CIS 4360
Secure Computer Systems

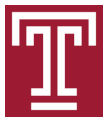
Threat Modeling

Professor Qiang Zeng

Spring 2017

Previous Class

- The CIA Triad as security objectives
- Threat: potential
- Attack: attempt
- Compromise: success
- Vulnerability: security flaw
- Attack Vectors vs. Exploits vs. Payloads

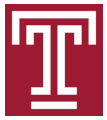


Previous class…

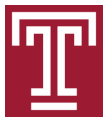
Attack Vector vs. Exploit vs. Payload

An *attack vector* is an attack delivery method;
An *exploit* is some specially crafted code or input that takes advantage of vulnerabilities
The *payload* in an exploit is to be executed to achieve the attacker's goal

An attack vector is to deliver an attack;
an exploit is used to deliver the payload

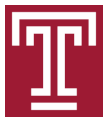


Analogy: in an air attack mission, “delivering missiles through an F-35” is the “attack vector”, “the missile” is the “exploit”, and “the warhead in the missile” is the “payload”, “the fragile part of the fort” is the “vulnerability”



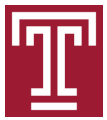
Outline

- Attack Surface and Attack Surface Reduction
- Threat model and Threat modeling
  - STRIDE model
  - Attack Tree



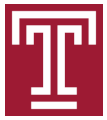
Attack Surface

- The attack surface of a system is a collection of components (e.g., network ports, programming interfaces, services) that can be reached and exploited by attackers
  - Keywords: reachable & exploitable
- From the perspective of social engineering, is an employee with access to sensitive information part of the attack surface?
  - Yes



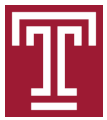
Attack Surface Reduction

- One practice to improve security is to reduce the attack surface, called Surface Reduction
- *Example*: the attack surface of a server contains all the *ports* that are used to receive requests (due to various services running on the server). Now, if you use firewall to block all the requests except at port 80 (used by web service), then the attack surface is reduced to the port 80 only (even you accidentally run some other services)



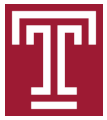
Attack Surface Reduction

- Strategies of attack surface reduction are to
  - reduce entry points available to attackers
  - eliminate unneeded services running on a server
  - reduce the number of users that can access a system
  - …



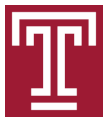
Adversaries and Adversary Model

- An adversary is a malicious entity trying to circumvent the security measures
  - Synonyms for Attackers, threat agents
- An Adversary model is to describe who the adversaries are and their capabilities
- Consider the online system of the Temple library
  - The adversaries include both unauthorized users and authorized users
  - Unauthorized users can request connecting to the service, scan the ports of the web server, etc.
  - Authorized users can, in addition, submit SQL queries, etc.



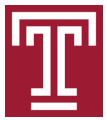
Threat Model

- A threat model is a collection of threats to a specific system
- What is the threat model of the Temple grading system?
  - The instructor's password may by leaked
  - The instructor's computer may be remotely controlled
  - The sever for the grading system may be hacked
  - Disgruntled sysadmin may delete all the data
  - …



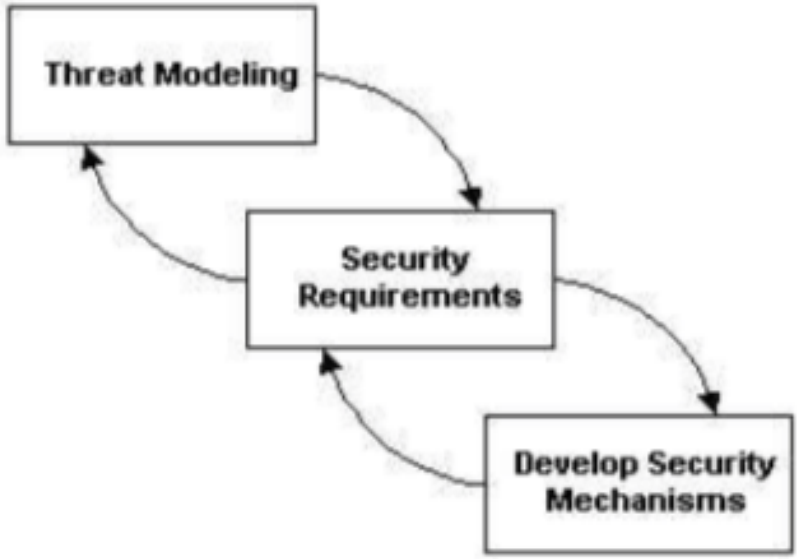
Threat Modeling

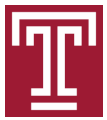
- Threat Modeling is a process of identifying (and prioritizing) threats to a system. It involves
  - Characterizing the system
  - Identifying the attack surface and adversary model
  - Identifying threats



Threat Modeling and Security Engineering

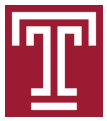
- Security engineering should be incorporated into the system design process as early as possible. It would be much more costly if security is later retrofitted into an existing system
- Threat modeling should be the first step taken for security engineering





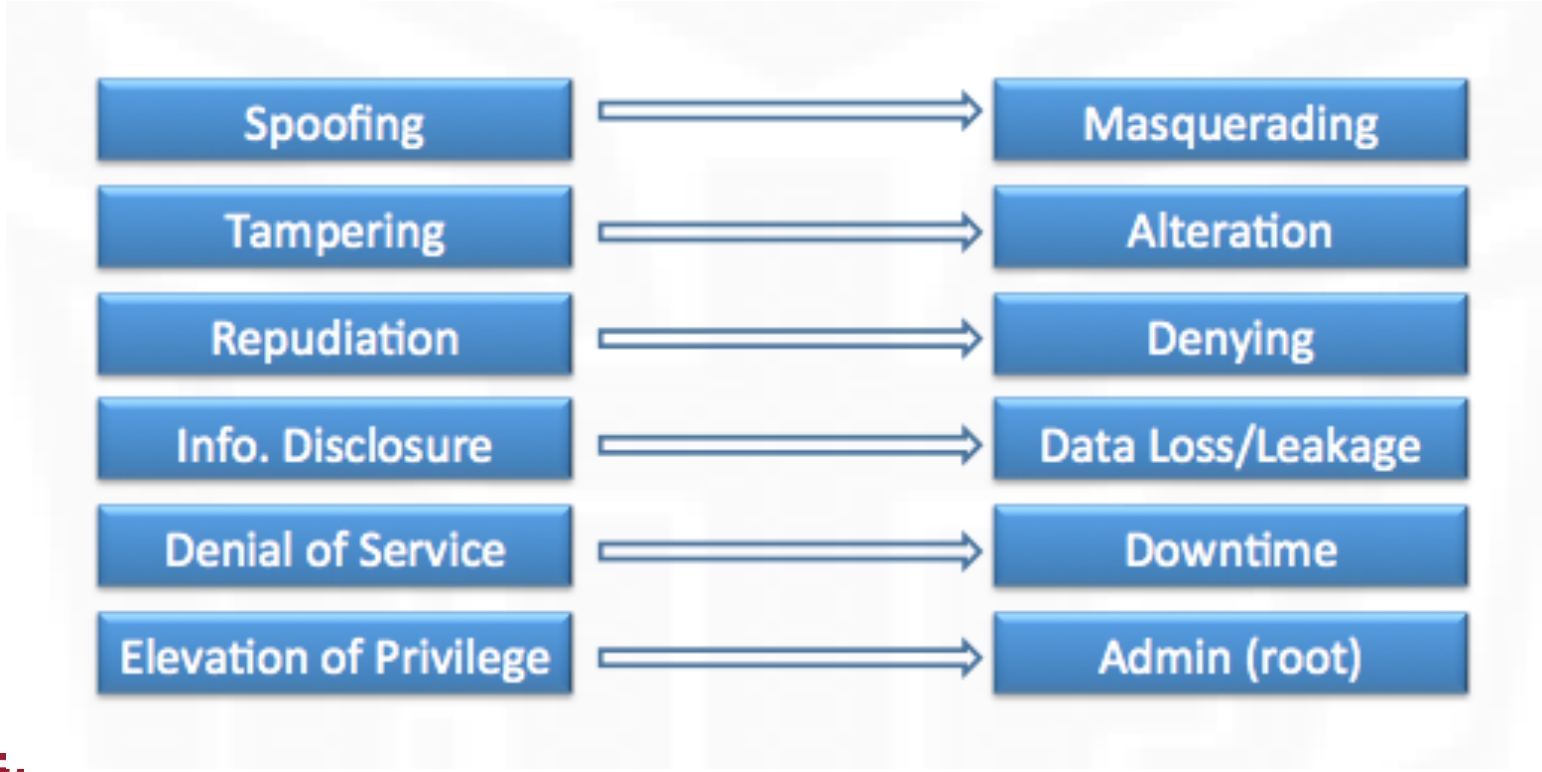
Threat Modeling and Security Requirements

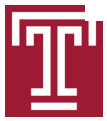
- Threat modeling helps define security requirements. But note that it is unlikely to mitigate all the threats. When defining the security requirements, it is important to distinguish threats that should be omitted and ones that we should address
- E.g., earthquakes in CA vs. earthquakes in PA



Microsoft's STRIDE Model

- During threat modeling, you can consider the following categories





Example

Identify example threats to the Temple online library system using the STRIDE model

Spoofing: an attacker may construct a fake website to collect the usernames and passwords of library users

Tampering: an attacker may tamer with the database

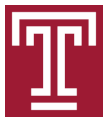
Repudiation: one may deny she/he has borrowed some book

Information disclosure: the list of books a client has borrowed can be leaked

Elevation-of-privilege: an adversary may compromise the library's online service and obtain the sysadmin privileges

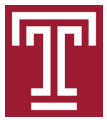
Attack Trees

- An Attack Tree is a tree-structured graph showing how a system can be attacked
  - Root node is the goal of the adversary; in a complex system, usually there are several goals, each needing a separate tree
  - Child nodes are the ways or steps to achieve the parent node

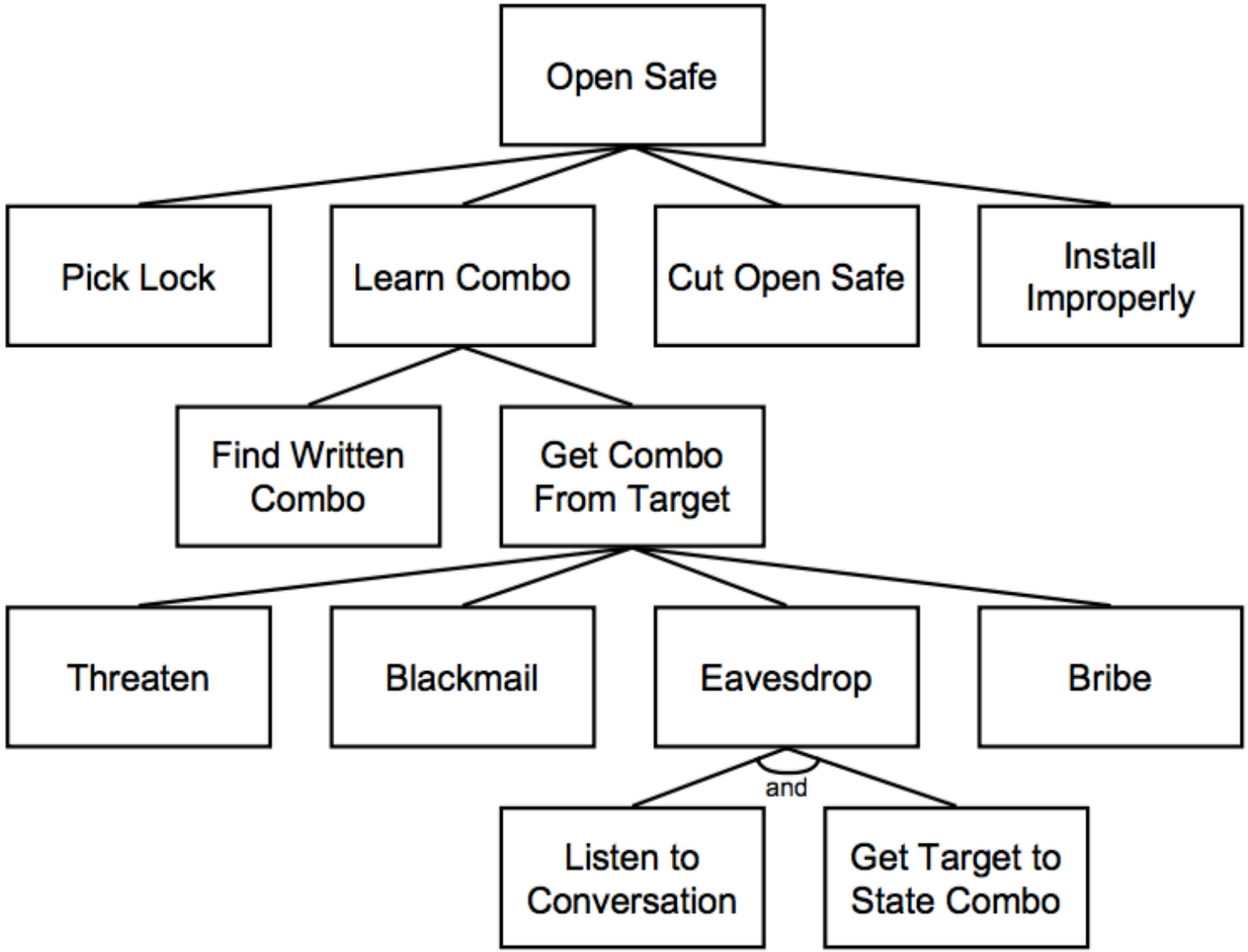


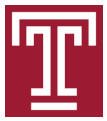
How to construct an Attack Tree

1. Identify goals. Each goal needs a separate attack tree
2. Identify attacks against goals; repeat if necessary
3. Existing attack (sub-)trees can be plugged in as appropriate

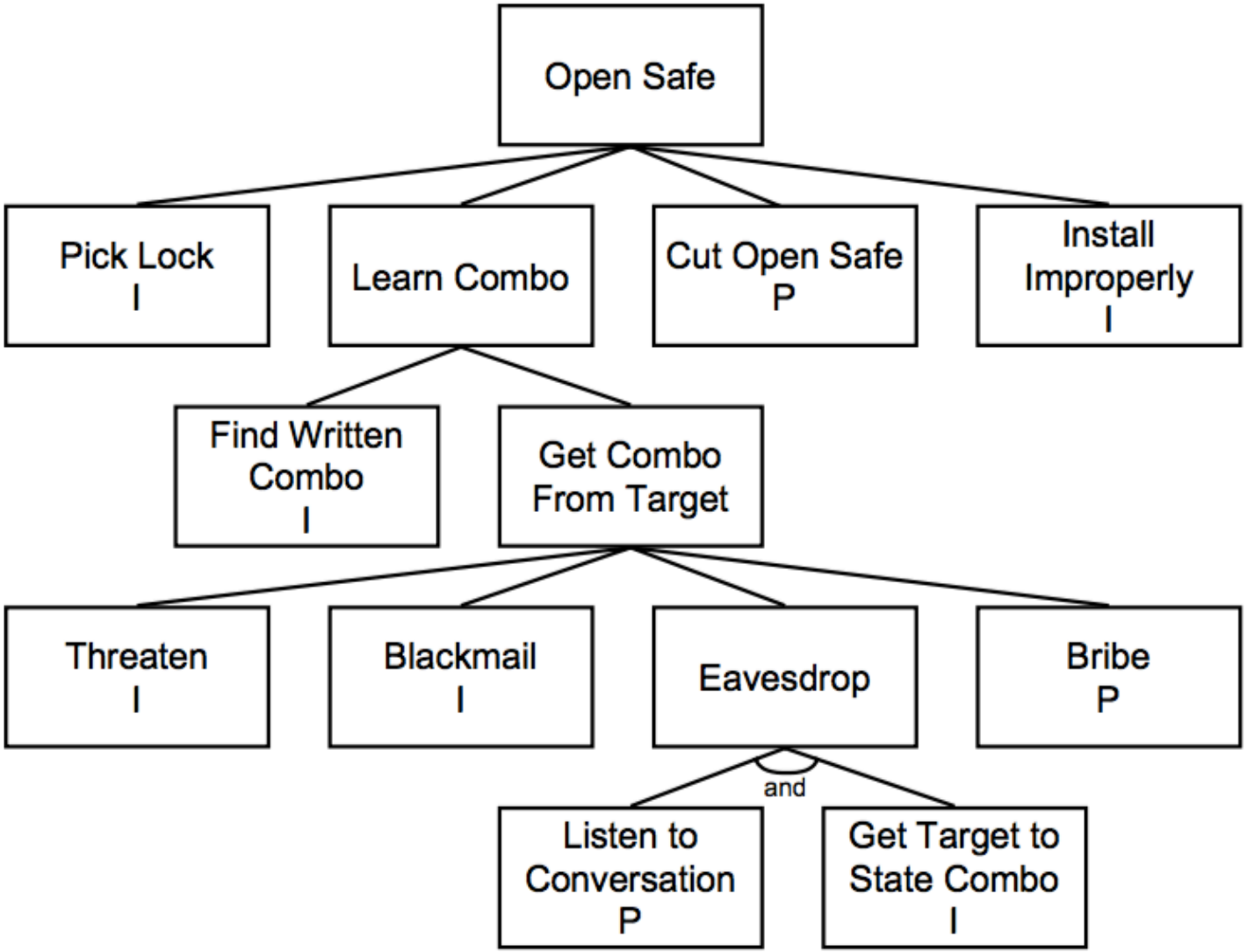


Example: Assume the system is a safe, and the adversary's goal is to open the safe



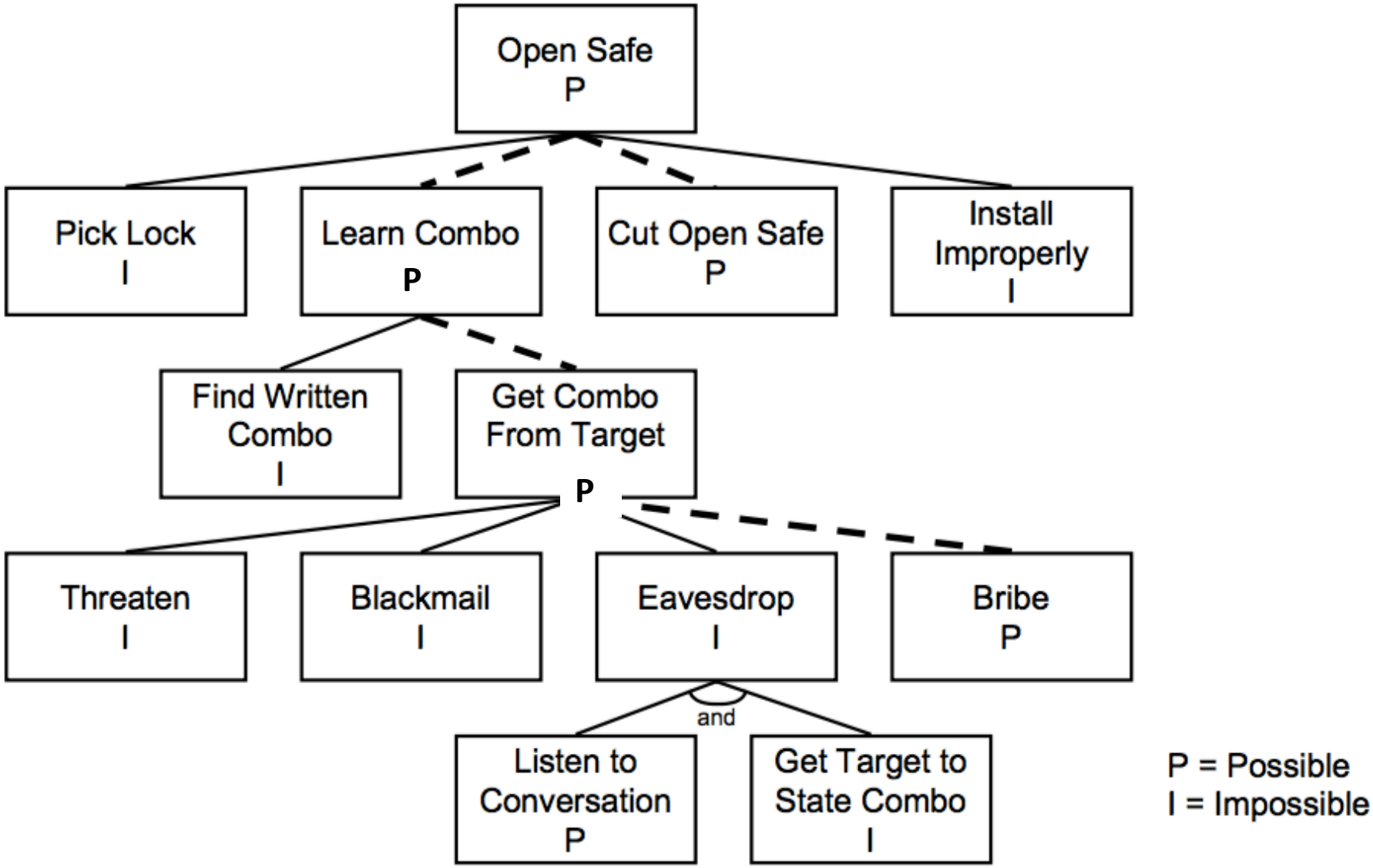


How to use the tree: Once a tree is created, different values can be assigned to the leaf nodes

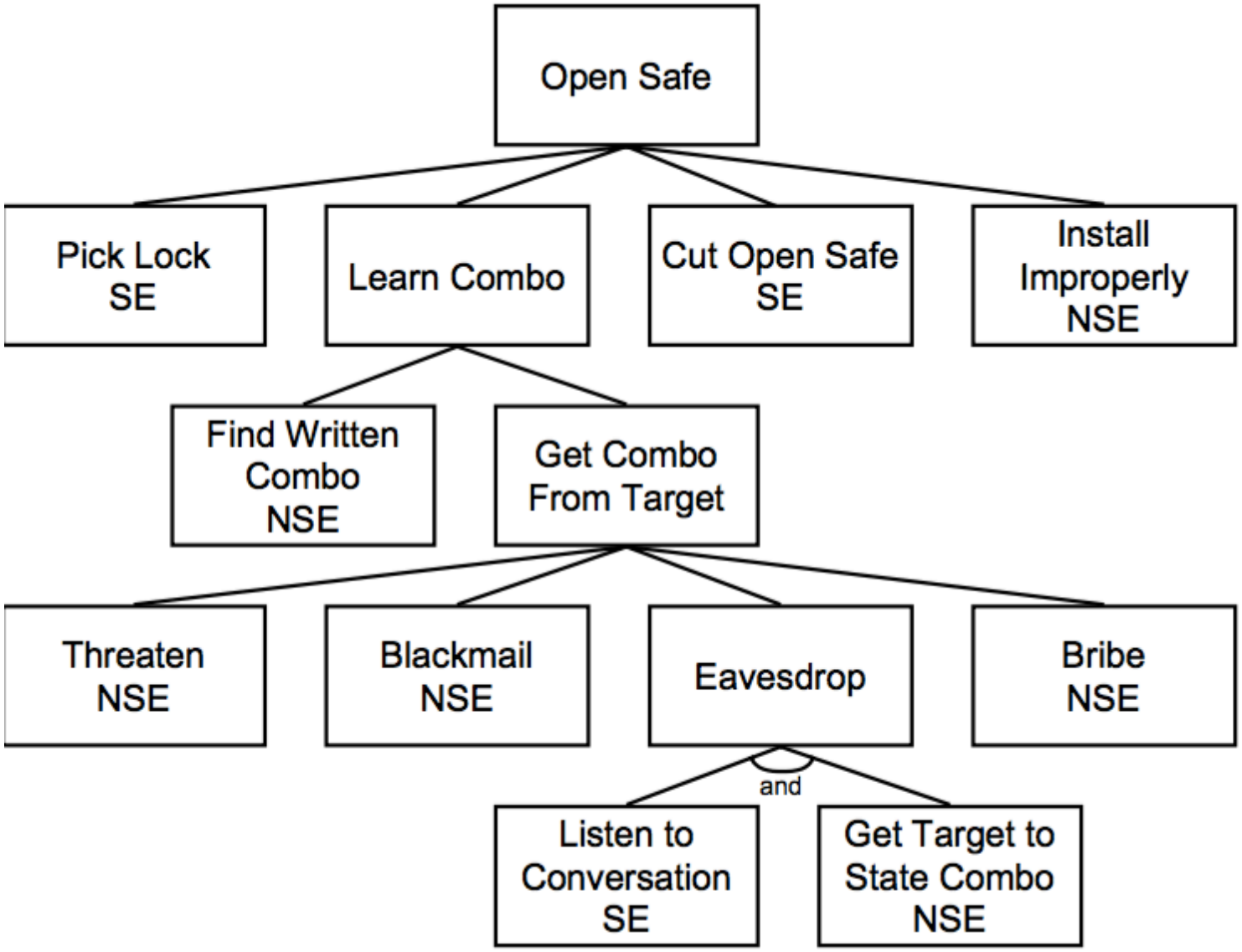


P = Possible
I = Impossible

How to use the tree: Then, these values can be propagated up the tree



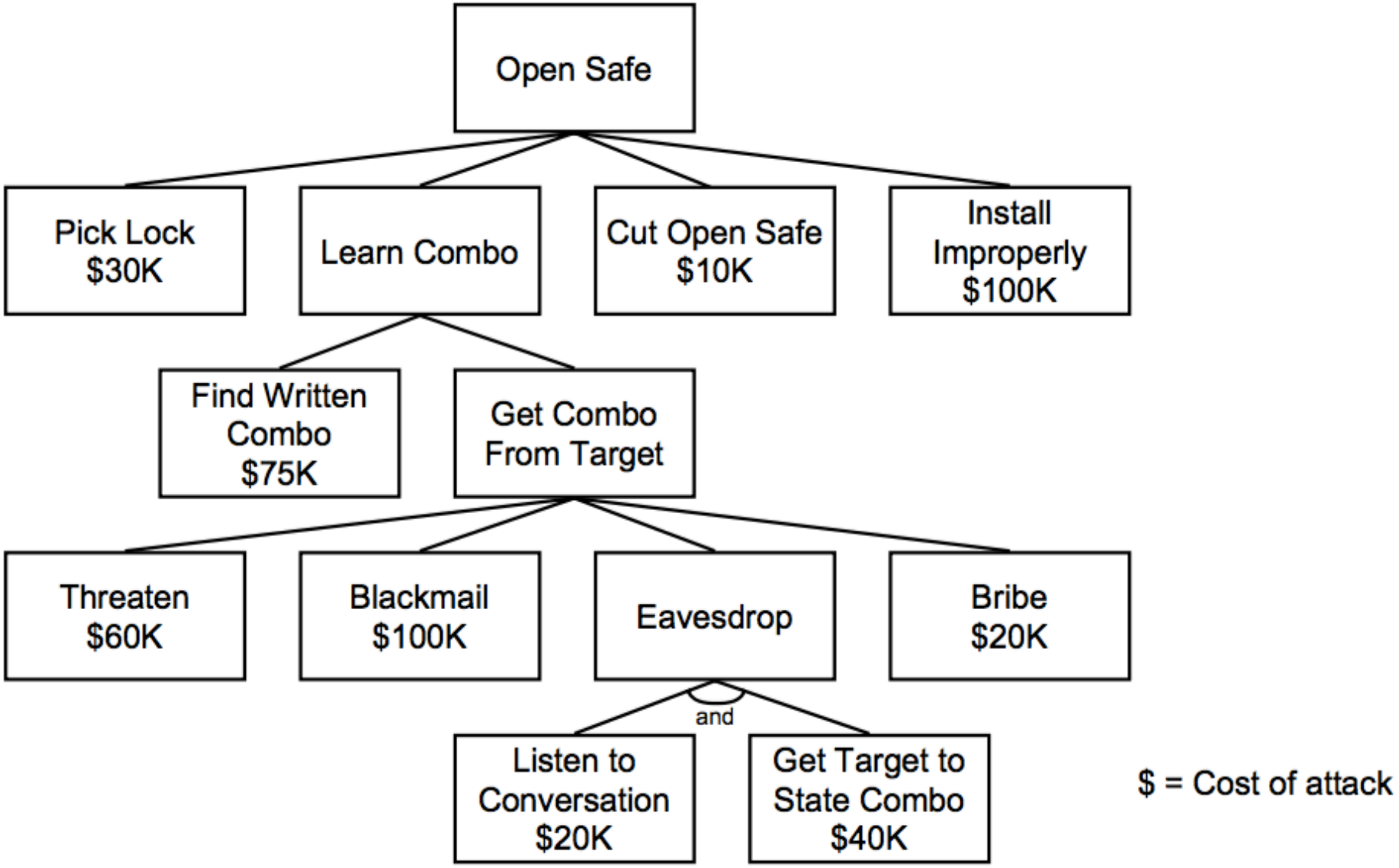
You can specify values that represent other different meanings



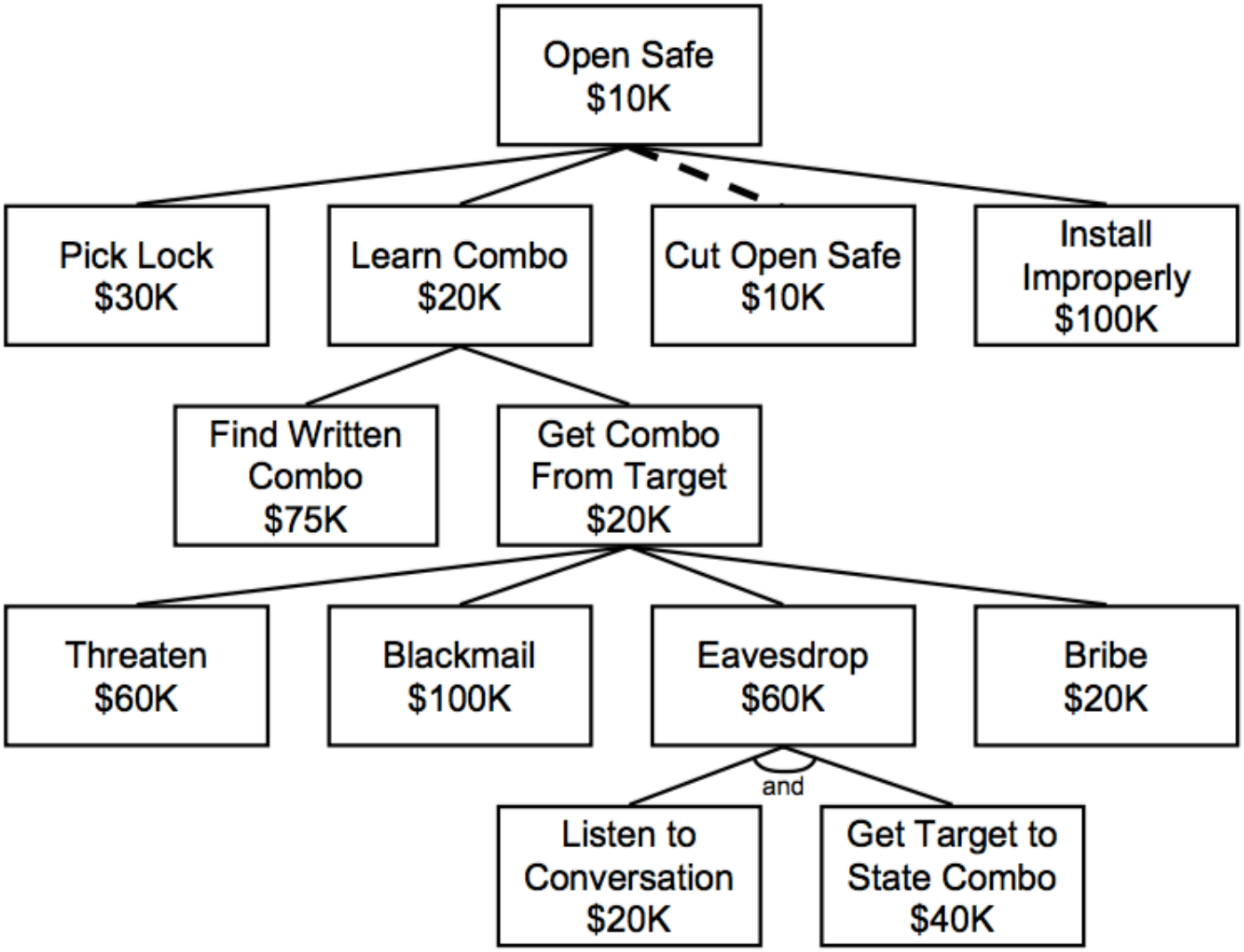
NSE = No special equipment

SE = Special equipment required

You can specify values that represent other different meanings



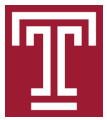
You can specify values that represent other different meanings



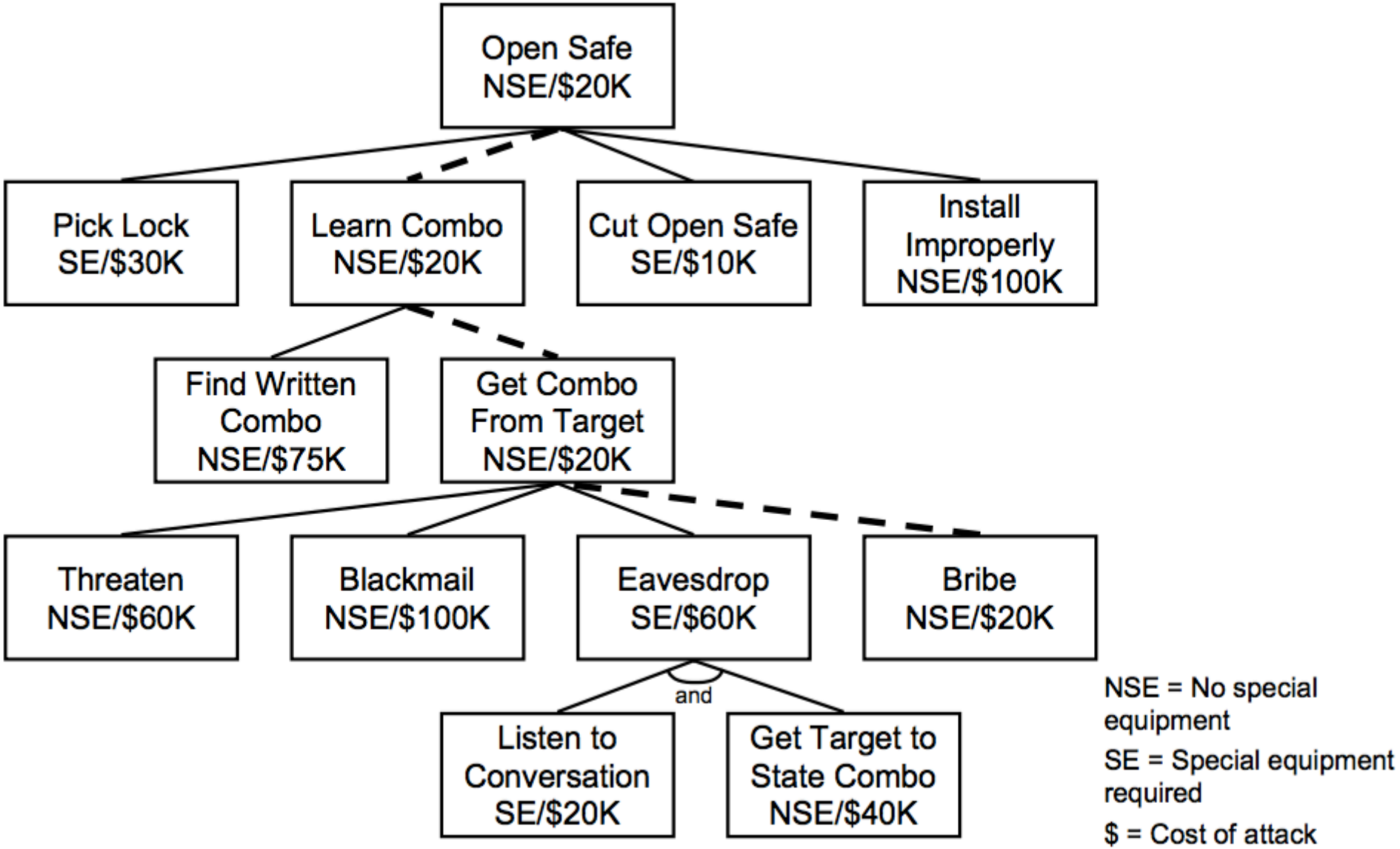
$ = Cost of attack

Combining Node Values

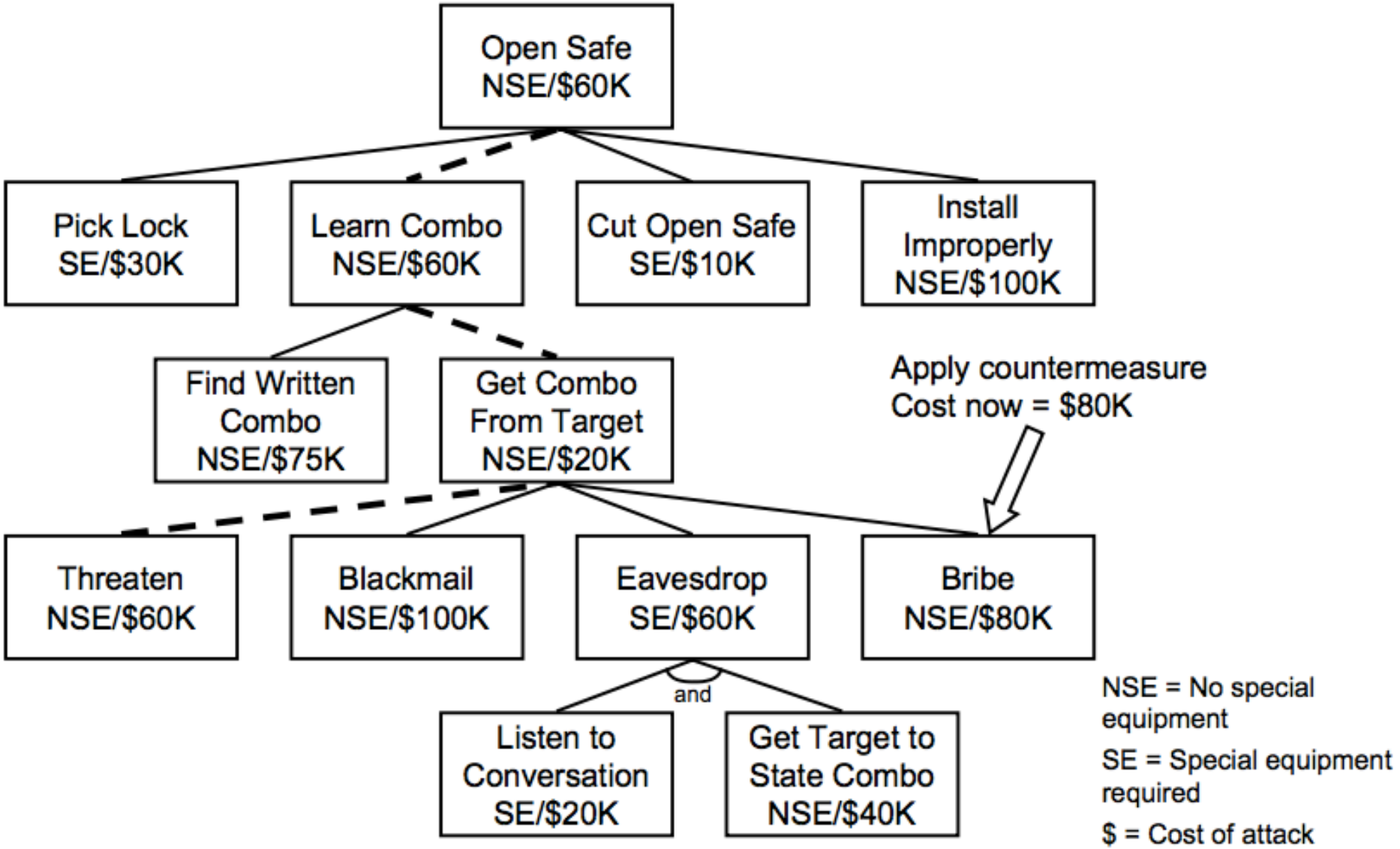
- Each node can have several values
- Can be used to make statements about attacks
- For example:
  - Cheapest low-risk attack
  - Most likely non-intrusive attack
  - Best low-skilled attack



Cheapest attack requiring no special equipment

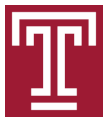


The tree changes when you apply countermeasures



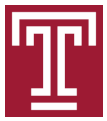
Using the Attack Tree to evaluate whether a security measure is worthwhile

- The analyst can check the difference of the cost of an attack before and after a security measure is applied



Summary

- Attack surface reduction
- Adversary model
- Three Big Steps in Security engineering
- Threat modeling
  - STRIDE
  - Attack trees



Writing Assignments

- What is the Attack Surface with regard to entering the SERC building illegally?
- Draw an Attack Tree representing the attack that tampers with the Temple library database