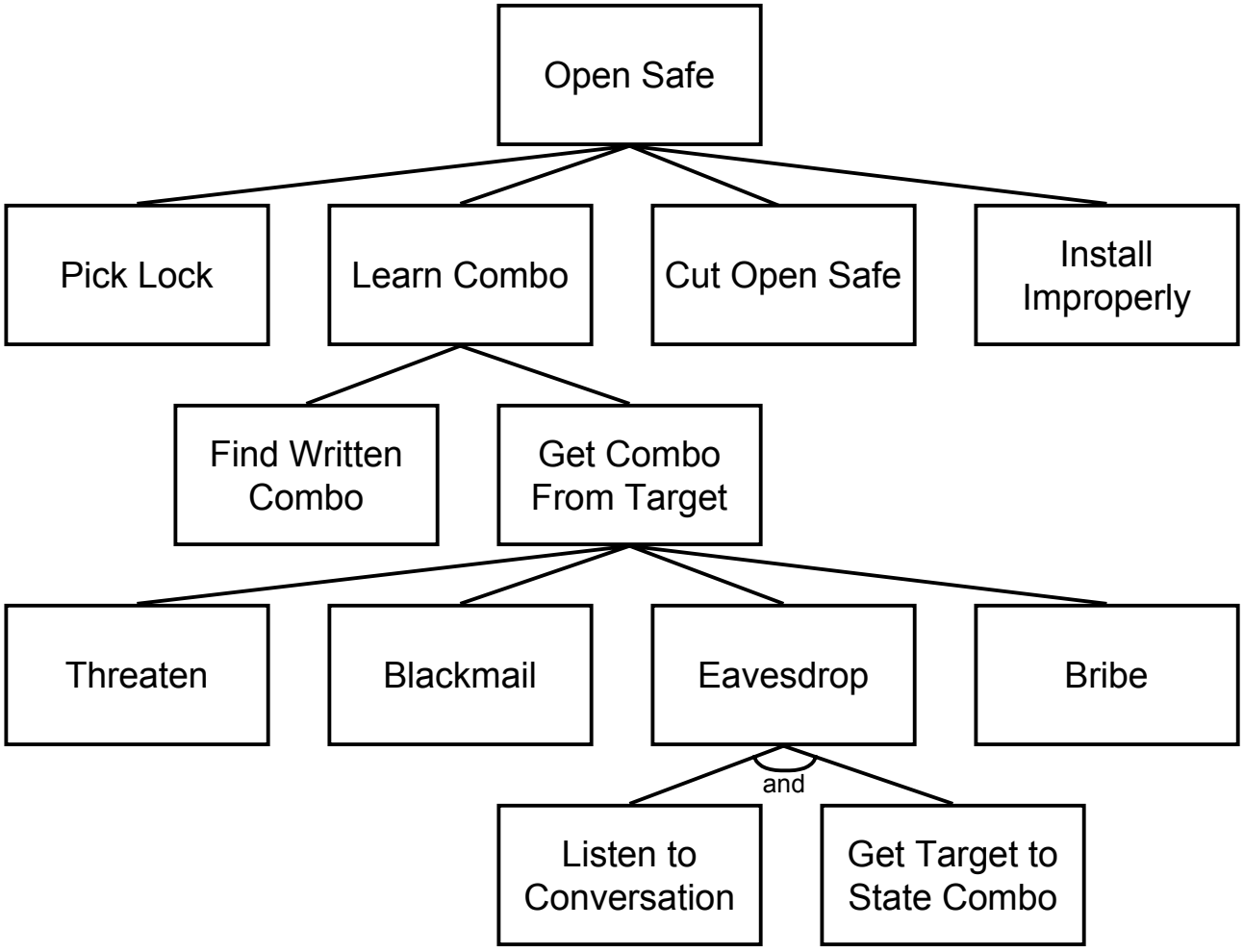
Attack Trees: What Are They?

- A way of thinking and describing security of systems and subsystems.
- A way of building an automatic database that describes the security of a system.
- A way of capturing expertise, and reusing it.
- A way of making decisions about how to improve security, or the effects of a new attack on security.

Attack Trees: How Do They Work?

- Represent the attacks and countermeasures as a tree structure.
- Root node is the goal of the attack.
  - In any complex system, there are several root nodes, each representing a different goal.
- Leaf nodes are attacks.

Basic Attack Tree



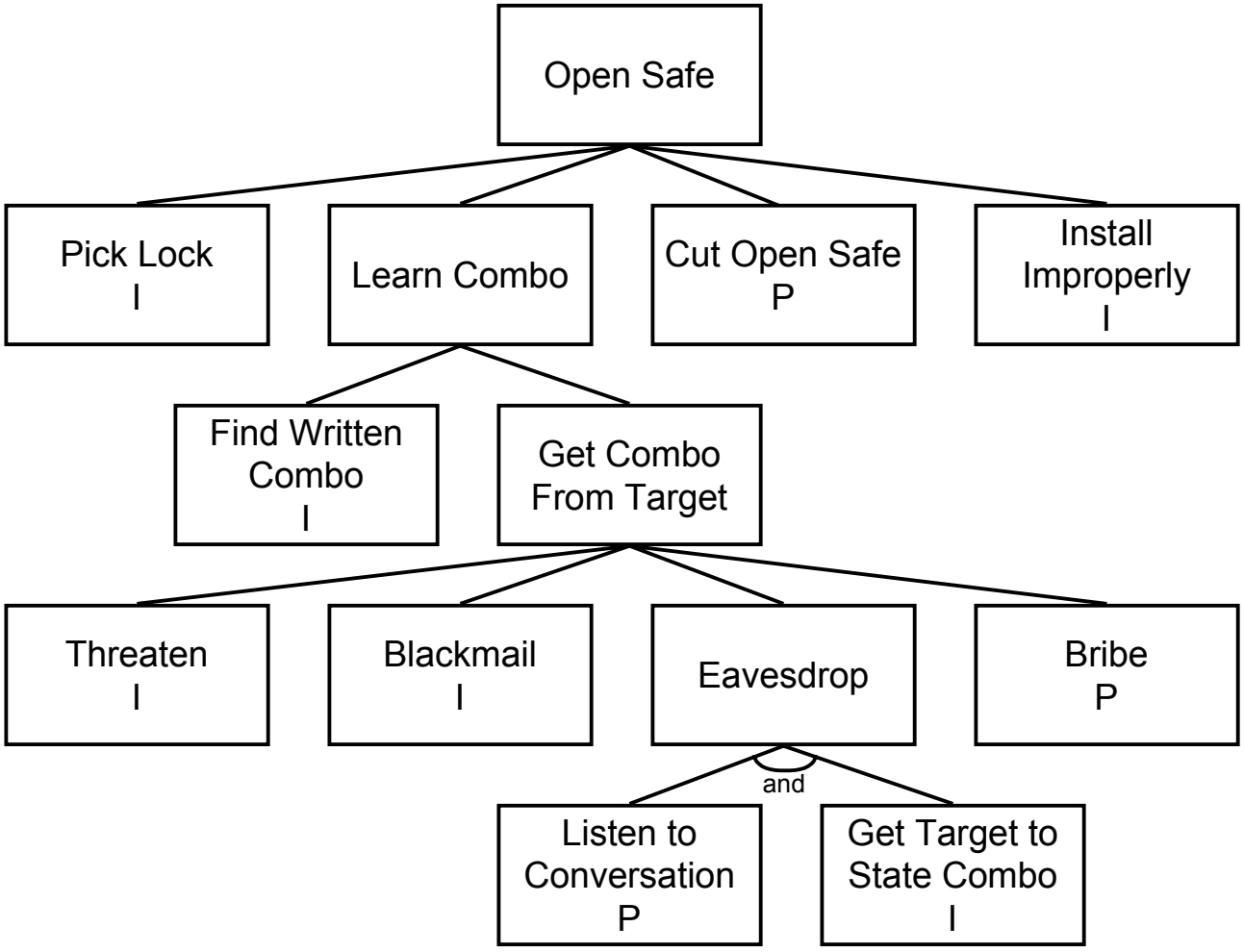
COUNTERPANE

"And" Nodes and "Or" Nodes

- "Or" nodes represent different ways to achieving the same goal.
  - For example, to break into a house you can either pick the door lock OR break a window.
- "And" nodes represent different steps in achieving a goal.
  - For example, to enter through a window you need to break the window AND climb through the opening.

COUNTERPANE

Possible and Impossible Nodes



P = Possible
I = Impossible

COUNTERPANE

Propagating Node Values Up the Tree

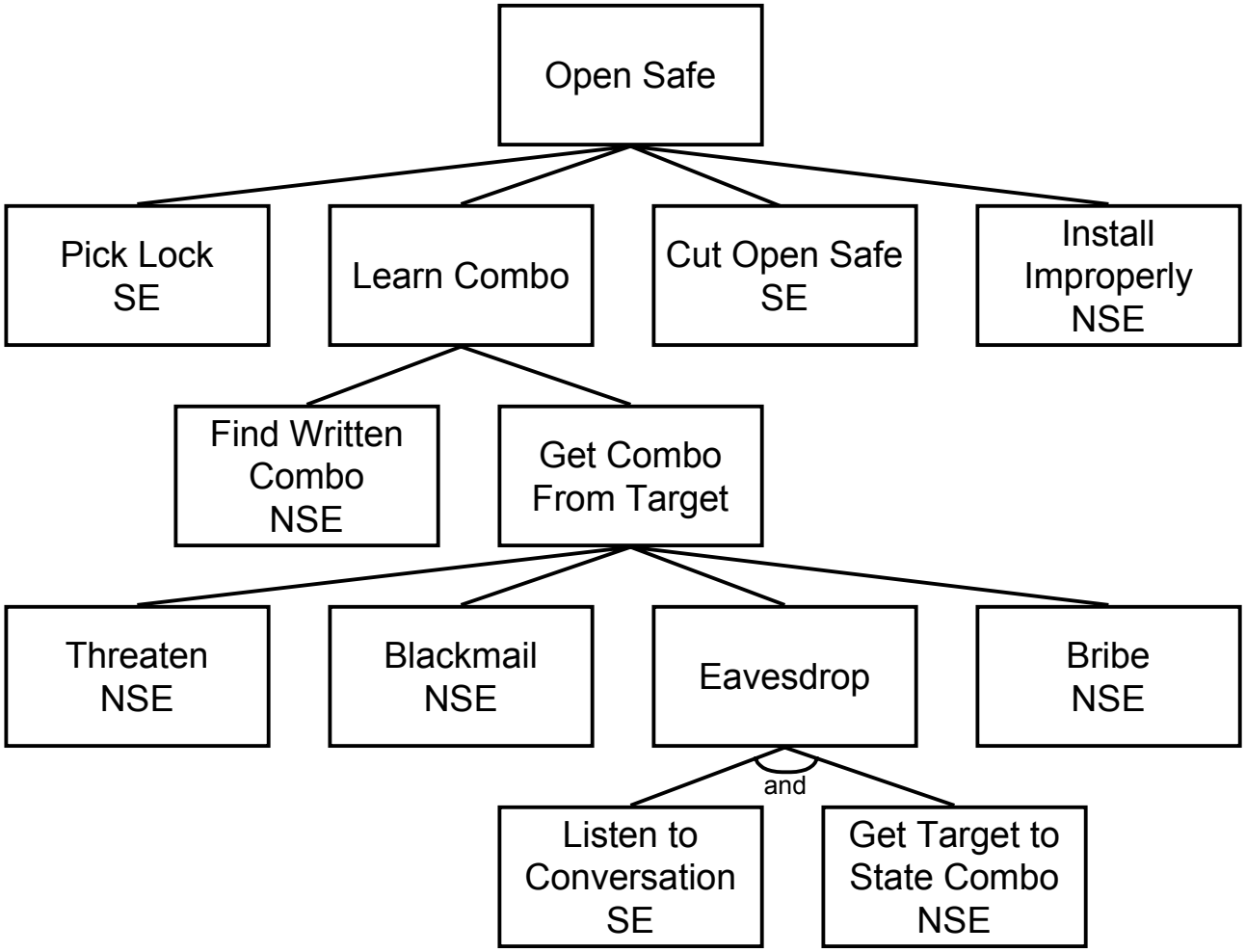
- A node's value is a function of its children's.
- Different calculation rules for AND nodes and OR nodes.
- Start at the leaf nodes and calculate up to the root.

COUNTERPANE

Other Boolean Node Values

- Any Boolean value can be codified in the leaf nodes and then used to prune the tree.
  - Easy and not easy.
  - Expensive and not expensive.
  - Intrusive and non-intrusive.
  - Legal and illegal.
  - Special equipment required and not required.

Special Equipment Required



NSE = No special equipment

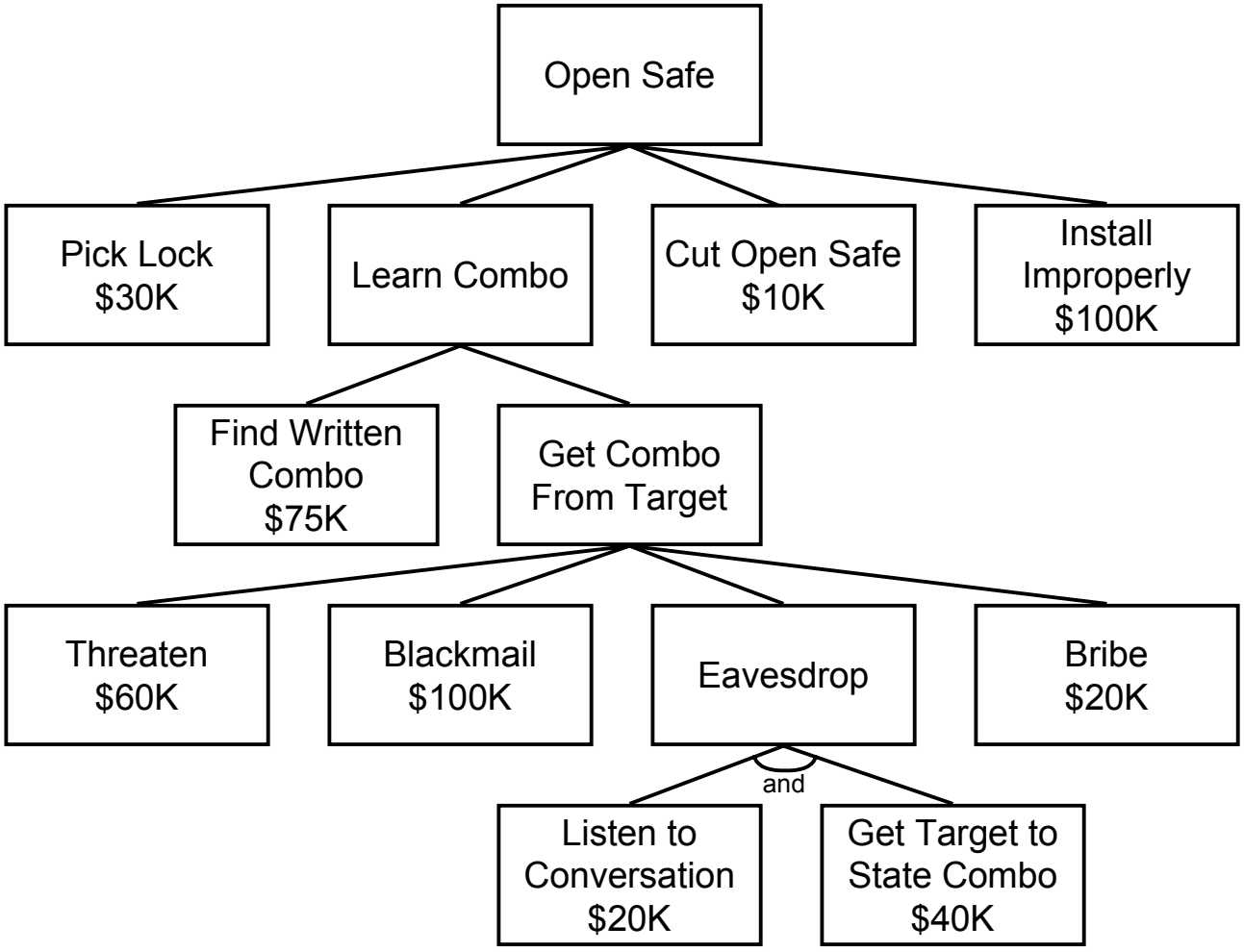
SE = Special equipment required

COUNTERPANE

Continuous Node Values

- Continuous node values can also be codified into the leaf nodes.
  - Cost in dollars to attack / defend.
  - Time to achieve / repulse.
  - Cost in resources to attack / defend.

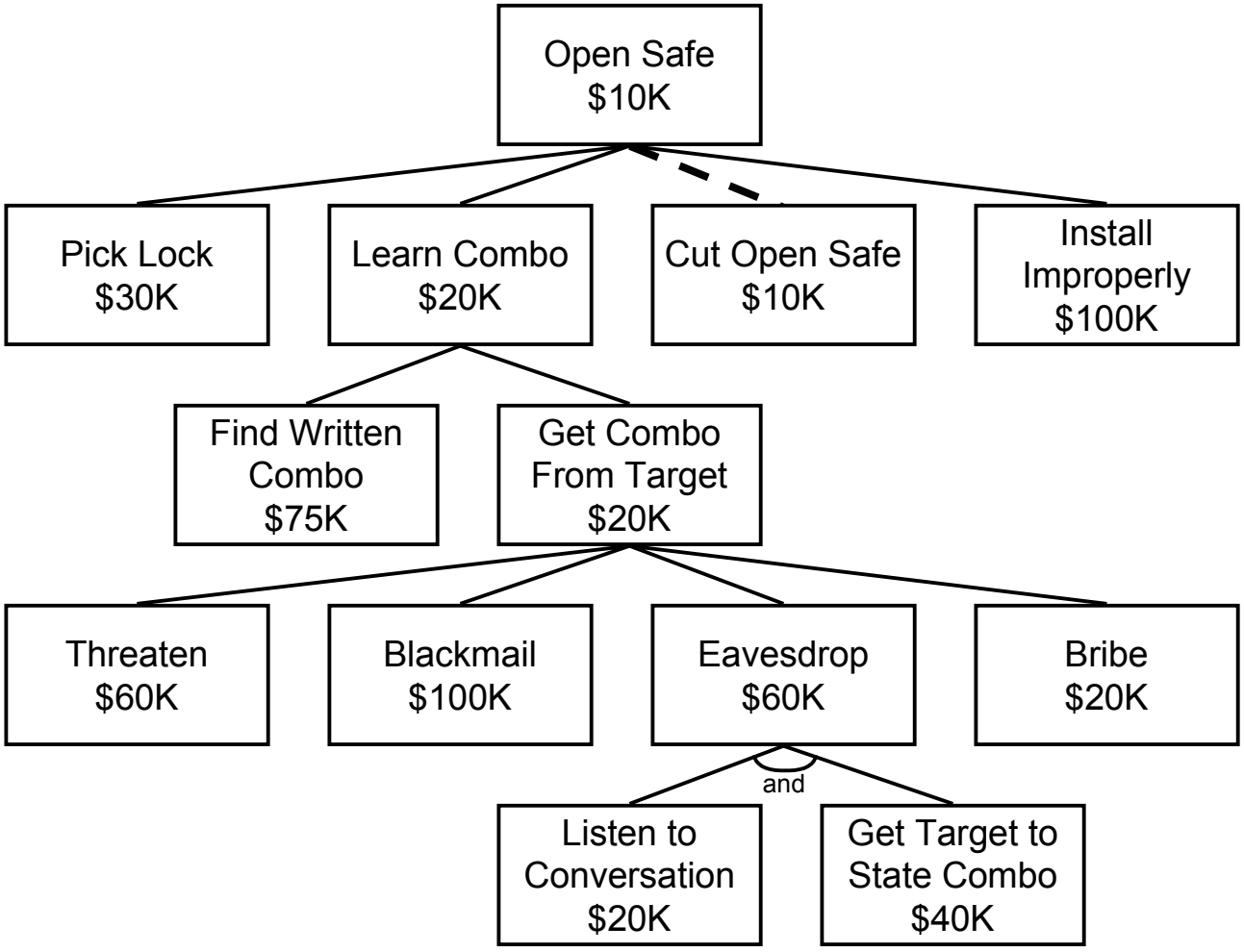
Cost of Attack



$ = Cost of attack

COUNTERPANE

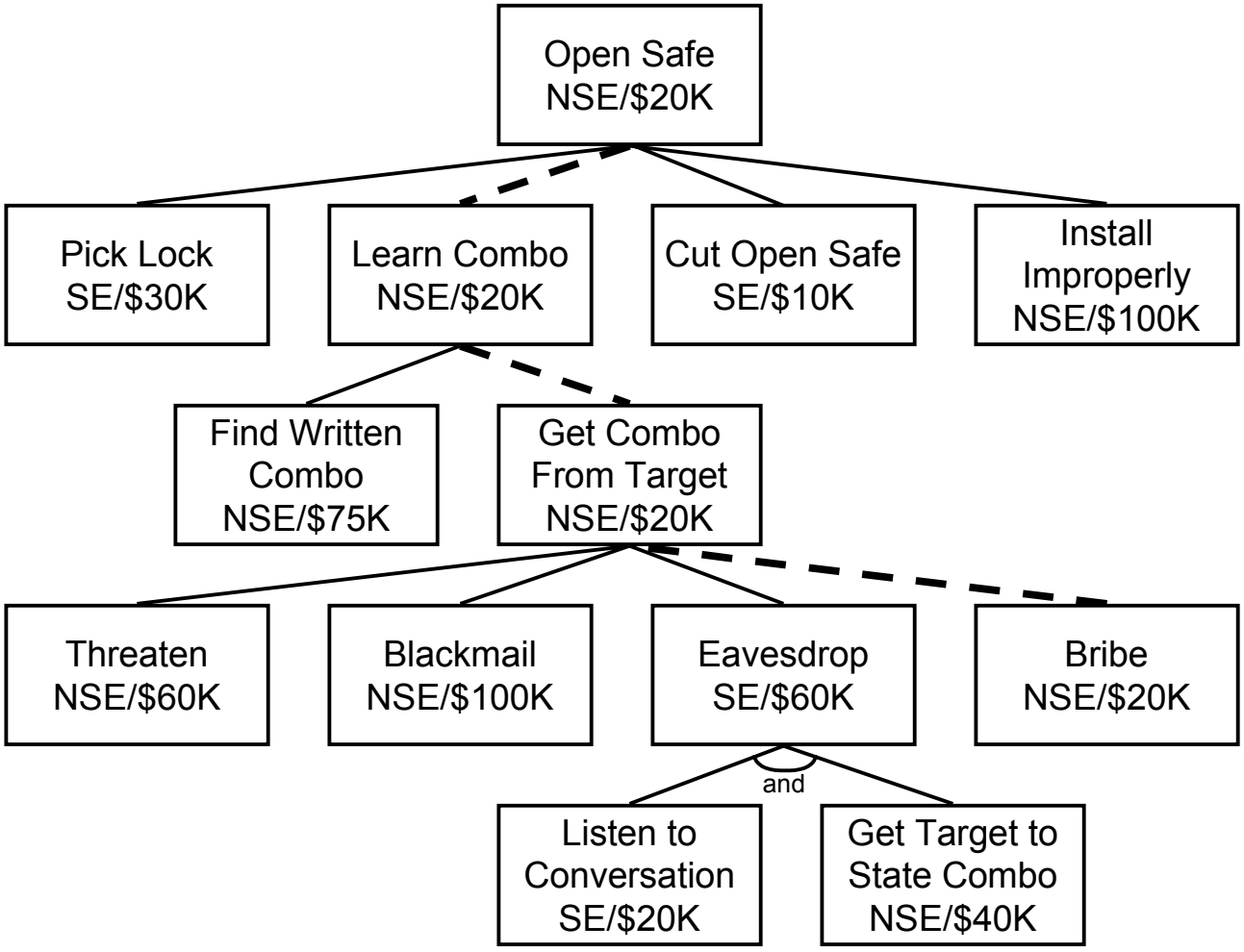
Cheapest Attack



$ = Cost of attack

COUNTERPANE

Cheapest Attack Requiring No Special Equipment



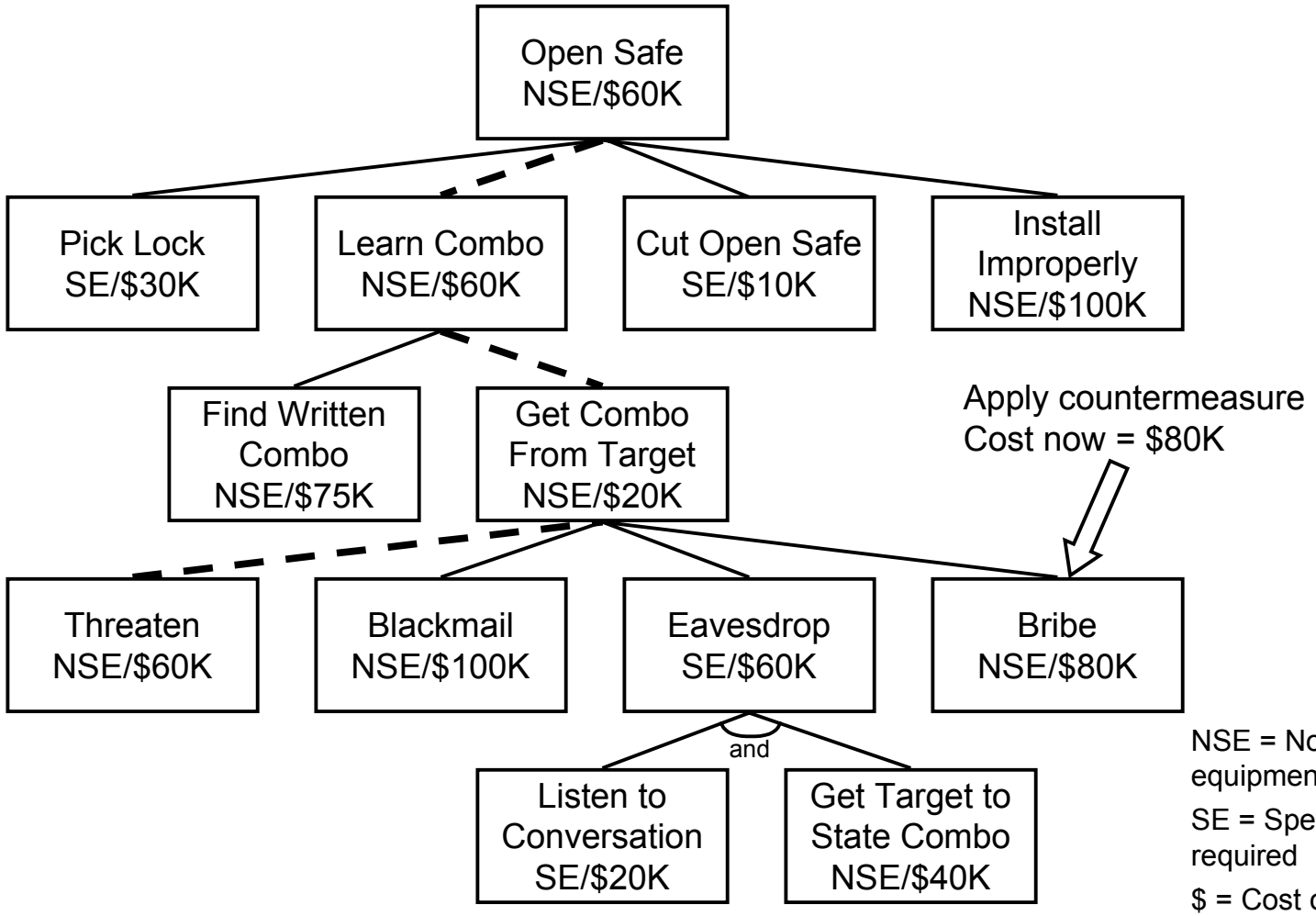
NSE = No special equipment

SE = Special equipment required

$ = Cost of attack

COUNTERPANE

Applying a Countermeasure– Cheapest NSE Attack Now $60K



NSE = No special equipment

SE = Special equipment required

$ = Cost of attack

COUNTERPANE

Other Continuous Node Values

- Probability of success of a given attack.
- Likelihood that an attacker will try a given attack.

COUNTERPANE

Combining Node Values

- Each node can have several values: Boolean and continuous.
- Can be used to make statements about attacks.
- For example:
  - Cheapest low-risk attack
  - Most likely non-intrusive attack
  - Best low-skilled attack
  - Cheapest attack with the highest probability of success

Tree Construction

- Step 0) Identify goals. Each goal is a separate attack tree.
- Step 1) Identify attack against goals; repeat as necessary.
- Step 2) Existing attack trees can be plugged in as appropriate.
- In general, once you have a library of general attack trees, you can create a specific tree out of these reusable components after the first couple of levels.

Using an Attack Tree to Determine the Vulnerability of a System Against an Attack

- After building an attack tree, an analyst can look at the value of the root node to see if the system goal is vulnerable to attack.
- For example, the presence of a possible Boolean value or an attacker's cost below a certain threshold.
- The analyst can also determine if the system is vulnerable to a particular type of attack.
  - Password guessing attacks, legal attacks, unskilled attacks, etc.

Using an Attack Tree to List the Security Assumptions of a System

- The attack tree can also be used to provide a comprehensive list of the assumptions of a security system.
  - For example, the security of this system assumes that no one can successfully bribe the president of our corporation.

What Else?

- Attack trees can show:
  - Intrusive vs. non-intrusive attacks.
  - Legal vs. illegal attacks.
  - Budget, skills, and/or access required of an attacker.
  - Probabilities of success for various attacks.
  - Likelihood of different attacks.
  - Value of different attacks.

What Else? (cont.)

- Attack trees can compare:
  - Effects of various countermeasures.
  - Security of different products.
- Attack trees can show:
  - What assumptions security is based on.
  - What happens when those assumptions are broken.
  - How to best use a security budget.

Scalability

- Attack trees become part of larger attack trees.
  - Attack tree against safe is part of a larger attack tree, whose goal is to read a document.
  - Attack tree against PGP is part of a larger attack tree, whose goal is to read a particular file.
- You can read the results of an attack tree without understanding its details.

Scalability (cont.)

- Changes at lower levels automatically propagate.
  - A new attack against PGP automatically affects the security of any tree that has PGP as a component.
  - A new attack against an encryption algorithm likewise propagates up.
- Subtrees are reusable components.
  - The PGP tree works everywhere PGP is used.

Conclusions

- In many systems, applying security measures is like sticking a tall spike in the ground and hoping that the enemy runs right into it.
- Attack trees are a methodology to ensure that security is a broad palisade.
- Attack trees are a rigorous way to think about security.
- Attack trees work.