Attack Modelling

Paolo Falcarin

Ca' Foscari University of Venice

Department of Enviromental Sciences, Informatics and Statistics

paolo.falcarin@unive.it

CM0626 – Software Security

CM0631-2 – Software Security

28 February 2025

Attack Trees

Ca' Foscari University of Venice

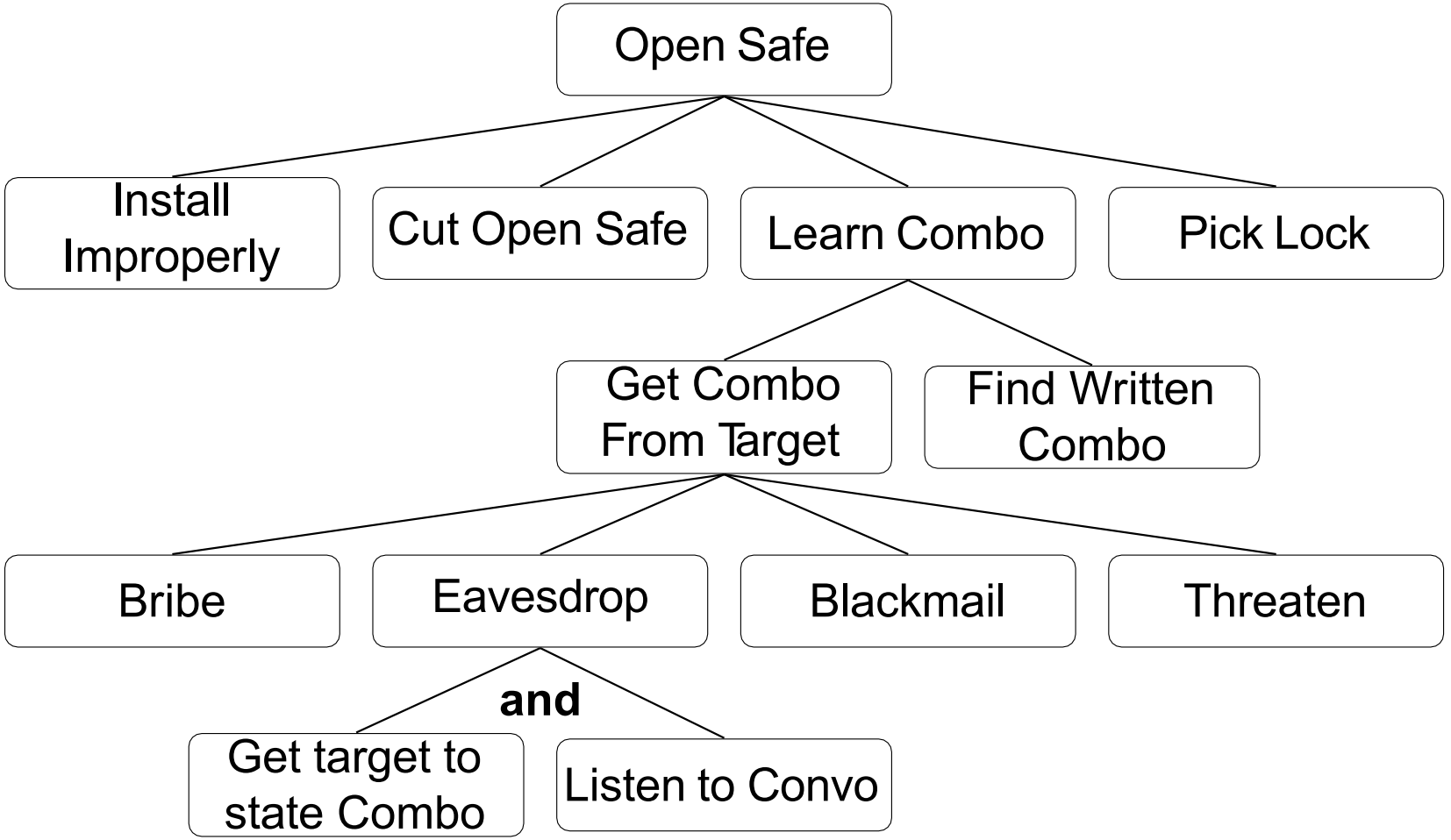
- We need to model threats against computer systems.
- What are the different ways in which a system can be attacked?
- If we can understand this, we can design proper countermeasures.
- Attack trees are a way to methodically describe the security of a system.

Structure of Attack Trees

- The root node is the overall goal the attacker wants to achieve.
- Attack trees have both AND and OR nodes:
  - OR: Alternatives to achieving a goal.
  - AND: Different steps toward achieving a goal.
- Each node is a subgoal.
- Child nodes are ways to achieve a subgoal.

Example I — Open a Safe

Ca' Foscari University of Venice

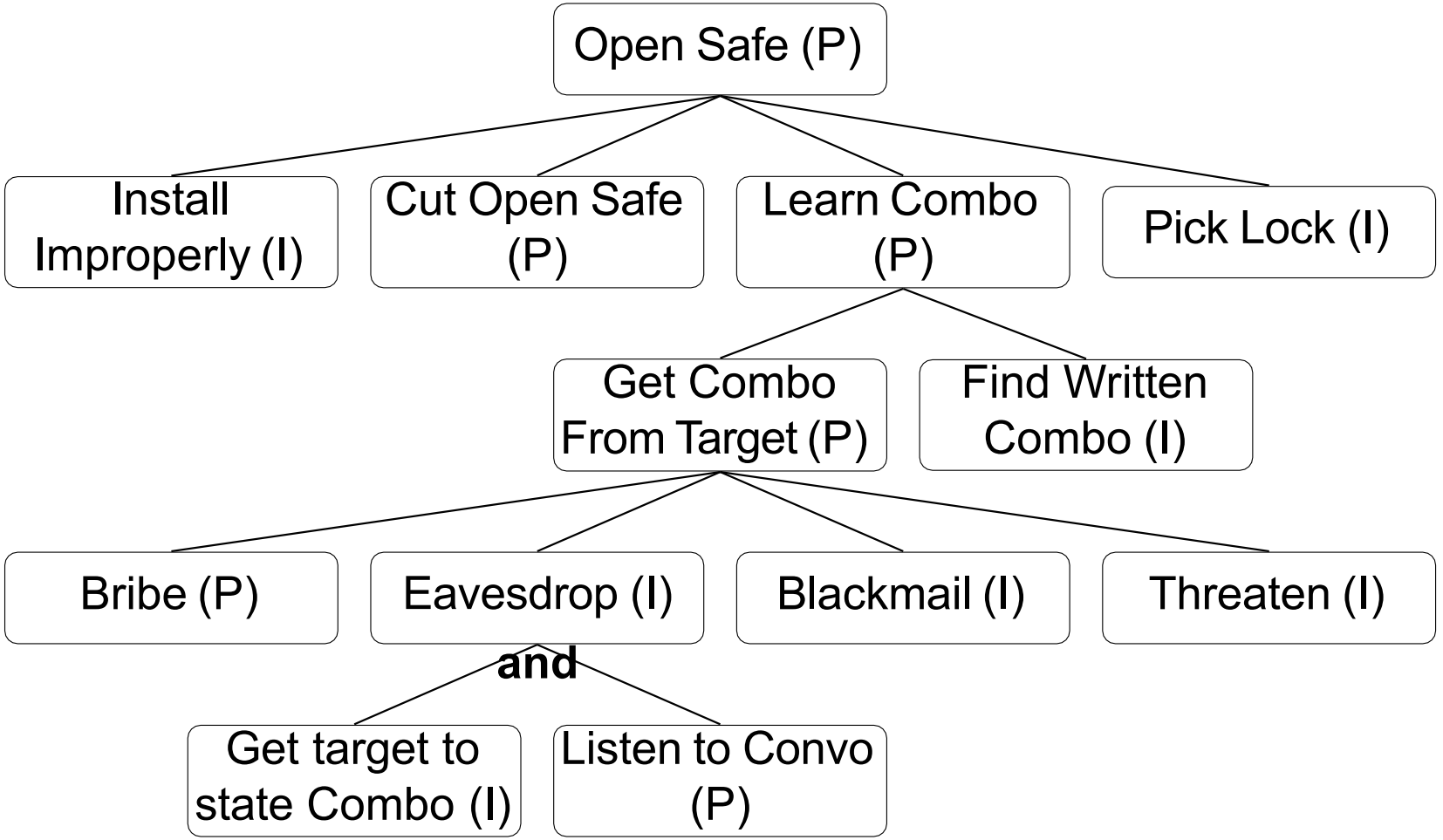


Example I — Open a Safe

Ca' Foscari University of Venice

- Examine the safe/safe owner/attacker's abilities/etc. and assign values to the nodes:
  - P = Possible
  - I = Impossible
- The value of an OR node is possible if any of its children are possible.
- The value of an AND node is possible if all children are possible.
- A path of P to s from a leaf to the root is a possible attack!
- Once you know the possible attacks, you can think of ways to defend against them!

Example I — Open a Safe



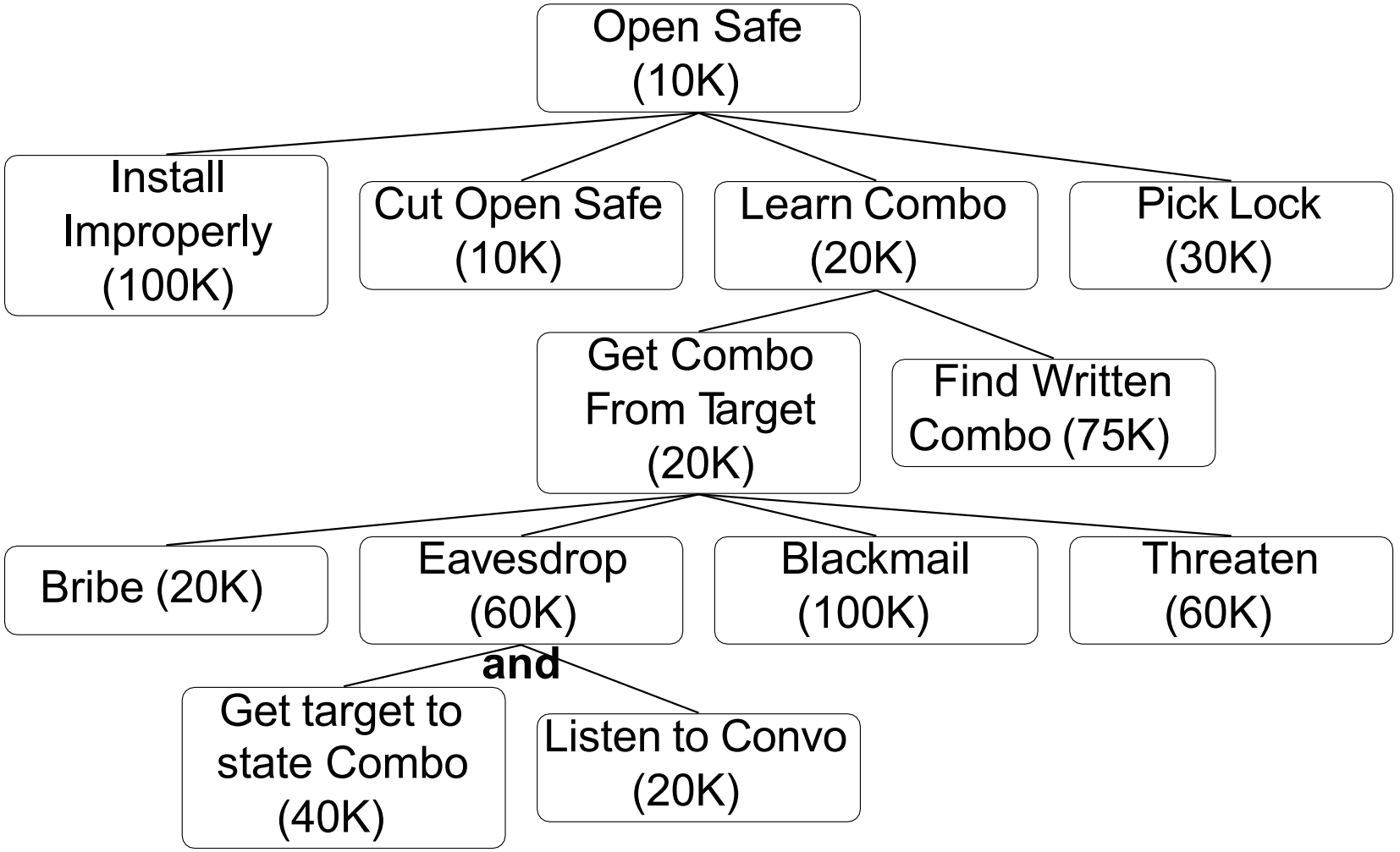
Example I — Open a Safe

Ca' Foscari University of Venice

- We can be more specific and model the cost of an attack.
- Costs propagate up the tree:
  - OR nodes: take the min of the children.
  - AND nodes: take the sum the children.

Example I — Open a Safe

Ca' Foscari University of Venice



Exercise — Read a Message

Ca' Foscari University of Venice

Goal:

Read a message sent from a sender on computer A to a receiver on computer B.

What can you do?

Start sketching an attack tree!

Example II — Read a Message

Ca' Foscari University of Venice

Goal: Read a message sent from computer A to B.

1. Convince sender to reveal message

- Bribe user, OR
- Blackmail user, OR
- Threaten user, OR
- Fool user

2. Read message while it is being entered

- Monitor electromagnetic radiation, OR
- Visually monitor computer screen.

Example II — Read a Message

Ca' Foscari University of Venice

3. Read message while stored on A's disk.

- Get access to hard drive, AND
- Read encrypted file.

4. Read message while being sent from A to B.

- Intercept message in transit, AND
- Read encrypted message.

Example II — Read a Message

Ca' Foscari University of Venice

5. Convince recipient to reveal message

- Bribe user, OR
- Blackmail user, OR
- Threaten user, OR
- Fool user

6. Read message while it is being read

- Monitor electromagnetic radiation, OR
- Visually monitor computer screen

Example II — Read a Message

Ca' Foscari University of Venice

7. Read message when being stored on B's disk.

- Get stored message from B's disk after decryption
  - Get access to disk, AND Read encrypted file.
- OR
- Get stored message from backup tapes after decryption.

8. Get paper printout of message

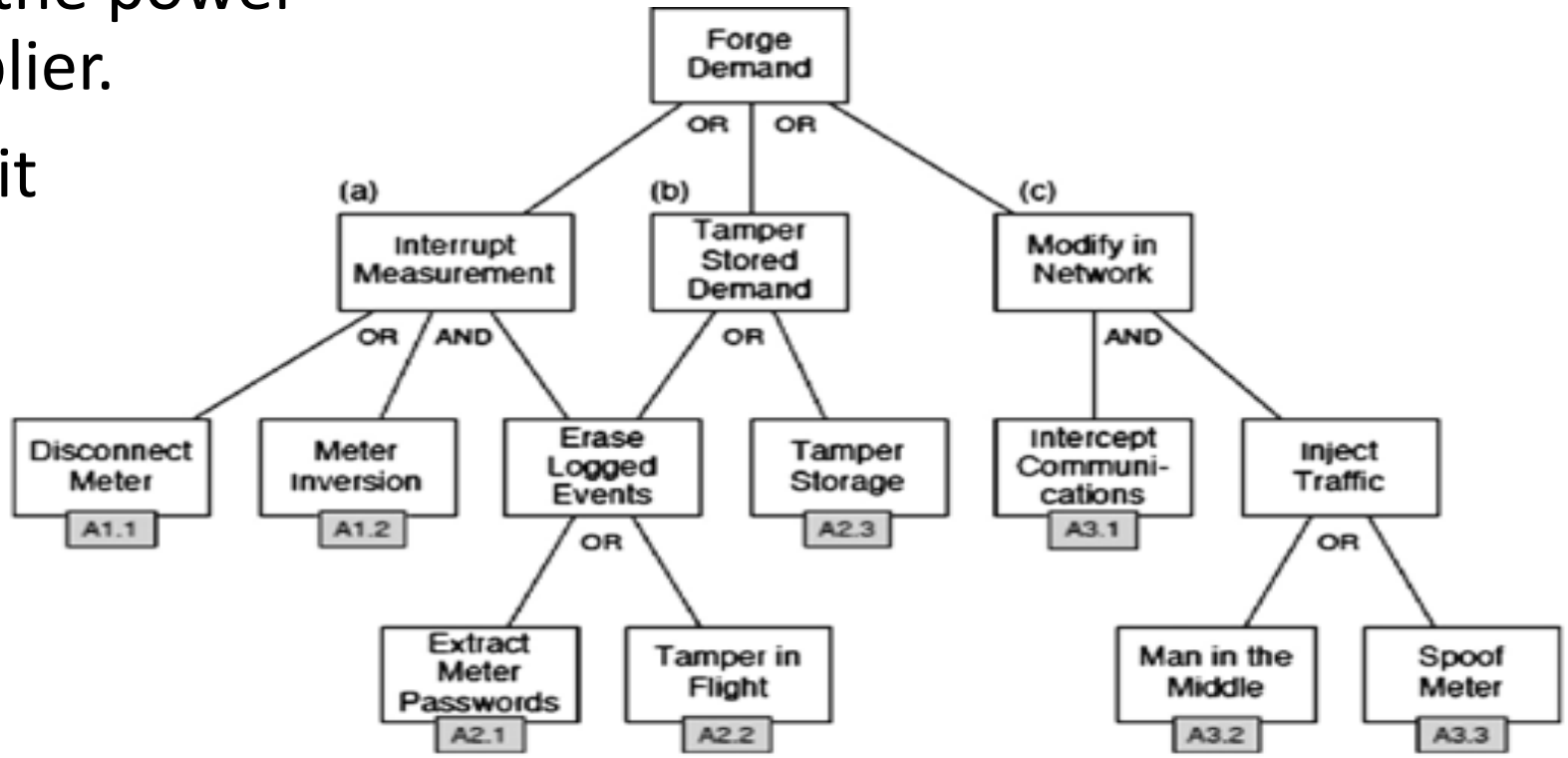
- Get physical access to safe, AND
- Open the safe.

Example Smart Meter

Ca' Foscari University of Venice

Smart meter is a device that communicate via network the power demand to the Power supplier.

It stores the logs and send it periodically to the server



Quiz

Ca' Foscari University of Venice

The main goal of the attacker is to "Forge Demand": which attack path here below is NOT enough to perform a successful attack?

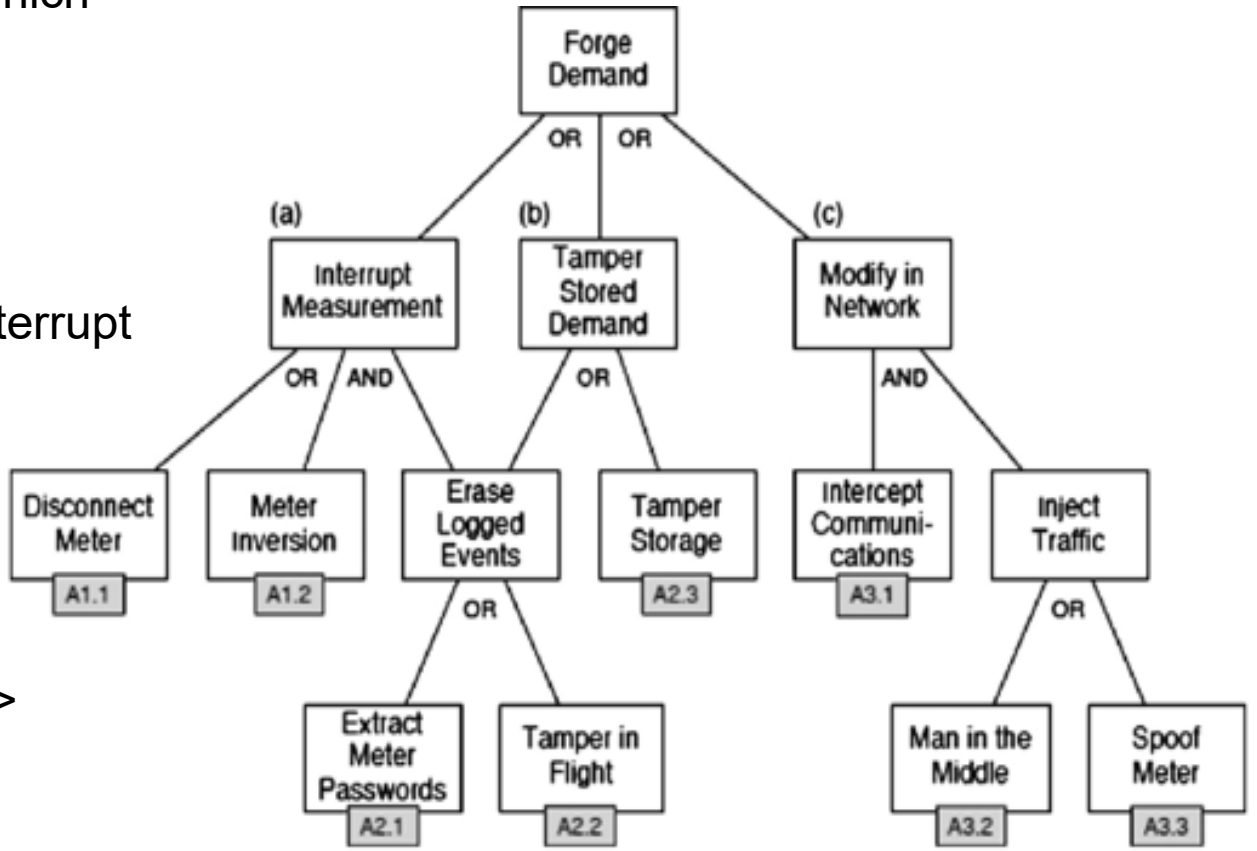
A. Disconnect Meter –> Interrupt Measurement

B. Meter Inversion –> Extract Meter Passwords –> Interrupt Measurement

C. Tamper Storage –> Tamper Stored Demand

D. Spoof Meter –> Inject Traffic –> Modify in network

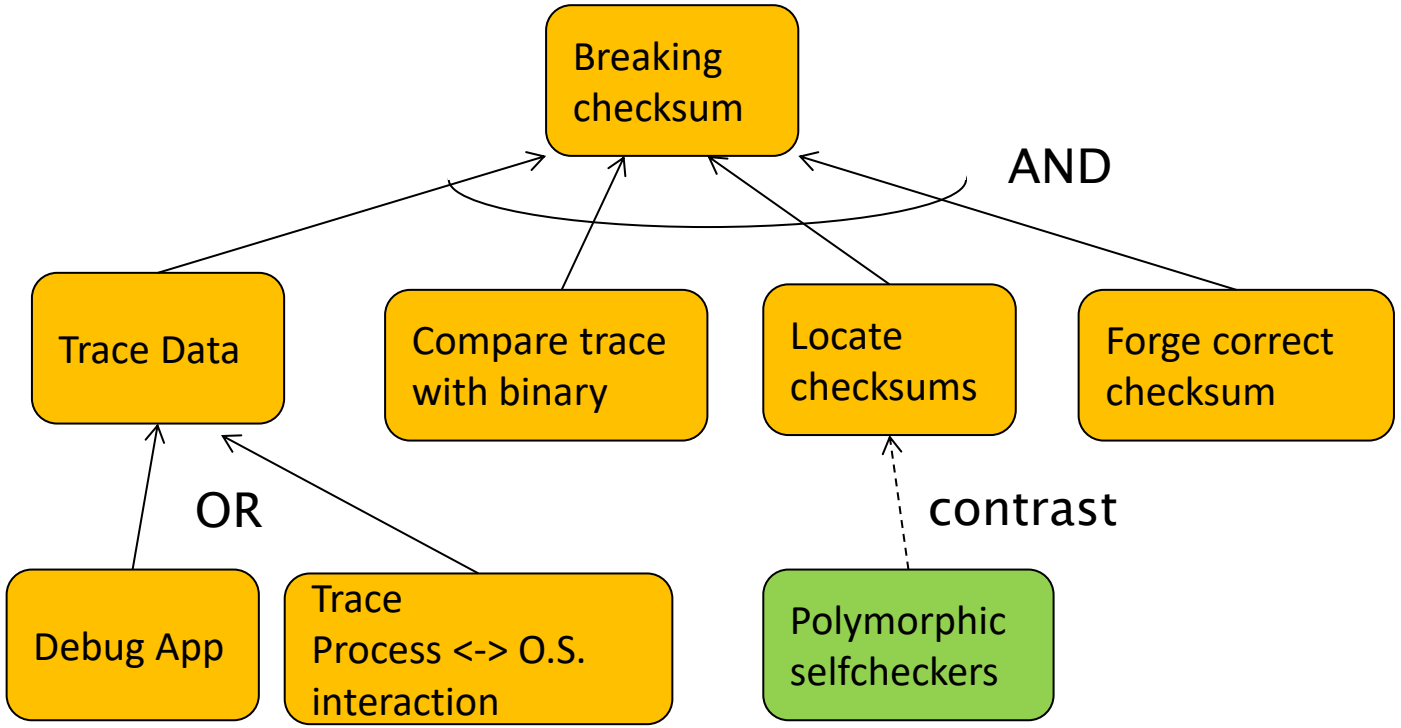
E. Extract Meter password -> Erase Logged Events -> Tamper Stored Demand



Attack Tree: Breaking Checksum

Ca' Foscari University of Venice

- Relate attack goal, subgoals
- Optionally link protections to the sub-goal they are contrasting



In-class Exercise 2

Ca' Foscari University of Venice

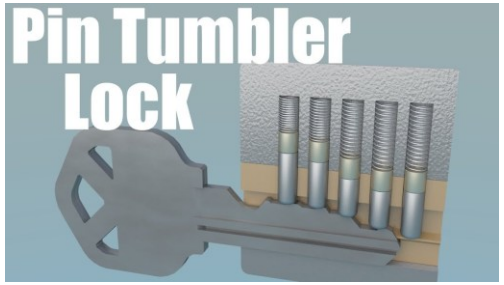
- Every night, Alice, 18, sits down with her laptop in front of the TV in the living room and adds a paragraph to her diary, describing her latest dating adventures.
- Bob, her 13-year-old bratty brother, would love to get his hands on her writings.
- Help Bob plan an attack (or Alice to defend herself against an attack!) by constructing a detailed attack tree!

In-class Exercise 2

Ca' Foscari University of Venice

Bob knows this about Alice:

- She writes and stores her diary directly on her laptop.
- The hard drive is encrypted with 512-bit AES.
- She's written down her pass-phrase on a post-it note.
- She stores the post-it note in a safe in her bedroom.
- The safe is locked with a 5-pin pin-and-tumbler lock.



- She carries the key to the safe on a chain around her neck wherever she goes.
- She leaves the laptop next to her bed at night.
- The laptop is always connected to the Internet over wifi.

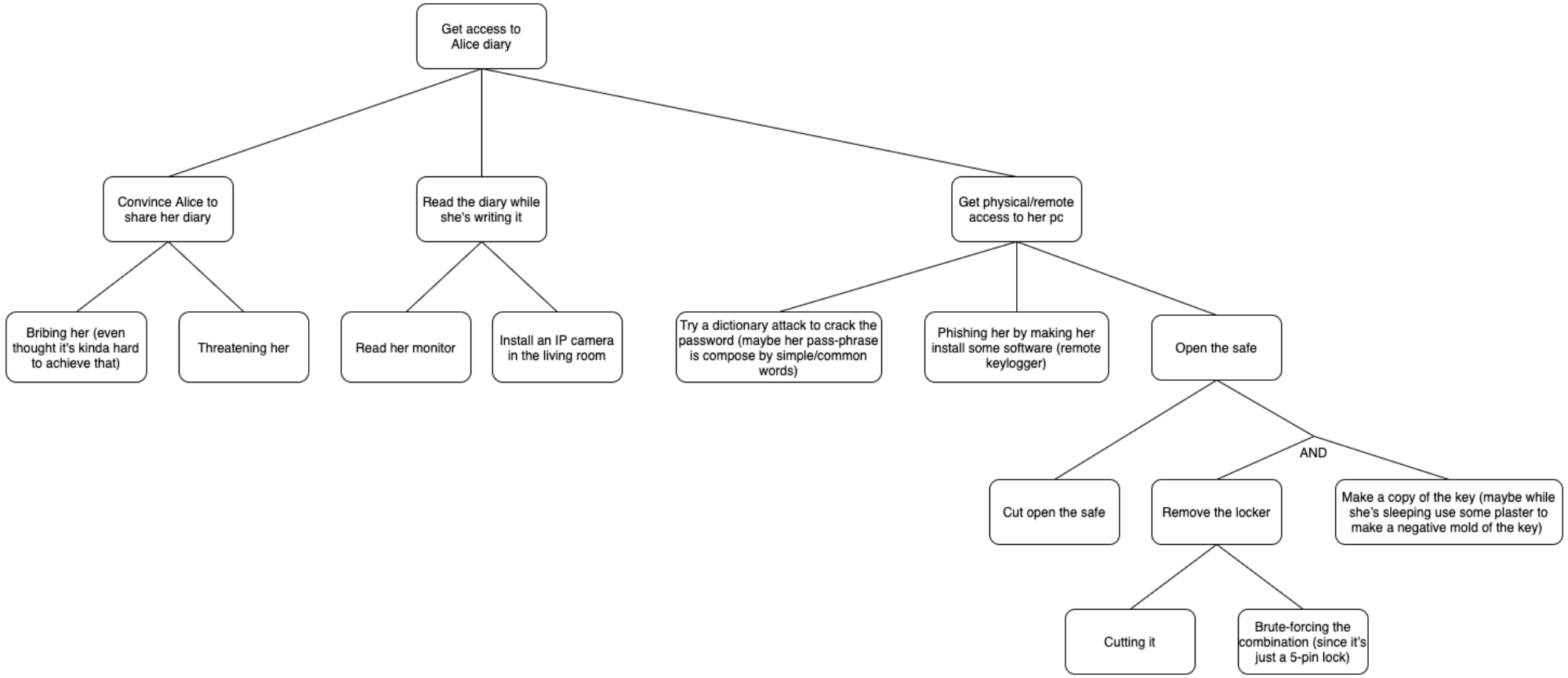
In-class Exercise 2

Ca' Foscari University of Venice

We know the following about Bob:

- He can roam freely around the house.
- His gaming skills has given him the financial means to purchase various attack tools off the Internet.
- Your solution should consider both physical attacks and cyber attacks.
- You don't have to assign costs to the nodes of the tree.
- Make sure to mark AND and OR nodes unambiguously.
- You can draw the actual tree or, if you prefer, represent the tree with indented, nested, numbered lists.

Possible Solution



Attack Trees
Software Protection Example

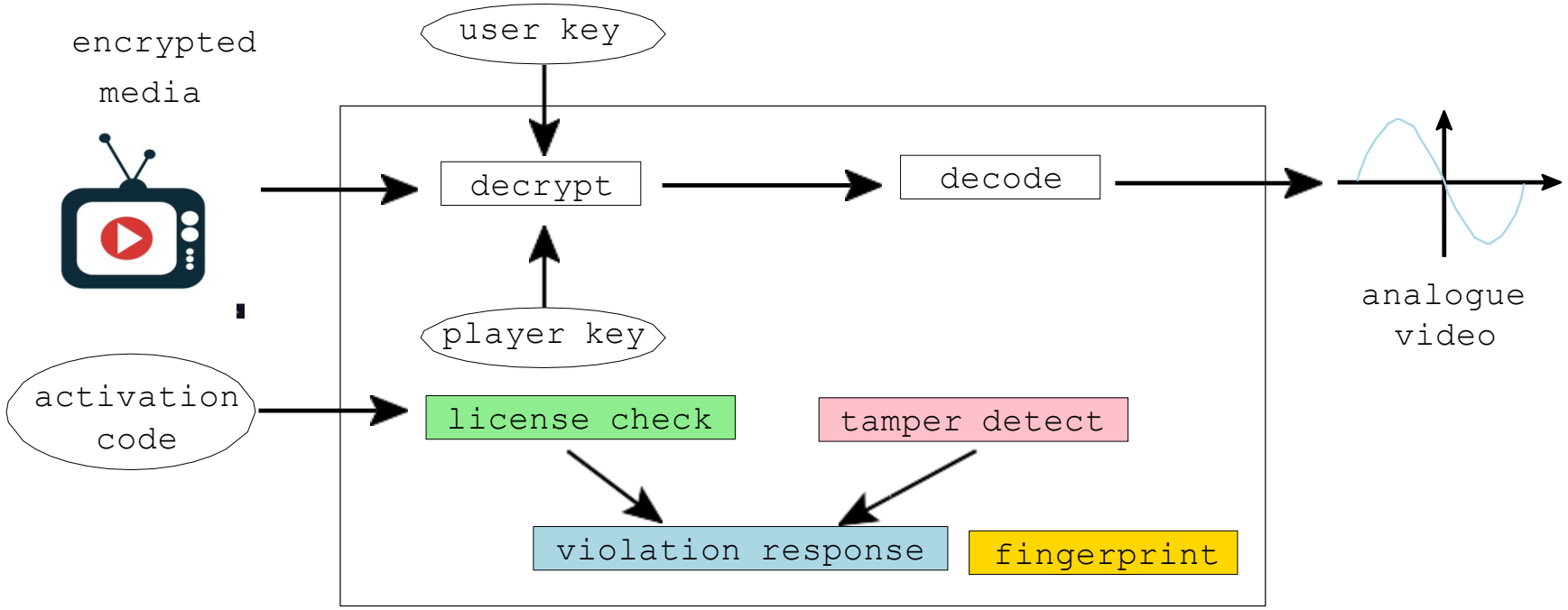
Who's our adversary?

Ca' Foscari University of Venice

- What does a typical program look like?
- What assets does the program contain?
- What is the adversary's motivation for attacking your program?
- What information does he start out with as he attacks your program?
- What is their overall strategy for reaching their goals?
- What tools do they have to their disposal?
- What specific techniques do they use to attack the program?

Example Program

Ca' Foscari University of Venice

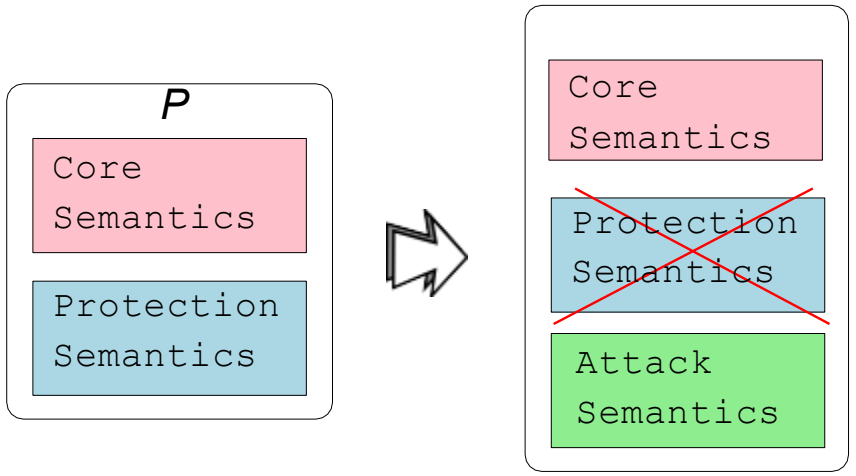


What's the Adversary's Motivation?

Ca' Foscari University of Venice

The adversary wants to

- remove the protection semantics.
- add his own attack semantics (ability to save game-state, print)
- ensure that the core semantics remains unchanged.



What does he want to do to the Player program?

Ca' Foscari University of Venice

- get decrypted digital media extract the player key
- use the program after the expiration date
- remove use-before check remove activation code
- distribute the program to other users
- remove fingerprint
- reverse engineer the algorithms in the player

What are the methods of attack?

Ca' Foscari University of Venice

1. The Black Box phase
   - feed the program inputs,
   - record its outputs
   - draw conclusions about its behavior.
2. The Dynamic Analysis phase
   - execute the program
   - record which parts get executed for different inputs
3. The Static Analysis phase
   - examining the executable code directly
   - use disassembler, decompiler, . . .

What are the methods of attack?

Ca' Foscari University of Venice

4. The editing phase

- use understanding of the internals of the program
- modify the executable disable license checks

5. The automation phase

- encapsulates his knowledge of the attack in an automated script
- use in future attacks.

Example Program

Ca' Foscari University of Venice

```
1  typedef unsigned int uint;
2  typedef uint* waddr_t;
3  uint player_key = 0xbabeca75;
4  uint the_key;
5  uint* key = &the_key;
6  FILE* audio;
7  int activation_code = 42;
```

Example Program

Ca' Foscari University of Venice

```
 7  void FIRST_FUN(){}
 8  uint hash (waddr_t addr, waddr_t last) {
 9      uint h = *addr;
10      for (;addr<=last;addr++) h^=*addr;
11  return h;
12  }
13  void die(char* msg) {
14      fprintf(stderr,"%s!\n",msg);
15      key = NULL;
16  }
```

Example Program

Ca' Foscari University of Venice

```
19  uint play(uint user_key,
20            uint encrypted_media[],
21            int media_len) {
22      int code;
23      printf("Please enter activation code: ");
24      scanf("%i",&code);
25      if (code!=activation_code) die("wrong code");
26
27      *key = user_key ^ player_key;
```

Example Program

Ca' Foscari University of Venice

```
27      int i;
28      for(i=0;i<media_len;i++) {
29          uint decrypted = *key ^ encrypted_media[i];
30
31
32          if (time(0) > 1221011472) die("expired");
33
34
35          float decoded = (float)decrypted;
36          fprintf(audio,"%f\n",decoded); fflush(audio);
37
38
39      }
40  }
```

Example Program


```
41 void LAST_FUN(){}
42 uint player_main (uint argc, char *argv[]) {
43     uint user_key = ···
44     uint encrypted_media[100] = ···
45     uint media_len = ···
46     uint hashVal = hash((waddr_t)FIRST_FUN,
47                         (waddr_t)LAST_FUN);
48     if (hashVal != HASH) die("tampered");
49     play(user_key, encrypted_media, media_len);
50 }
```