Attack Trees
Attack-Defense Trees

Laurie Williams
williams@csc.ncsu.edu

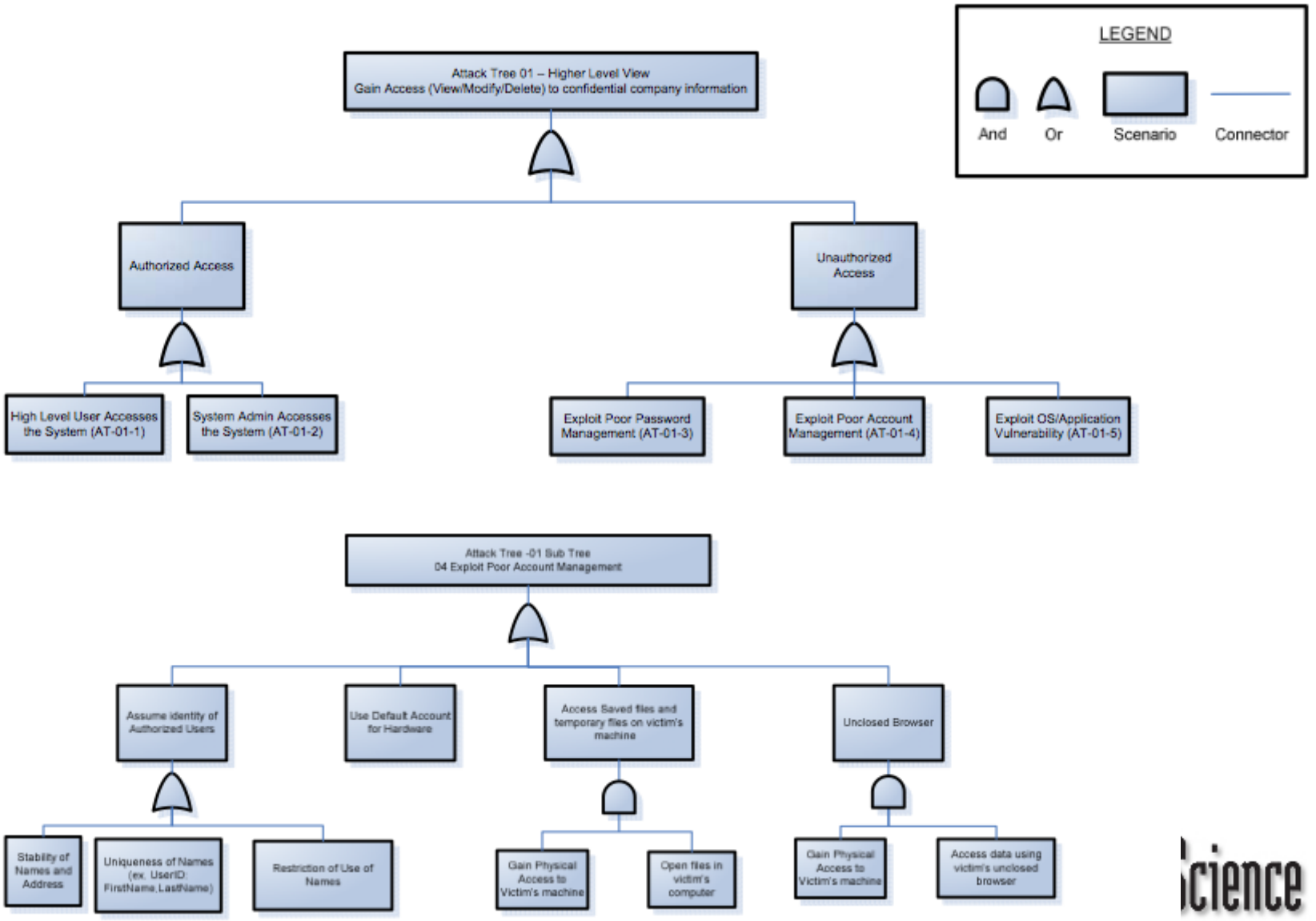
Computer Science
NC STATE UNIVERSITY

http://www.owasp.org/index.php/Application_Threat_Modeling

Attack Trees

- Provide a formal, hierarchical way of describing the security threats to a system based upon the types of attacks that could happen and how they could be realized.
- Attacker's goal listed as the root node and leaves represent different ways to achieve that goal.

Attack trees



http://www.sei.cmu.edu/reports/05tr009.pdf

Another example

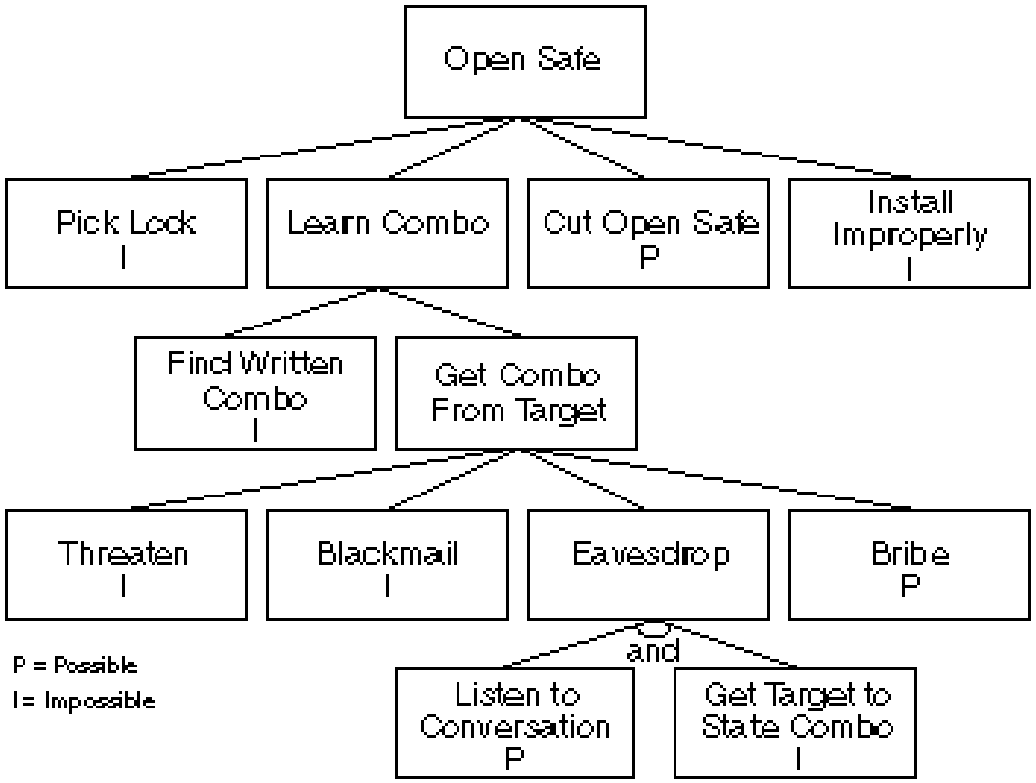


Figure 1: Attack Nodes

https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Prioritizing …

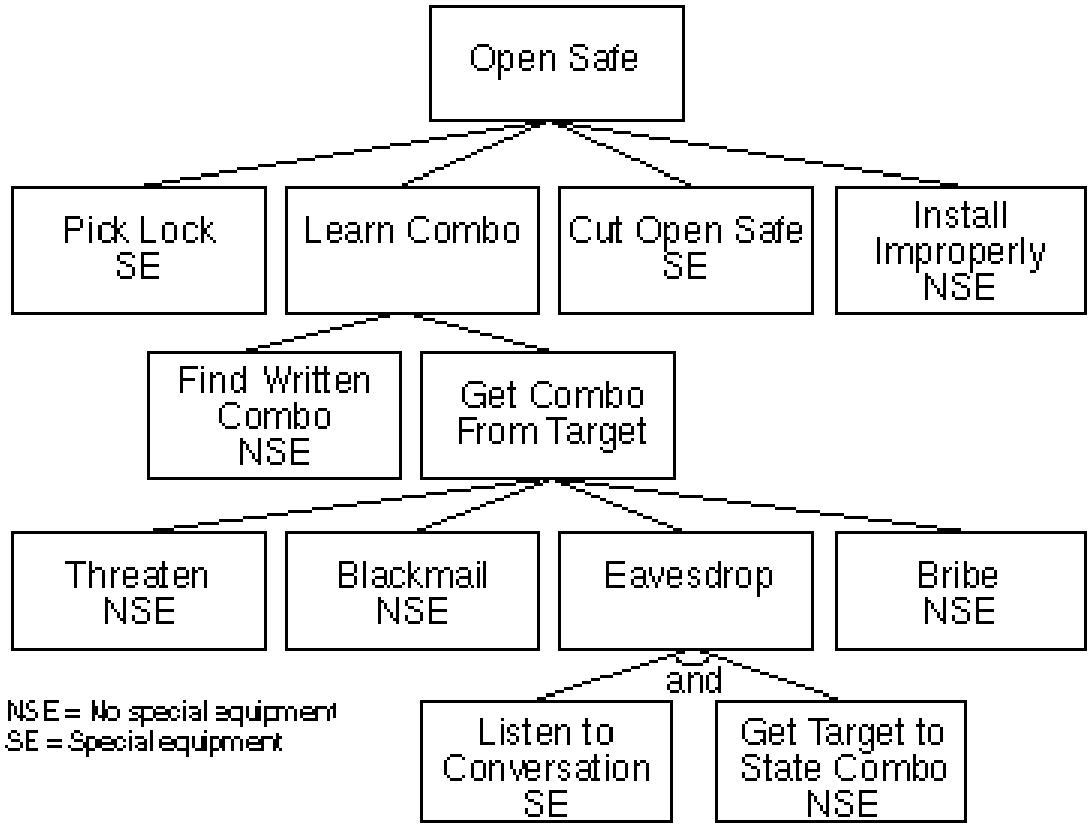


Figure 3: Special Equipment Required

https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Prioritizing …

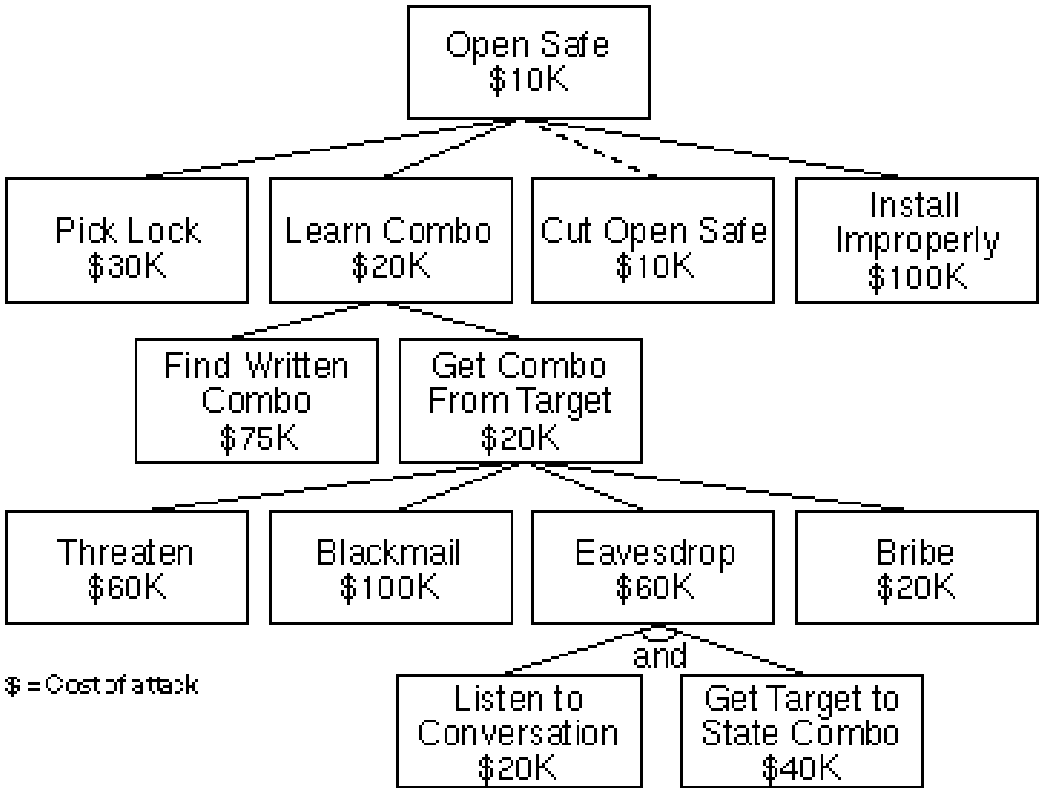


Figure 4: Cost of Attack

https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Prioritizing …

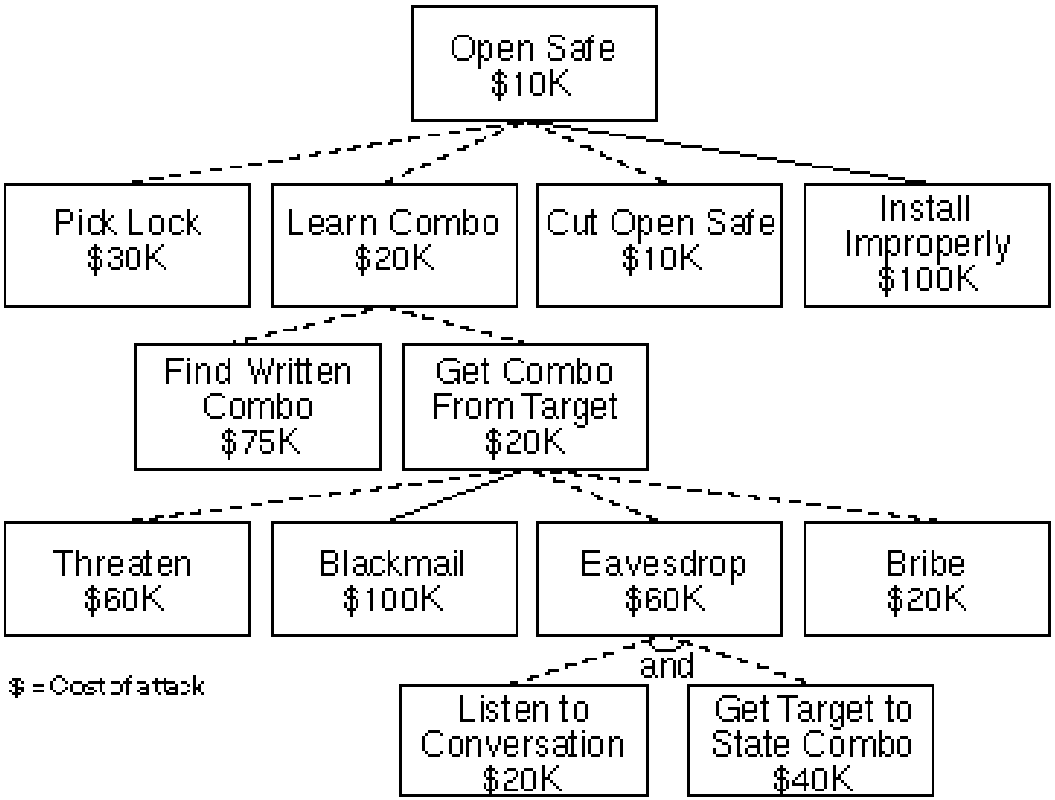


Figure 5: All Attacks Less than $100,000

https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Prioritizing …

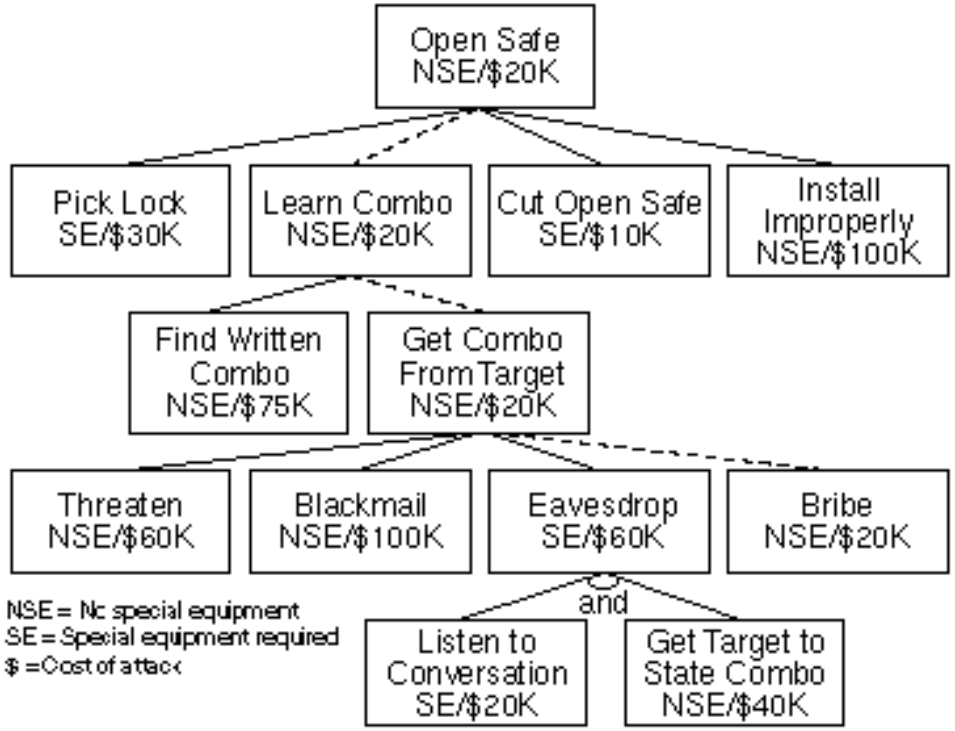


Figure 6: Cheapest Attack Requiring No Special Equipment

Different attackers have different levels of skill, access, risk aversion, money, and so on.

https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Computer Science
NC STATE UNIVERSITY

Classic risk

- Classic Risk = probability of success * impact

Table 1 - System Impact Definitions and Numerical Ranges

Numerical Range	Impact Definition
1-3	Minor impact to system. May be a nuisance but is easily detected and/or repaired
4-6	Moderate impact to system. Confidentiality, integrity, and/or availability of system affected. Requires non-trivial effort to detect and/or repair.
7-9	Severe impact to system. Significant damage results to system. Considerable effort required to detect and/or repair damage.
10	System completely compromised, inoperable, or destroyed

Edge, K., et al, USING ATTACK AND PROTECTION TREES TO ANALYZE THREATS AND DEFENSES TO HOMELAND SECURITY, 2006

Attack tree risk

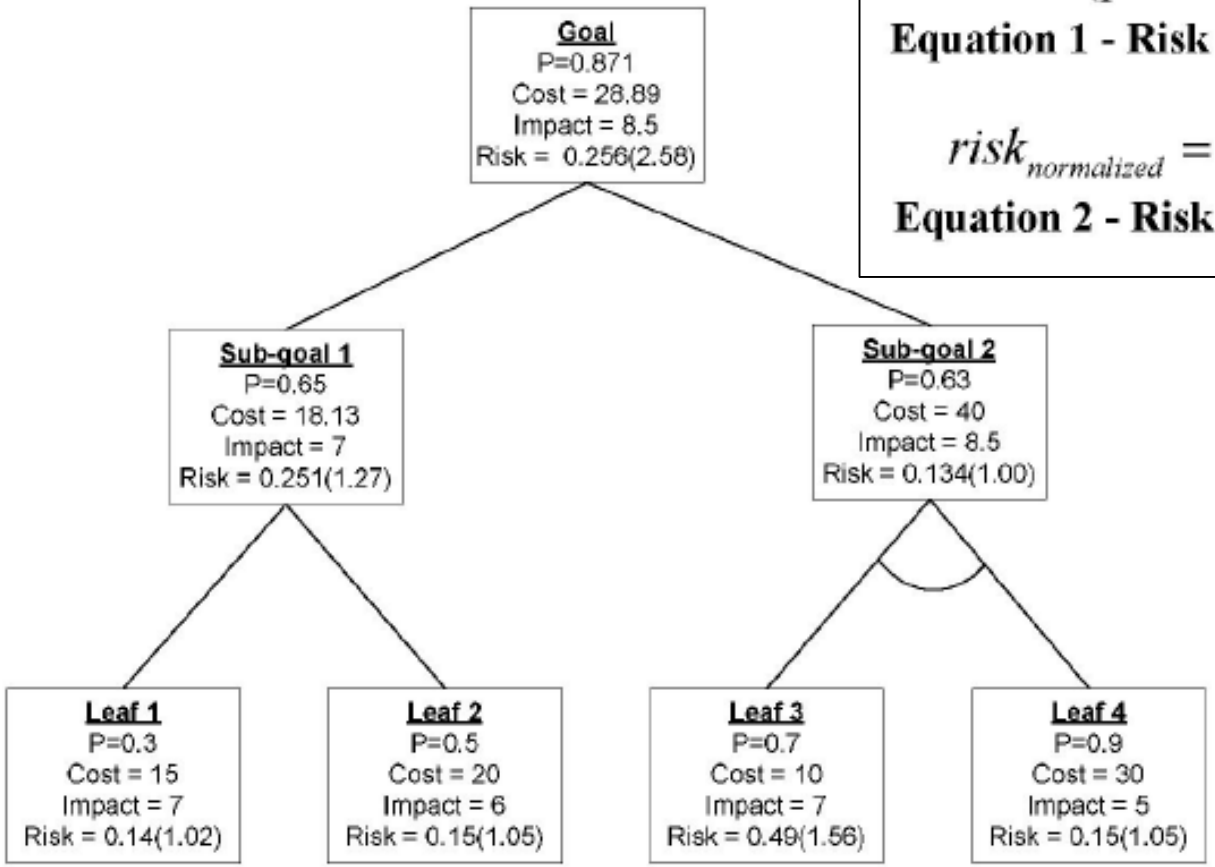
- Classic Risk = probability * impact

$$risk = (probability / cost) \times impact$$

Equation 1 - Risk Calculation for Leaf Nodes

$$risk_{normalized} = \log(risk / risk_{\min} \times 10)$$

Equation 2 - Risk Normalization Calculation



Edge, K., et al, USING ATTACK AND PROTECTION TREES TO ANALYZE THREATS AND DEFENSES TO HOMELAND SECURITY, 2006

Computer Science
NC STATE UNIVERSITY

Propogate Metrics Up Tree

Table 2 – Rule Set to Propagate Metrics Up Tree

	AND	OR
Probability	$\prod_{i=1}^{n} prob_i$	$1-\prod_{i=1}^{n}(1-prob_i)$
Cost	$\sum_{i=1}^{n} cost_i$	$\frac{\sum_{i-1}^{n} prob_i \times cost_i}{\sum_{i=1}^{n} prob_i}$
Impact	$\frac{10^n - \prod_{i=1}^{n}(10-impact_i)}{10^{(n-1)}}$	$Max_{i=1}^{n} impact_i$

$prob \in (0,1], cost \in (0,\infty), impact \in [1,10], n = \#$ of child nodes

Edge, K., et al, USING ATTACK AND PROTECTION TREES TO ANALYZE THREATS AND DEFENSES TO HOMELAND SECURITY, 2006

Attack Tree Process - 1

- Identify the possible attack goals. Each goal forms a separate tree, although they might share subtrees and nodes.
- Think of all attacks against each goal. Add them to the tree. Repeat this process down the tree until you are done.
- Give the tree to someone else, and have him think about the process and add any nodes he thinks of.
- Repeat as necessary.

Attack Tree Process - 2

- Assign the node values.
- Recalculate the nodes based on the new information and see how the goal node is affected.
- Compare and rank attacks -- which is cheaper, which is more likely to succeed, and the like.

Uses of attack trees

- See if the system goal is vulnerable to an attack based upon the "how"s.
- Guides you to consider the security assumptions of the system.
- Can be used to determine the impact of a system modification.
- Can be used to compare and rank attacks.

What else?

- Attack trees can show:
  - Intrusive versus non-intrusive attacks
  - Legal versus illegal attacks
  - Budget, skills, and/or access required of the attacker.
  - Probabilities of success for various attacks.
  - Likelihood of different attacks.
  - Value of different attacks.
  - Compare
    - Effects of countermeasures
    - Security of different products

From: http://tnlandforms.us/cs494-cns01/attacktrees.pdf

Protection (or Defense) Trees

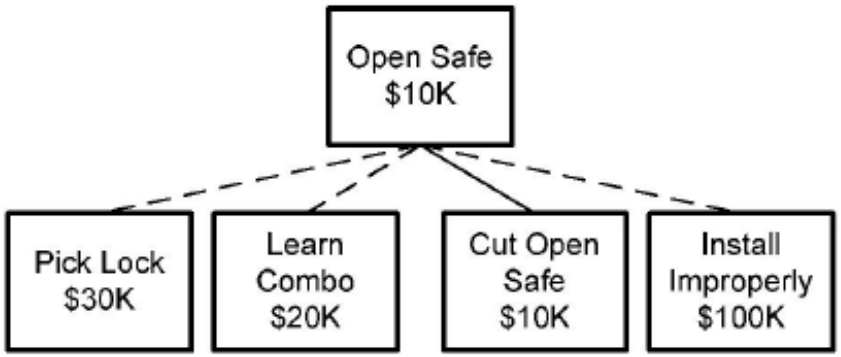


Figure 3 - Partial Attack Tree To Open a Physical Safe **[3]**.

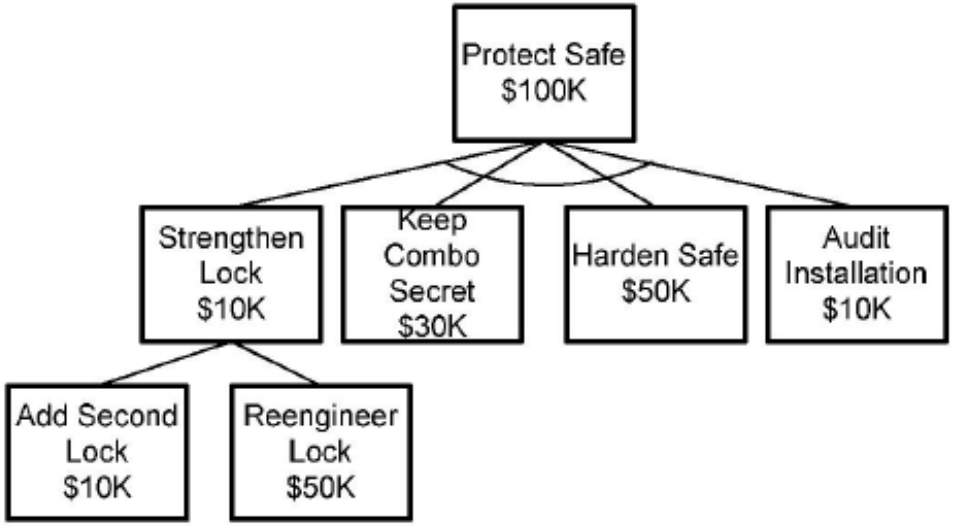


Figure 4 - A Partial Protection Tree for the Safe Attack

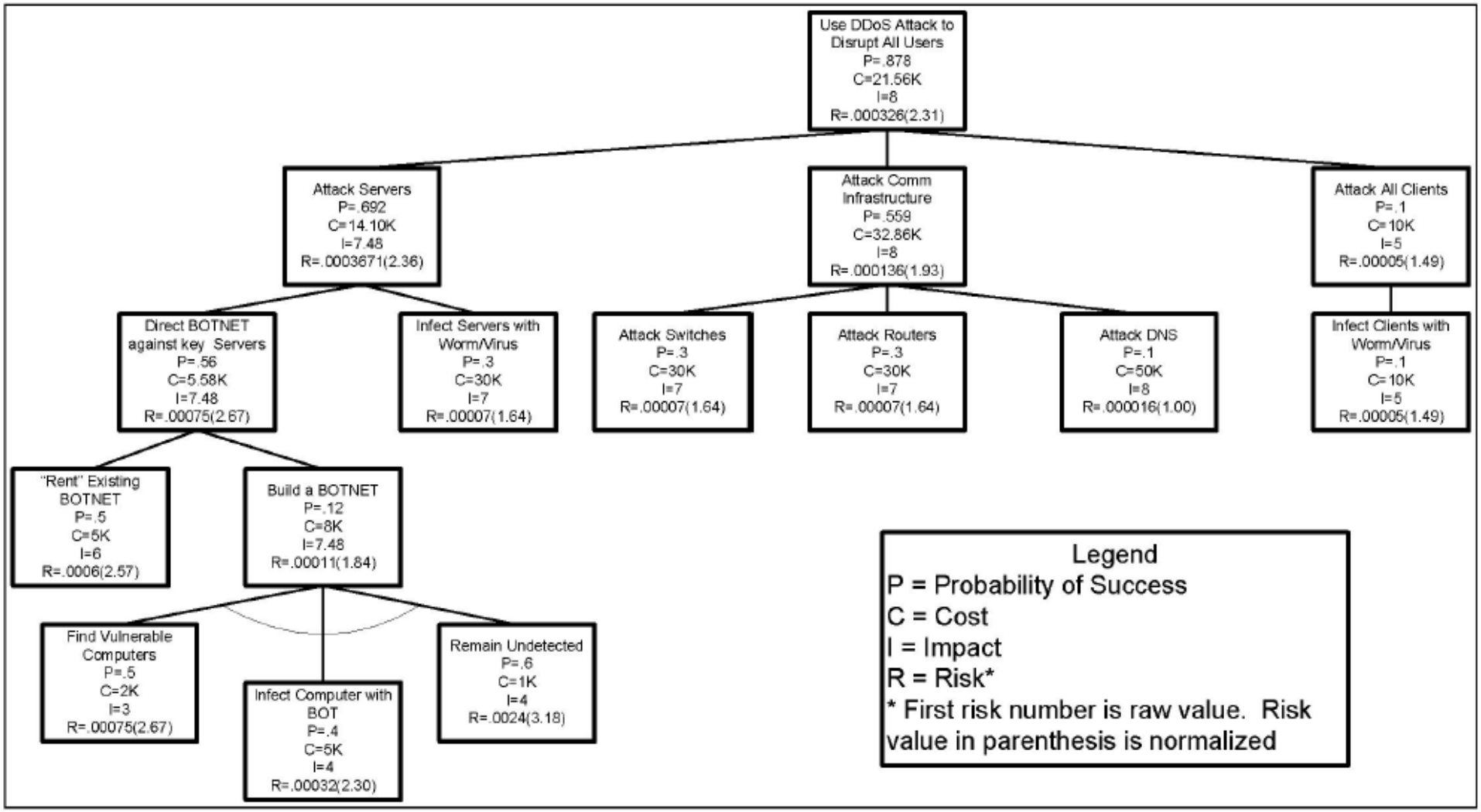


Figure 7 - DDoS Attack Tree

Edge, K., et al, USING ATTACK AND PROTECTION TREES TO ANALYZE THREATS AND DEFENSES TO HOMELAND SECURITY, 2006

Computer Science
NC STATE UNIVERSITY

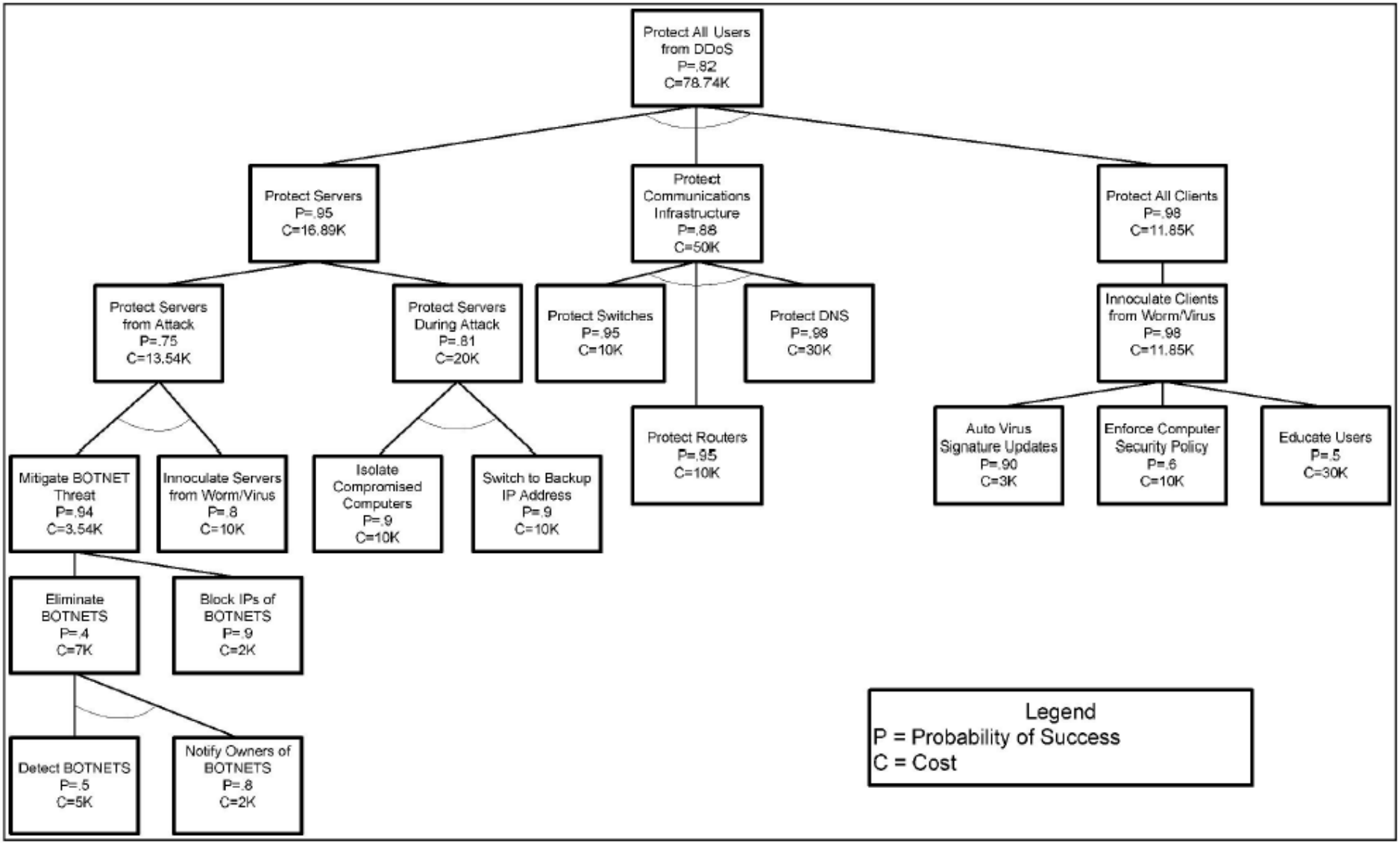


Figure 8 - DDoS Protection Tree

Edge, K., et al, USING ATTACK AND PROTECTION TREES TO ANALYZE THREATS AND DEFENSES TO HOMELAND SECURITY, 2006

Computer Science
NC STATE UNIVERSITY