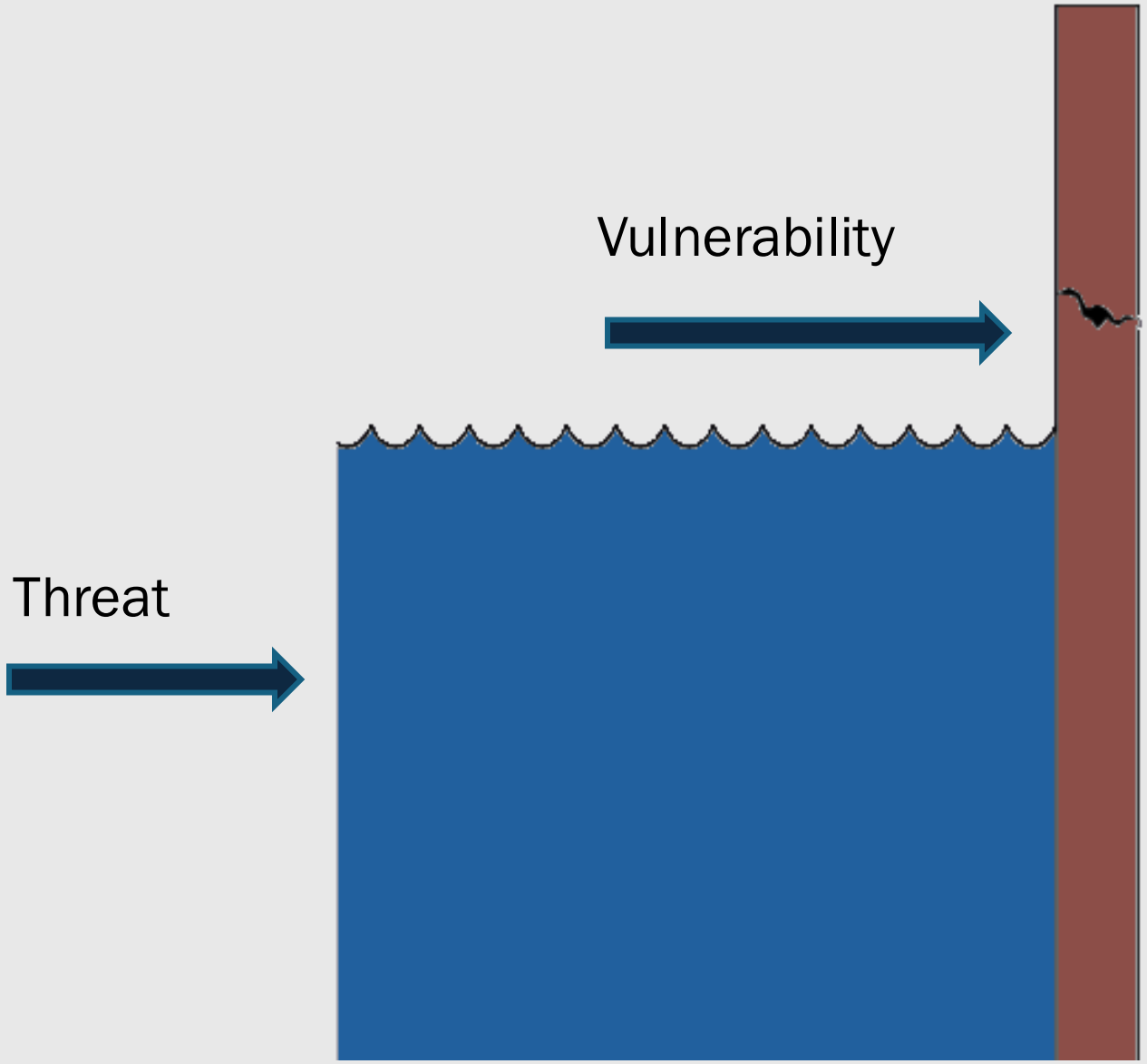
COMP435: *SECURITY CONCEPTS!*

Lecture 2: Intro to Threat Modeling

Please don’t sit in the back 4 rows ☺

THREATS, ATTACKS, AND COUNTERMEASURES



Potential Harm:

- getting wet
- drowning

From last time: Some terminology

- Harm: a violation of a desired security policy
  - Ex: getting wet or drowning
- Vulnerability: a weakness that could be exploited to cause harm
  - Ex: a crack in the wall
- Threat: a set of circumstances that could cause harm
  - Ex: Water that might overflow or cause the wall to collapse

ATTACKS

Attack

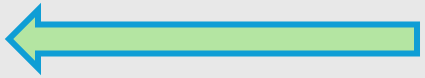
- Definition: deliberate actions taken to exploit a vulnerability and cause harm
- E.g., a person waits until the house is empty and the door is left open, and then walks in.

Attack Terminology

- Attack
- Attack Surface
- Attack Vector
- Threat Agent
- Adversary
- Attacker

Attack Terminology

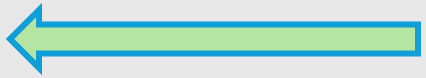
- ***Attack***
- Attack Surface
- Attack Vector
- Threat Agent
- Adversary
- Attacker



Def: deliberate actions taken to exploit vulnerabilities and cause harm

Attack Terminology

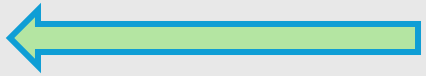
- Attack
- ***Attack Surface***
- Attack Vector
- Threat Agent
- Adversary
- Attacker



Def: the reachable and exploitable vulnerabilities in a system

Attack Terminology

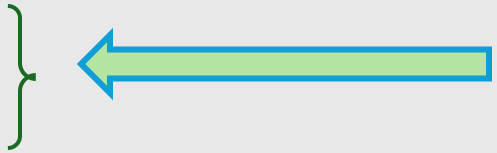
- Attack
- Attack Surface
- ***Attack Vector***
- Threat Agent
- Adversary
- Attacker



Def: specific sequence of steps by which attacks are carried out

Attack Terminology

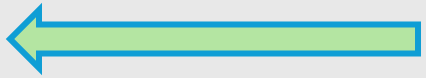
- Attack
- Attack Surface
- Attack Vector
- ***Threat Agent***
- ***Adversary***
- Attacker



Def: source of the threat; entity that might attack

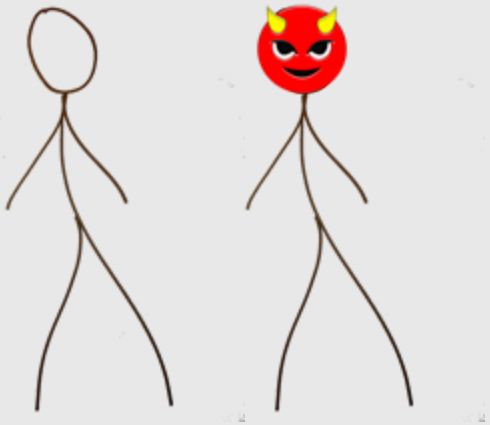
Attack Terminology

- Attack
- Attack Surface
- Attack Vector
- Threat Agent
- Adversary
- ***Attacker***



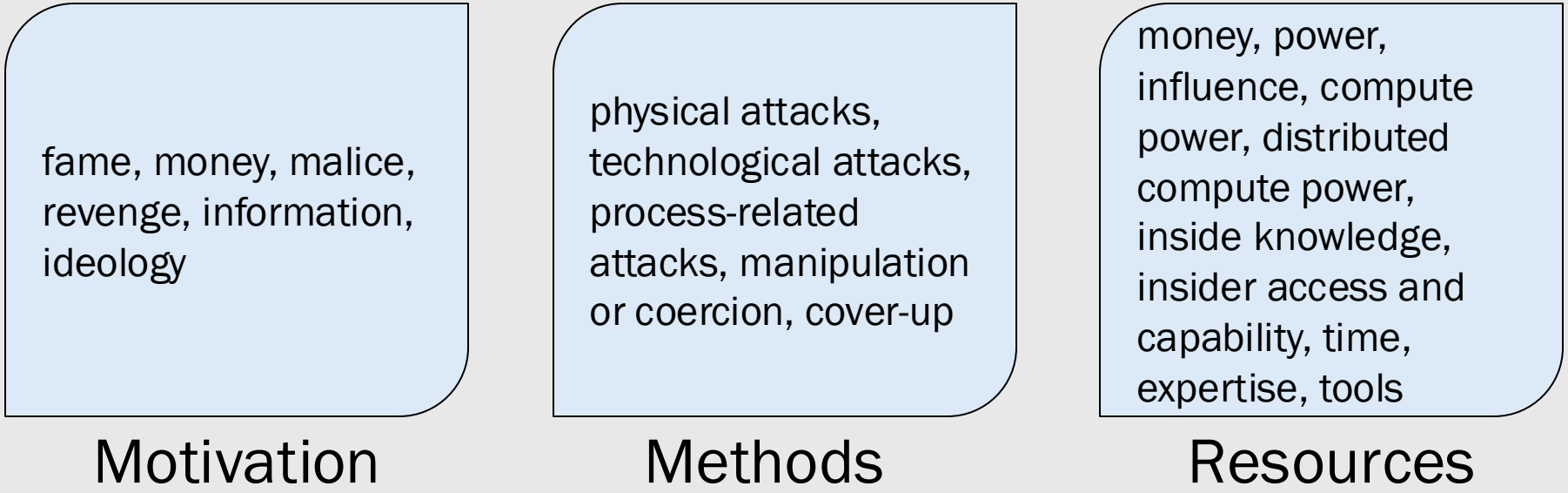
Def: an adversary who has actually attacked

THE ADVERSARY & THE VICTIM



Adversaries

- Informs what types of attacks we need to consider



Adversaries

- Individuals
- Organized crime
- Politically motivated groups
- Industrial competitors
- State-funded agencies
- Terrorists

Human Impact

- emotional
- financial
- physical
- personal data
- relationships
- societal well-being

CONTROLS & COUNTERMEASURES

Controls & Countermeasures

- Prevention vs. Detection
- Pre- vs. Post- Deployment
- Technical vs. Procedural vs. Physical

HOW?: protocols, access control, monitoring, security evaluation, penetration testing, auditing, logging

Policy:

- only family members and their guests may enter
- only family members can take objects out of the house

Adversary:

- motivation: steal money
- resources: knowledge of family schedule
- first attack: walk in open door

Assumptions:

Countermeasures

1. locks on doors
2.
3.
4.

New Attacks

1. opening a window
2.
3.
4.

Security is Challenging

- The attacker has the advantage
- There is a trade-off between security and usability
- Getting the policy right is difficult

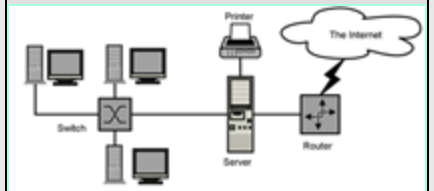
THREAT MODELING

Threat Model

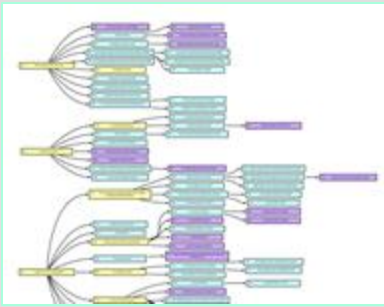
- Def: identifies the threats, adversaries, and attack vectors of a system
- I.e., what it is that we need to defend against.

Threat Modeling

Trees



Diagrams



Lists

- Spoofing
- Tampering
- Repudiation
- Information disclosure
- Denial of service
- Escalation of privilege

STRIDE

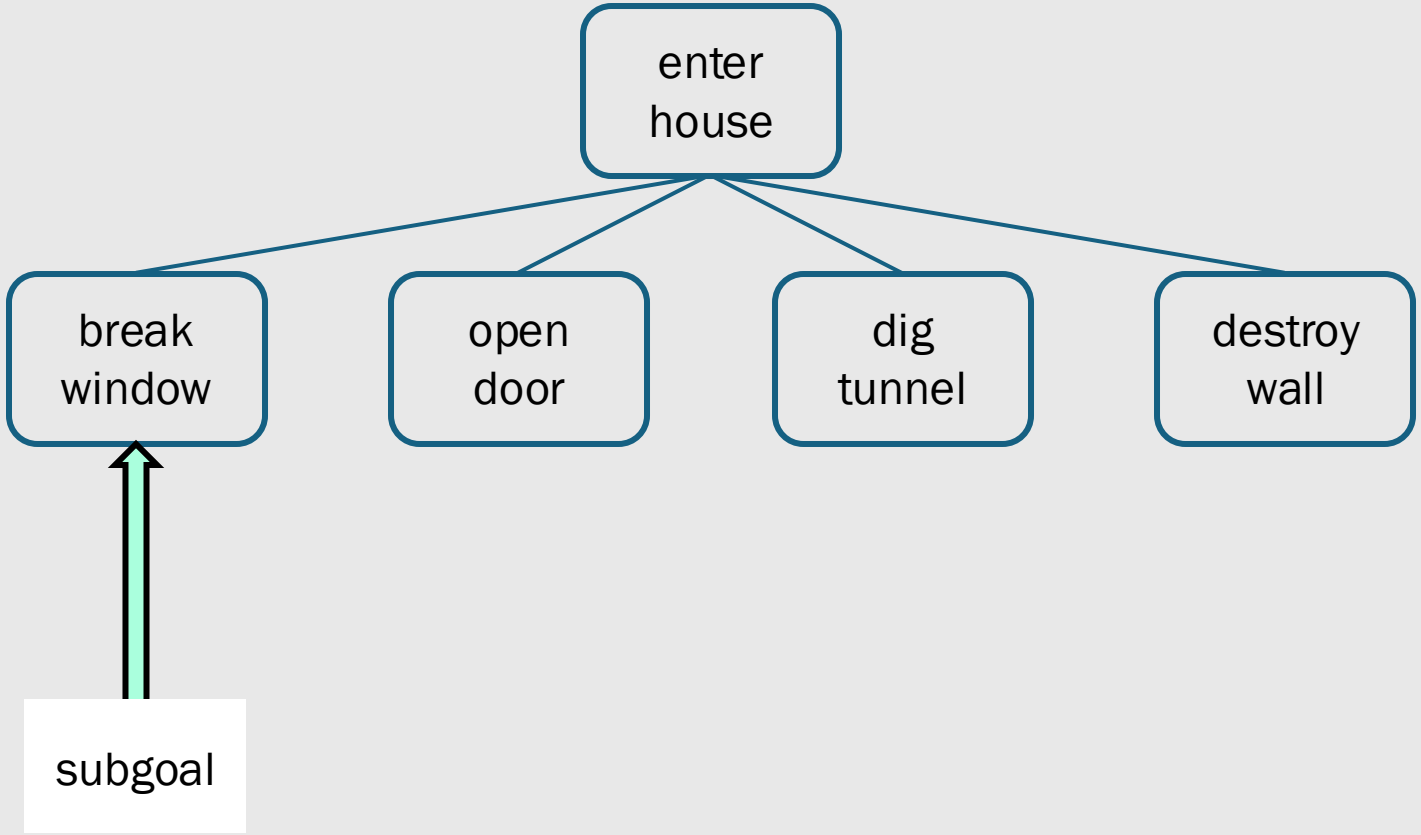
https://commons.wikimedia.org/wiki/File:Attack_tree_virus.png
https://en.wikipedia.org/wiki/File:Sample-network-diagram.png

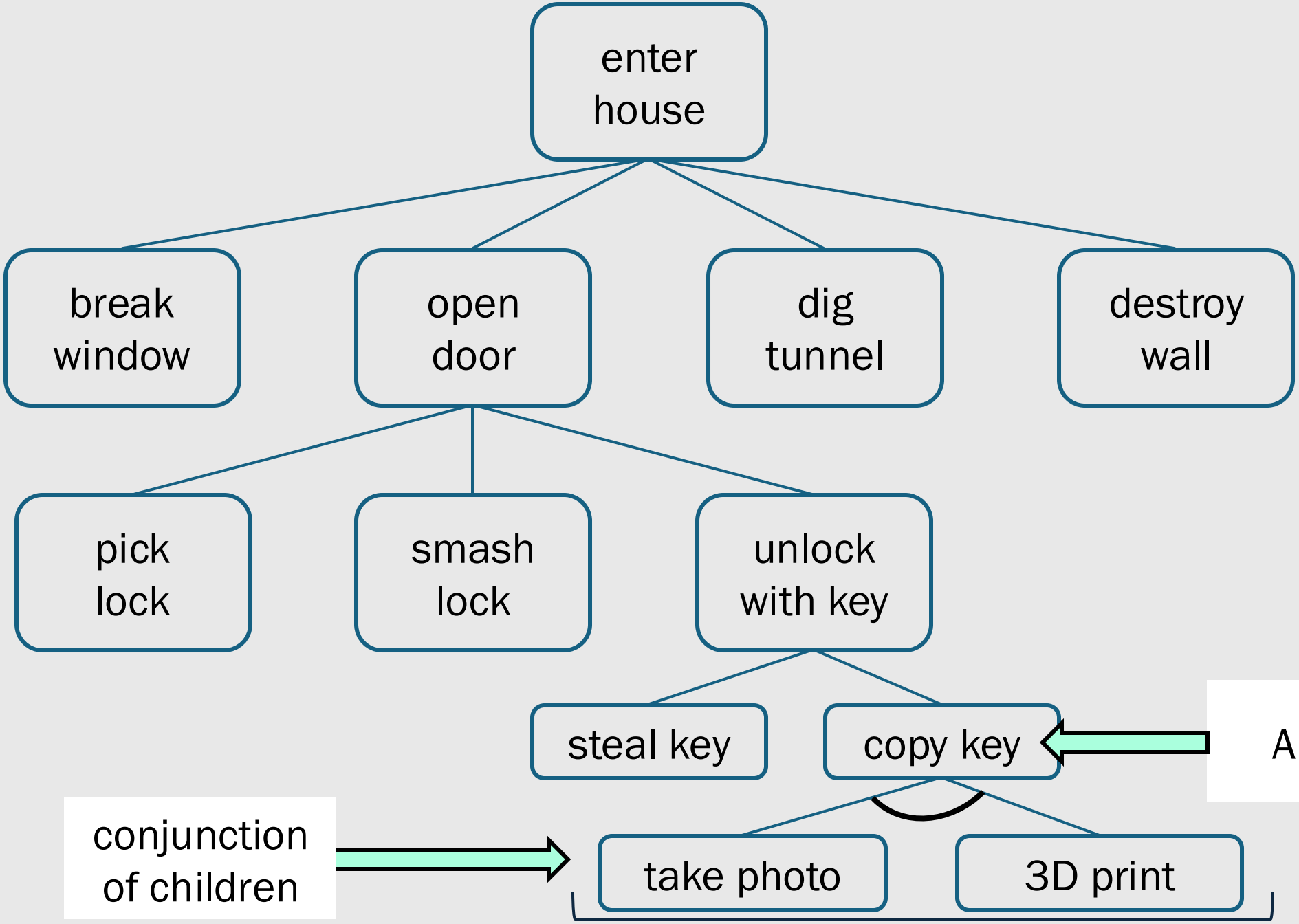
ATTACK TREES

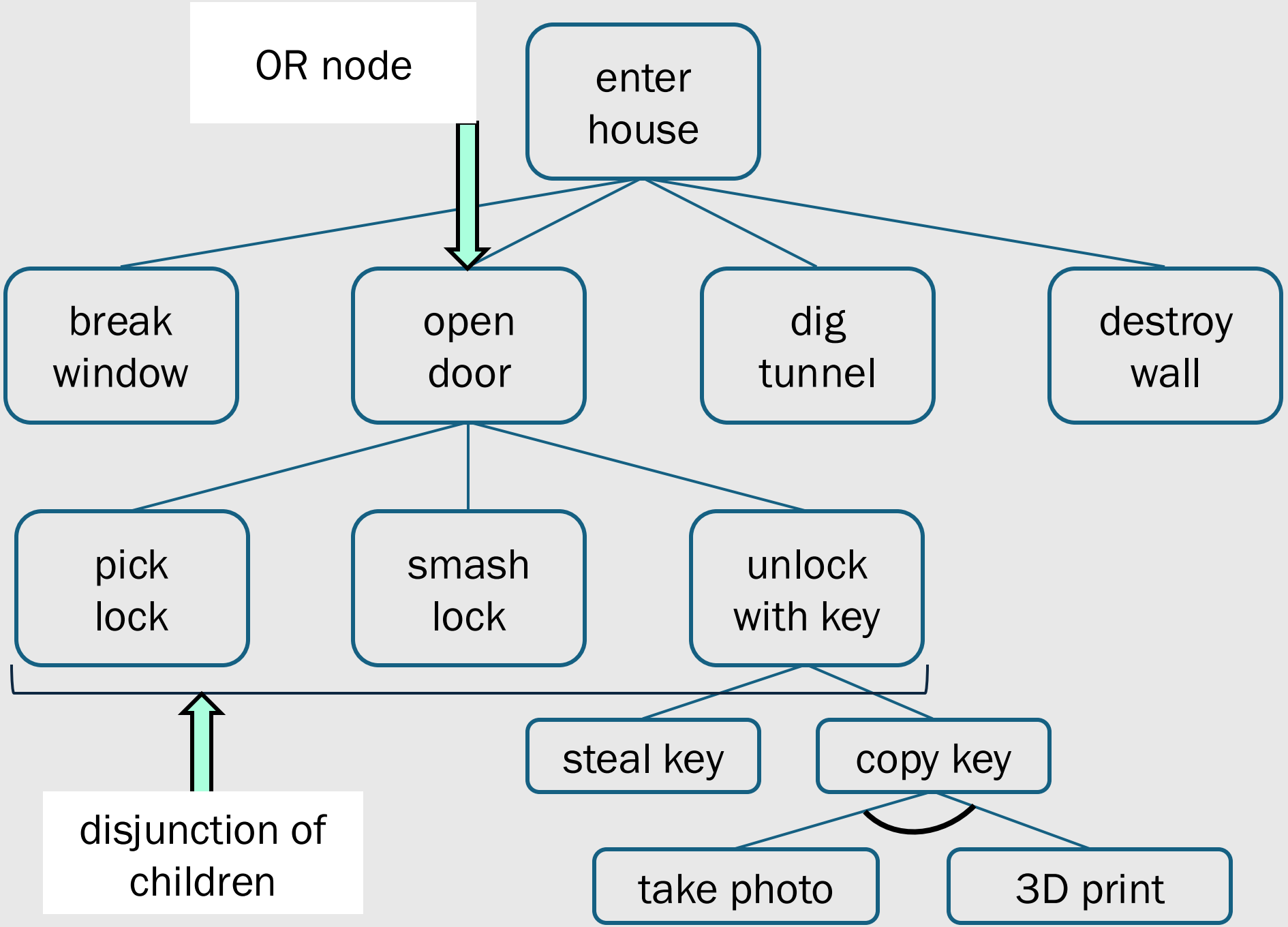
Bruce Schneier, “Attack Trees”
https://www.schneier.com/academic/archives/1999/12/attack_trees.html

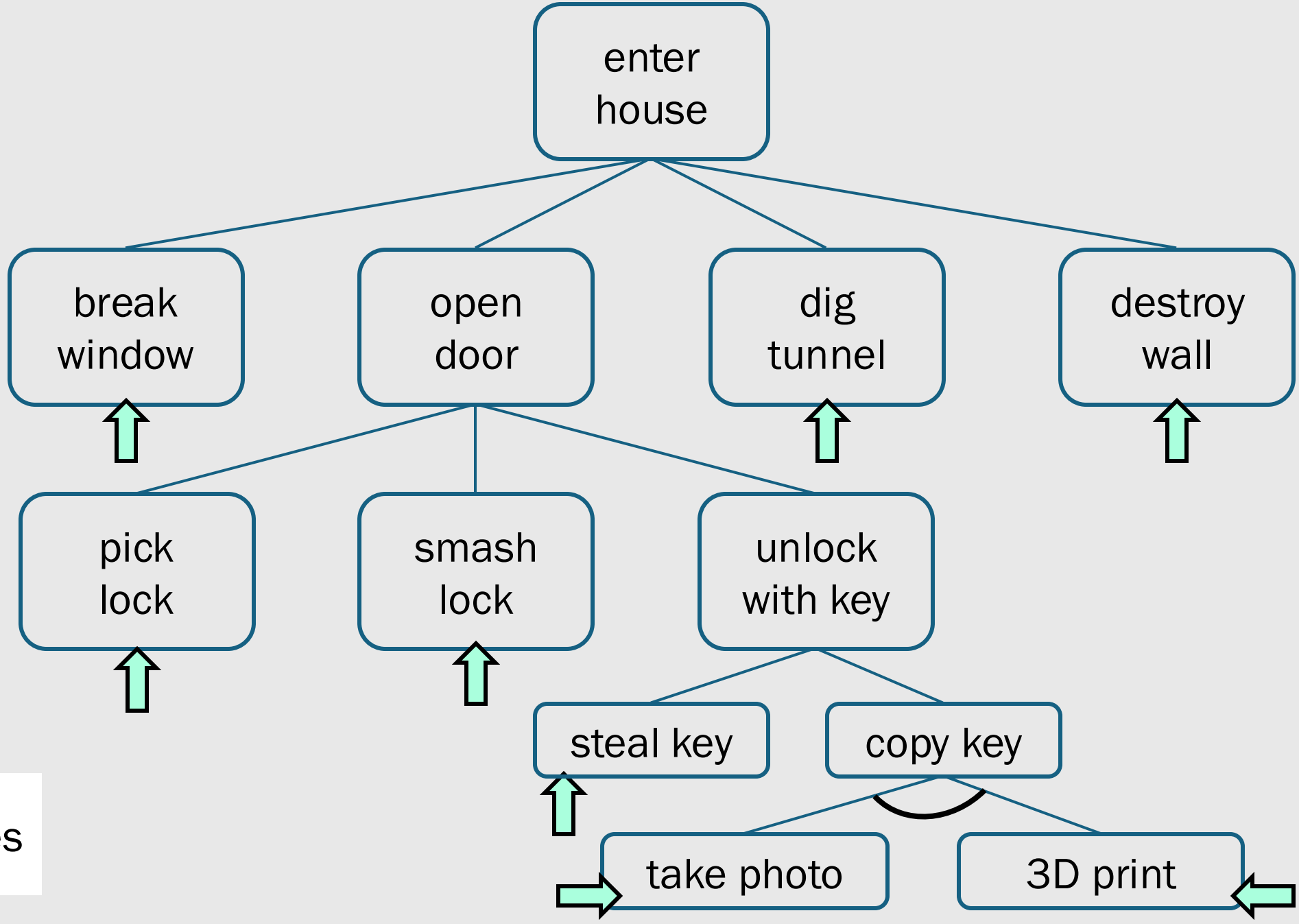
root node:
goal of attack

enter
house

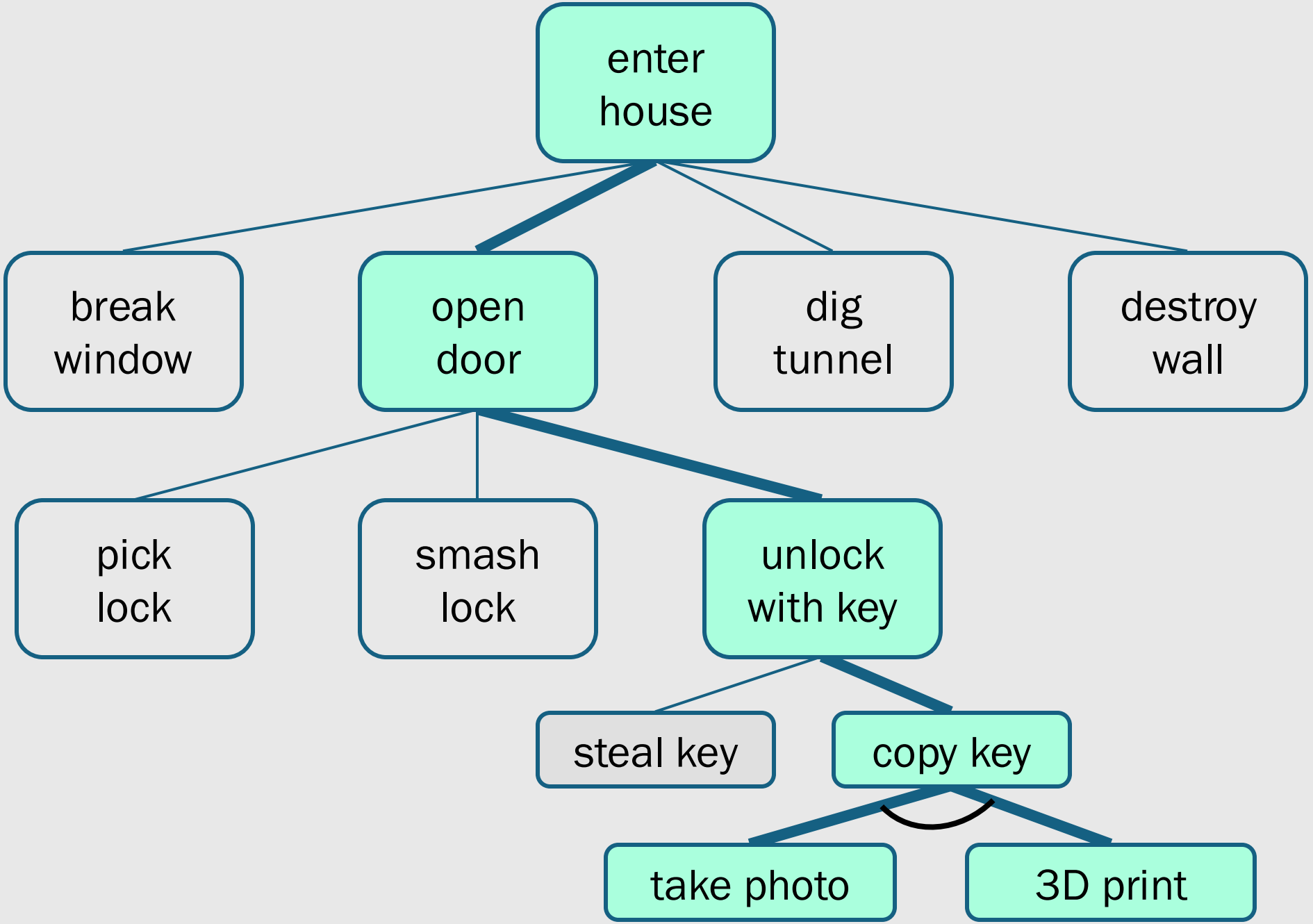

enter house
break window
open door
dig tunnel
destroy wall
subgoal

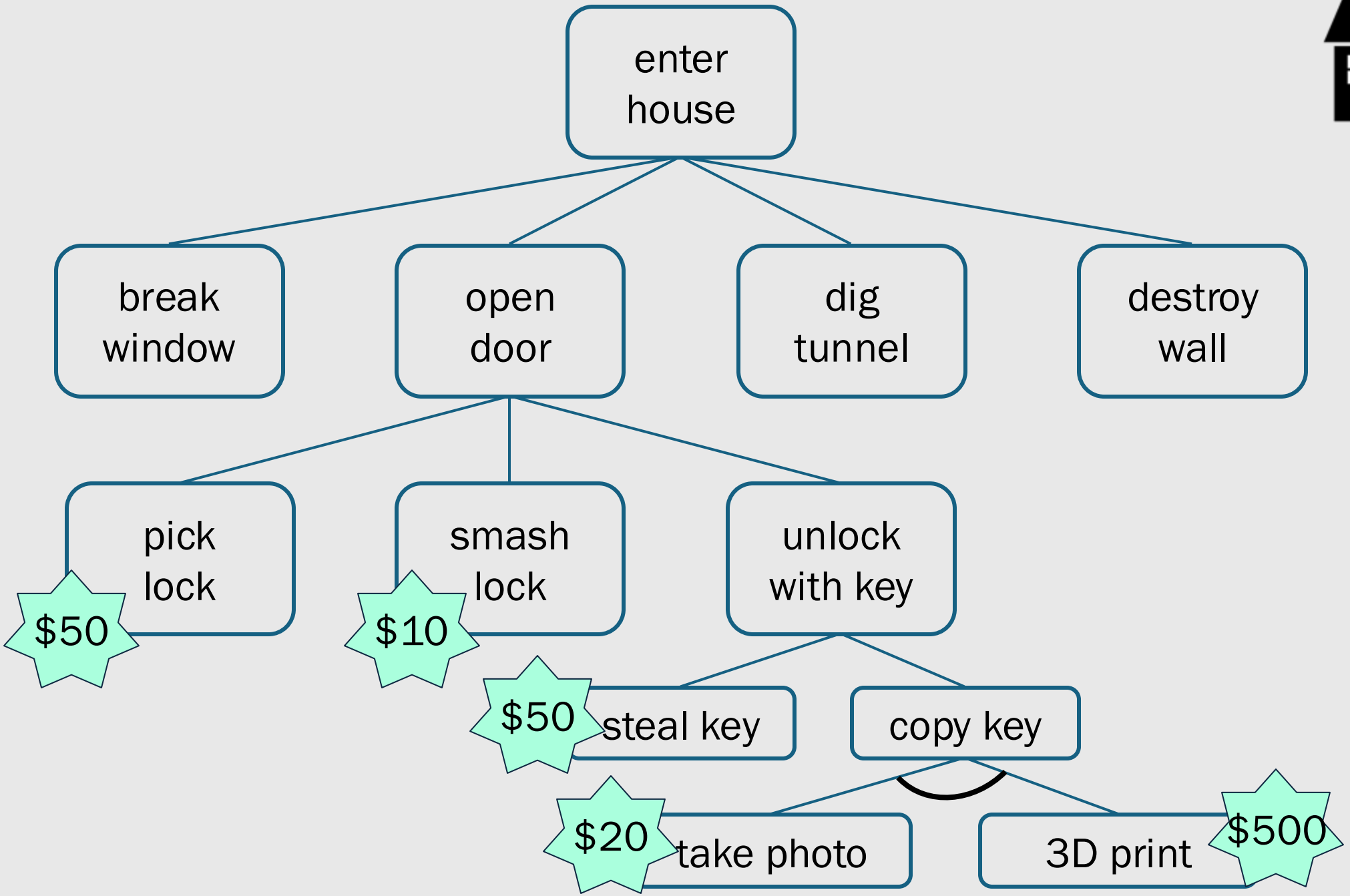

enter house
break window
open door
dig tunnel
destroy wall
pick lock
smash lock
unlock with key
steal key
copy key
AND node
conjunction of children
take photo
3D print

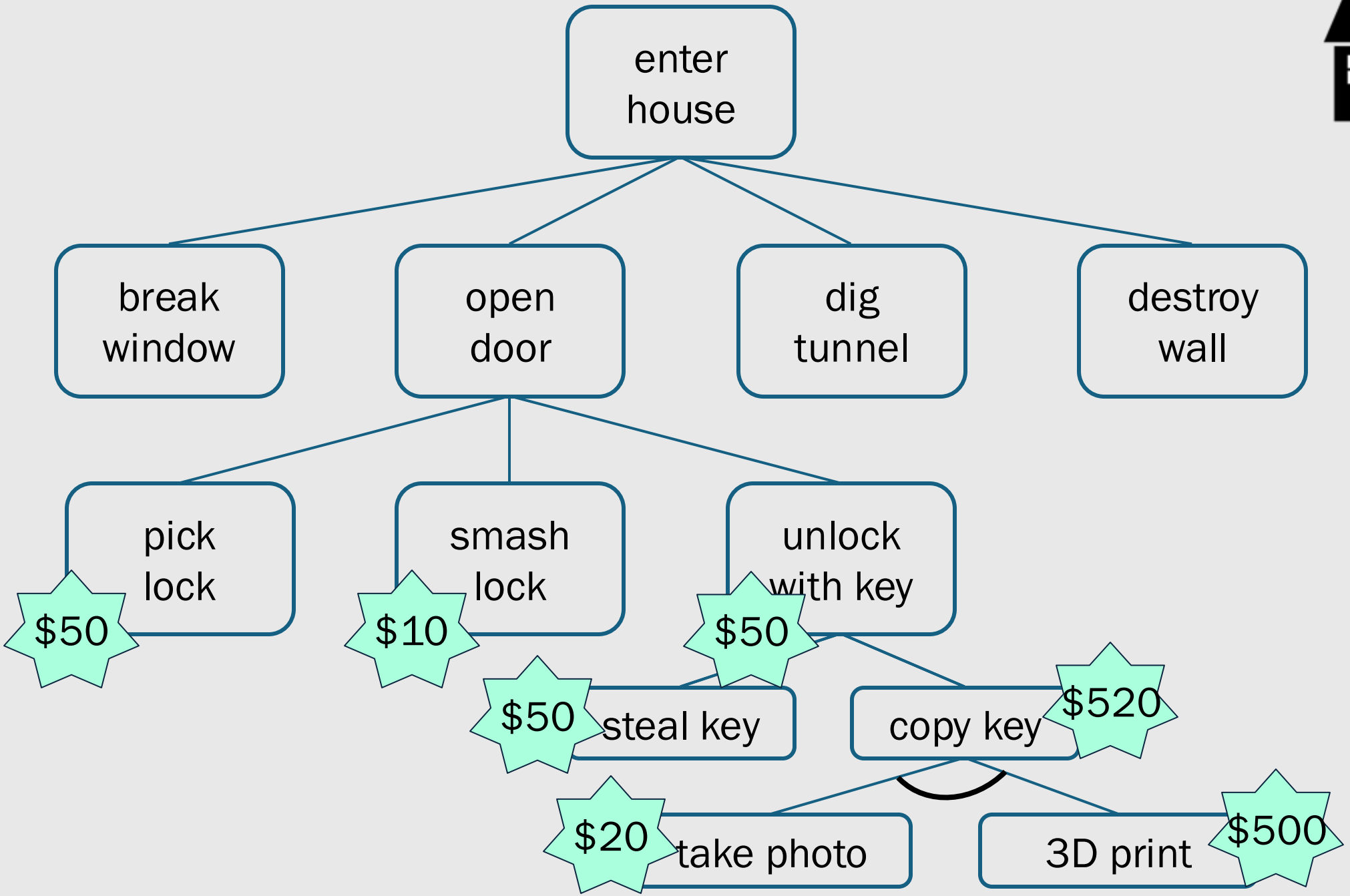

OR node
enter house
break window
open door
dig tunnel
destroy wall
pick lock
smash lock
unlock with key
steal key
copy key
take photo
3D print
disjunction of children

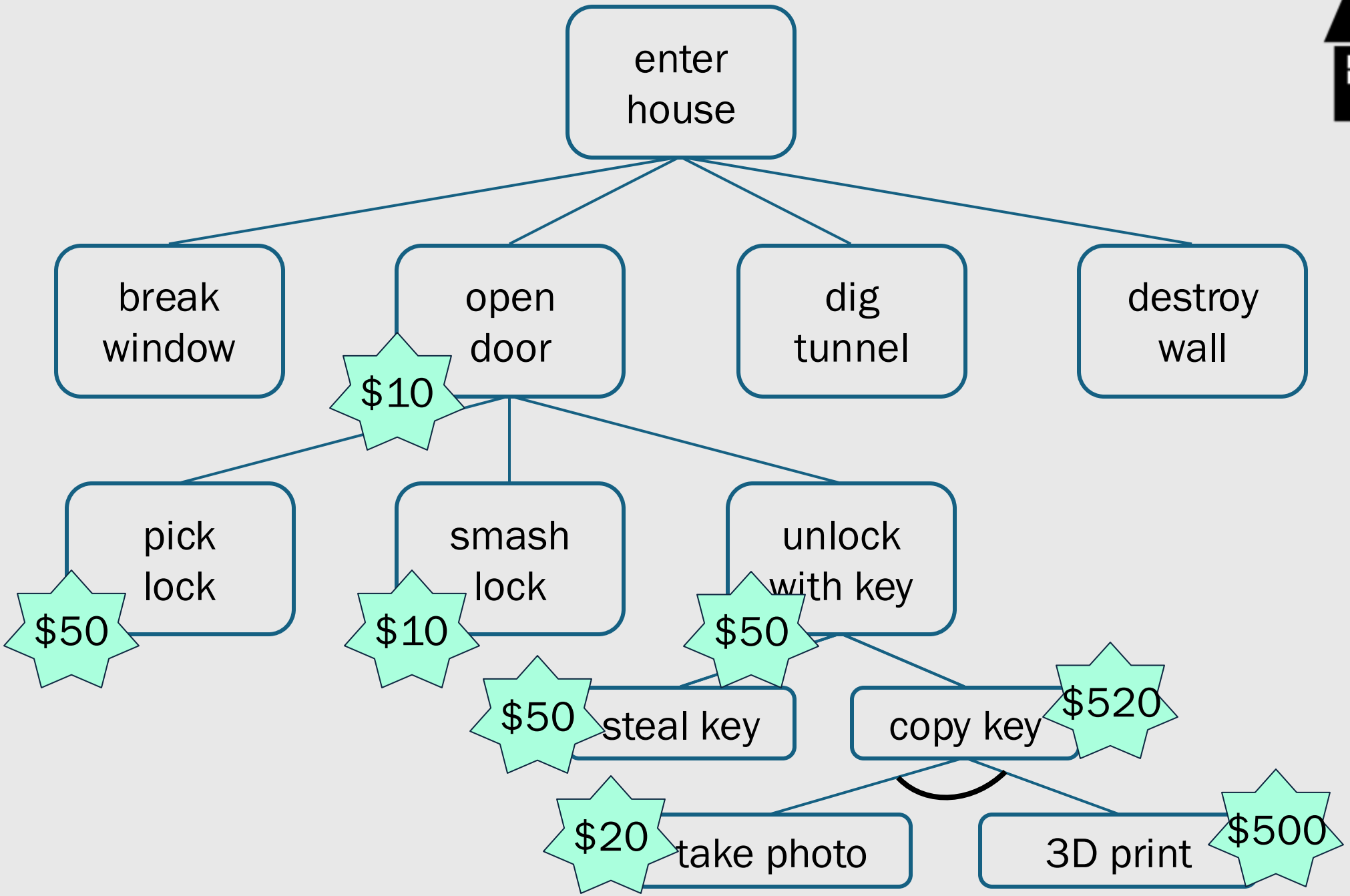

enter house
break window
open door
dig tunnel
destroy wall
pick lock
smash lock
unlock with key
steal key
copy key
take photo
3D print

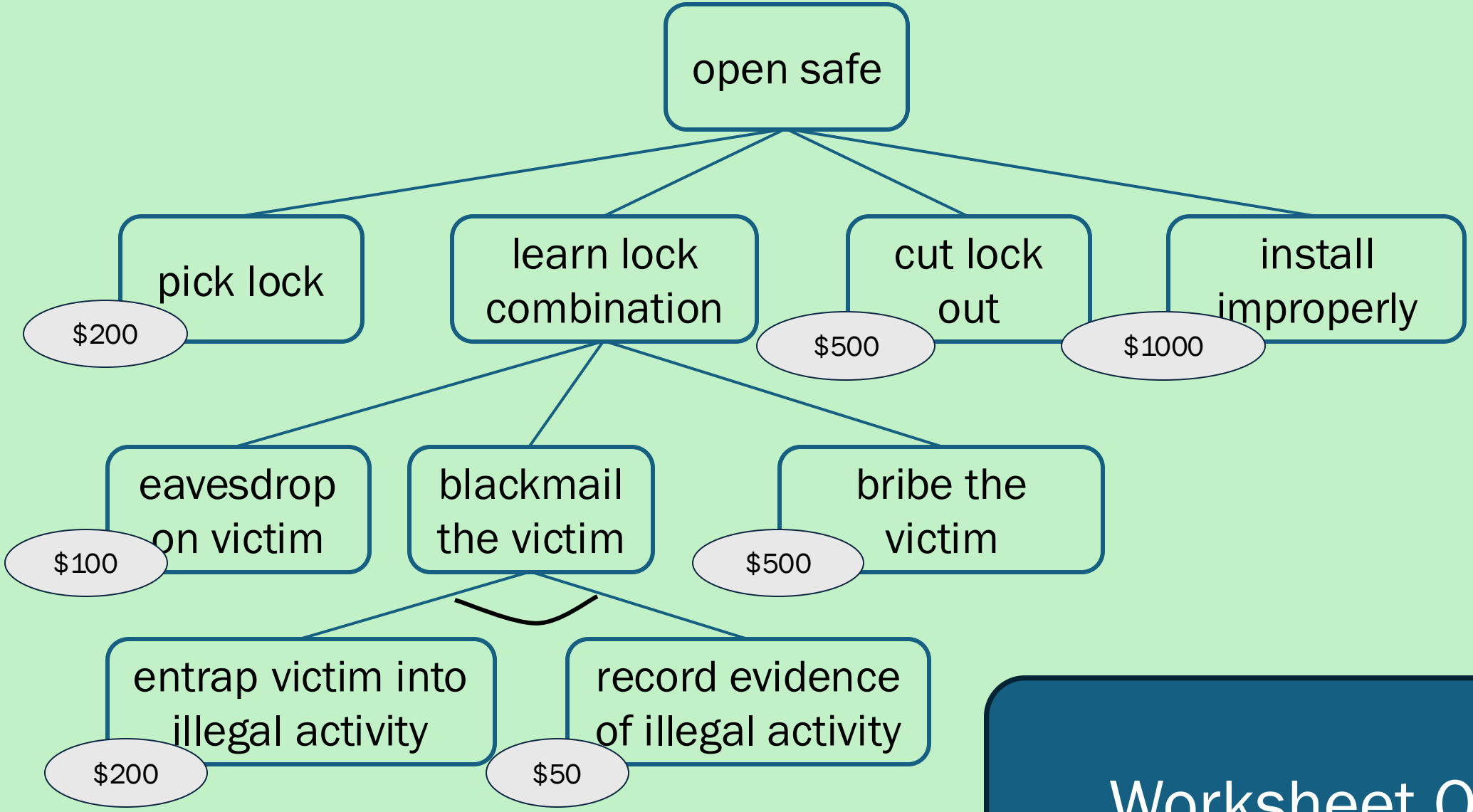
leaf nodes


enter house
break window
open door
dig tunnel
destroy wall
pick lock
smash lock
unlock with key
steal key
copy key
take photo
3D print


enter house
break window
open door
dig tunnel
destroy wall
pick lock
smash lock
unlock with key
$50
$10
$50
steal key
copy key
$20
take photo
3D print
$500

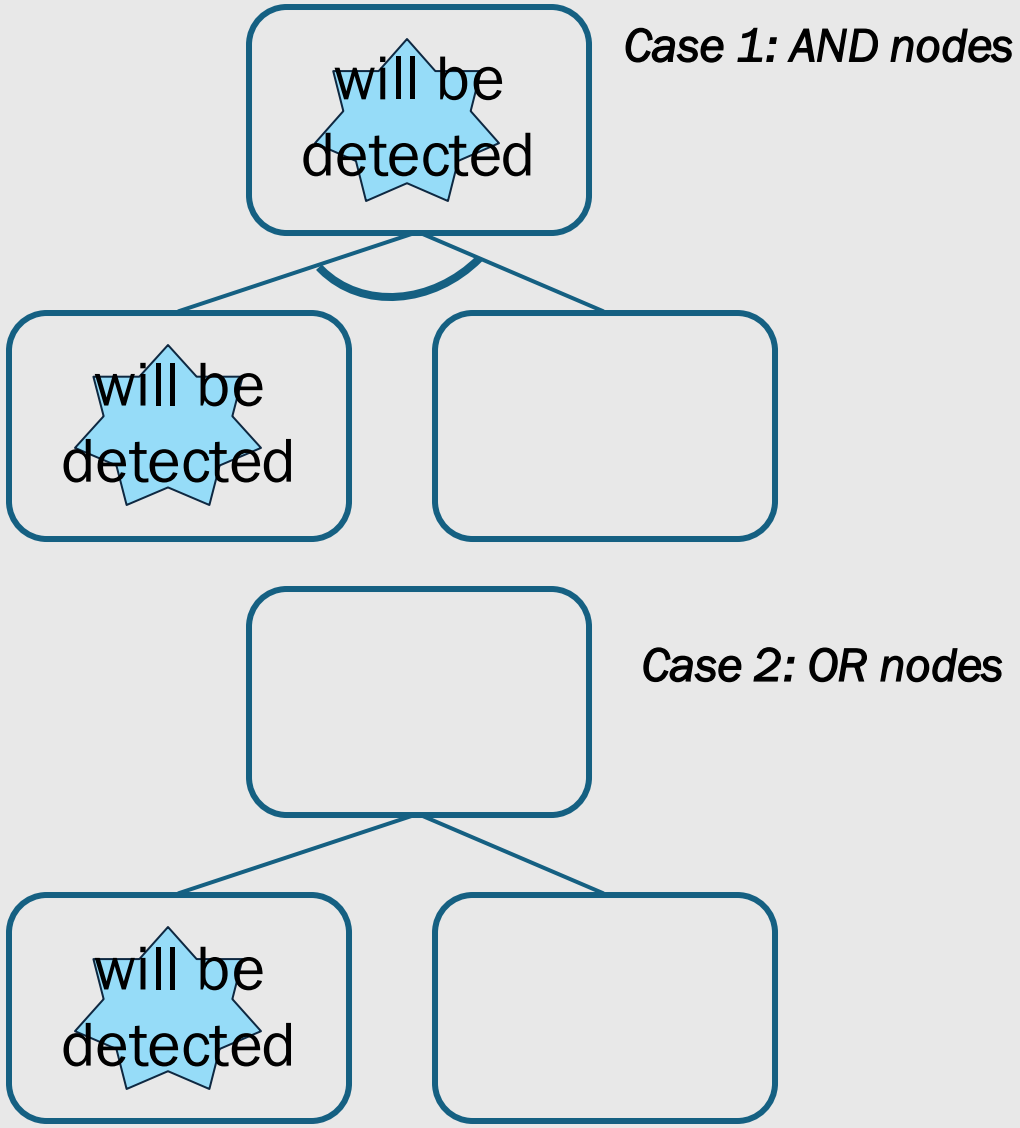

enter house
break window
open door
dig tunnel
destroy wall
pick lock
smash lock
unlock with key
$50
$10
$50
$50
steal key
copy key
$520
$20
take photo
3D print
$500


enter house
break window
open door
dig tunnel
destroy wall
$10
pick lock
smash lock
unlock with key
$50
$10
$50
$50
steal key
copy key
$520
$20
take photo
3D print
$500



Worksheet Q2!

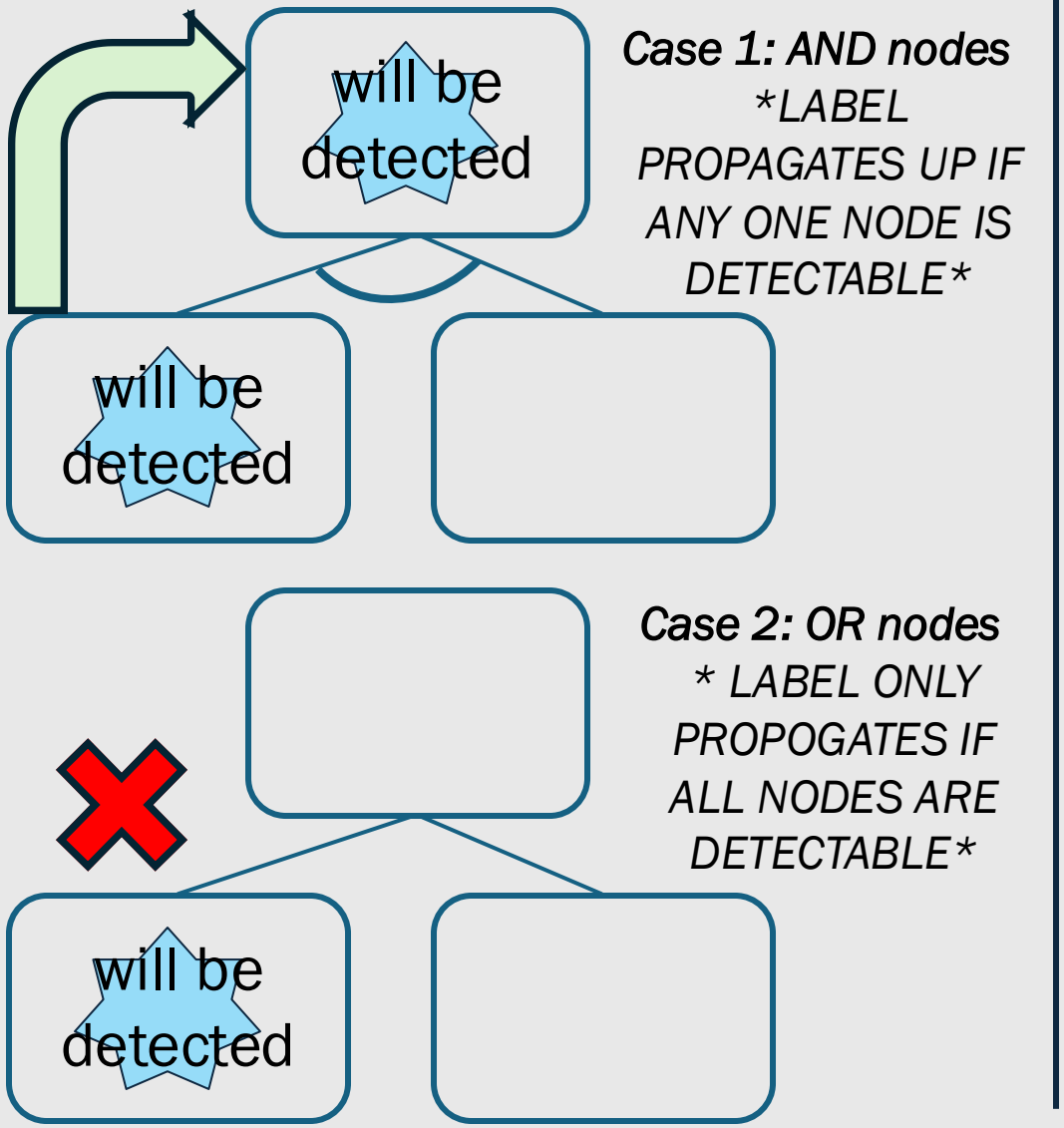
Will be detected?



Case 1: AND nodes

Case 2: OR nodes

Will be detected?



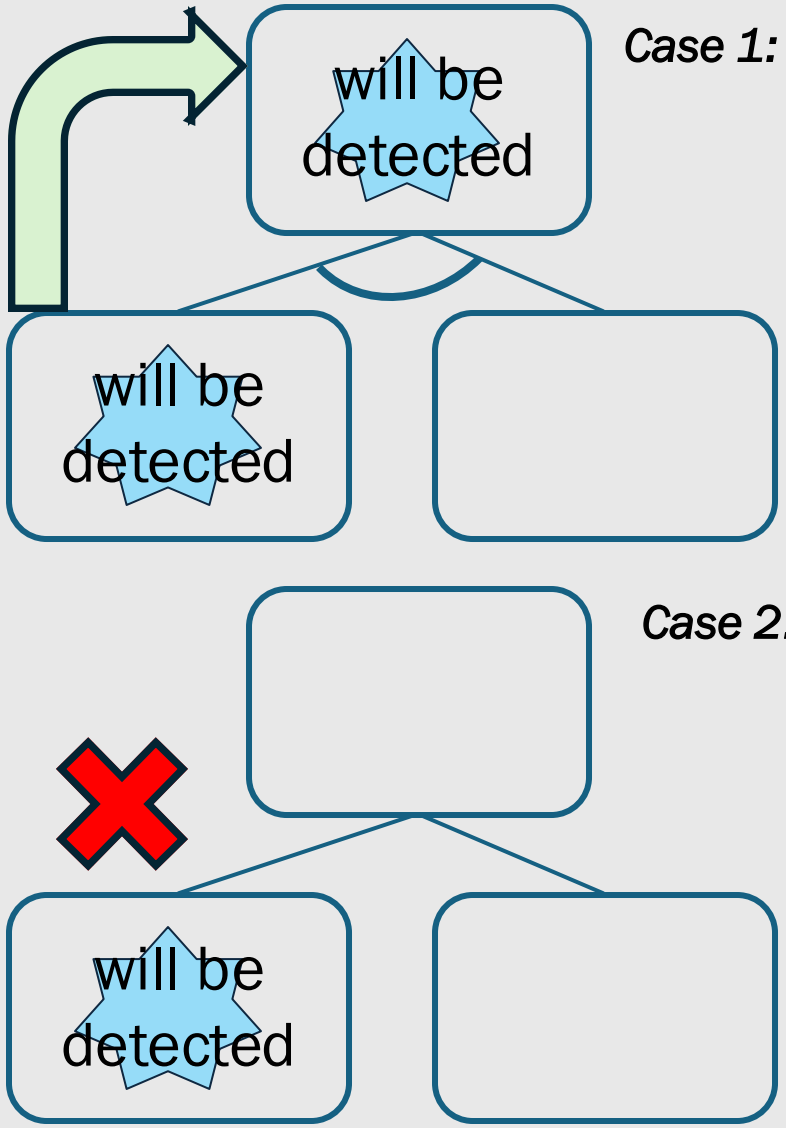
Case 1: AND nodes

LABEL PROPAGATES UP IF ANY ONE NODE IS DETECTABLE

Case 2: OR nodes

** LABEL ONLY PROPOGATES IF ALL NODES ARE DETECTABLE**

Will be detected?

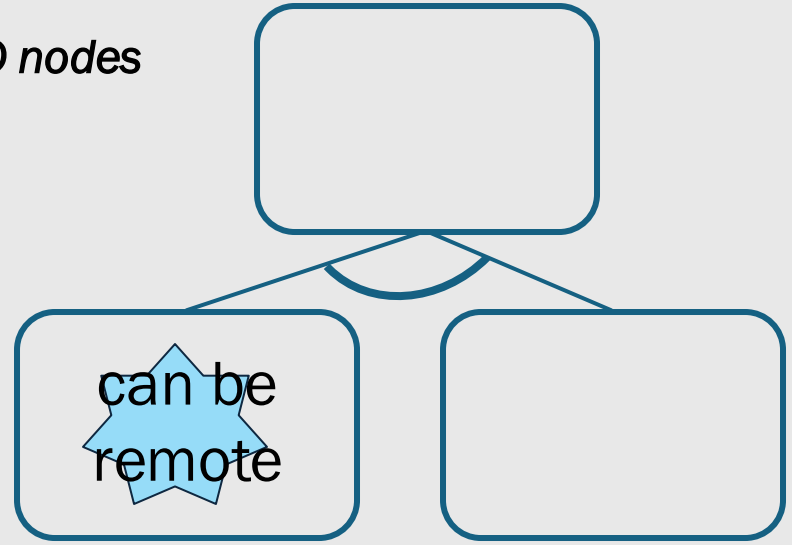


Case 1: AND nodes

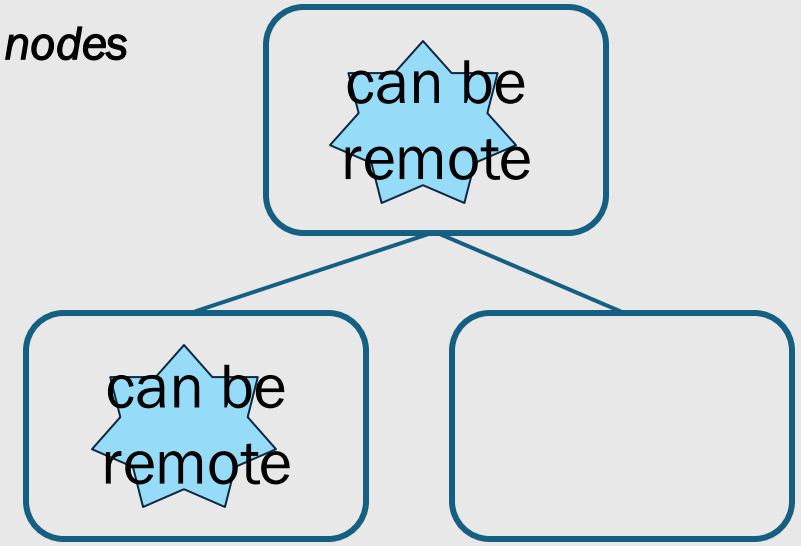
Case 2: OR nodes

Can be launched remotely?

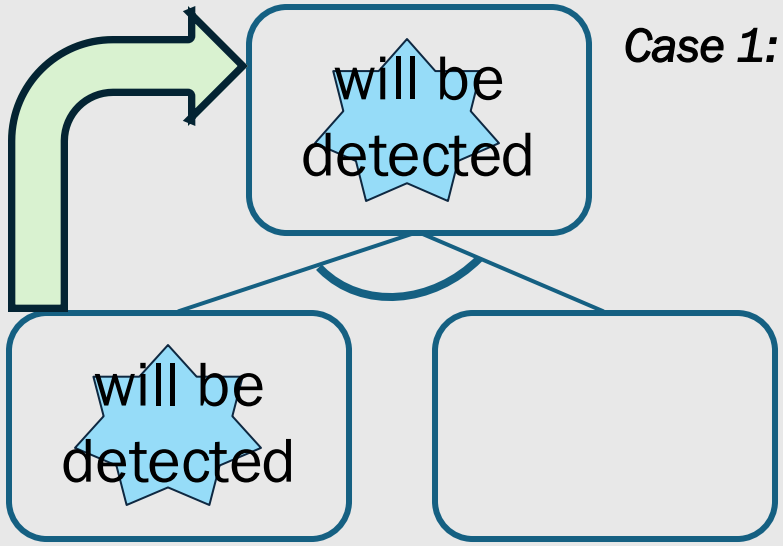
Case 1: AND nodes



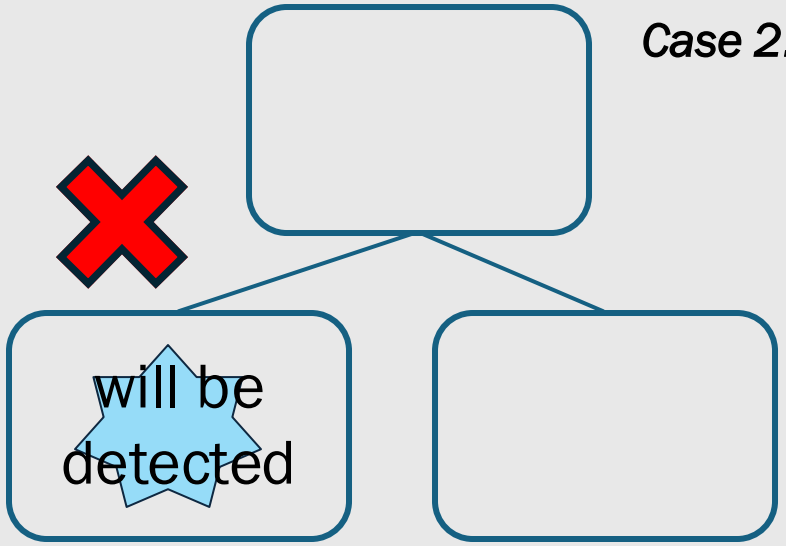
Case 2: OR nodes



Will be detected?



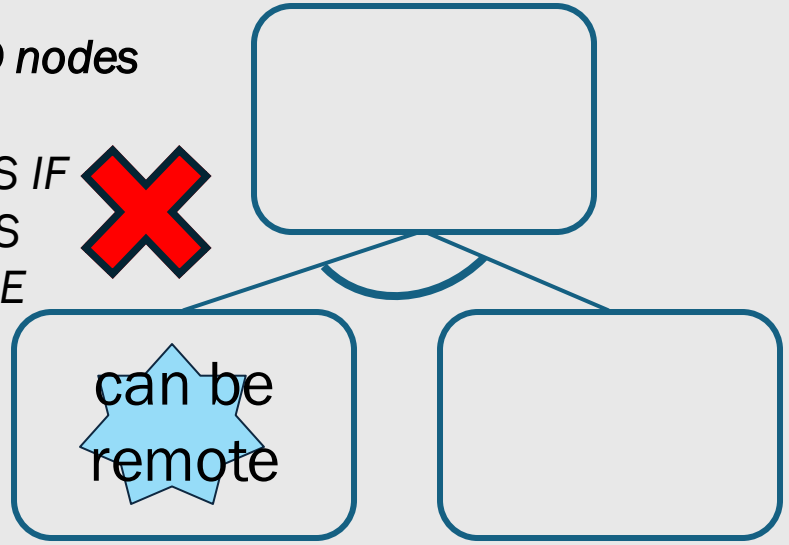
Case 1: AND nodes



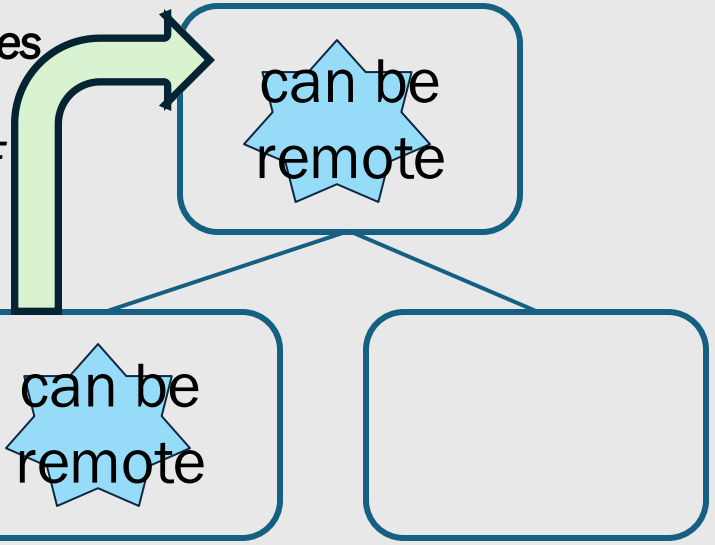
Case 2: OR nodes

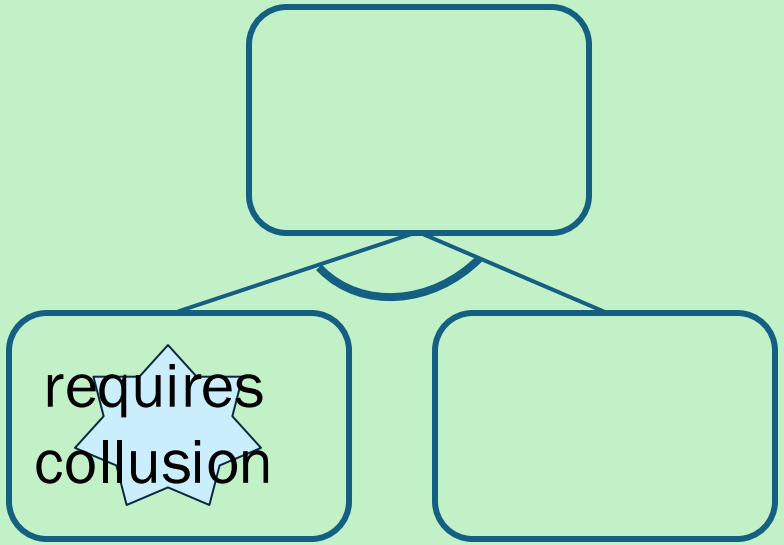
Can be launched remotely?

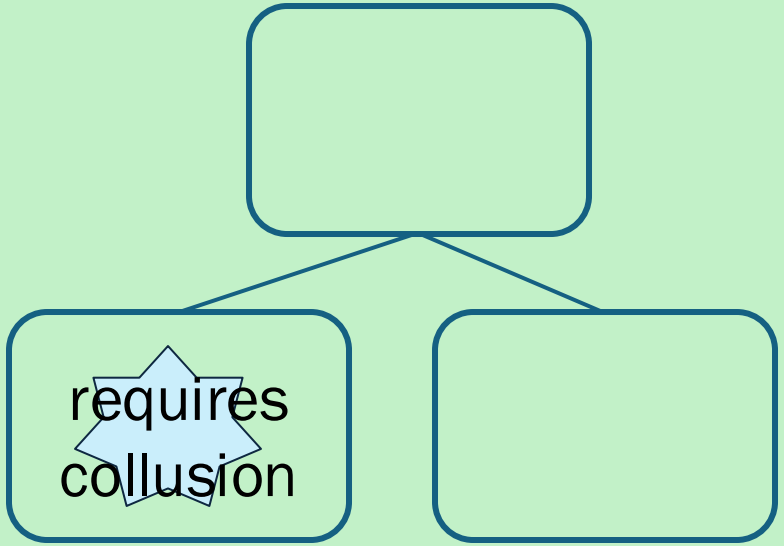
Case 1: AND nodes
LABEL PROPAGATES IF BOTH NODES LAUNCHABLE REMOTELY



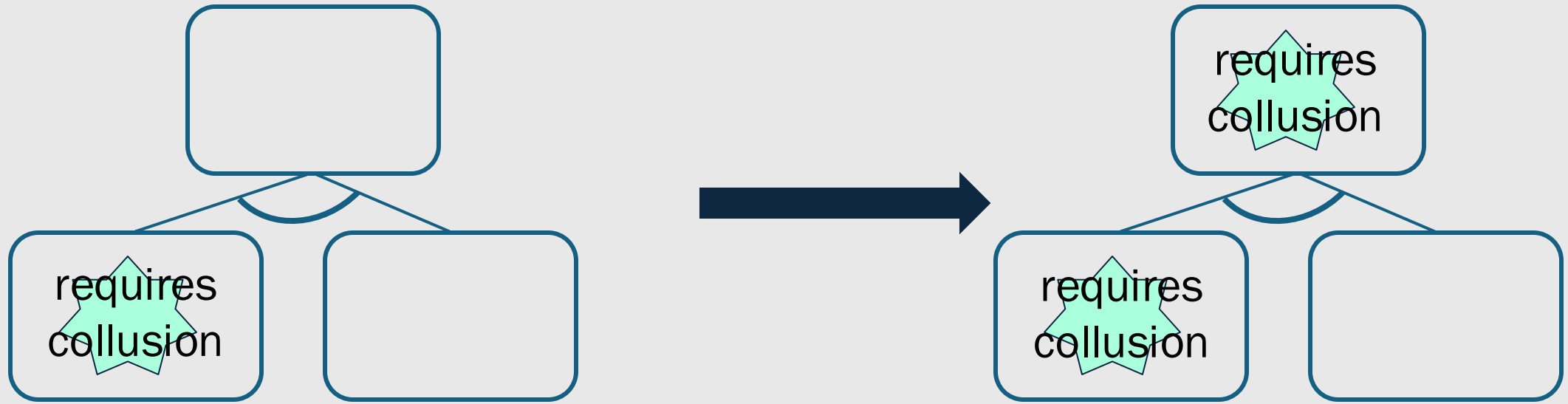
Case 2: OR nodes
** LABEL PROPOGATES IF ANY NODE LAUNCHABLE**

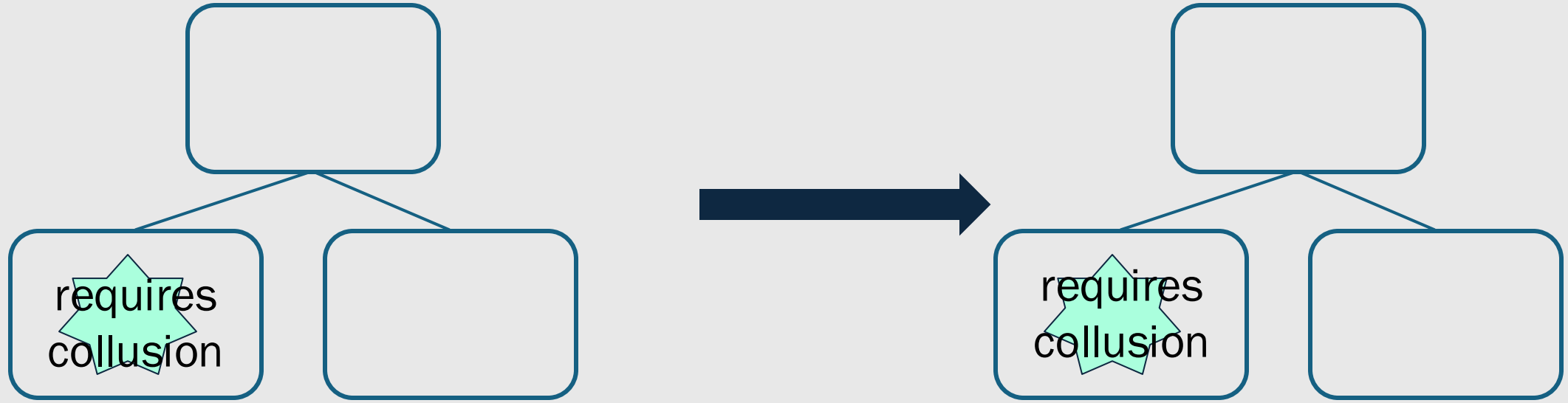


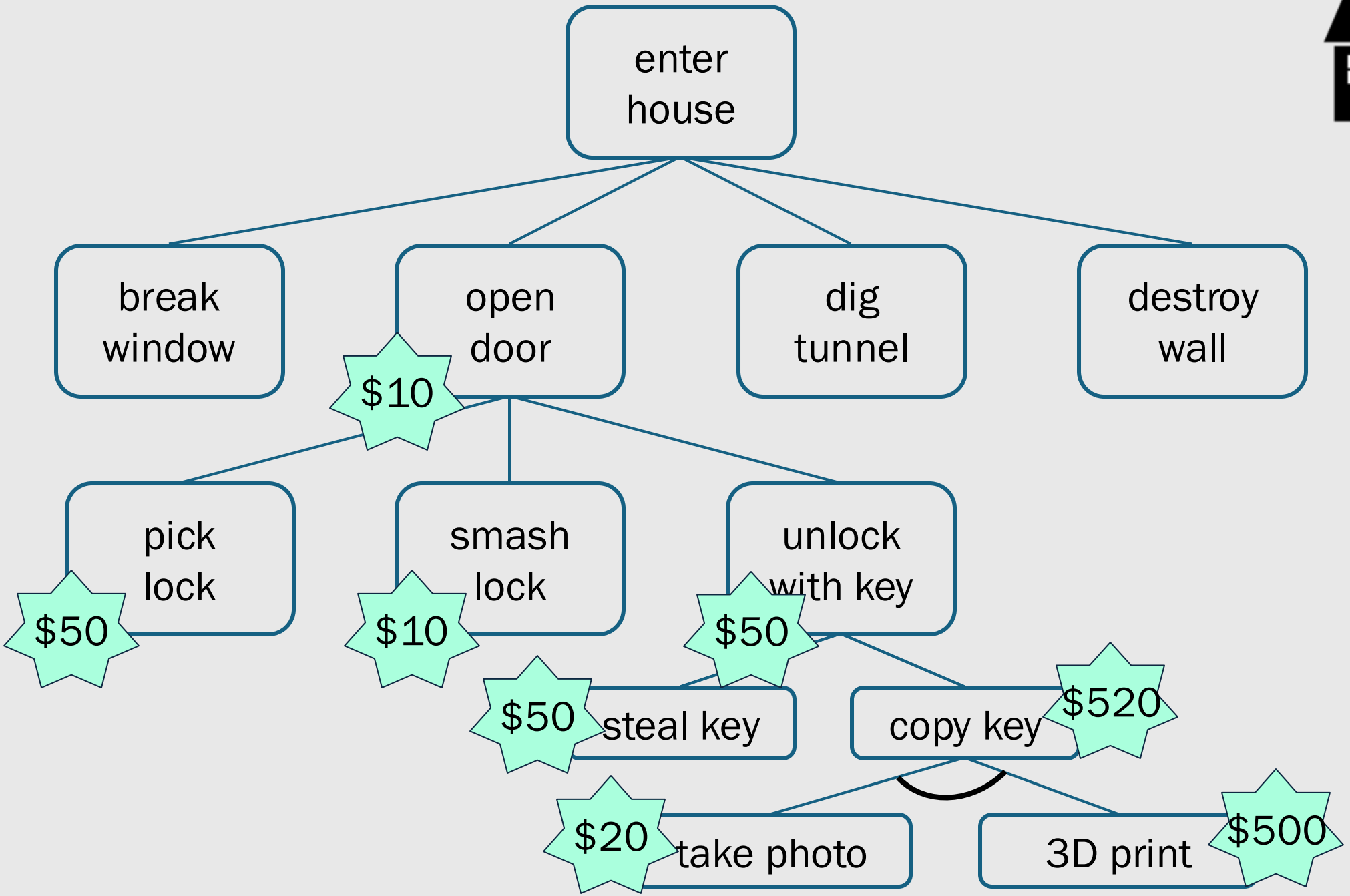




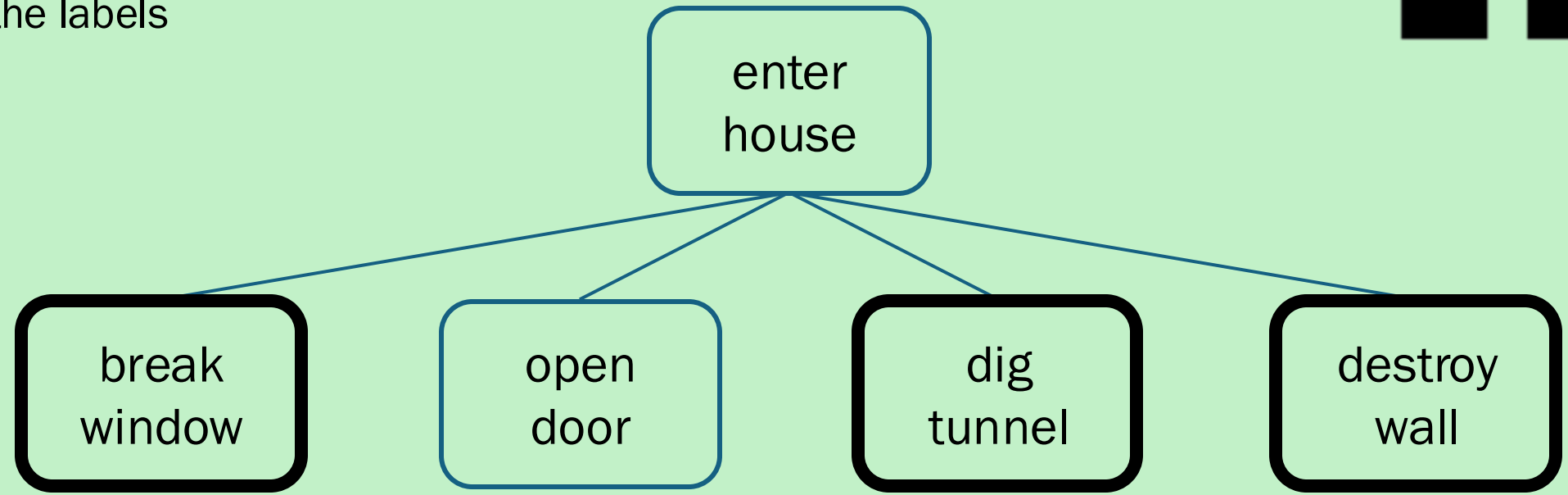
Worksheet Q3!


requires
collusion
requires
collusion
requires
collusion


requires
collusion
requires
collusion


enter house
break window
open door
dig tunnel
destroy wall
$10
pick lock
smash lock
unlock with key
$50
$10
$50
$50
steal key
copy key
$520
$20
take photo
3D print
$500

1. Expand window, tunnel, or wall by two levels
2. Add “2+ adversaries required” labels
3. Propagate the labels



Worksheet Q4!

Attack Trees

- Methodical
- Builds knowledge base
- Useful during design

Pros

- False sense of accuracy & security
- Never complete
- Time consuming

Cons