GameSS

EDUCATIONAL MATERIAL IN CYBER SECURITY

THREAT MODELLING & ASSESSMENT WITH ATTACK TREES: PUT SECURITY ON THE TABLE BEFORE IT'S TOO LATE!

WHO IS THE MATERIAL FOR?

- Students and professionals interested in methodologies and tools that support security-related decision-making activities.
- Security professionals interested in early identification of potential vulnerabilities and preventive design options.
- Software developers, security analysts, and managers interested in having a common dialogue tool that helps them communicate with each other, overcoming the usual language barriers from their own realities.
- Participants interested in dialogue tools that allow them to
    - collaborate in the analysis of vulnerabilities and security-related design decisions,
    - acquire a common understanding of the key assets to protect and their potential threats
    - align their views on prioritizing the design of preventive measures.



WHO MADE THIS MATERIAL?

Alberto Lluch Lafuente

Technical University of Denmark

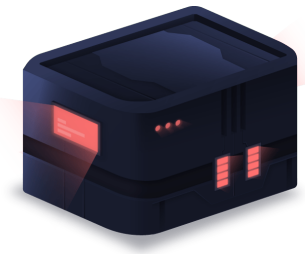
albl@dtu.dk

linkedin.com/in/albertolluch

imm.dtu.dk/~albl/

WHAT ARE THE MAIN TAKEAWAYS FOR THIS CONTENT?

- Attack Trees provide a structured methodology to threat modelling, supported by solid theories and effective tools.
- Attack Trees provide a visual representation of possible actions an attacker might take in order to compromise a system, and the defensive measures that a defender can employ to protect the system.
- Attack Trees can model several aspects of interests such as feasibility of attacks, probability of attack success and failure, effectiveness of countermeasures, and cost of attacks and countermeasures.
- Attack Tree tools such as ADTool can be used to automatise the assessment of Attack Trees.



INTRODUCTION

A key dilemma of security is to decide where to better invest resources to prevent security hazards. Threat modelling & assessment methodologies support this by promoting a security-by-design mindset, and providing structured processes and tools that help in finding a common understanding of the assets that need to be protected, their attack surface, expected vulnerabilities and possible countermeasures. Among all methodologies, attack trees have emerged as a lightweight, easy-to-adopt and flexible graphical notation to model and assess security.

INTRODUCTION

Attack trees provide a representation of possible actions an attacker might take in order to compromise a system, and the defensive measures that a defender can employ to protect the system. Attack trees provide an effective dialogue tool between the different stakeholders usually involved in threat modelling: designers and developers of system providing in-depth details about the attack-surface, security experts identifying vulnerabilities and countermeasures, and managers contributing with business-driven priorities and decisions.

INTRODUCTION

In this course, we will explore the key principles, tools, and techniques that enable organizations to model and assess security threats using attack trees. You will learn how use attack trees to summarize attack scenarios in a graphical way, how to determine which attack scenarios are captured or excluded by an attack tree, how to assess and compare different attack scenarios, and how to incorporate countermeasures in your threat model to prevent specific vulnerabilities.

INTRODUCTION

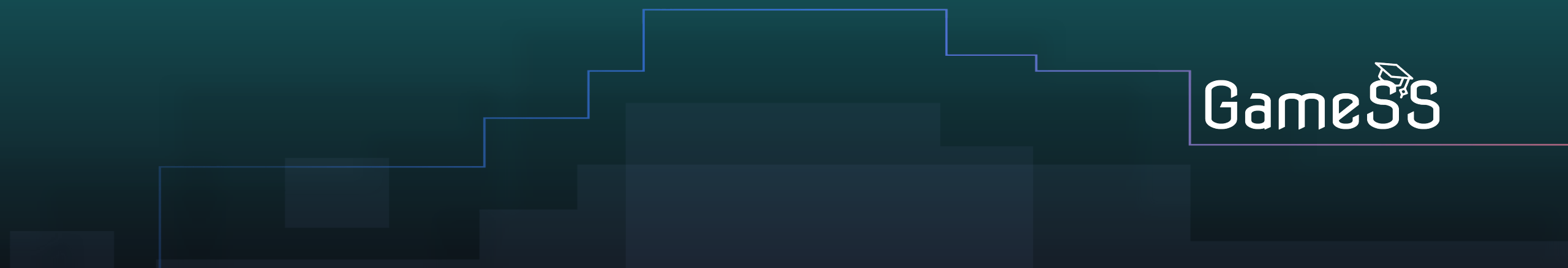
In addition to the comprehensive theoretical knowledge, this course offers an exciting opportunity to put practice and test skills using software tools to solve challenges specifically designed for threat modelling and assessment with attack trees.

INTRODUCTION

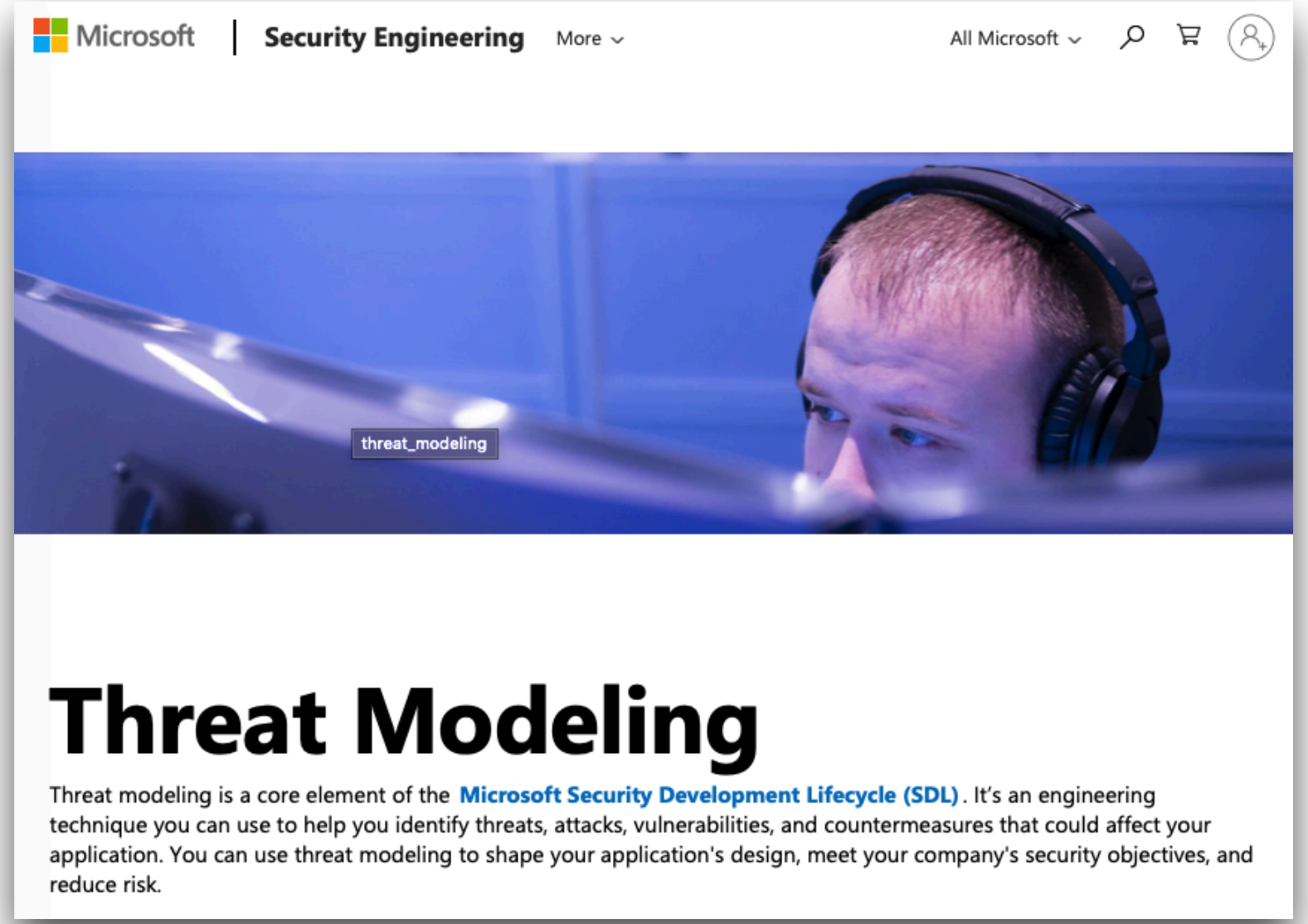
Whether you are a developer, a security analyst or a manager seeking to enhance your organisation's security posture, this course will equip you with the knowledge and skills needed to adopt a lightweight, yet effective approach to threat modelling and assessment.

Join us on this learning journey as we unlock the power of attack trees and empower you to be better at communicating about security threats and security-related decisions.

What is threat modelling and why should I care?



What is Threat Modelling?

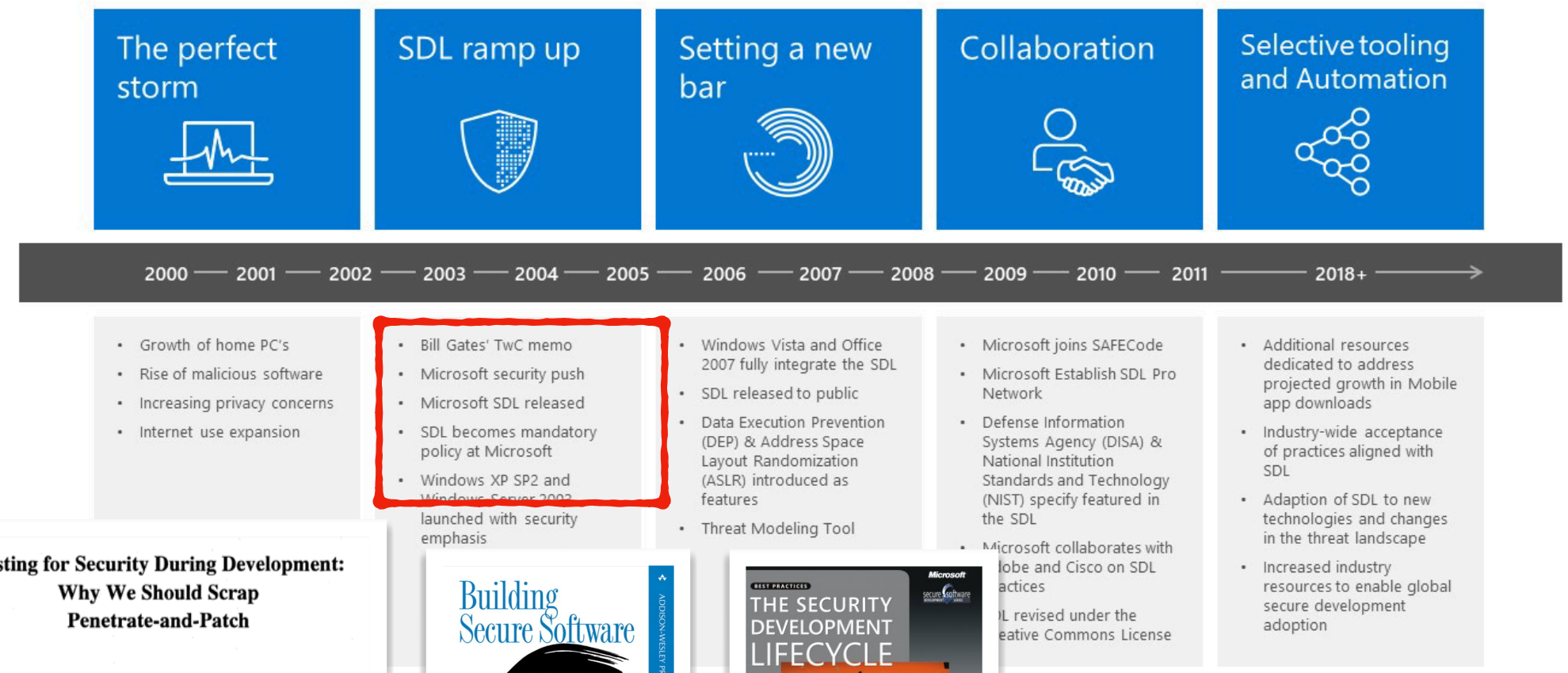


Source: https://www.microsoft.com/en-us/securityengineering/sdl/

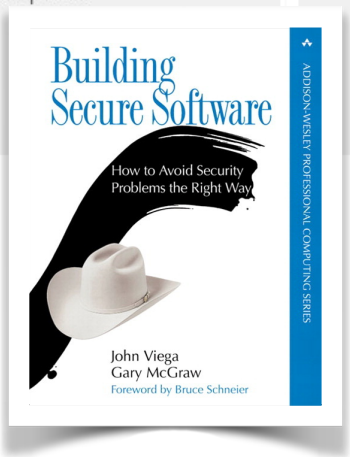
Why should I care about Threat Modelling?

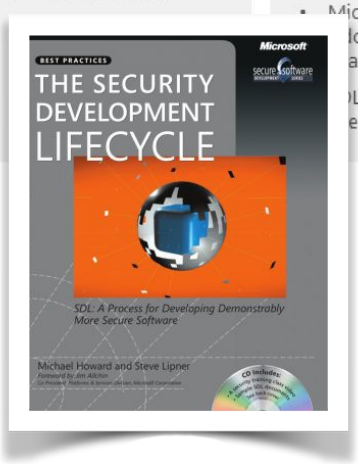
SDL Timeline

Source: https://www.microsoft.com/en-us/securityengineering/sdl/



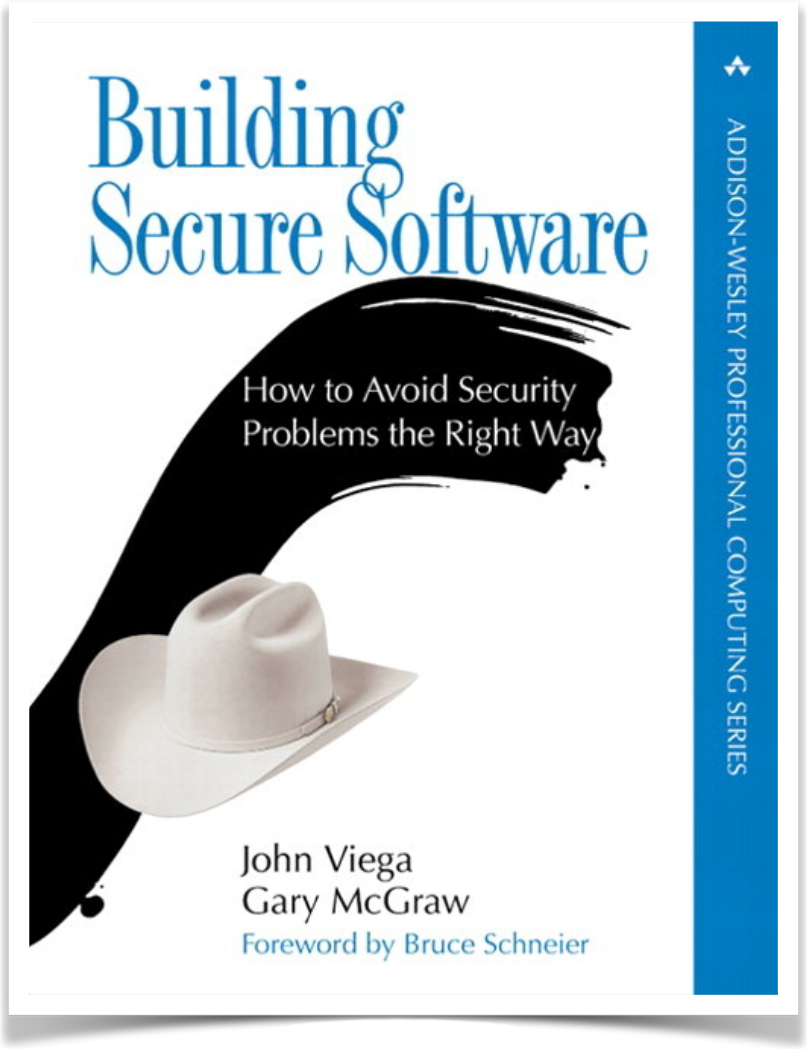


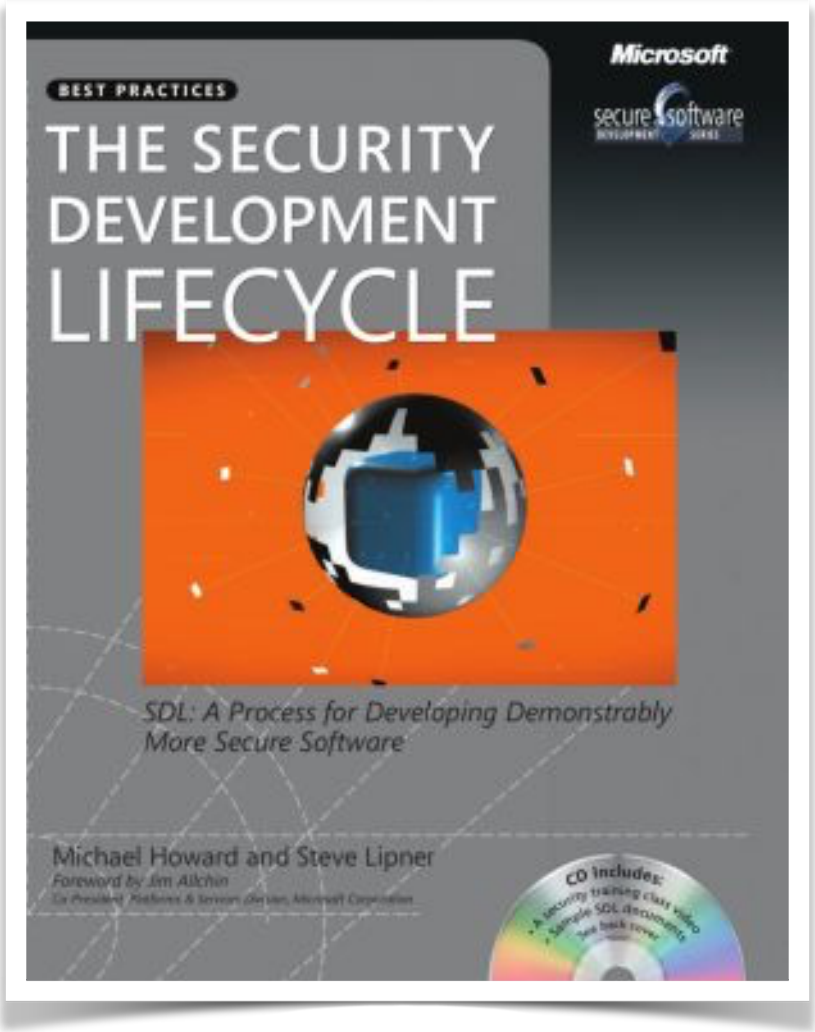




Proactive Software Analysis (McGraw, 1998)

Software lifecycle: security steps in





Source: https://www.amazon.com

This has evolved into methodologies like DevSecOps and the like

Models can be used for assessment

Modelling per se is useful but we can use models to raise flags, draw attention to important security issues.

However…too many alarms are almost as bad as no alarm at all.

> Example from software analysis:
> a false positive rate of more than 20% is unacceptable to most developers [*].

[*] M. Christakis and C. Bird, “What developers want and need from program analysis: an empirical study,” in Proceedings of the 31st IEEE/ACM international conference on automated software engineering, 2016, pp. 332–343.

Models can be used for assessment

Modelling per se is useful but we can use models to raise flags, draw attention to important security issues.

However…too many alarms are almost as bad as no alarm at all.

> Example from software analysis:
> a false positive rate of more than 20% is unacceptable to most developers [*].

Usable threat models should provide meaningful ways of ranking of priorities:

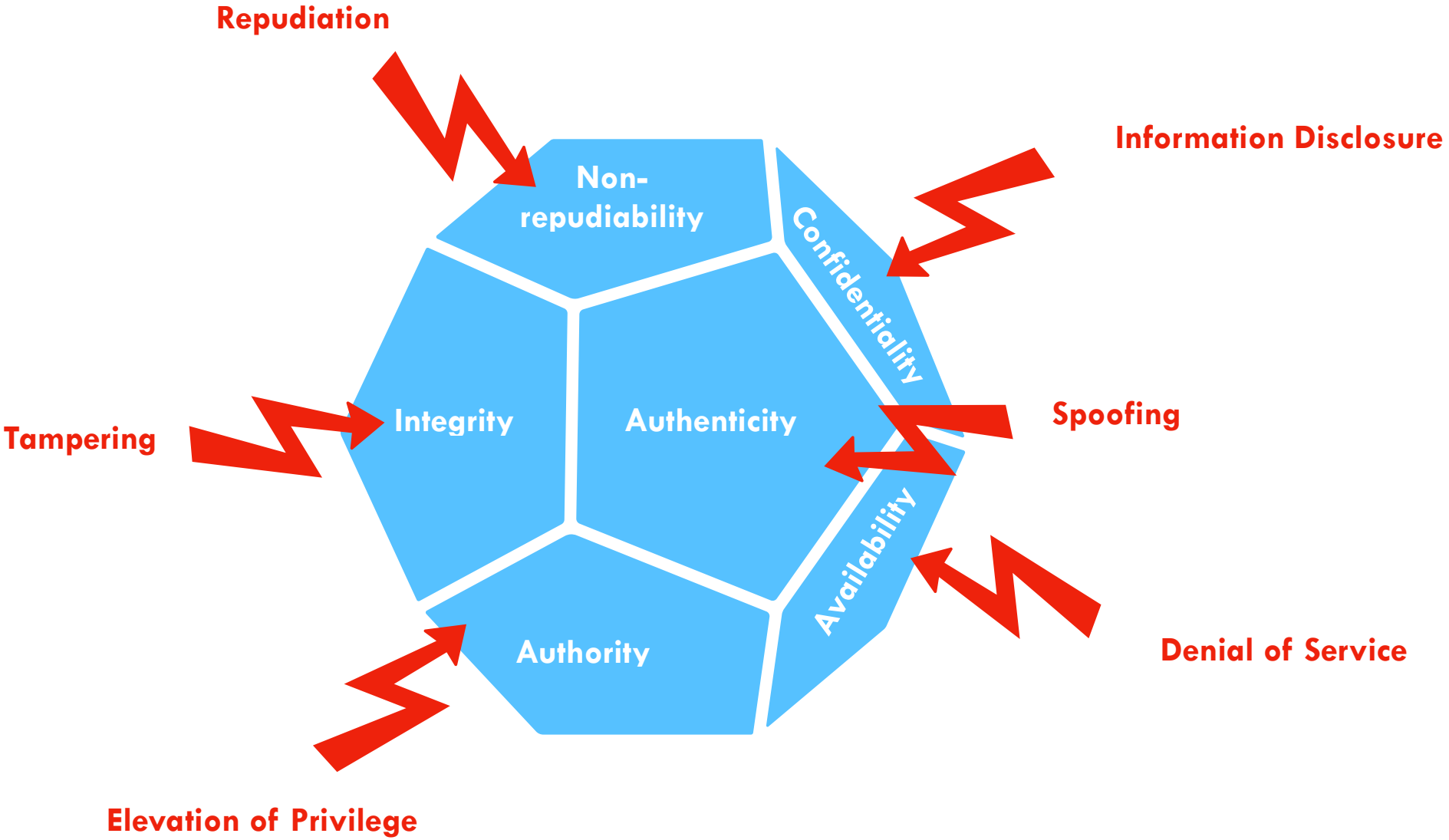
- What threats are more likely?
- What threats are more severe?
- What threats have a higher cost of prevention?
- …

Threat assessment supports this.

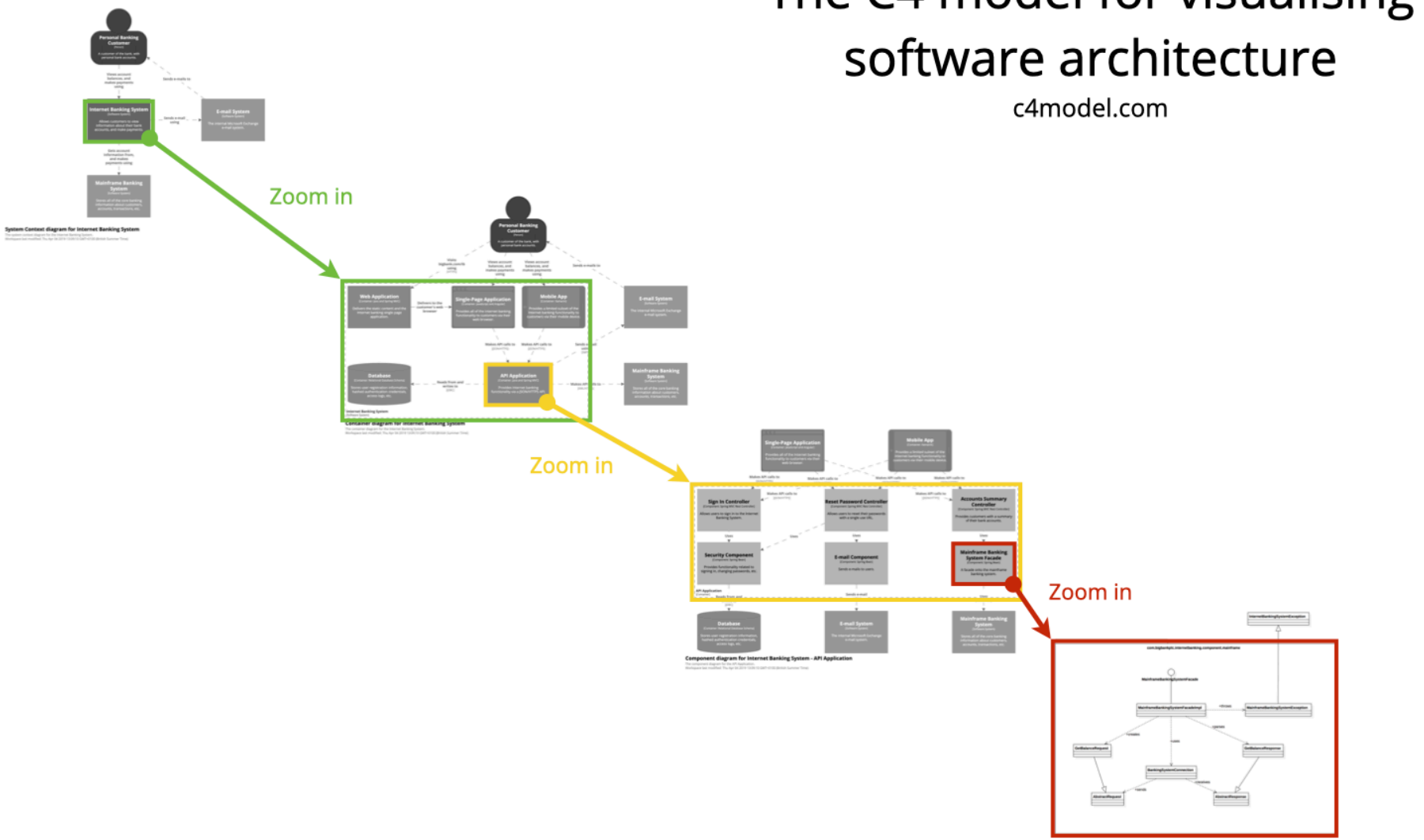
[*] M. Christakis and C. Bird, "What developers want and need from program analysis: an empirical study," in Proceedings of the 31st IEEE/ACM international conference on automated software engineering, 2016, pp. 332–343.

Example of threat-driven threat modelling: STRIDE

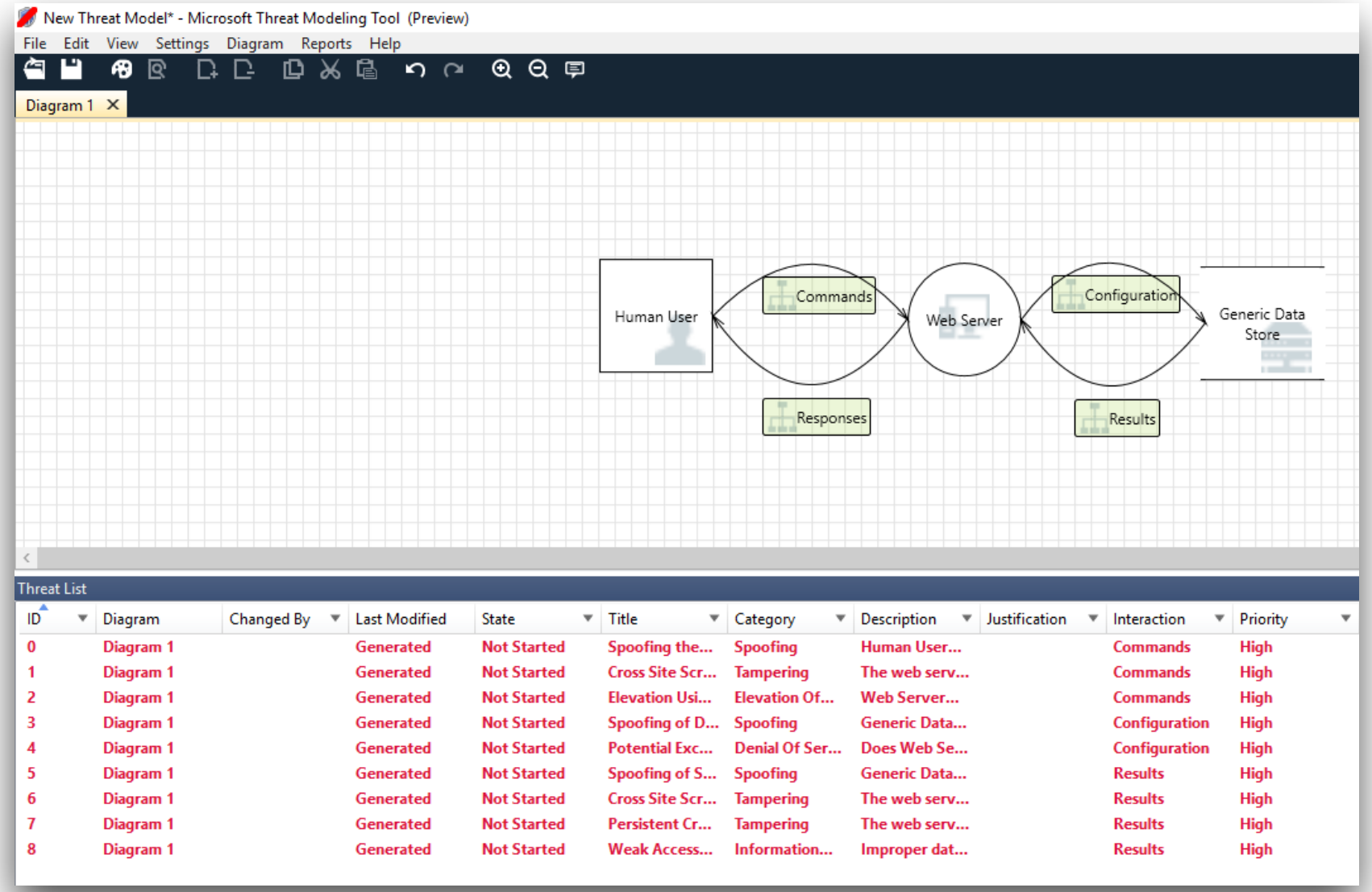
STRIDE focuses more on specific threats and the properties they can compromise



Example of asset-driven threat modelling: C4



Microsoft's Threat Modelling Tool



Threat List

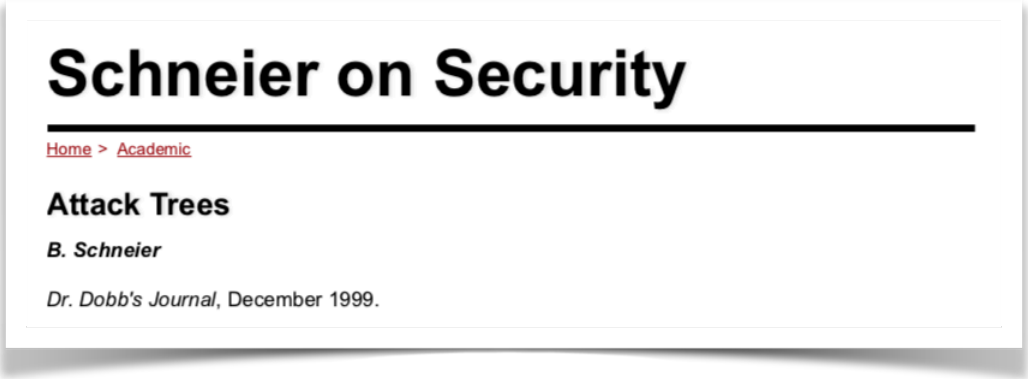
ID	Diagram	Changed By	Last Modified	State	Title	Category	Description	Justification	Interaction	Priority
0	Diagram 1		Generated	Not Started	Spoofing the...	Spoofing	Human User...		Commands	High
1	Diagram 1		Generated	Not Started	Cross Site Scr...	Tampering	The web serv...		Commands	High
2	Diagram 1		Generated	Not Started	Elevation Usi...	Elevation Of...	Web Server...		Commands	High
3	Diagram 1		Generated	Not Started	Spoofing of D...	Spoofing	Generic Data...		Configuration	High
4	Diagram 1		Generated	Not Started	Potential Exc...	Denial Of Ser...	Does Web Se...		Configuration	High
5	Diagram 1		Generated	Not Started	Spoofing of S...	Spoofing	Generic Data...		Results	High
6	Diagram 1		Generated	Not Started	Cross Site Scr...	Tampering	The web serv...		Results	High
7	Diagram 1		Generated	Not Started	Persistent Cr...	Tampering	The web serv...		Results	High
8	Diagram 1		Generated	Not Started	Weak Access...	Information...	Improper dat...		Results	High

Source: https://www.microsoft.com/en-us/securityengineering/sdl/

Threat modelling with Attack Trees

Attack trees are very flexible and driven by a “what can go wrong and how” mind setting.

Ex. Start with an asset and discuss how it could be compromised.



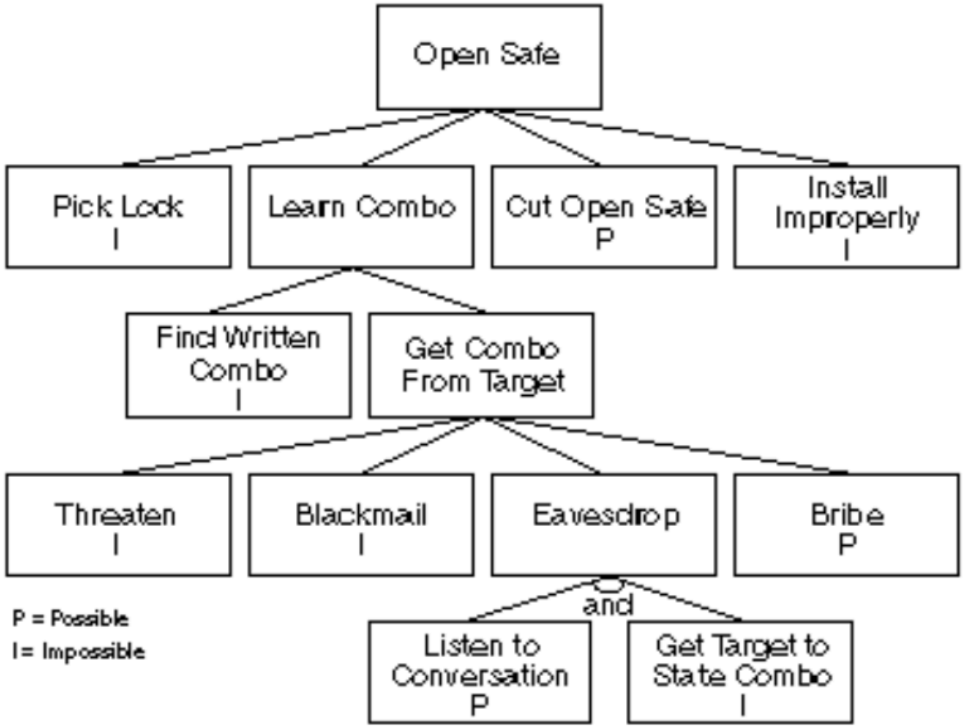
Schneier on Security

Home > Academic

Attack Trees

B. Schneier

Dr. Dobb's Journal, December 1999.



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

Not just code/software

Attack trees are a general methodology, which can be applied to variety of systems. In Scheire's words… *"Attack trees provide a formal methodology for analyzing the security of systems and subsystems".*

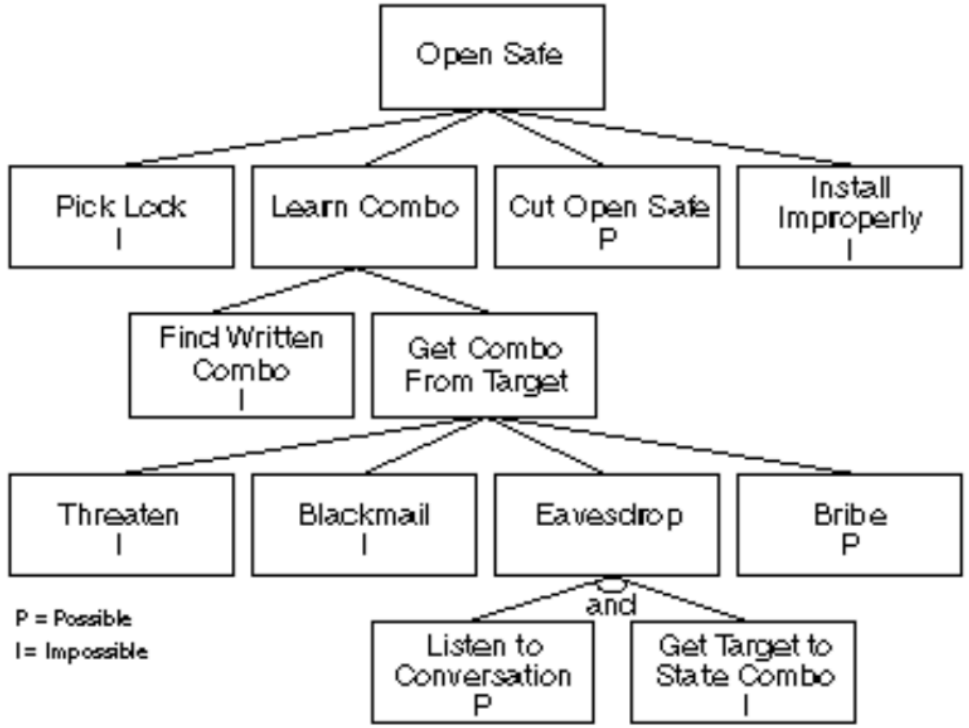
Schneier on Security

Home > Academic

Attack Trees

B. Schneier

Dr. Dobb's Journal, December 1999.



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

Why Attack Trees?

- One of the most popular graphical models for system security analysis

  Gadyatskaya, O., Trujillo-Rasua, R.: New Directions in Attack Tree Research: Catching up with Industrial Needs. In: GraMSec. LNCS, vol. 10744, pp. 115–126. Springer (2017)

- Understandable, easy to use, gentle learning curve, useful, and prone to adoption

  Assessing the Understandability and Acceptance of Attack-Defense Trees for Modelling Security Requirements Giovanna Brocci, Maurice H. ter Beek, Alberto Lluch Lafuente, Paola Spoletini, and Alessio Ferrari, In: REFSQ 2024, LNCS 14588

- Solid foundations based on mathematics & computer science (aka formal methods)

  Barbara Kordy, Ludovic Piètre-Cambacédès, Patrick Schweitzer: DAG-based attack and defense modeling: Don't miss the forest for the attack trees. Comput. Sci. Rev. 13-14: 1-38 (2014)

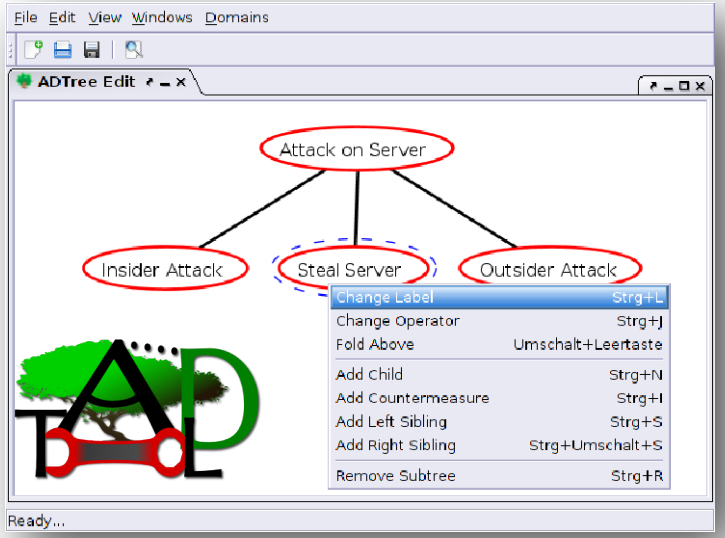
  Widel, W., Audinot, M., Fila, B., Pinchinat, S.: Beyond 2014: Formal Methods for Attack Tree-based Security Modeling. ACM Comput. Surv. 52 (4),75:1–75:36 (2019)

- Complements other threat methodologies (STRIDE, Mitre ATT&CK…)

- Supported by software tools (see next slide)

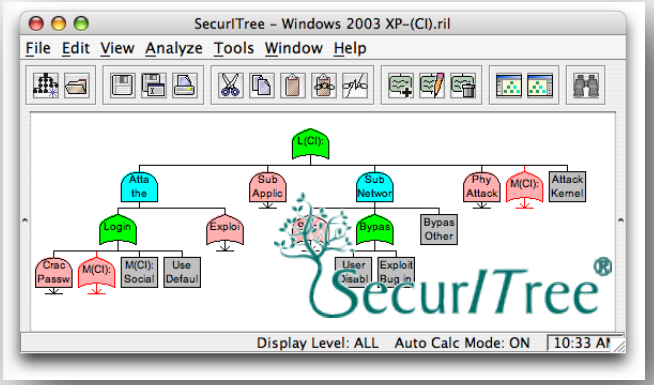
Attack-trees tools

ADTool



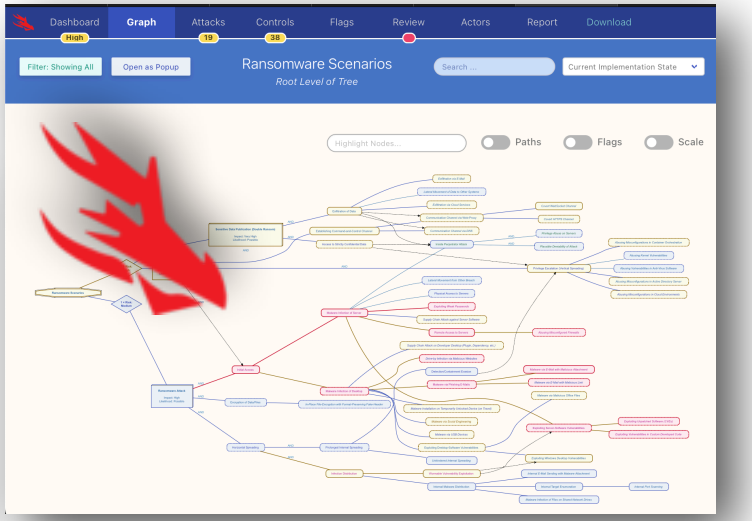
https://satoss.uni.lu/members/piotr/adtool/

SecurITree



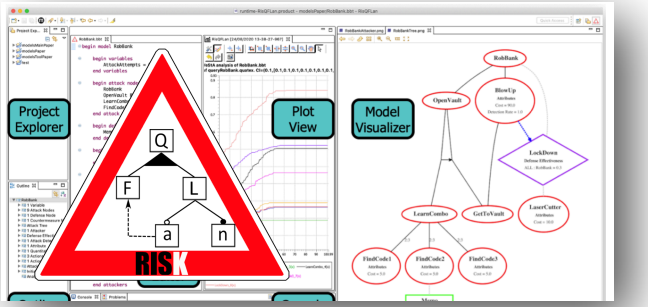
https://www.amenaza.com/SS-main.php

Agile Attack Tree Toolkit



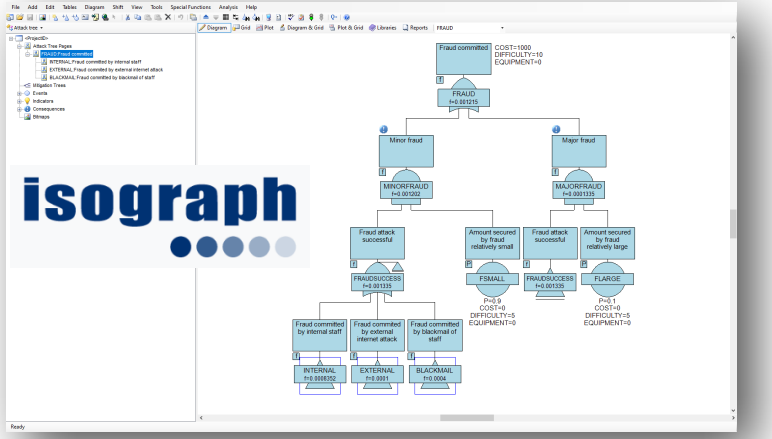
https://attacktree.online/

RISQFlan



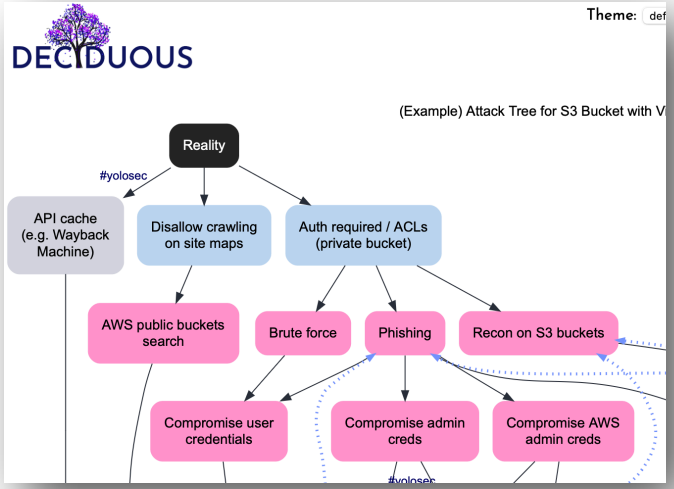
https://github.com/risqflan/risqflan/wiki

Isograph



https://www.isograph.com/software/attacktree/

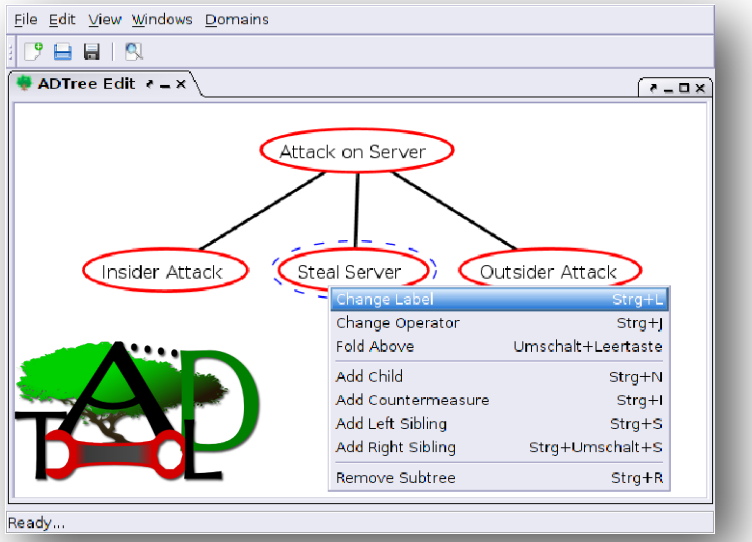
Deciduous



https://www.deciduous.app/

Attack-trees tools

ADTool

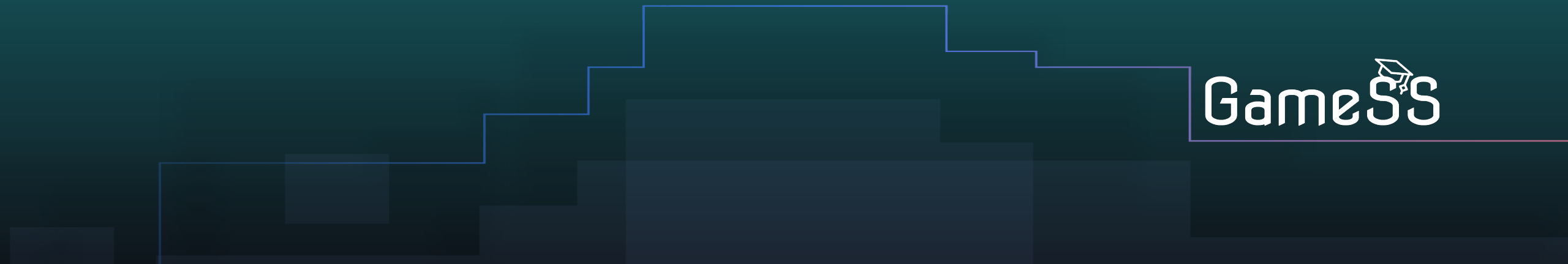


In this lecture we will use ADTool.

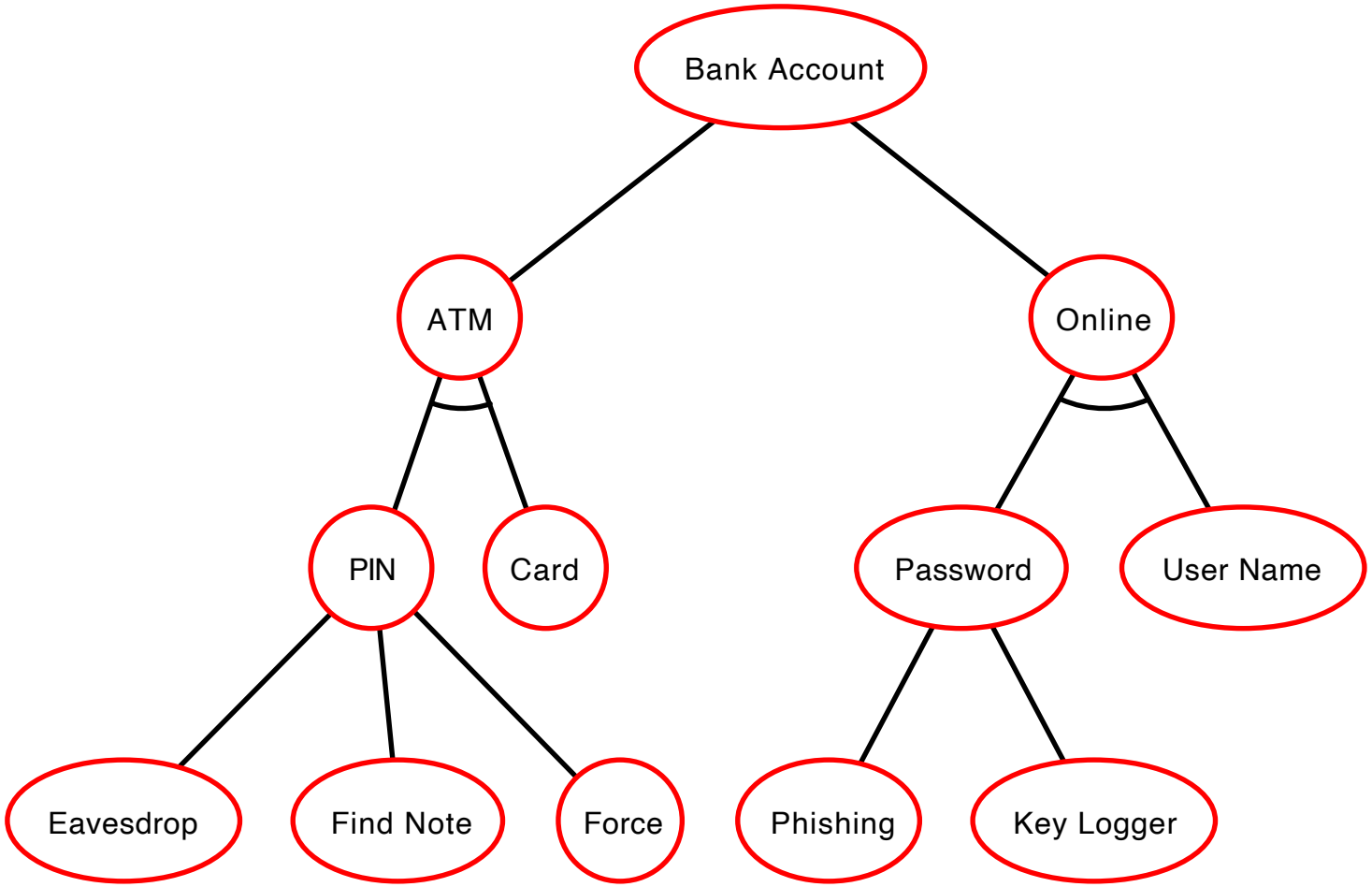
Available for download at https://satoss.uni.lu/members/piotr/adtool/

Manual available at https://satoss.uni.lu/members/piotr/adtool/manual.pdf

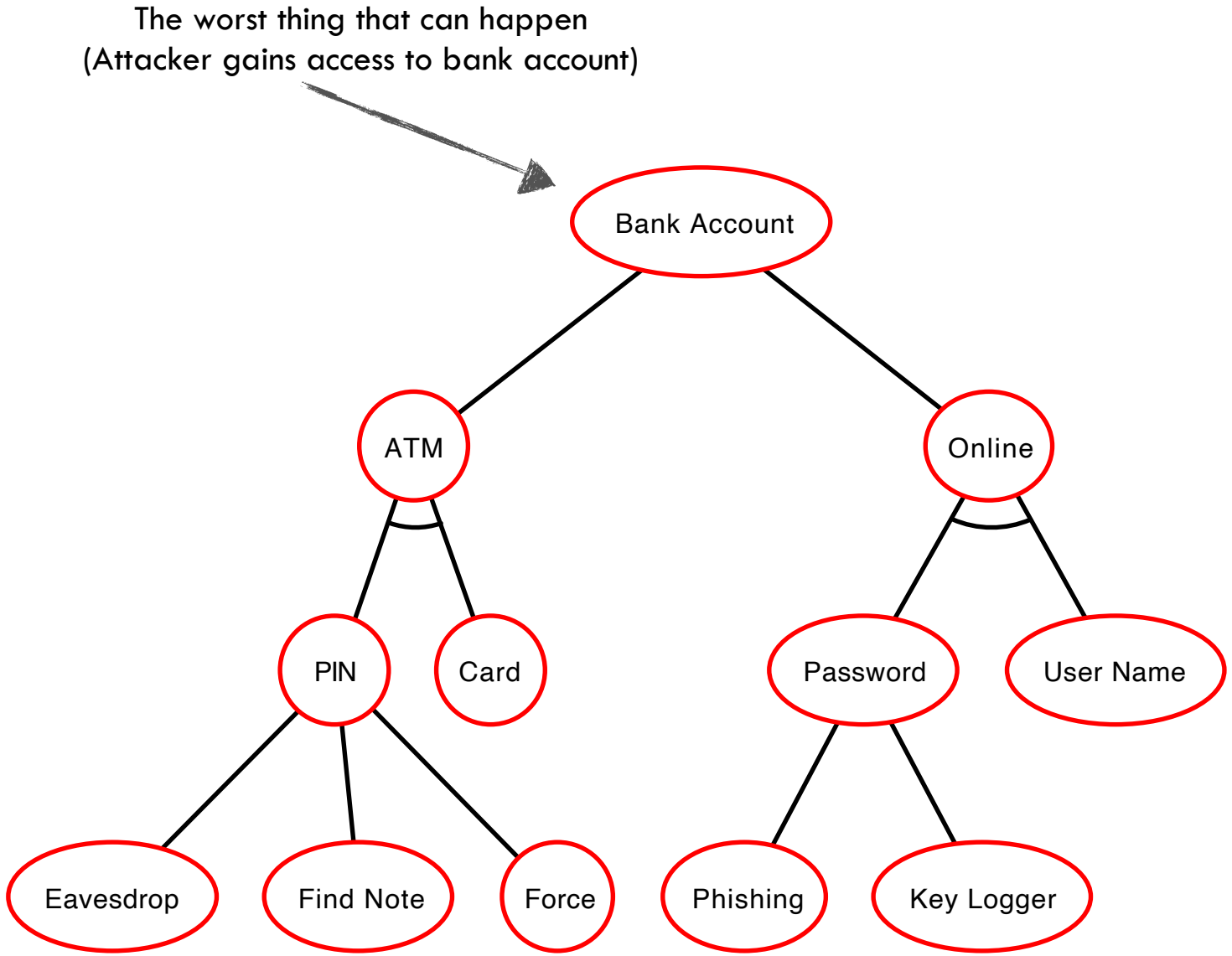
Attack Trees



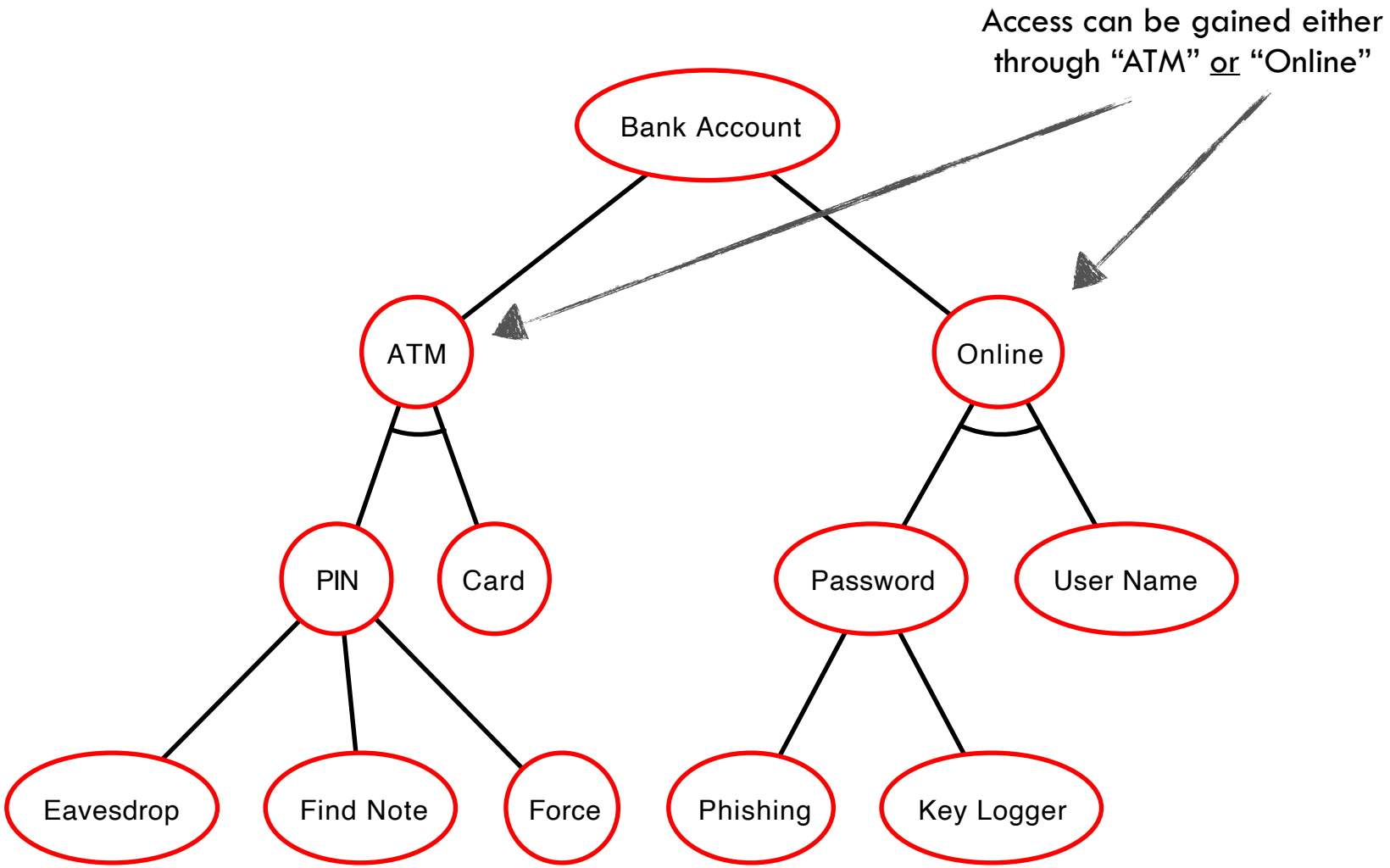
Let's have a look at our first Attack Tree



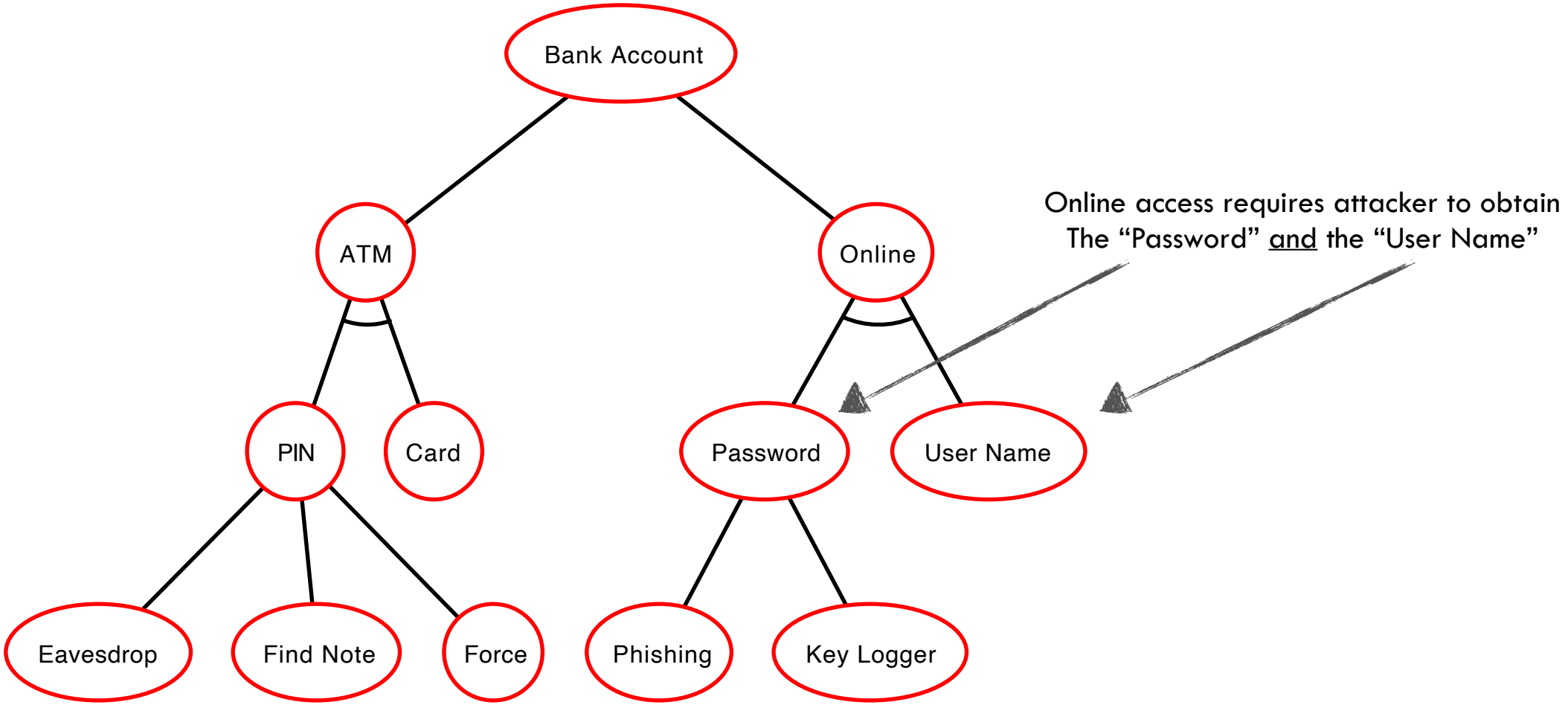
Let's have a look at our first Attack Tree



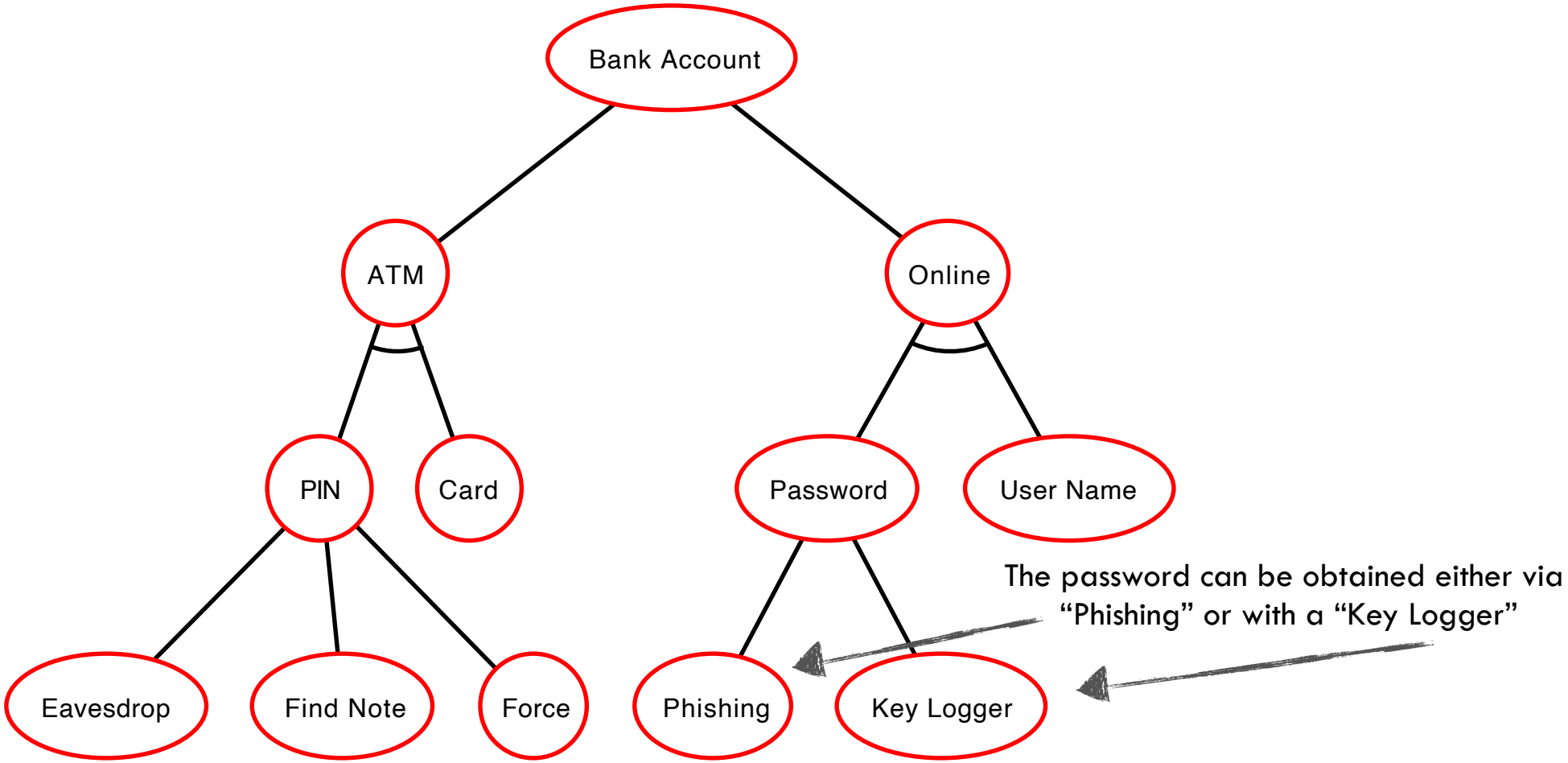
Let's have a look at our first Attack Tree



Let's have a look at our first Attack Tree

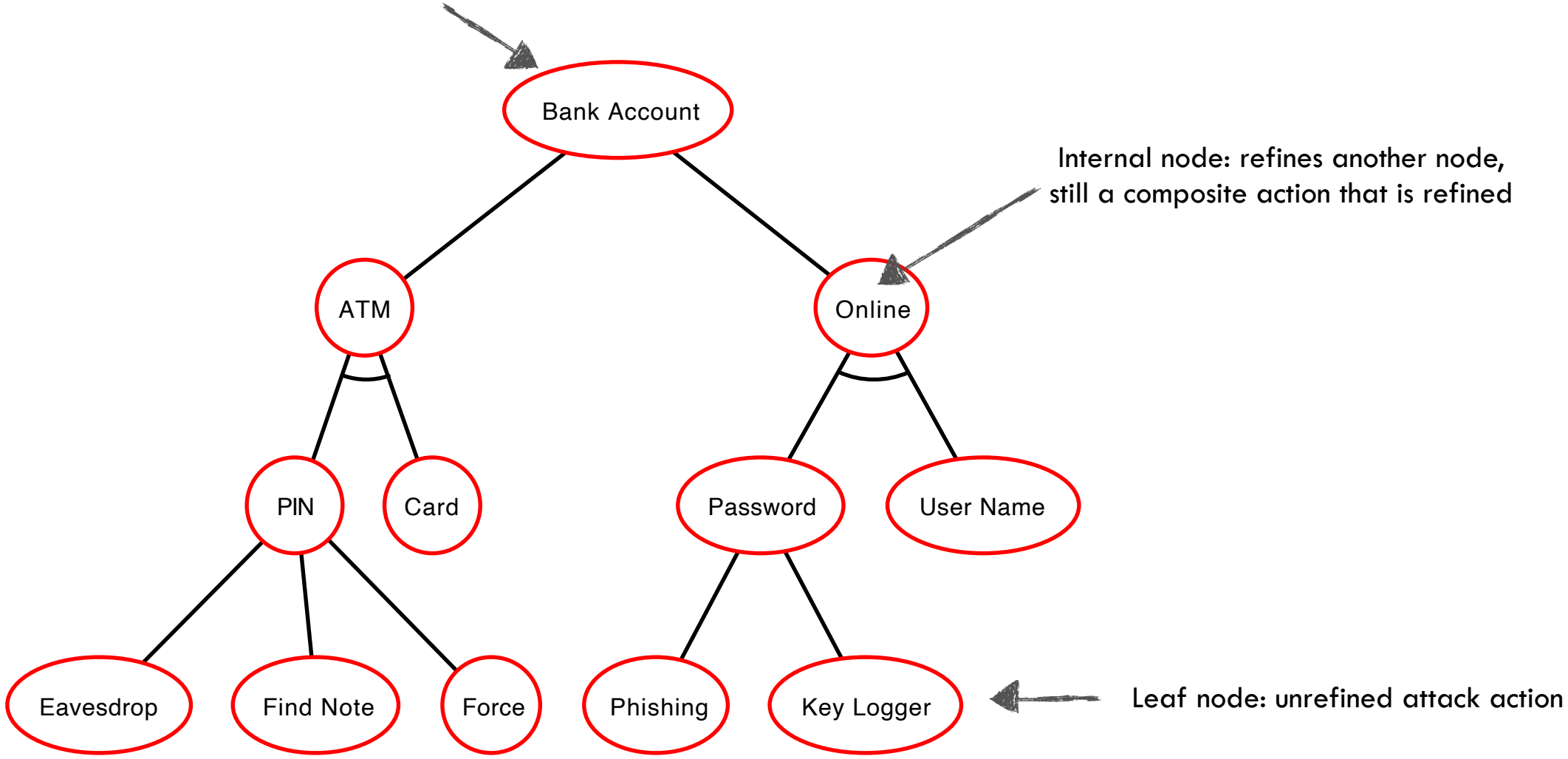


Let's have a look at our first Attack Tree



Attack Tree concepts

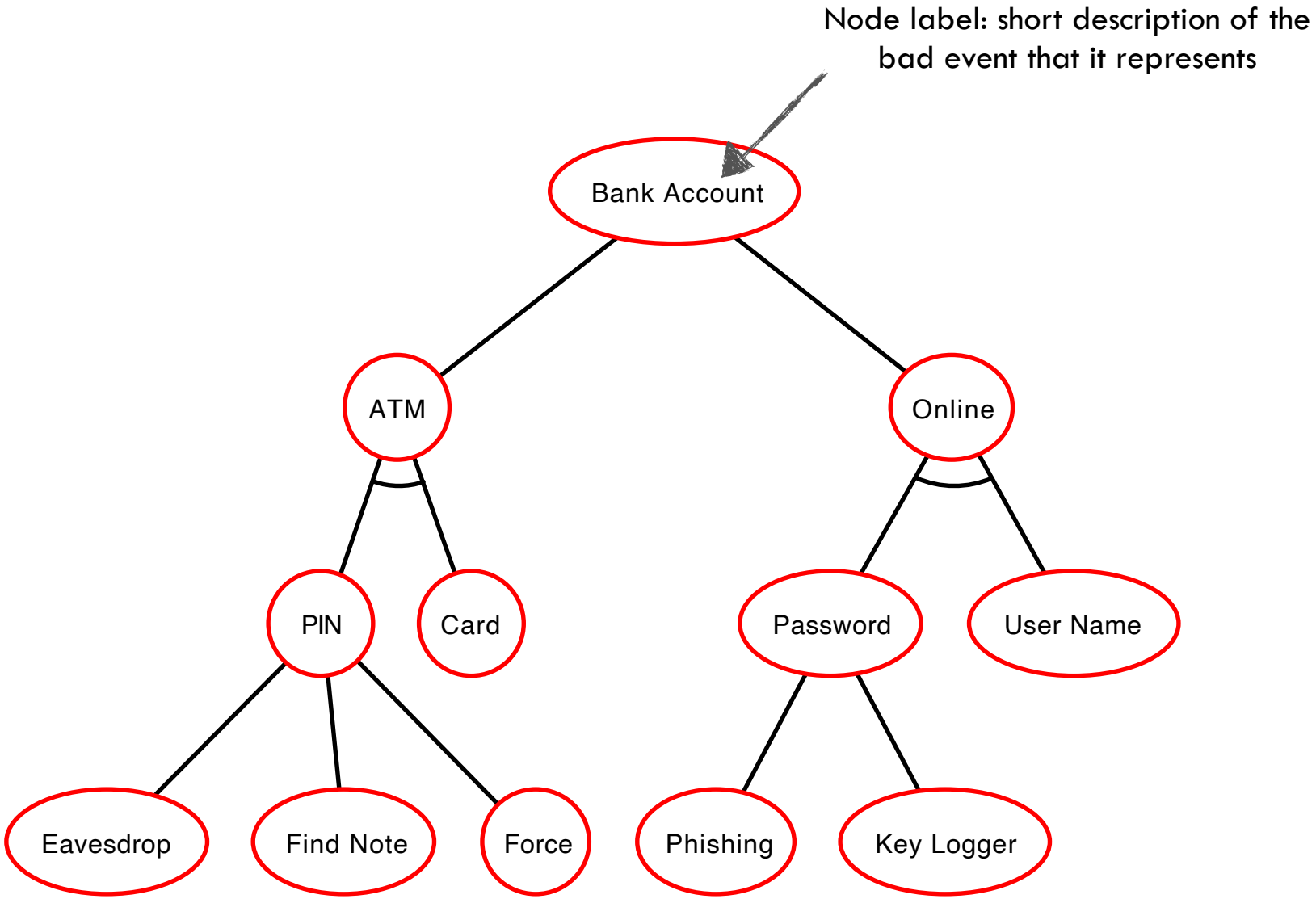
Root: the worst thing that can happen,
a node with no parent



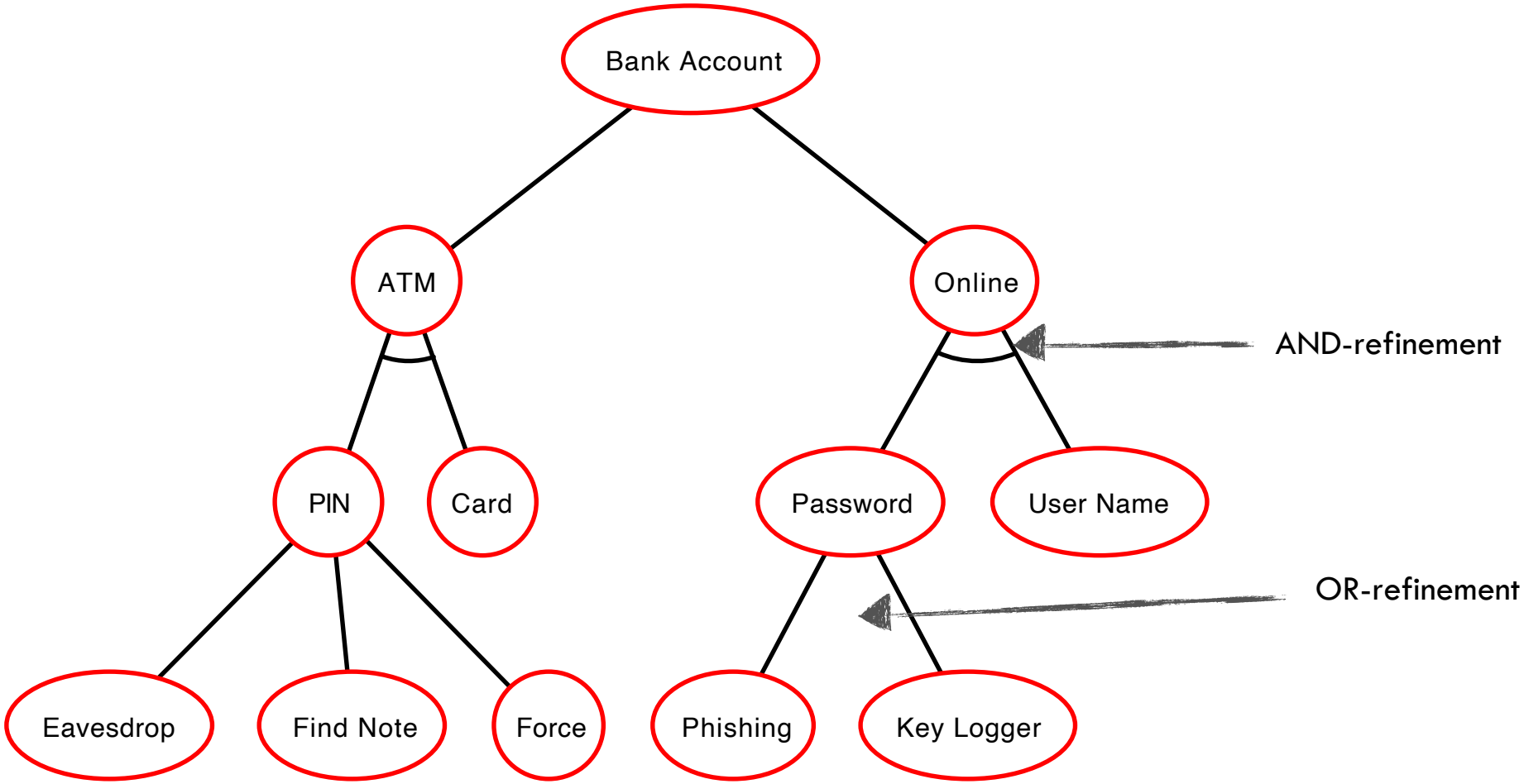
Internal node: refines another node,
still a composite action that is refined

Leaf node: unrefined attack action

Attack Tree concepts

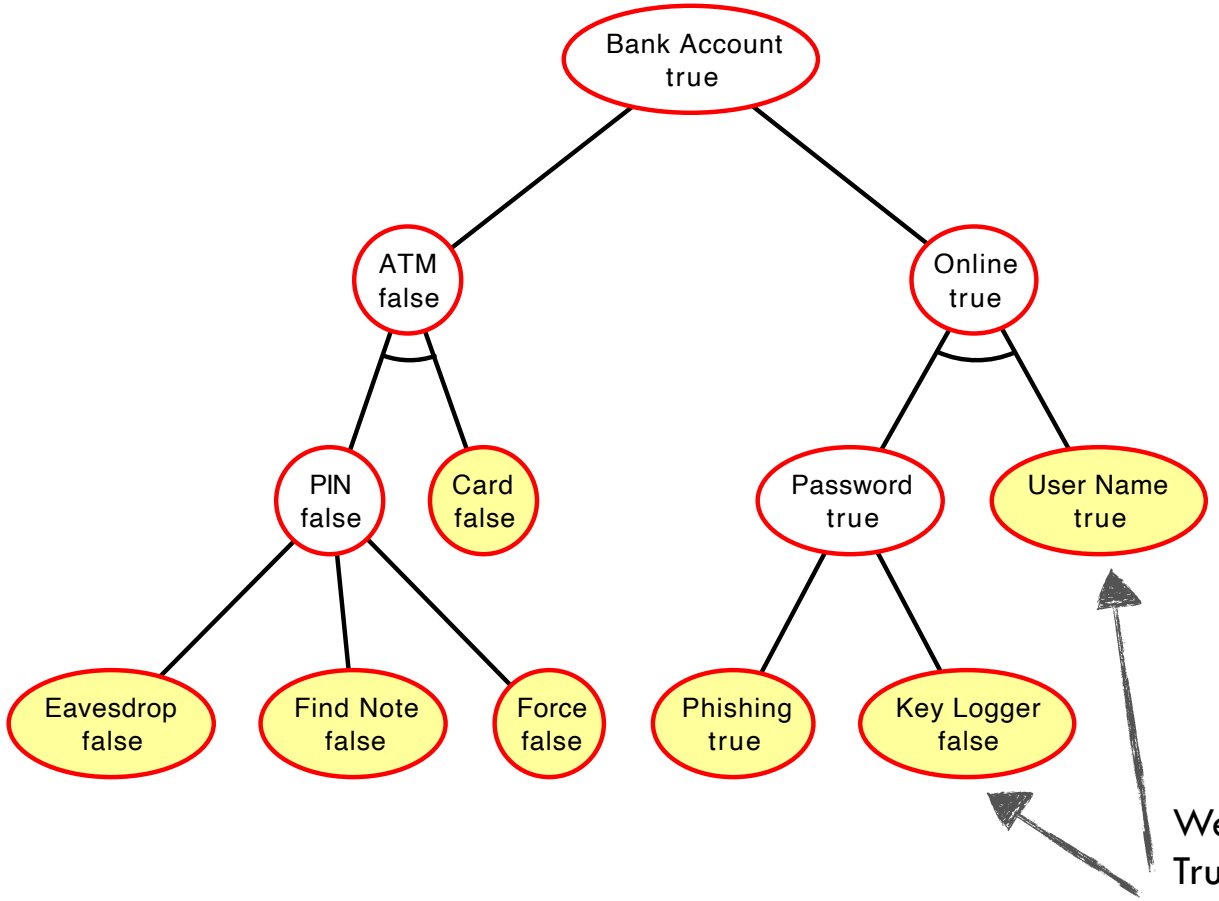


Attack Tree concepts



Attack Feasibility Analysis

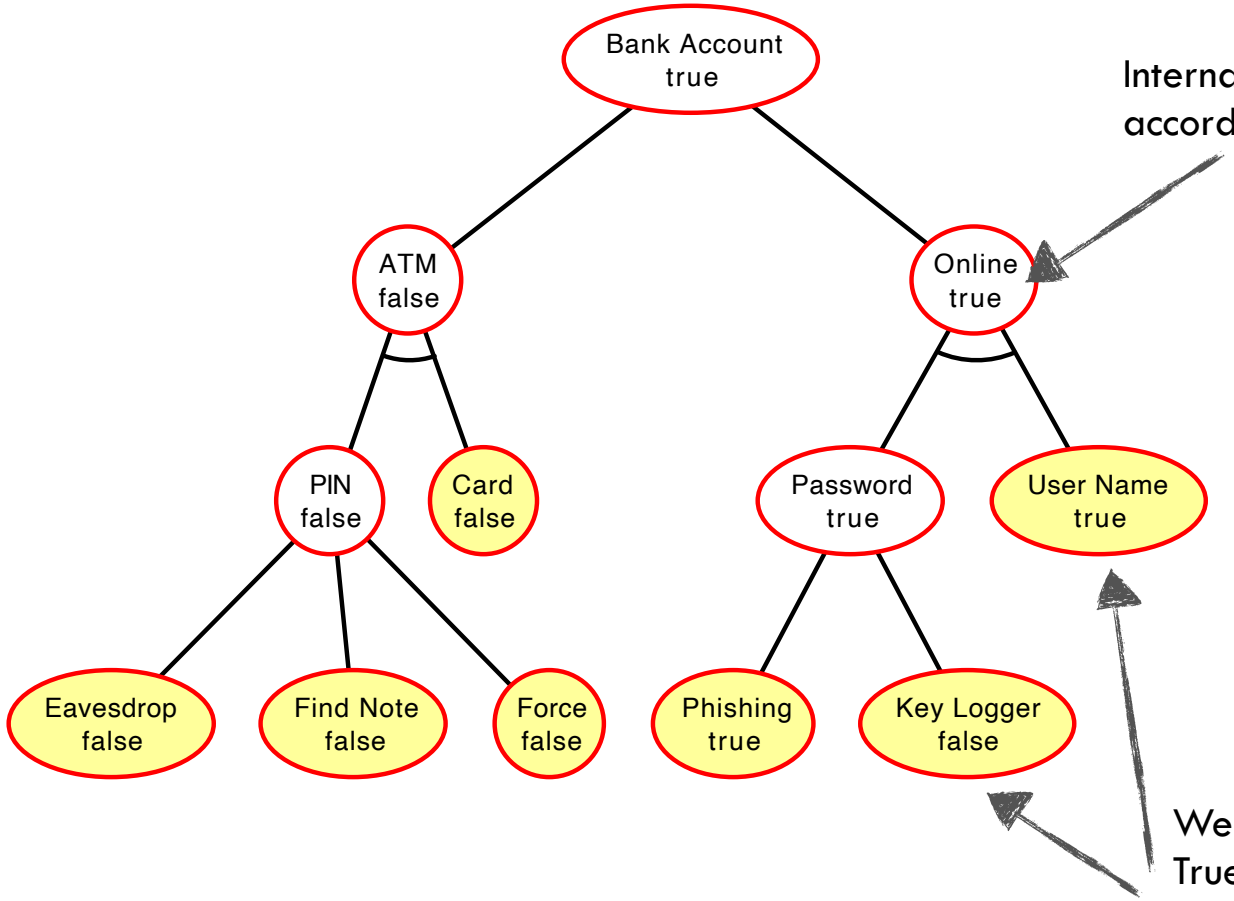
An attack is defined by a set of attack actions. For example {Phishing, User Name}.



We can represent attacks by decorating the actions with True (if the action is part of the attack) or False (otherwise)

Attack Feasibility Analysis

An attack is defined by a set of attack actions. For example {Phishing, User Name}.

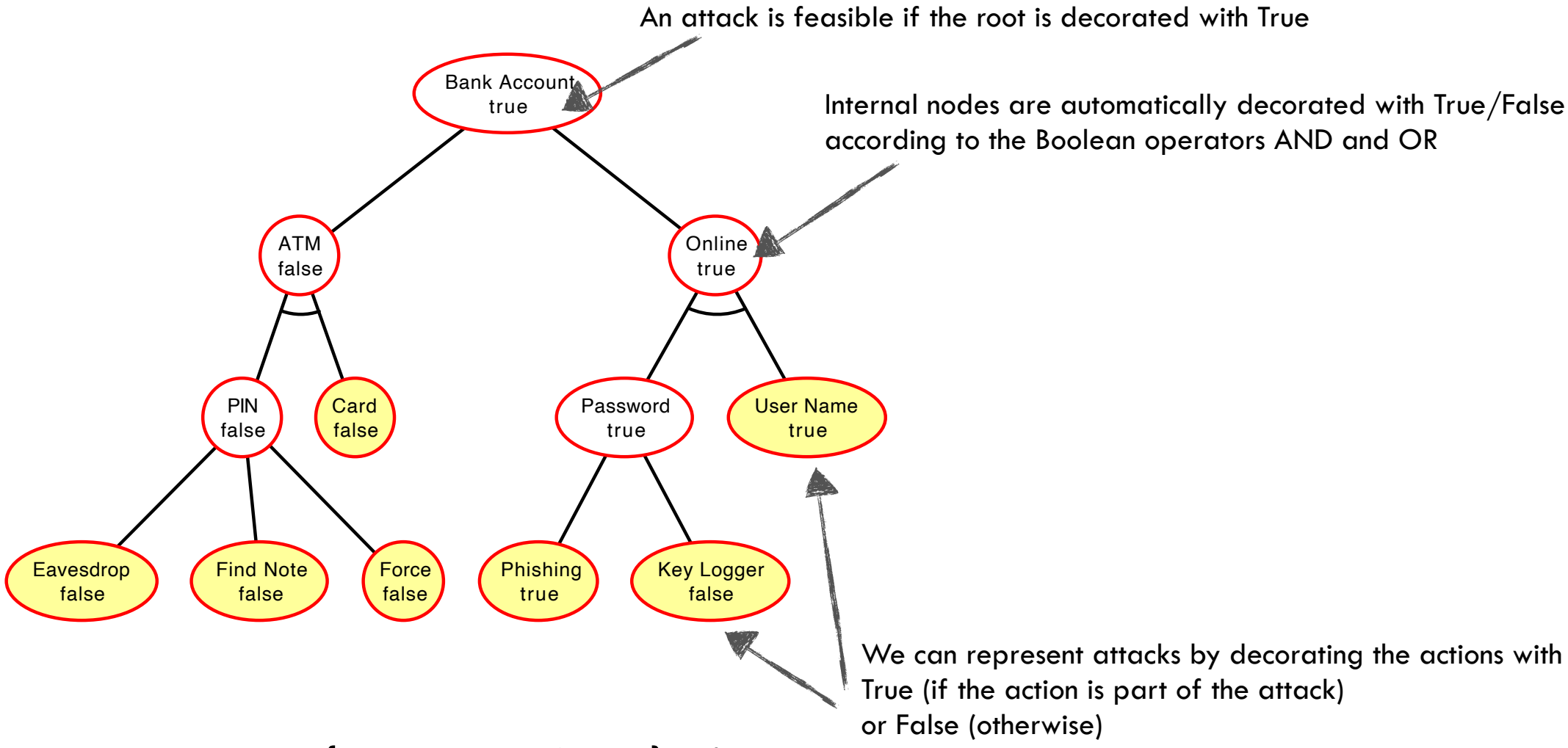


Internal nodes are automatically decorated with True/False according to the Boolean operators AND and OR

We can represent attacks by decorating the actions with True (if the action is part of the attack) or False (otherwise)

Attack Feasibility Analysis

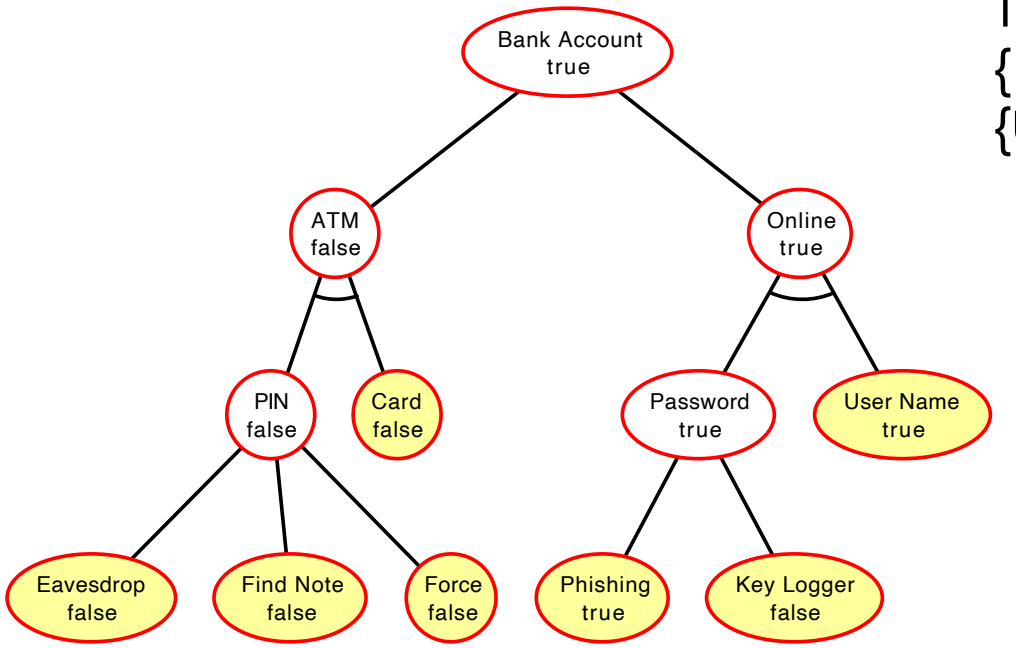
An attack is defined by a set of attack actions. For example {Phishing, User Name}.



The example attack {Phishing, User Name} is feasible

Attack Feasibility Analysis

An feasible attack is minimal if removing any action from it would make it unfeasible.



The example attack {Phishing, User Name} is minimal since
{Phishing} is not feasible
{User Name} is not feasible

Instead, the feasible attack {Phishing, Username, Key Logger} is *not* minimal since removing “Key Logger” results in the feasible attack {Phishing, User Name}.

Attack Tree approach to Threat Modelling

What is allowed?

- Generally speaking, almost nothing is forbidden.
- An Attack Tree can have as many nodes as one wants, as long as it constitutes a tree.
- An Attack Tree can be arbitrarily deep. Every action can be refined.
- Bear in mind usability and the beauty of simplicity.

How are Attack Trees created?

- Attack Trees have to be used as a dialogue tool for a team interested in identifying threat scenarios.
- The guiding questions could be “how could an attacker achieve this?”, “what if…”.
- The structure of the tree guides the dialogue too.

How to get started?

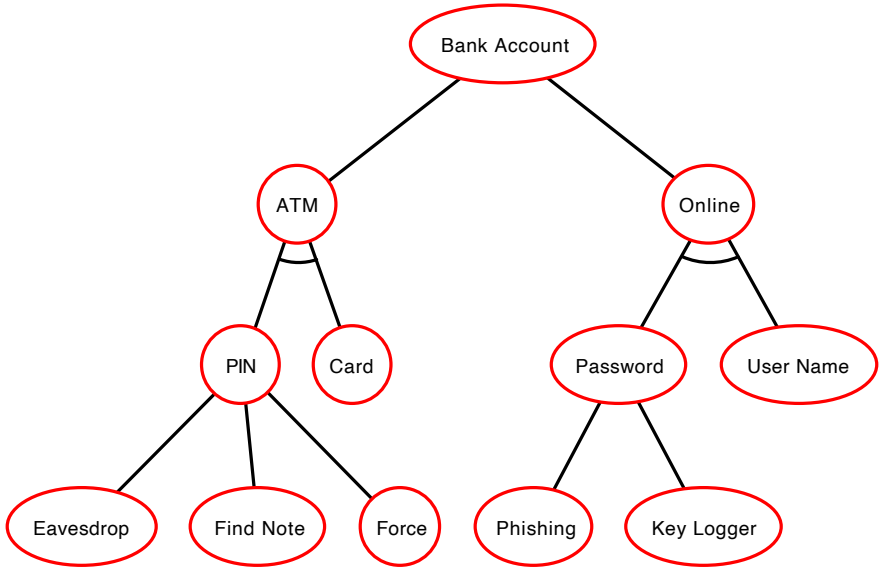
- Ask your self “what is the most valuable asset?”, “what is the worst thing that can happen”
- There are also tools to automatically obtain initial proposals (https://arxiv.org/abs/2302.14479)

When should I do the assessment?

- Modelling and assessment should be done in feedback loops.
- For example, results of the analysis can drive the attention to specific actions to further refine.

EXERCISES

Consider our example Attack Tree.



Exercise A.1. Consider the following sets of attack actions:
a) {Eavesdrop, Find Note, Card}
b) {Eavesdrop, Card}
c) {Eavesdrop, Phishing}
d) {Keylogger, User Name}
For each set, determine if it constitutes a feasible attack.

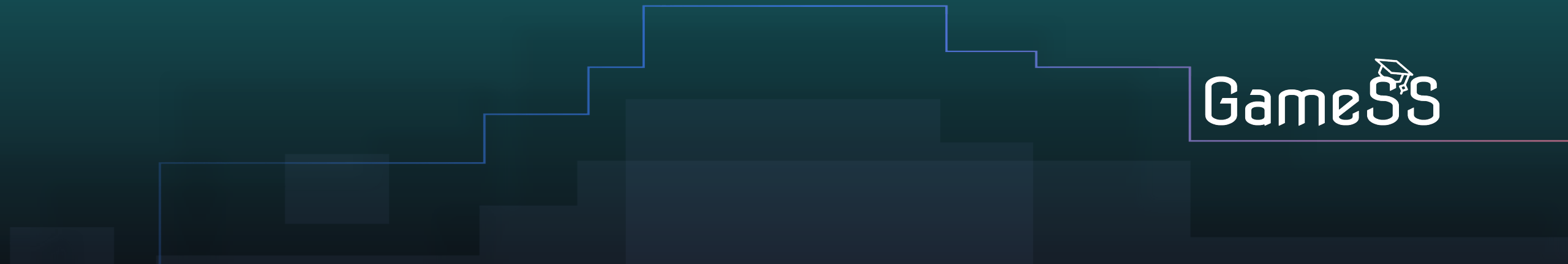
Exercise A.2. List all possible minimal attacks.

Exercise A.3. True or False?
a) Every feasible attack including action “Phishing” includes also the action “User Name”.
b) Every minimal feasible attack including action “Phishing” includes also the action “User Name”.
c) Every minimal feasible attack including action “User Name” includes also the action “Phishing”.

Exercise A.4. Let us assume that the bank decides to implement a second factor authentication as part of the online access. The set of actions {Password, User Name} does not constitute a feasible attack any more. The attacker also needs to perform additional actions. Modify the Attack Tree accordingly.

Hint: use ADTool to check your solutions. Solutions are provided at the end of the slide deck.

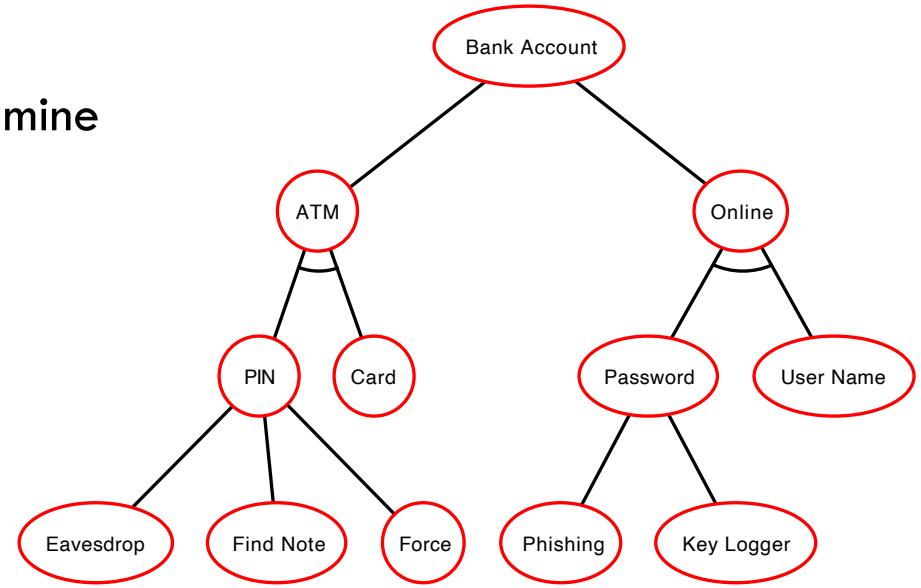
Attack Trees with Costs



Attack Cost Analysis

We have seen so far that we can analyse Attack tree to determine

- What are attacks are feasible?
- What attacks are minimal?



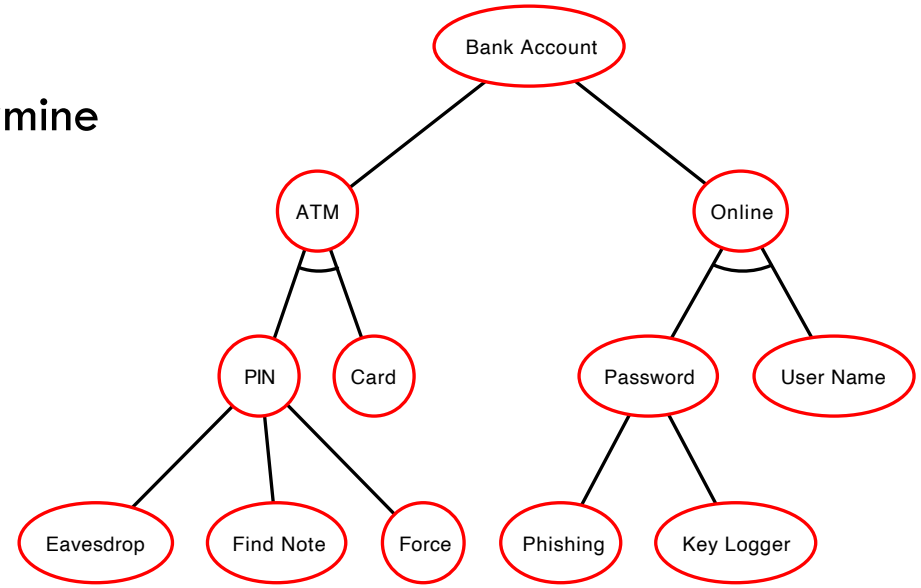
Attack Cost Analysis

We have seen so far that we can analyse Attack tree to determine

- What are attacks are feasible?
- What attacks are minimal?

Another interesting question would be

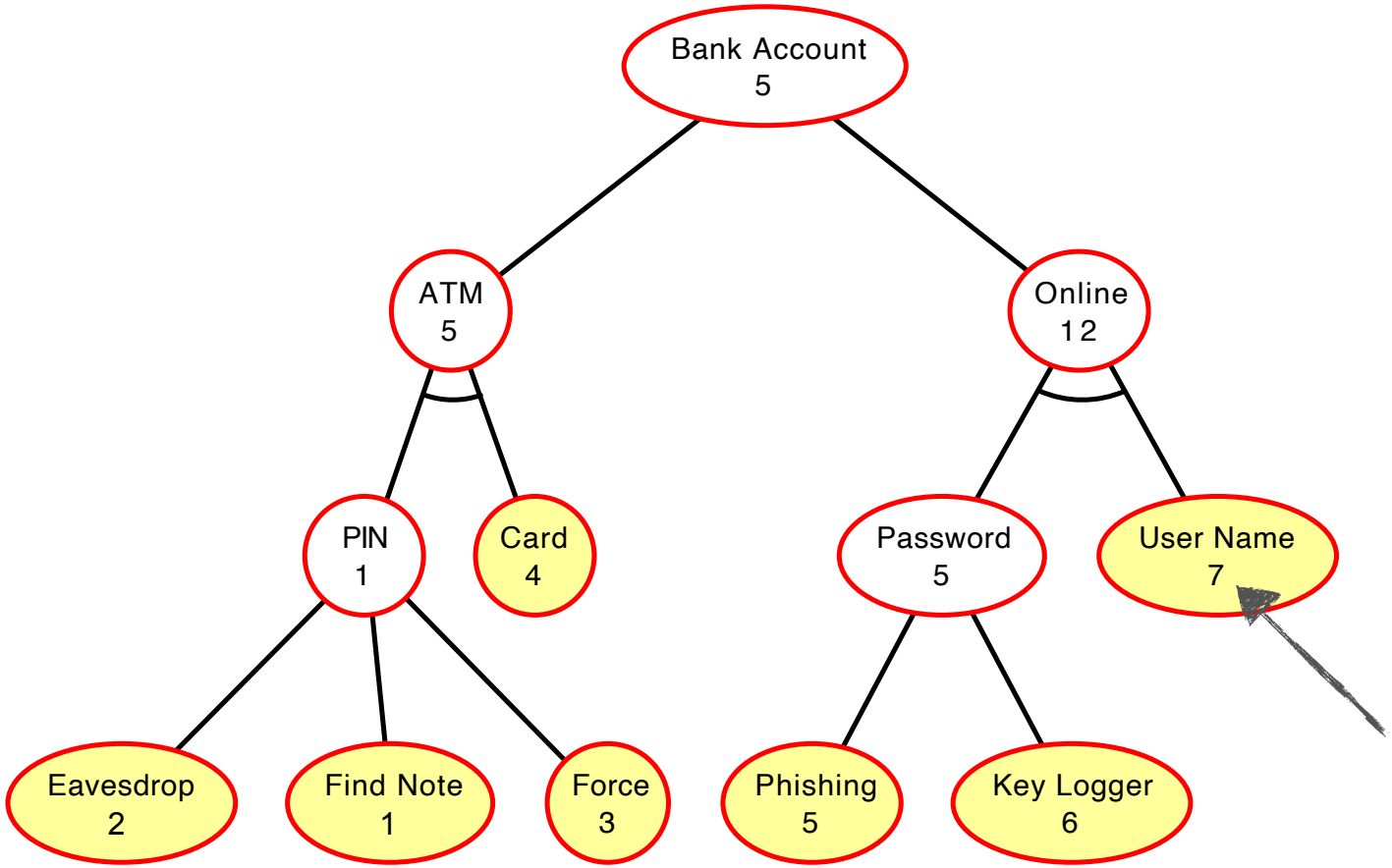
- What is the cheapest attack?
- What attacks have cost higher than a certain amount (e.g. the potential benefit for an attacker)?



To support this kind of analysis, Attack Trees can be enriched with cost annotations.

Attack Tree with costs

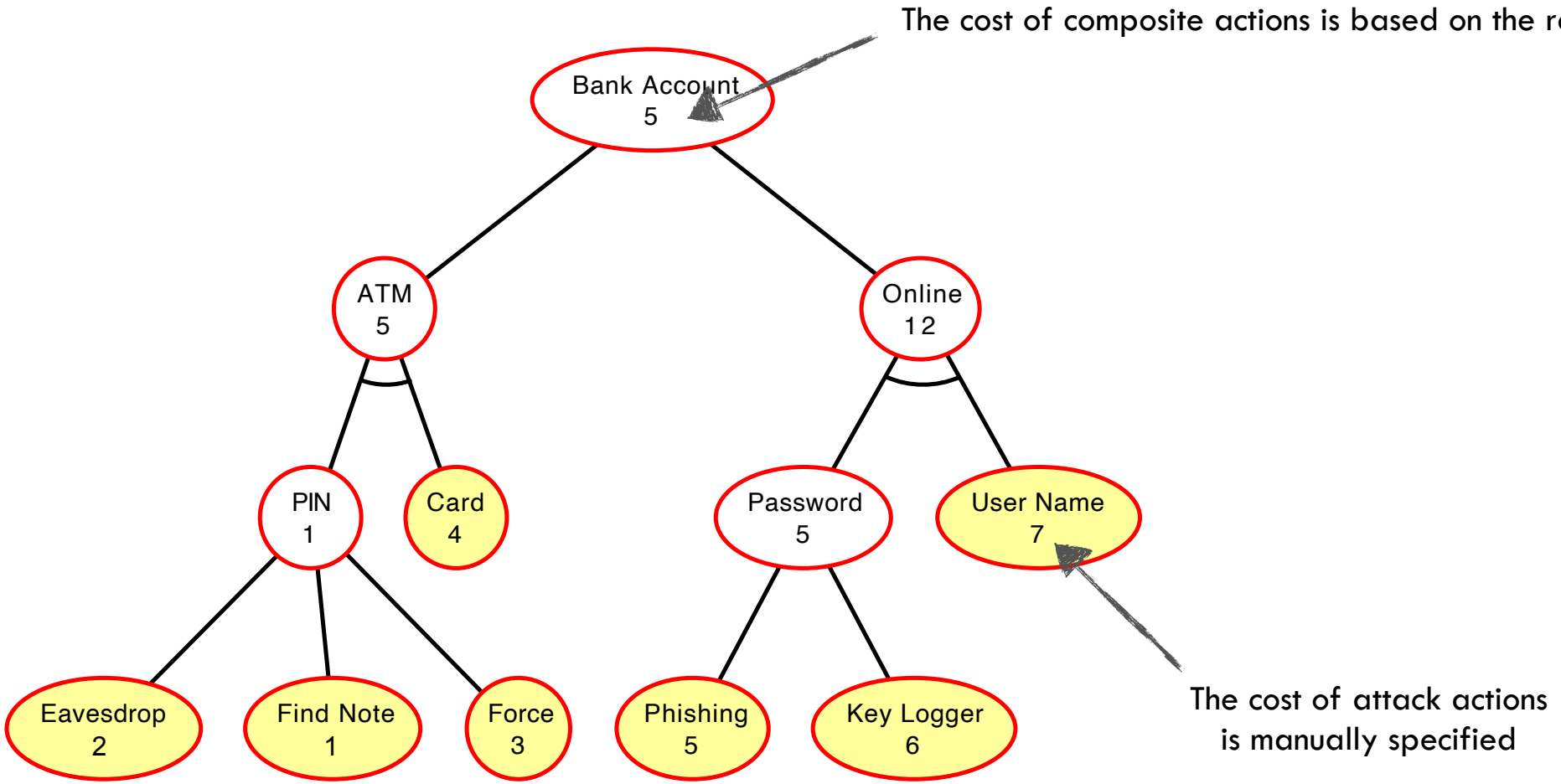
Each node of the Attack Tree is now decorated with a number, representing cost.



The cost of attack actions is manually specified

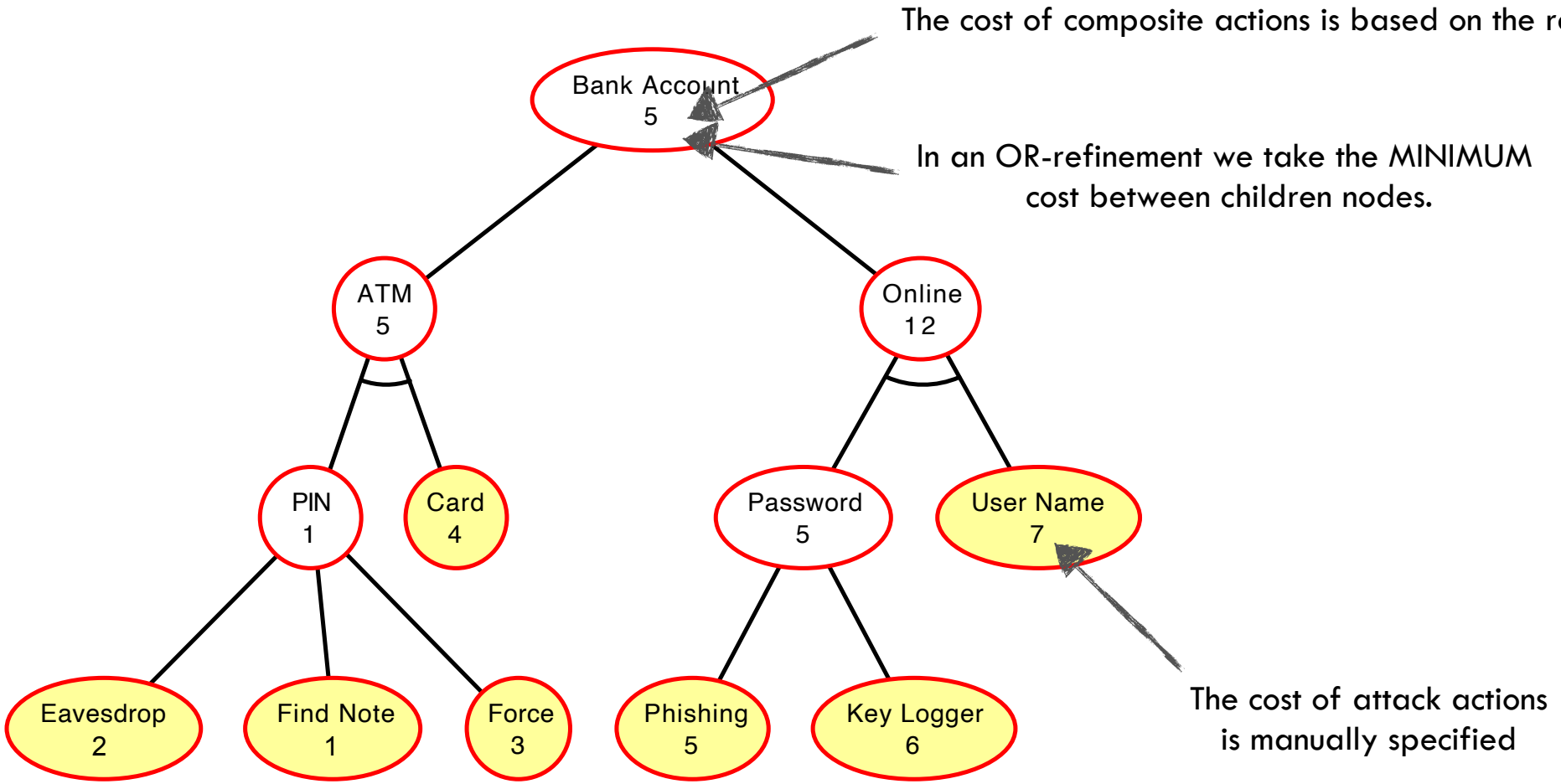
Attack Tree with costs

Each node of the Attack Tree is now decorated with a number, representing cost.



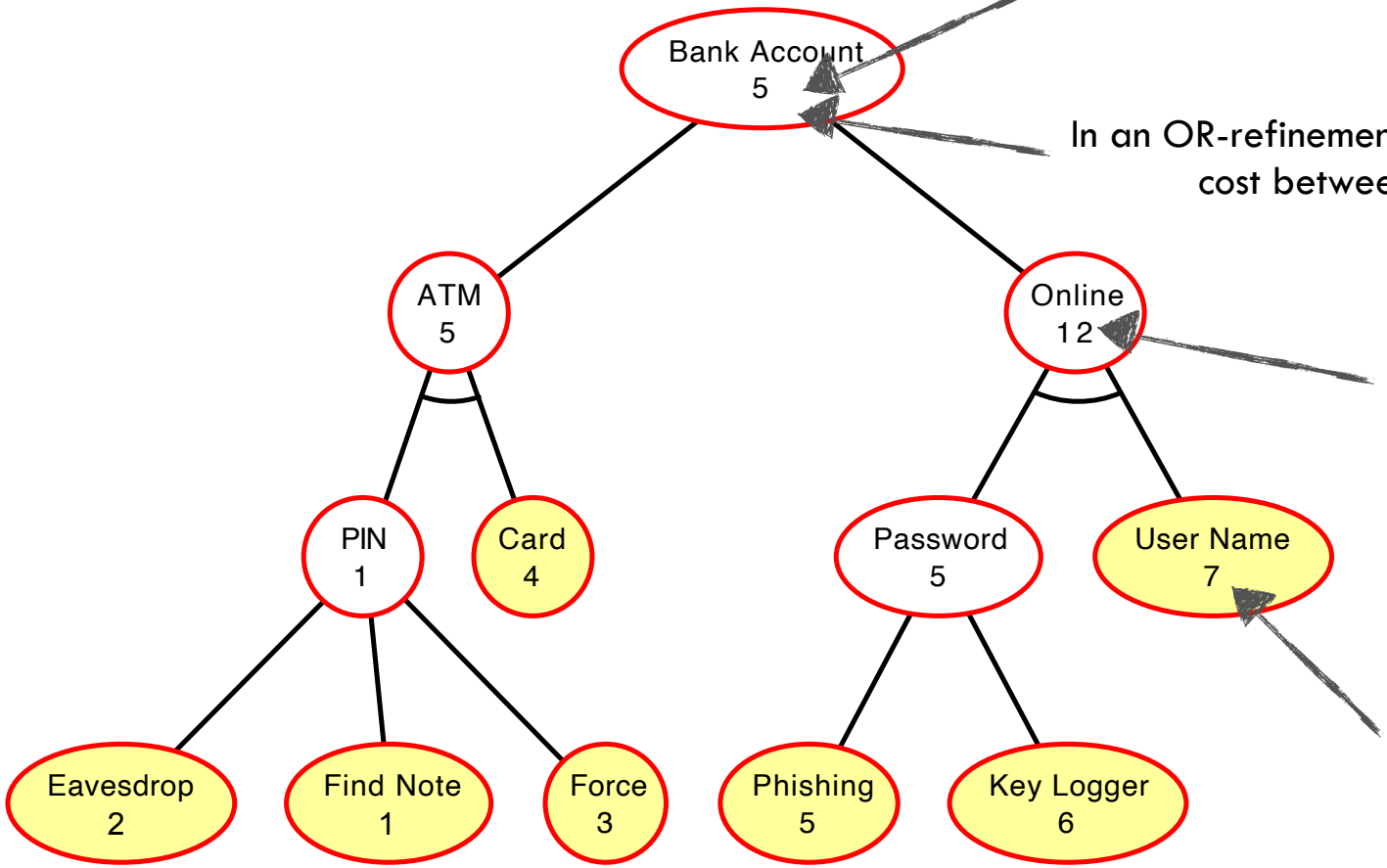
Attack Tree with costs

Each node of the Attack Tree is now decorated with a number, representing cost.



Attack Tree with costs

Each node of the Attack Tree is now decorated with a number, representing cost.



The cost of composite actions is based on the refinement.

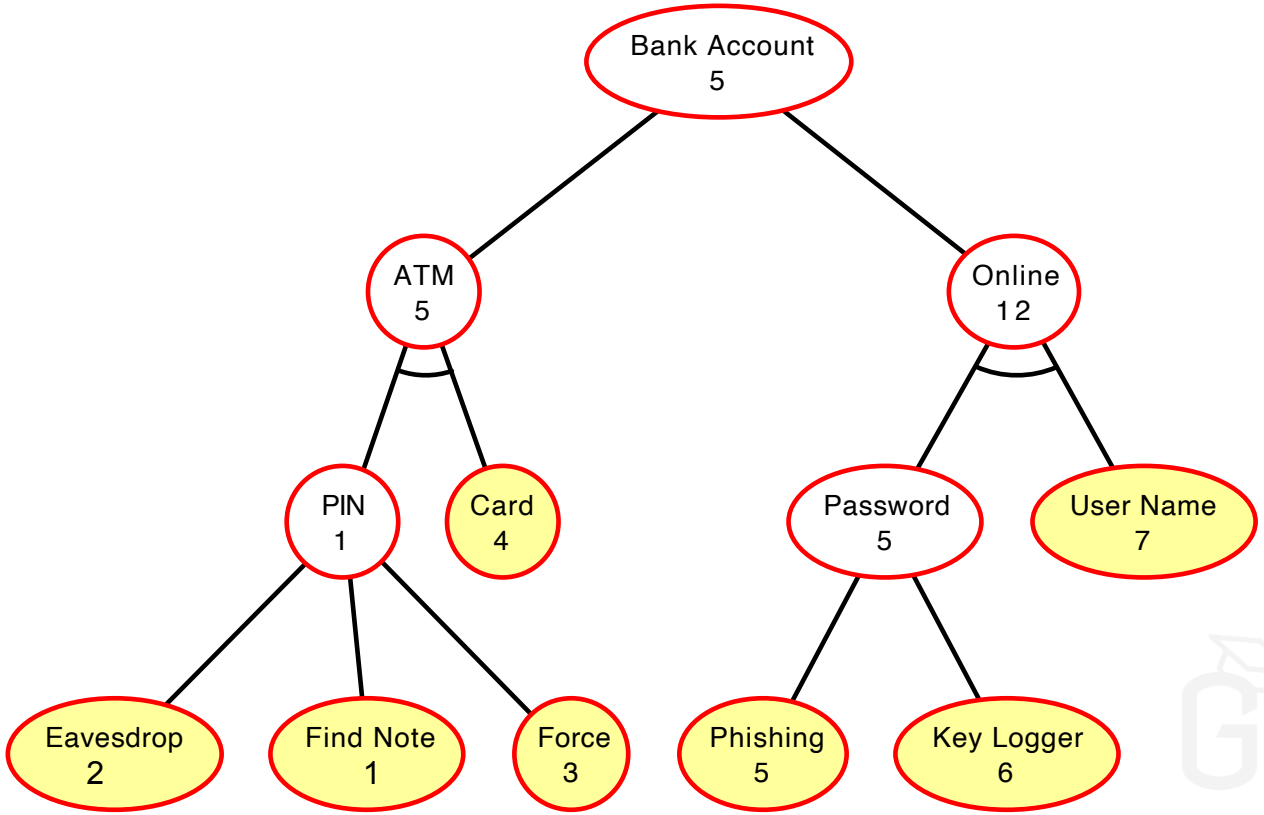
In an OR-refinement we take the MINIMUM cost between children nodes.

In an AND-refinement we take the SUM of the cost of the children nodes

The cost of attack actions is manually specified

Minimal Cost Analysis

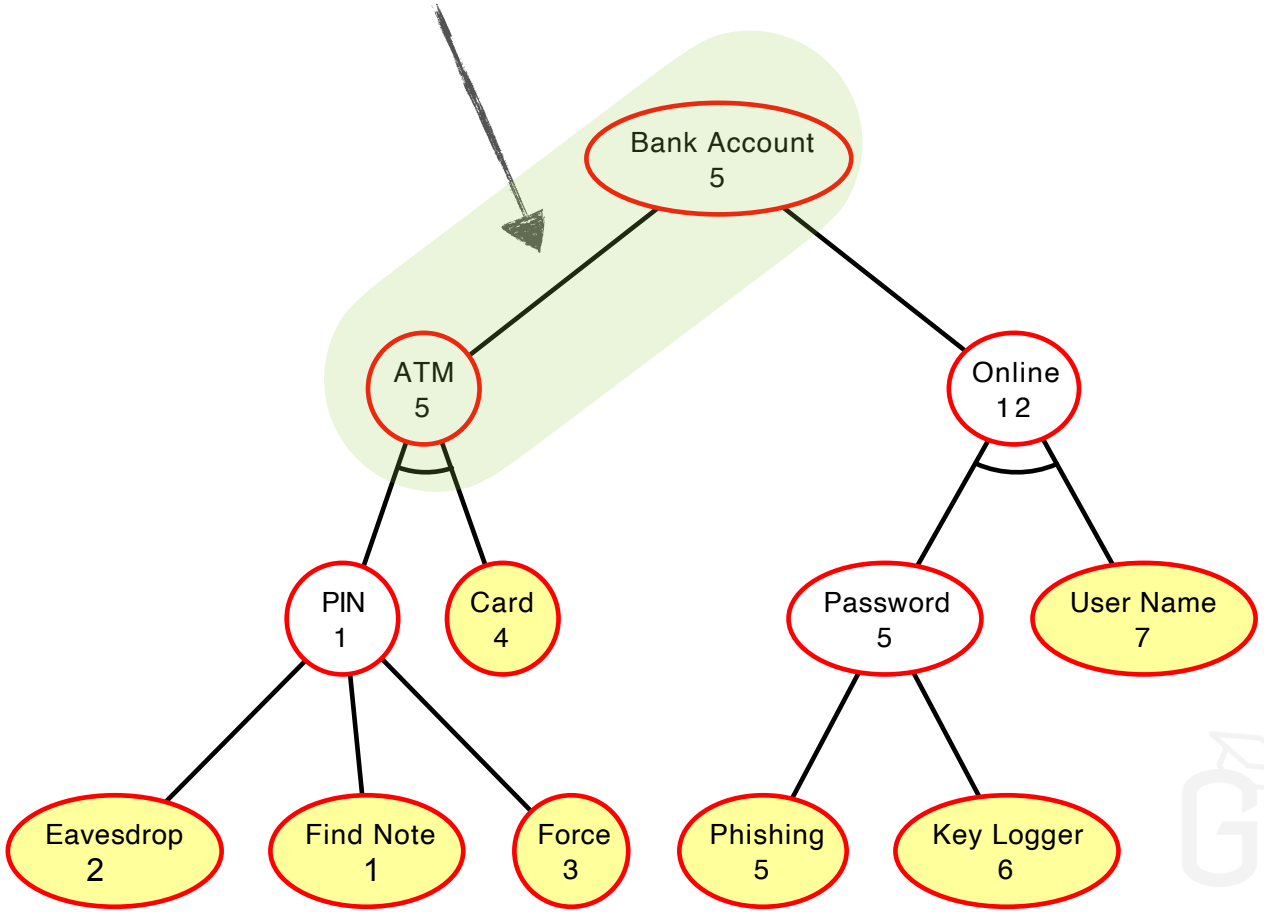
To determine the cheapest attack, we can use the cost-annotated Attack Tree:



Minimal Cost Analysis

To determine the cheapest attack, we can use the cost-annotated Attack Tree:

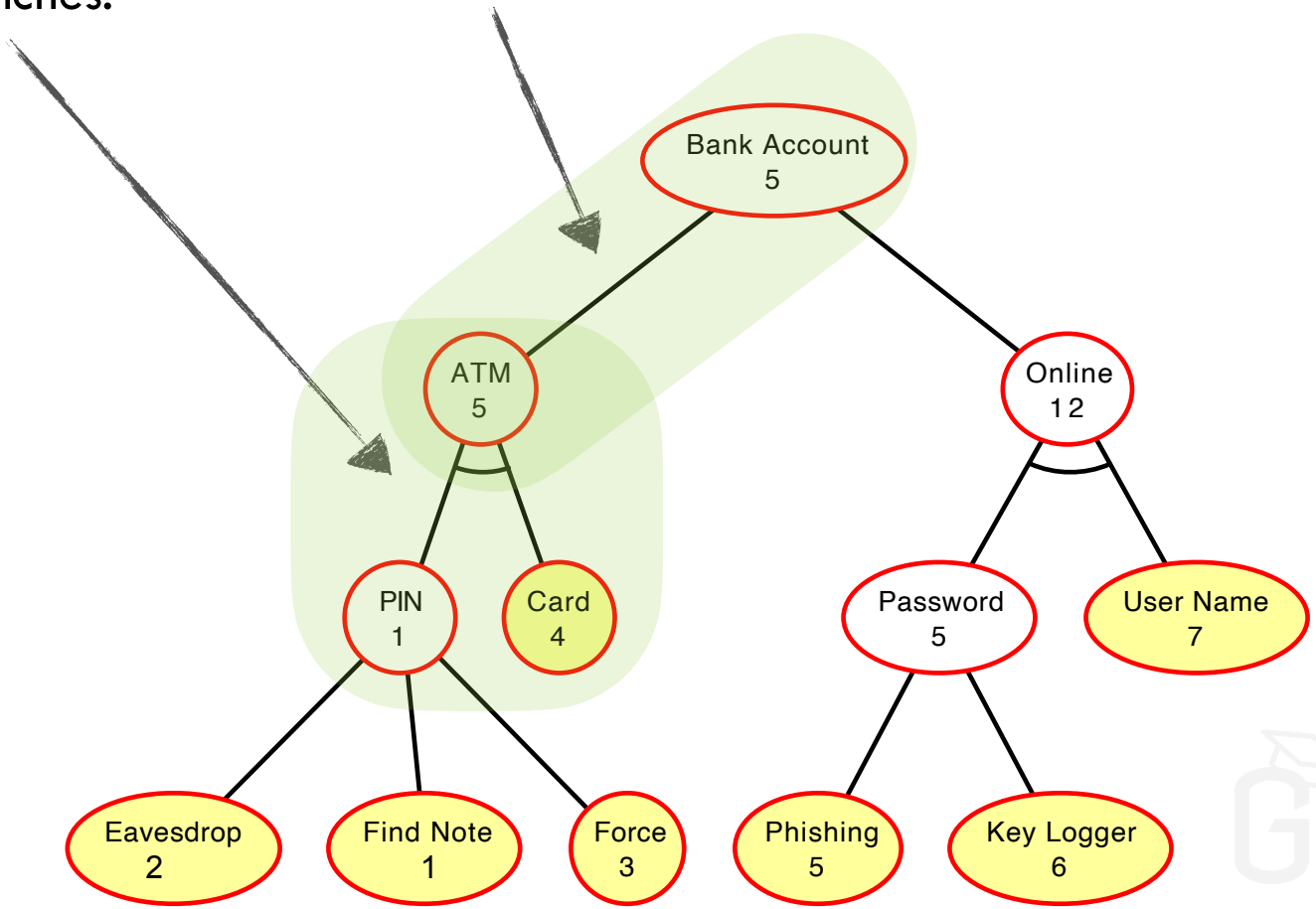
- In a node refined with OR, take a branch that provided minimal cost



Minimal Cost Analysis

To determine the cheapest attack, we can use the cost-annotated Attack Tree:

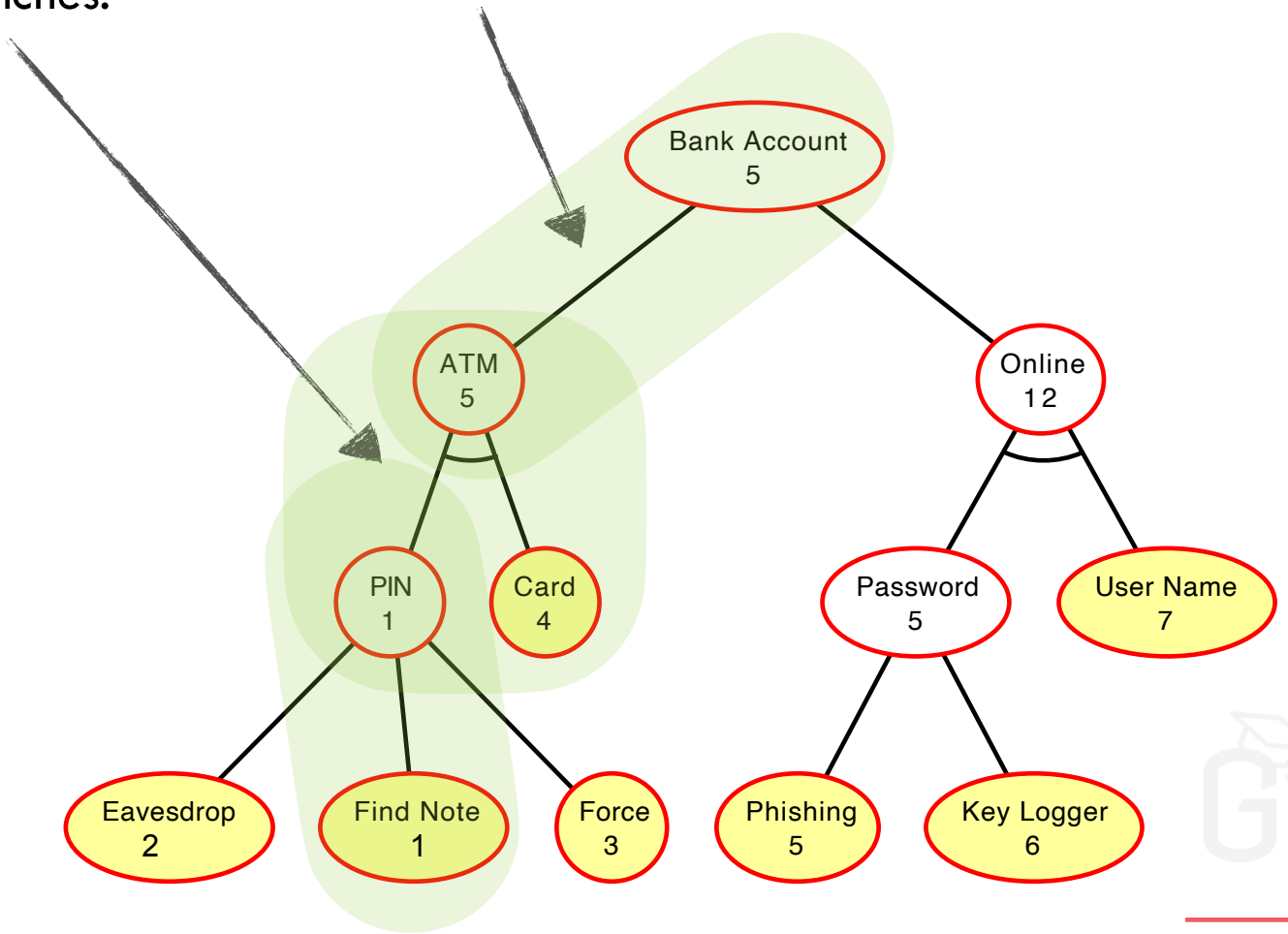
- In a node refined with OR, take a branch that provided minimal cost
- In a node refined with AND, take both branches.



Minimal Cost Analysis

To determine the cheapest attack, we can use the cost-annotated Attack Tree:

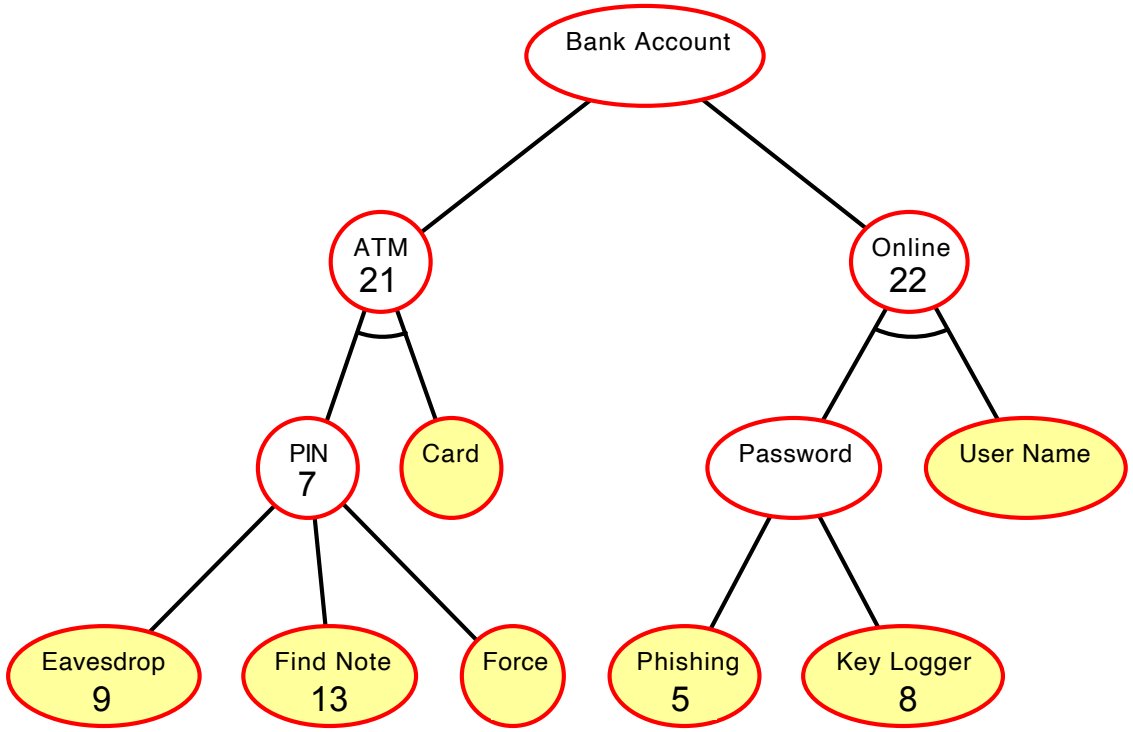
- In a node refined with OR, take a branch that provided minimal cost
- In a node refined with AND, take both branches.



In the example, the cheapest attack is {Find Note, Card}. The cost is 5.

EXERCISES

Consider the example Attack Tree on the right.



Exercise B.1. Complete the Attack Tree by adding the missing costs.

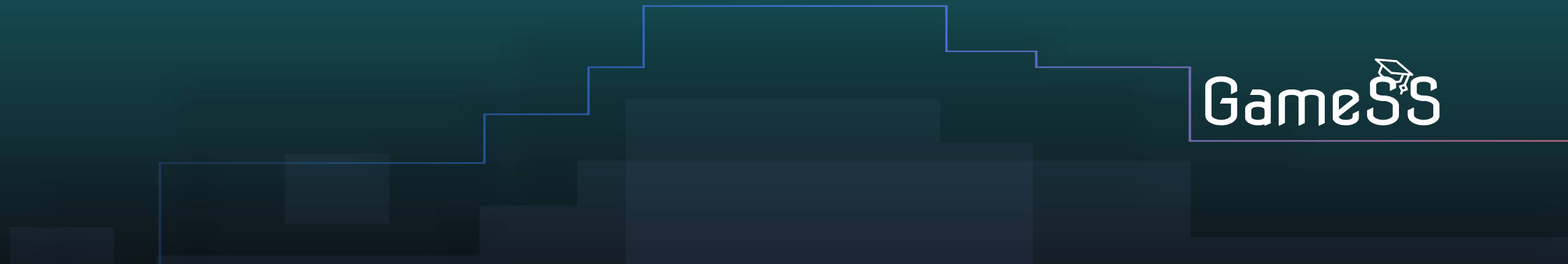
Exercise B.2. Which is the cheapest attack?

Exercise B.3. True or False?

a) Every Attack Tree has exactly one cheapest attack.
b) In general, the cost of a feasible attack is greater than the most costly action in the tree.
c) In general, the cost of a feasible attack is greater than the most costly action in the attack.
d) In general, the cheapest attack is cheaper than the sum of all attack actions.

Hint: use ADTool to check your solutions. Solutions are provided at the end of the slide deck.

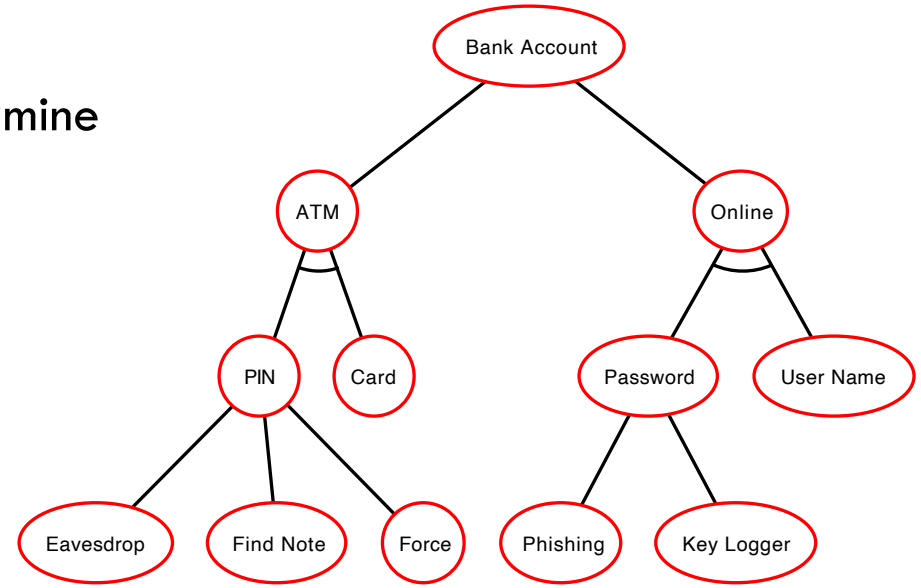
Attack Trees with Probabilities



Attack Probability Analysis

We have seen so far that we can analyse Attack tree to determine

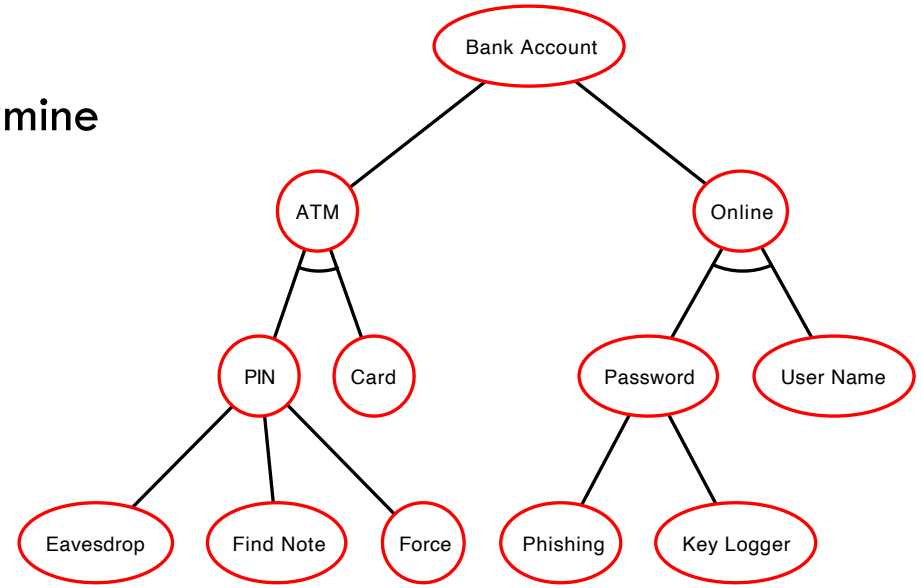
- What are attacks are feasible?
- What attacks are minimal?
- What is the cheapest attack?



Attack Probability Analysis

We have seen so far that we can analyse Attack tree to determine

- What are attacks are feasible?
- What attacks are minimal?
- What is the cheapest attack?



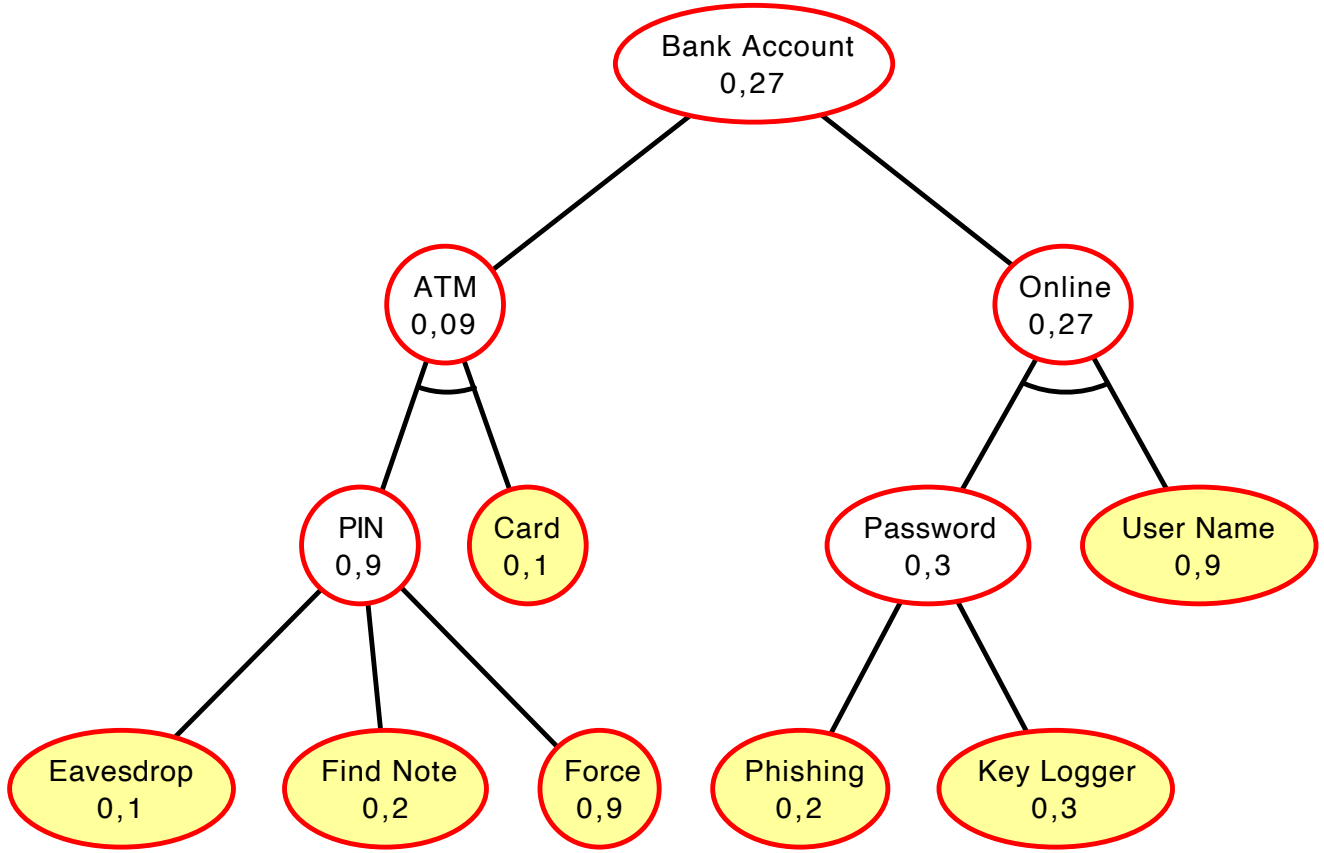
Another interesting question would be

- What attacks have higher probability?

To support this kind of analysis, Attack Trees can be enriched with probabilities.

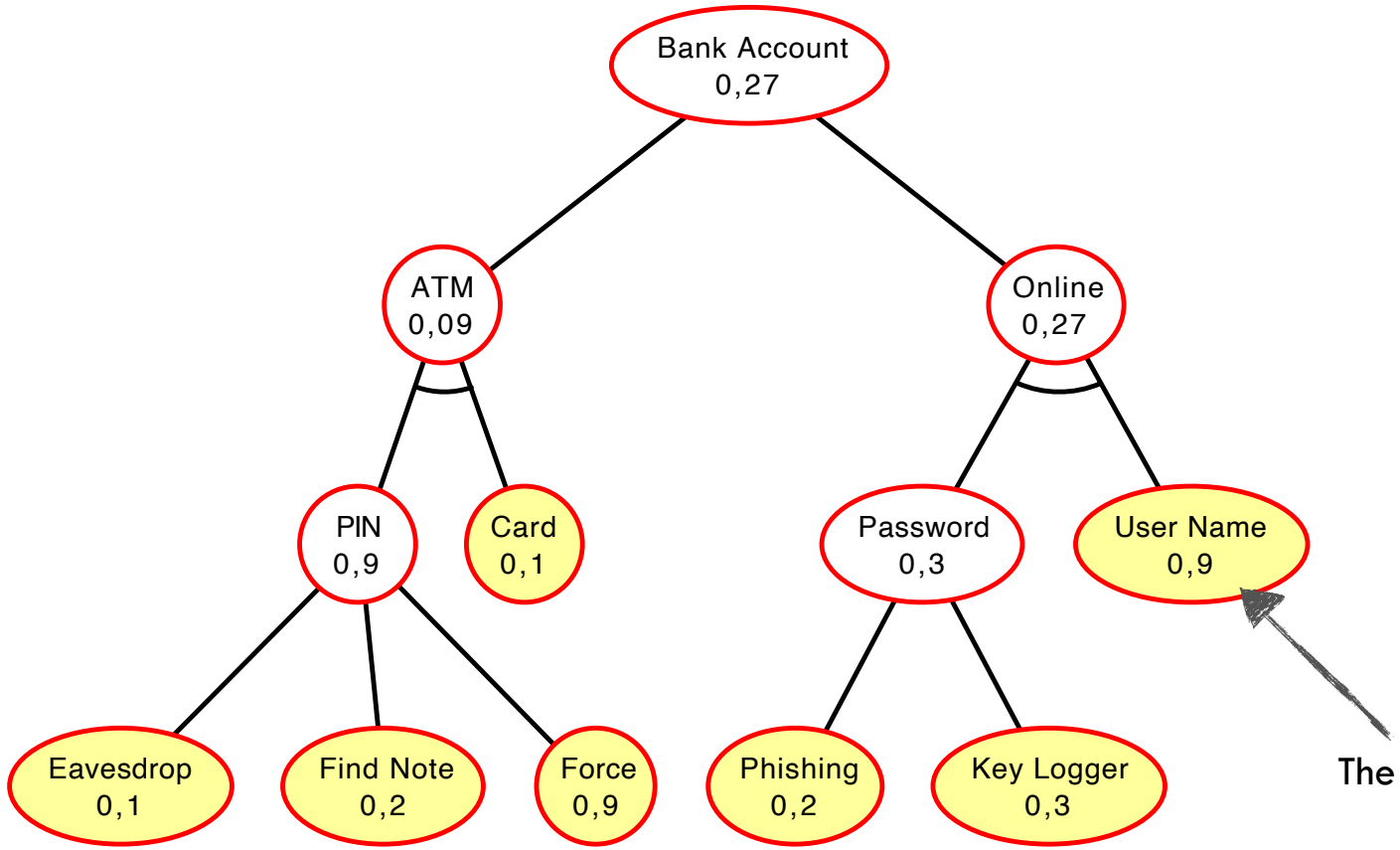
Attack Tree with probabilities

Each node of the Attack Tree is now decorated with a number, representing success probability.



Attack Tree with probabilities

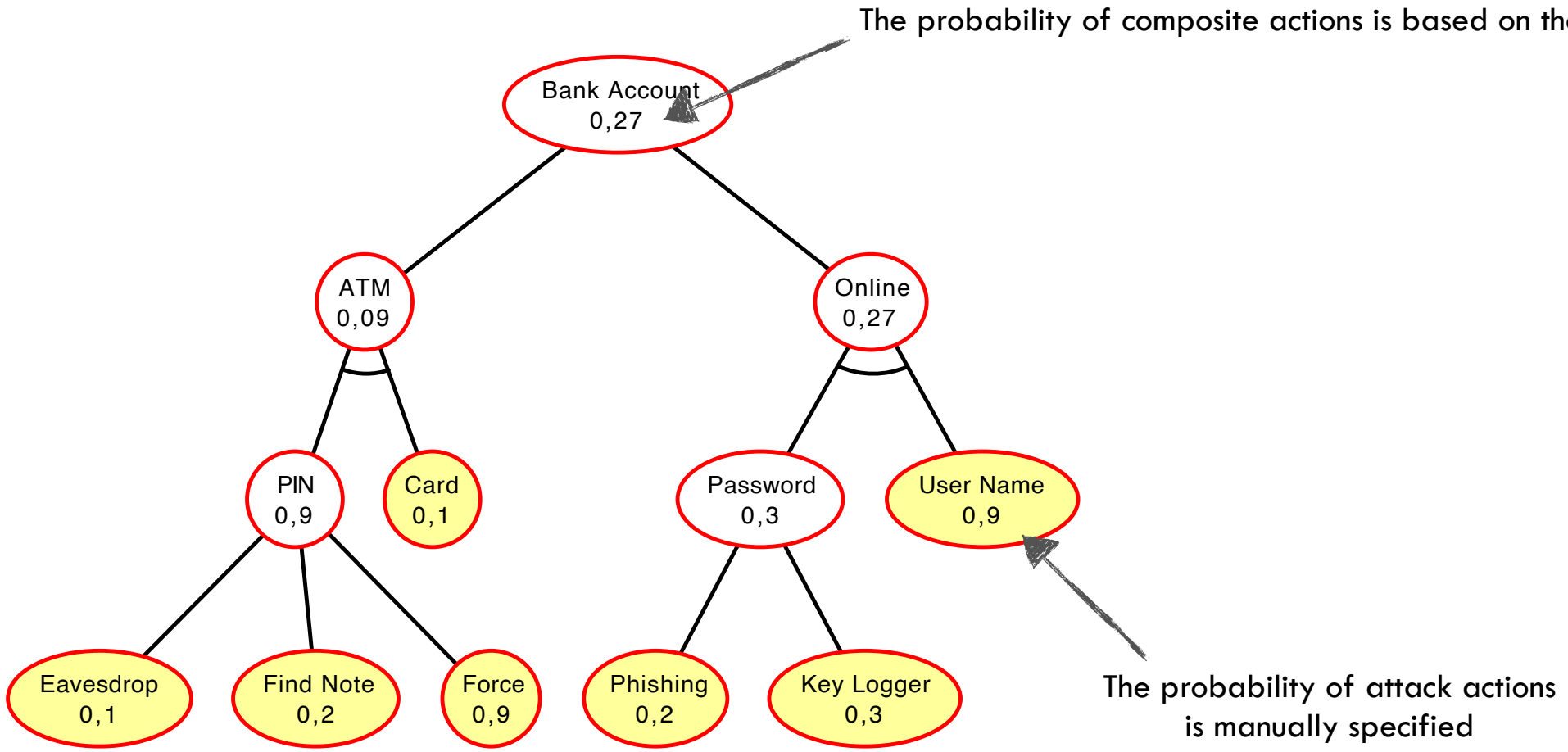
Each node of the Attack Tree is now decorated with a number, representing success probability.



The probability of attack actions is manually specified

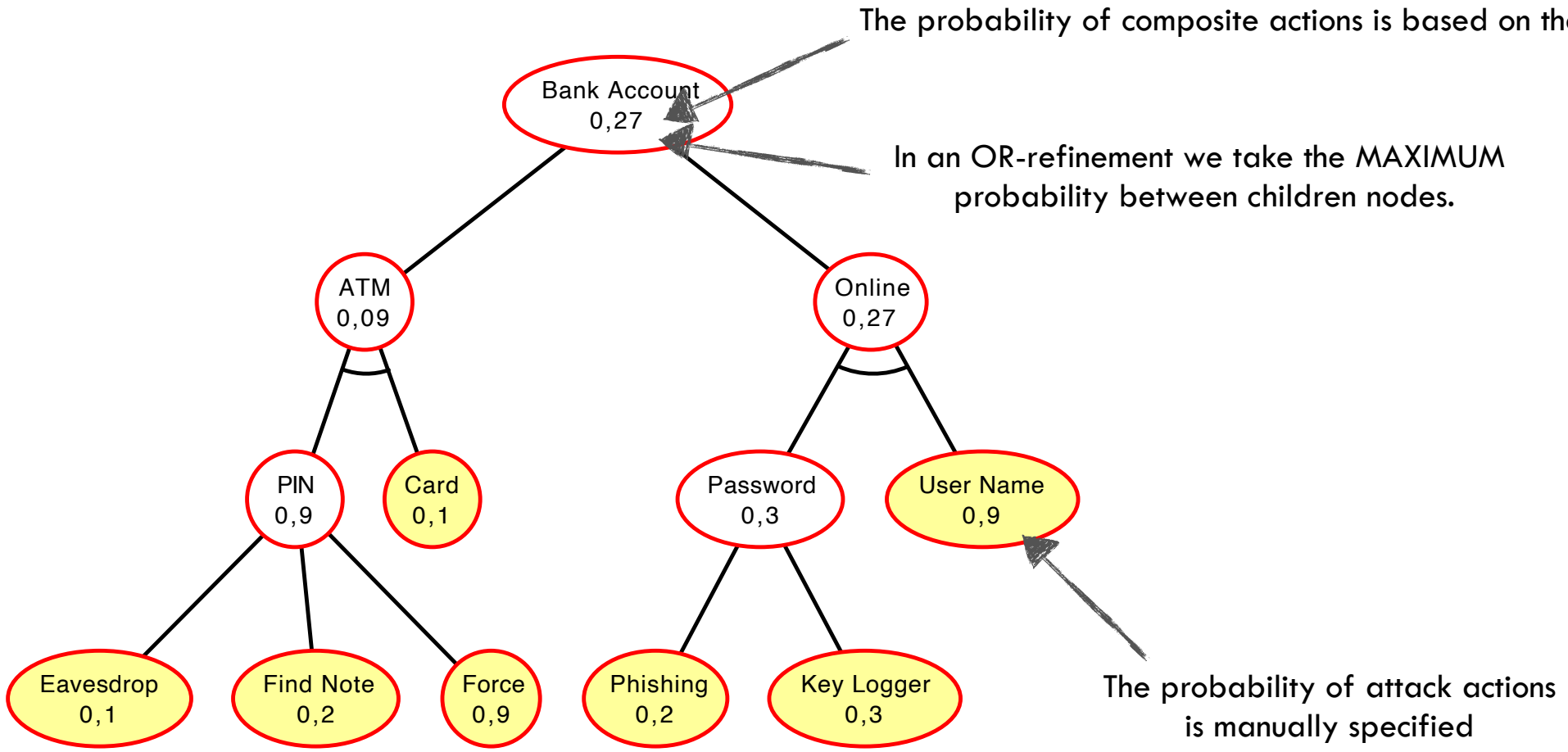
Attack Tree with probabilities

Each node of the Attack Tree is now decorated with a number, representing success probability.



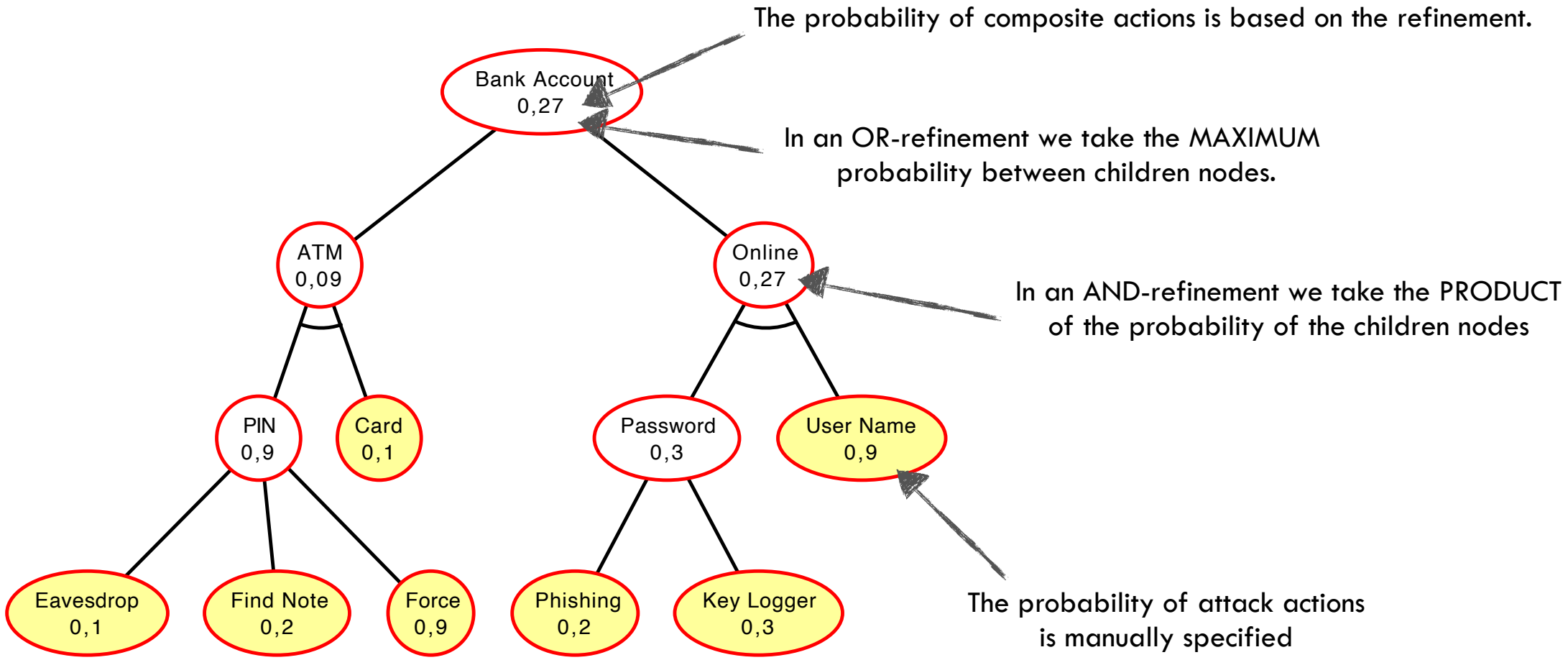
Attack Tree with probabilities

Each node of the Attack Tree is now decorated with a number, representing success probability.



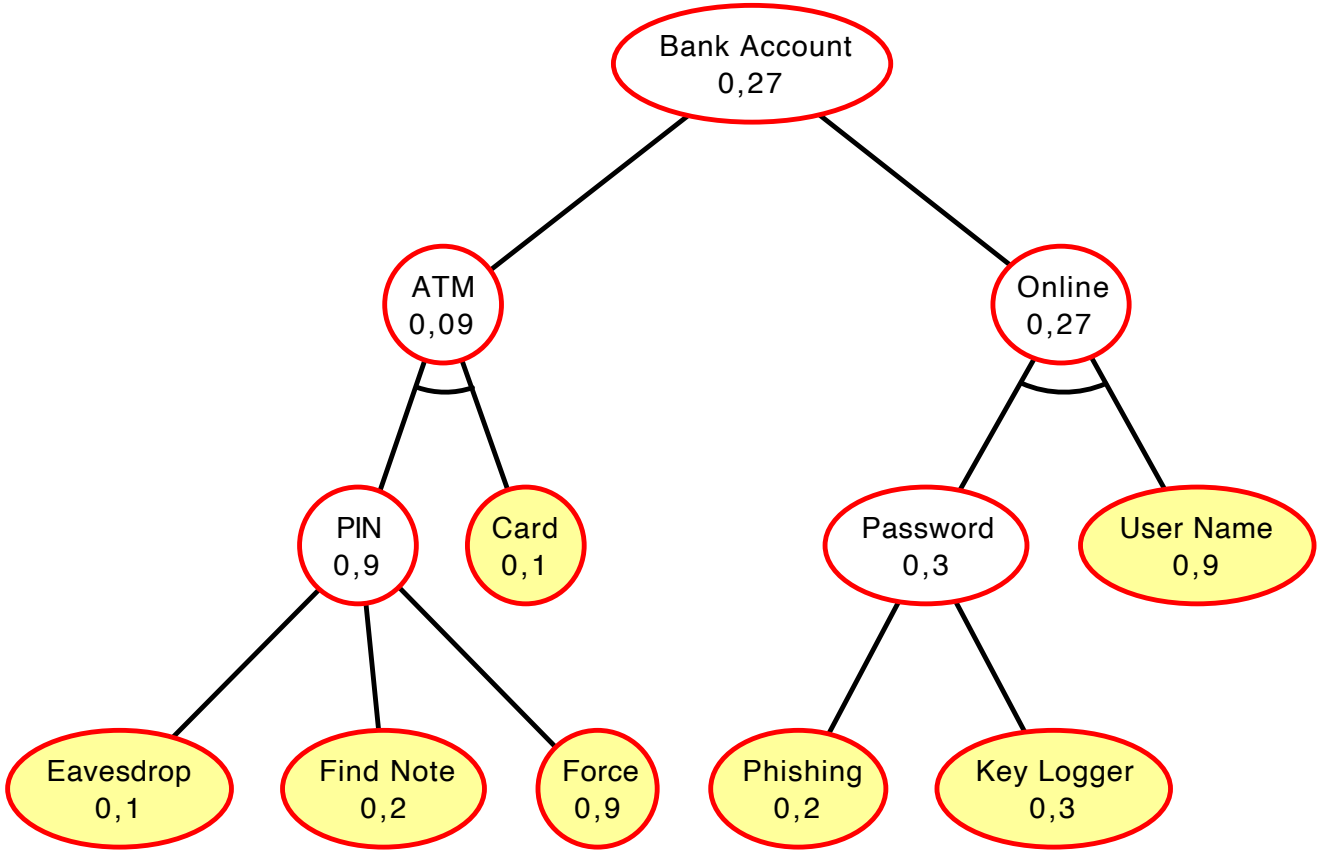
Attack Tree with probabilities

Each node of the Attack Tree is now decorated with a number, representing success probability.



Attack Likelihood Analysis

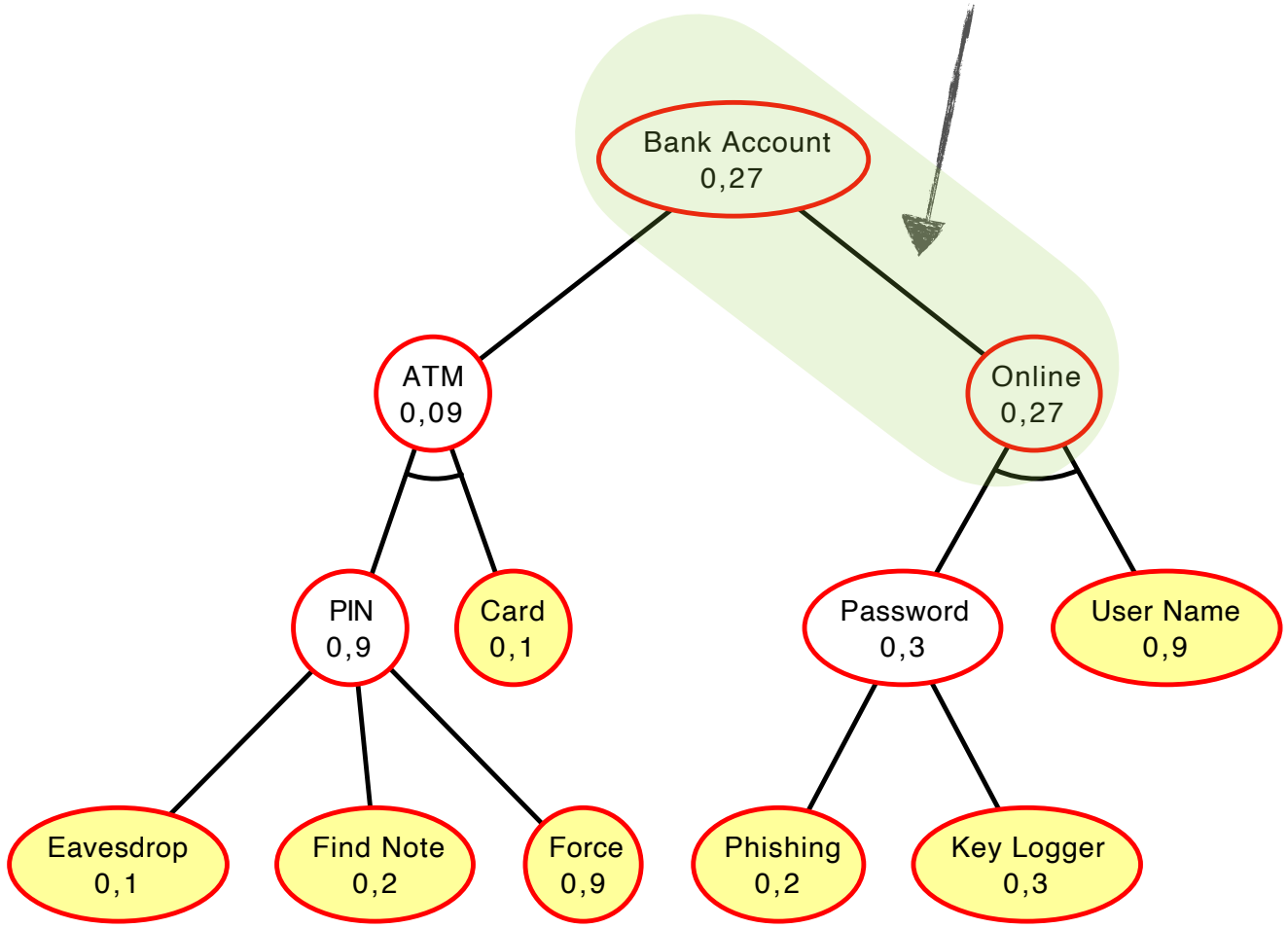
To determine the most likely attack, we use the annotated Attack Tree:



Attack Likelihood Analysis

To determine the most likely attack, we use the annotated Attack Tree:

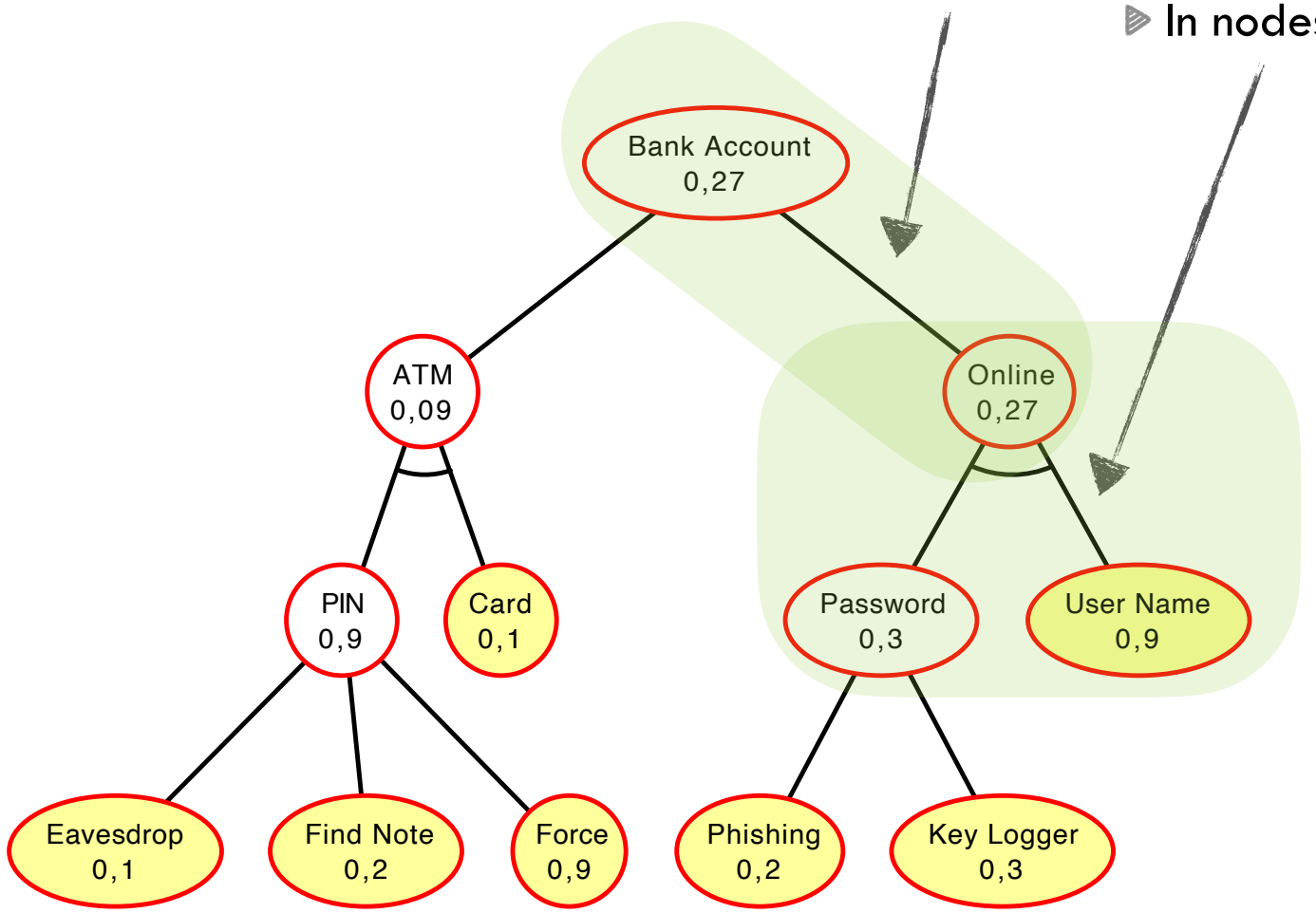
- In nodes refined with OR, take the branch that provided minimal cost



Attack Likelihood Analysis

To determine the most likely attack, we use the annotated Attack Tree:

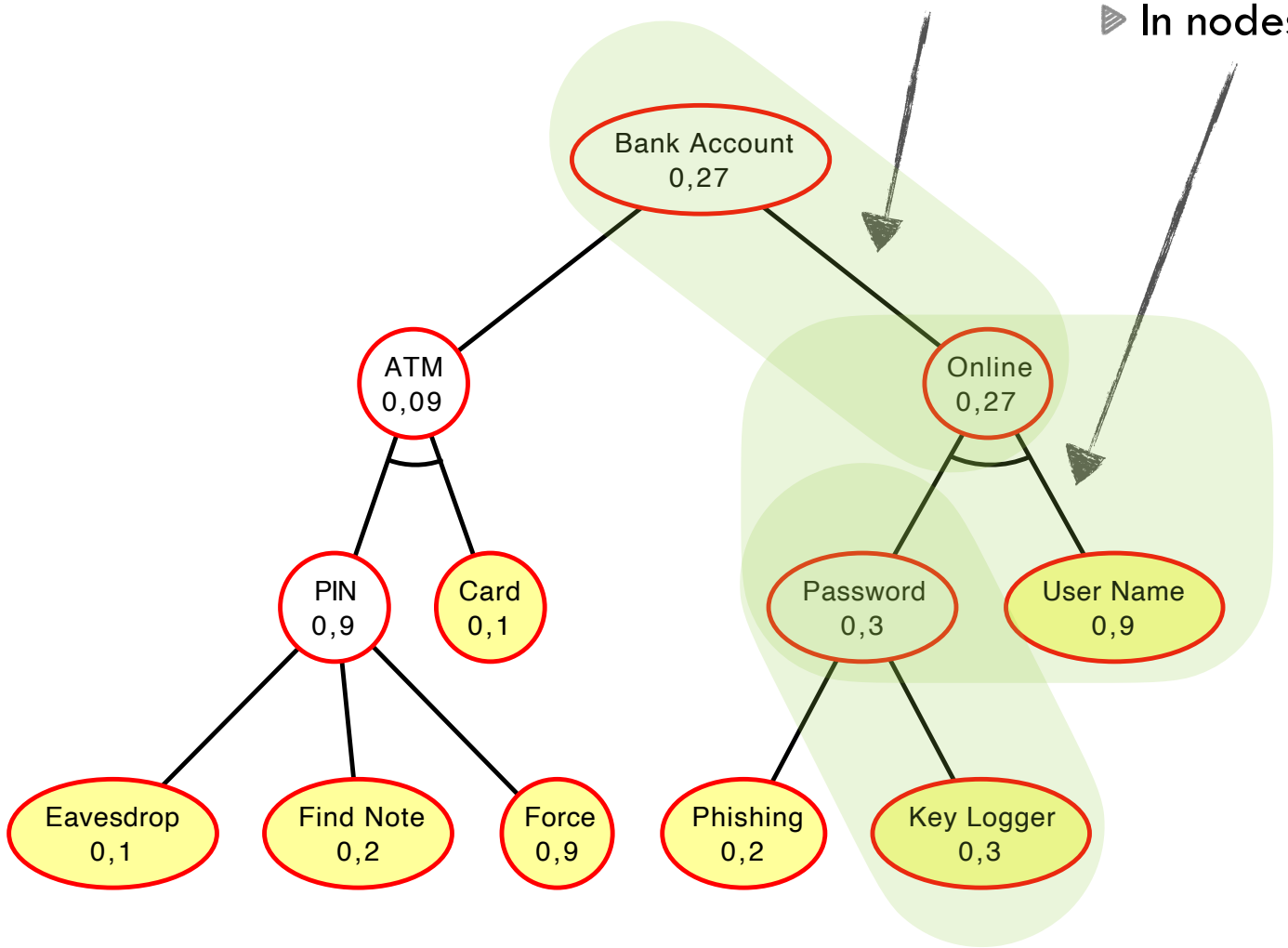
- In nodes refined with OR, take the branch that provided minimal cost
- In nodes refined with AND, take both branches.



Attack Likelihood Analysis

To determine the most likely attack, we use the annotated Attack Tree:

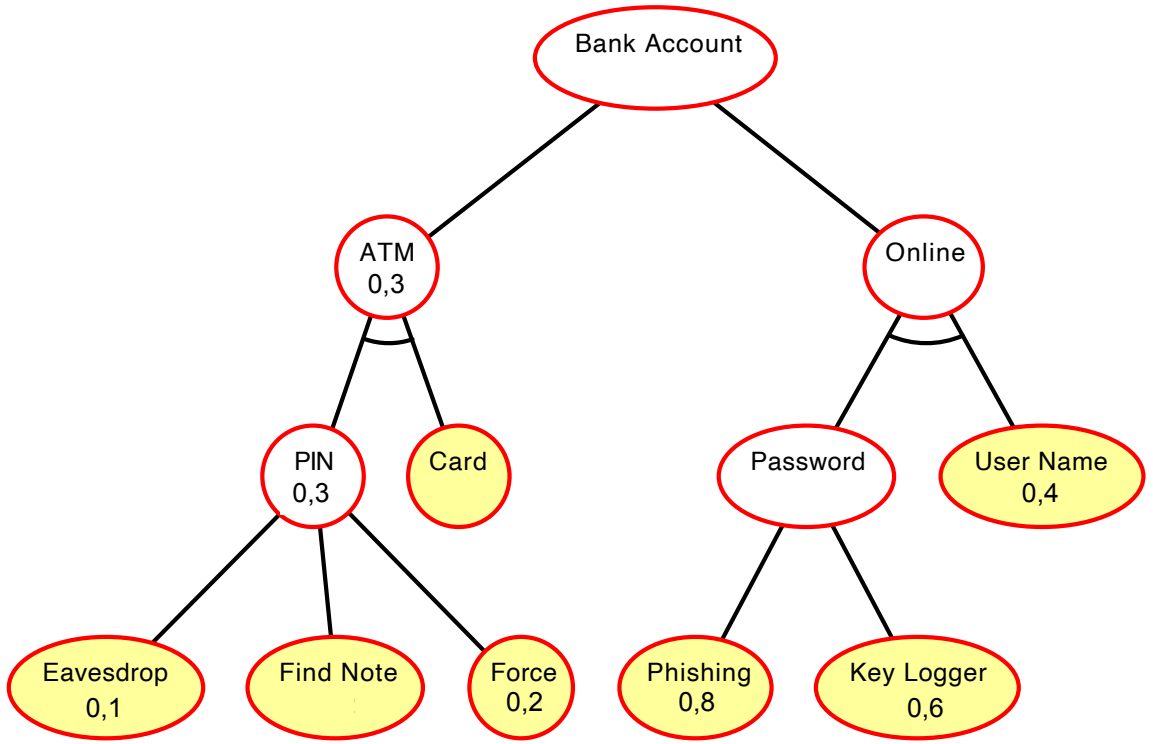
- In nodes refined with OR, take the branch that provided minimal cost
- In nodes refined with AND, take both branches.



In the example, the most likely attack is {Key Logger, User Name}. The probability is 27%.

EXERCISES

Consider the example Attack Tree on the right.



Exercise C.1. Complete the Attack Tree by adding the missing probabilities.

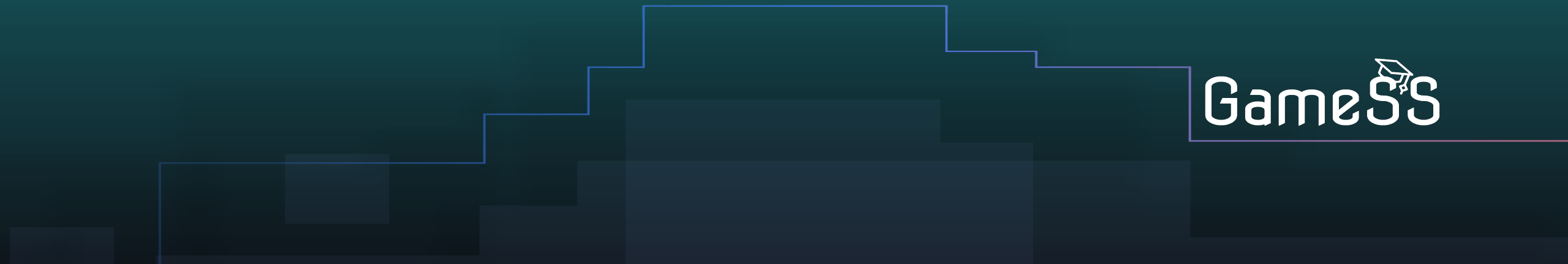
Exercise C.2. Which is most likely attack?

Exercise C.3. True or False?

a) The most likely attack and the least likely attack are always different.
b) When comparing two attacks, the one with the most likely attack action will be the most likely attack.
c) The probability of an attack is smaller than the product of all its attack actions.
d) The probability of an attack is smaller than the probability of its most likely attack action.

Hint: use ADTool to check your solutions. Solutions are provided at the end of the slide deck.

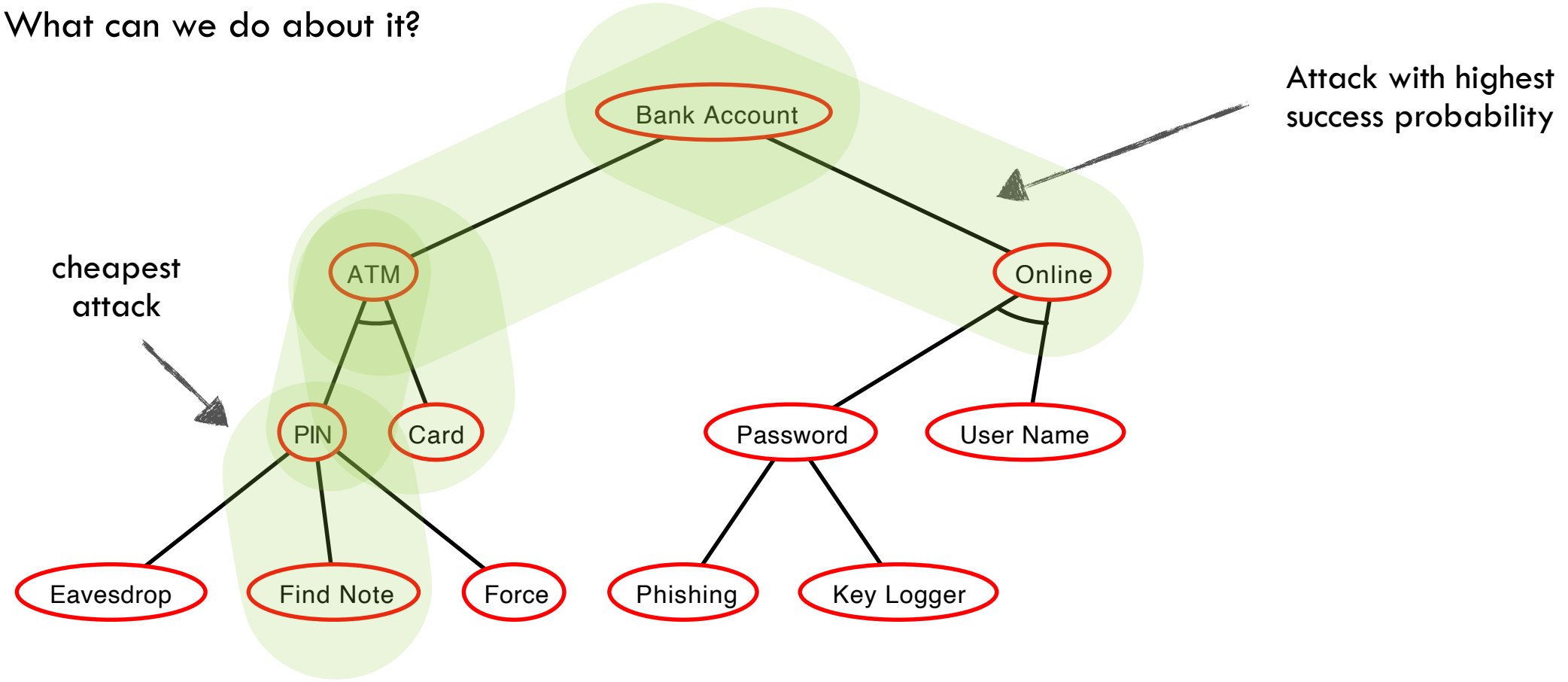
Attack Trees with Defences (aka Attack-Defence Trees)



Attack Defence Trees (ADTs)

Our analysis of the Attack Tree revealed attacks that are cheap or have high probability of success

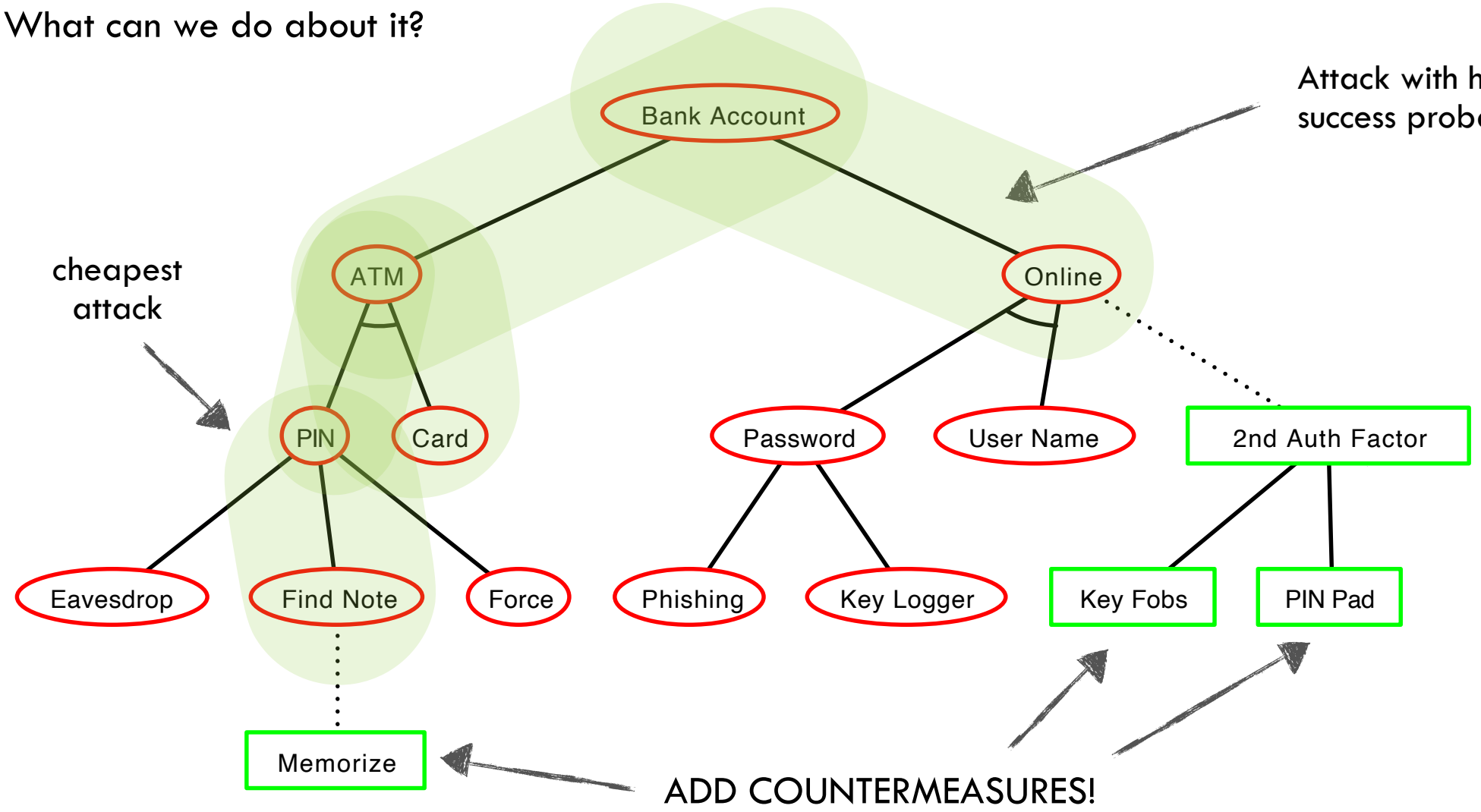
What can we do about it?



Attack Defence Trees (ADTs)

Our analysis of the Attack Tree revealed attacks that are cheap or have high probability of success

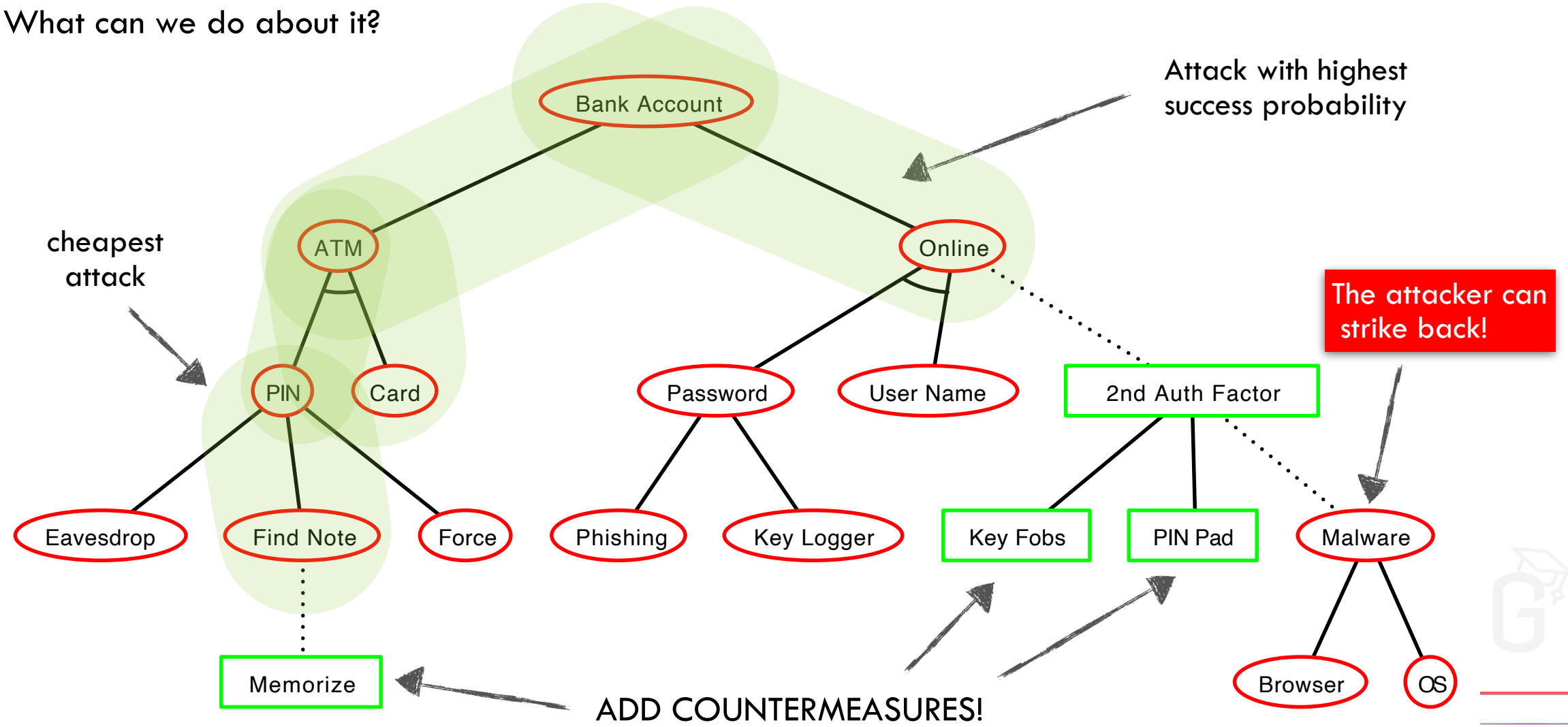
What can we do about it?



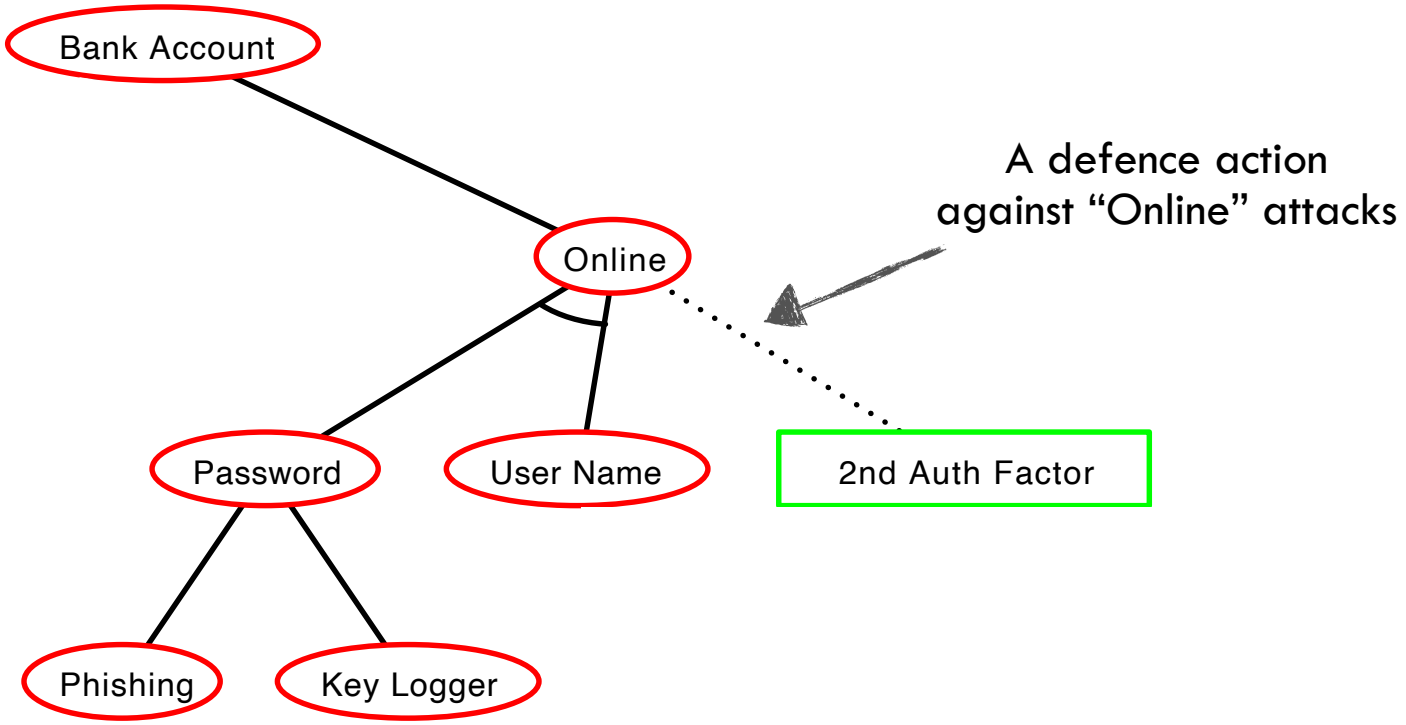
Attack Defence Trees (ADTs)

Our analysis of the Attack Tree revealed attacks that are cheap or have high probability of success

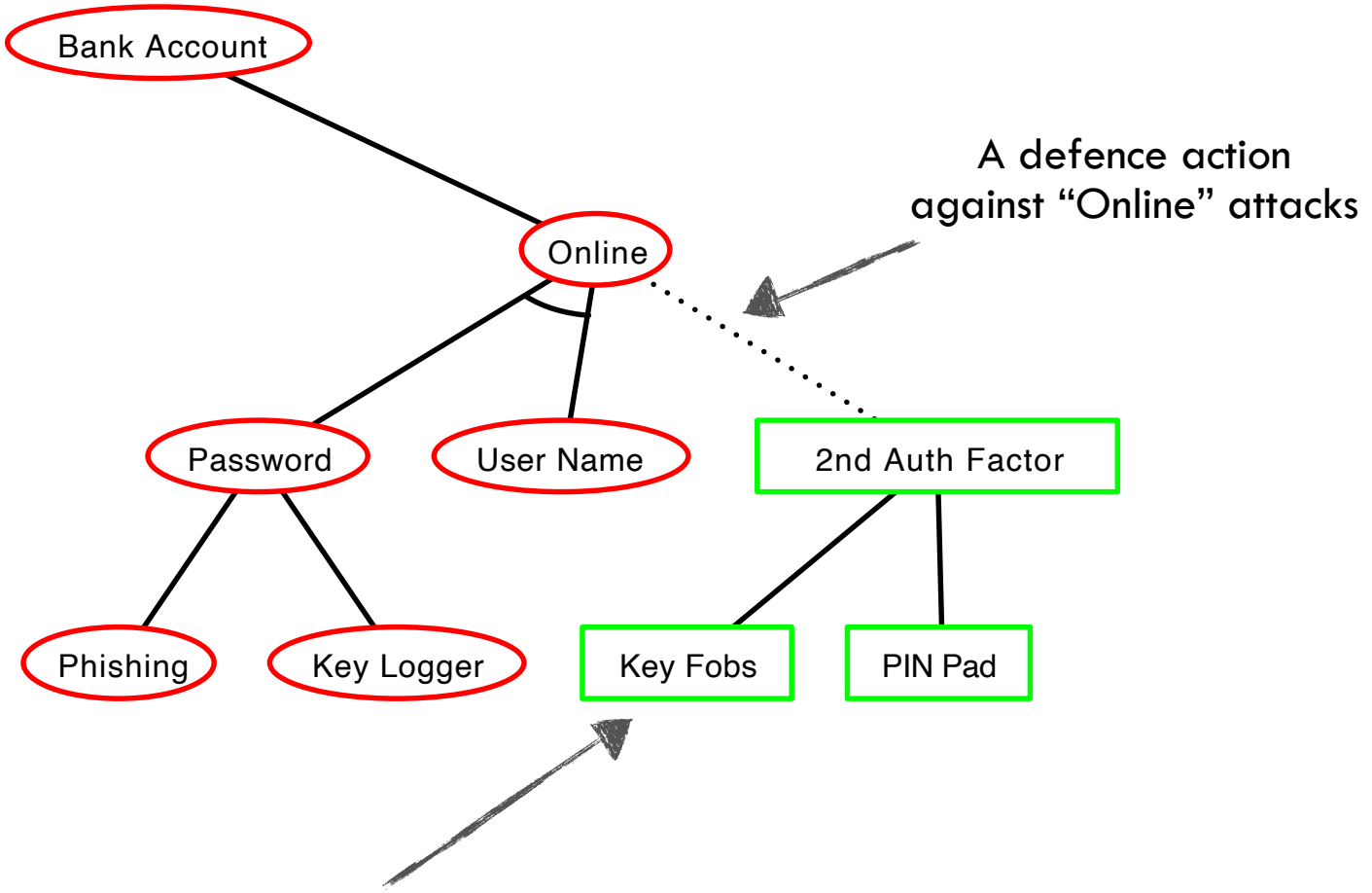
What can we do about it?



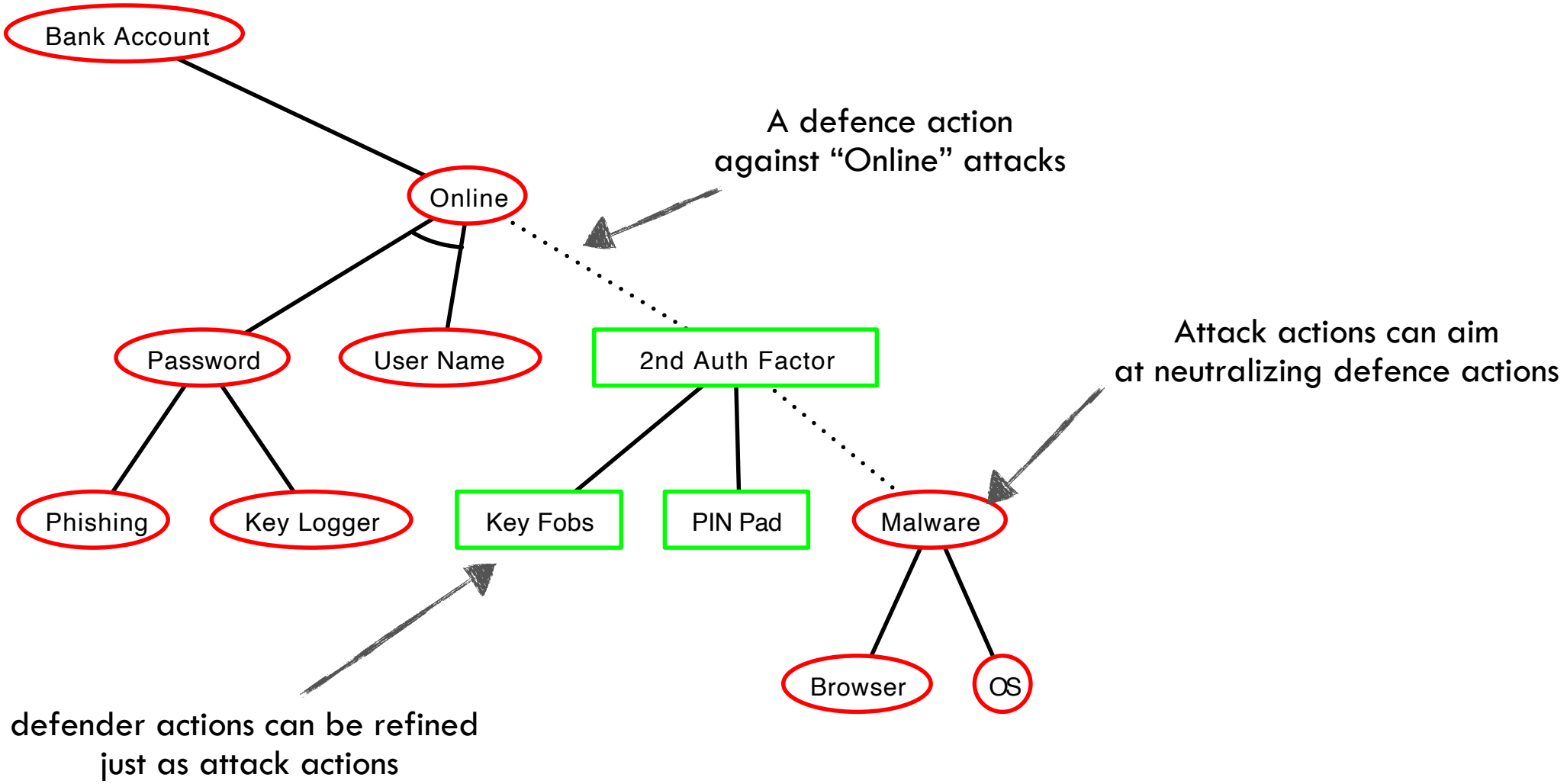
Defence actions vs attack actions



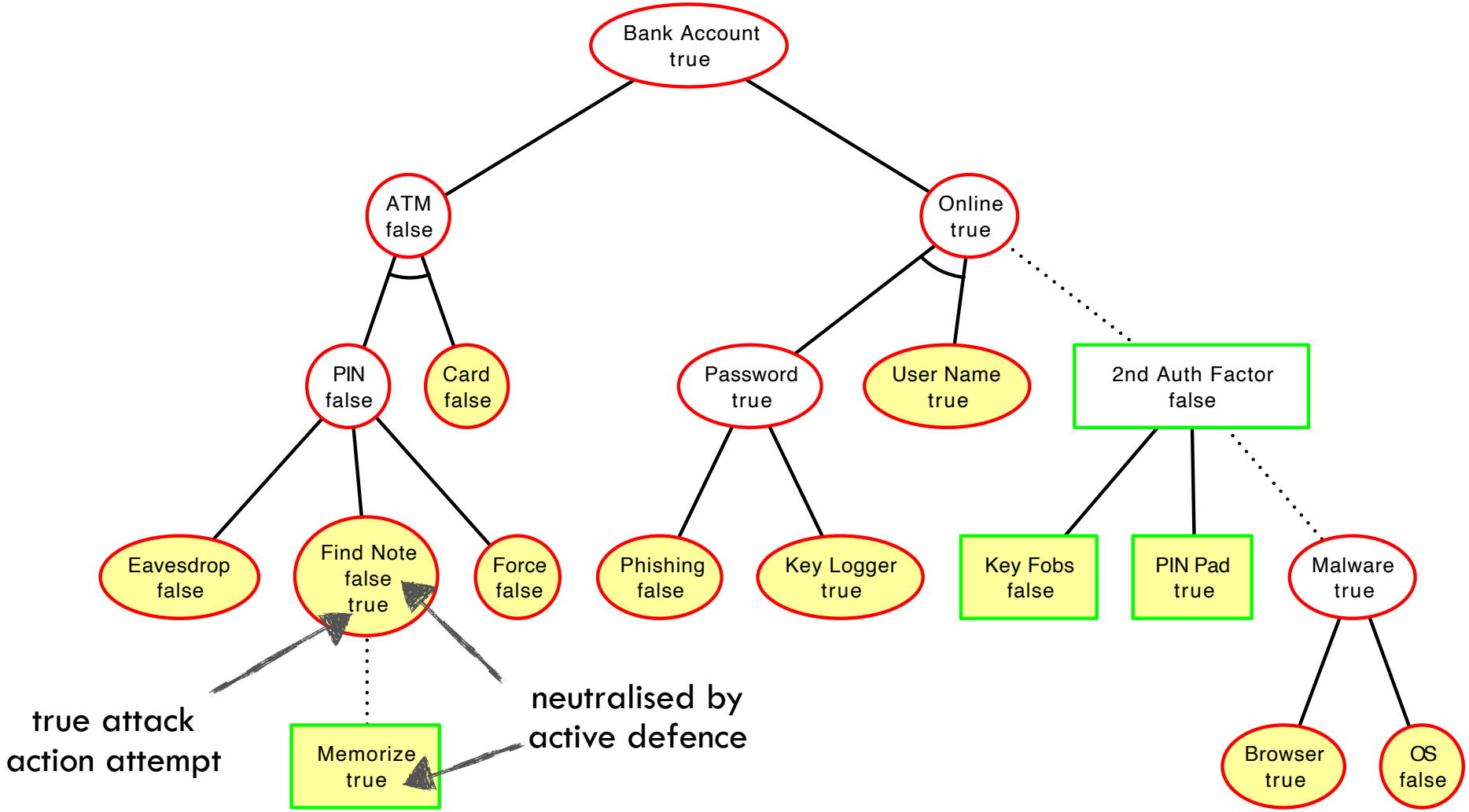
Defence actions vs attack actions



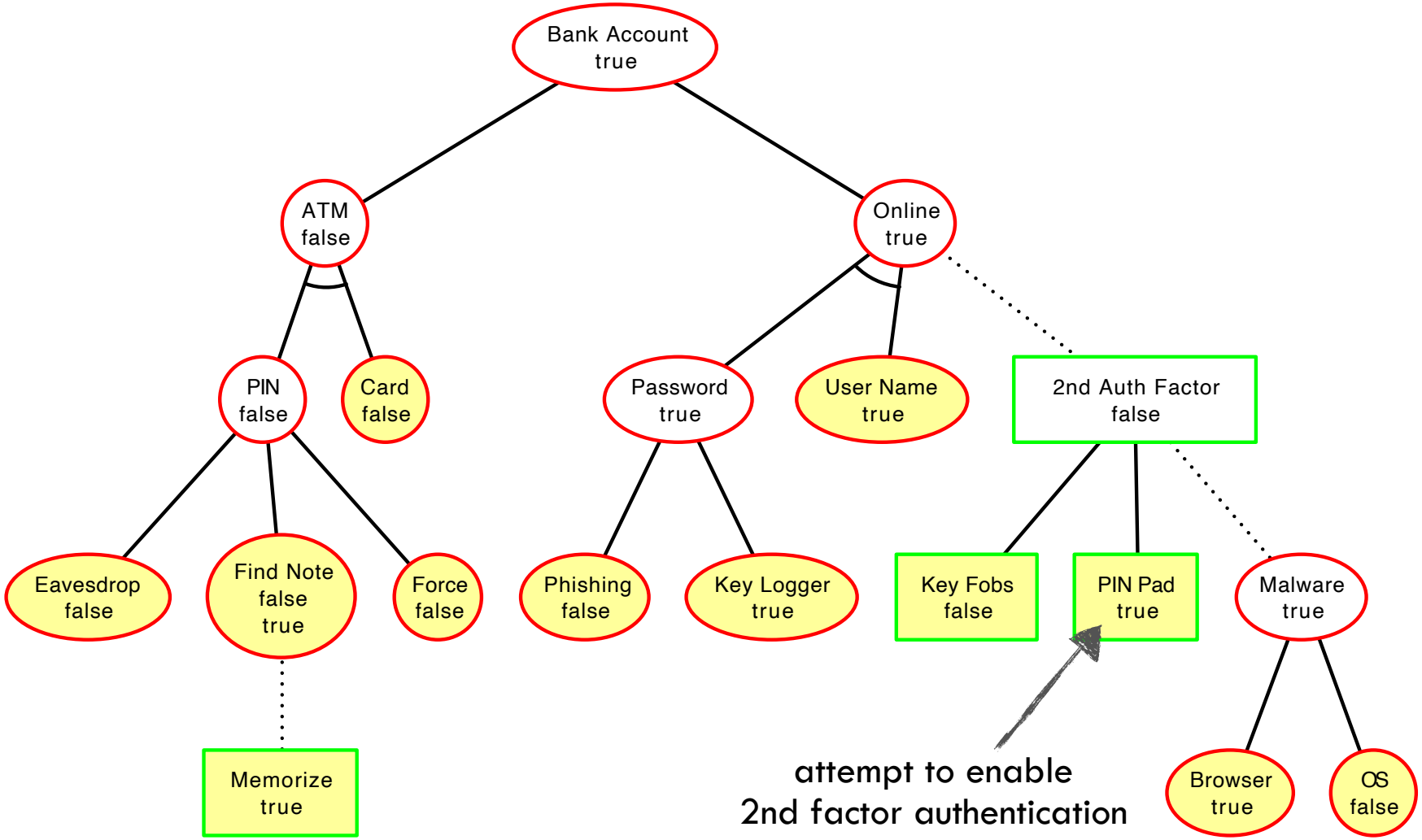
Defence actions vs attack actions



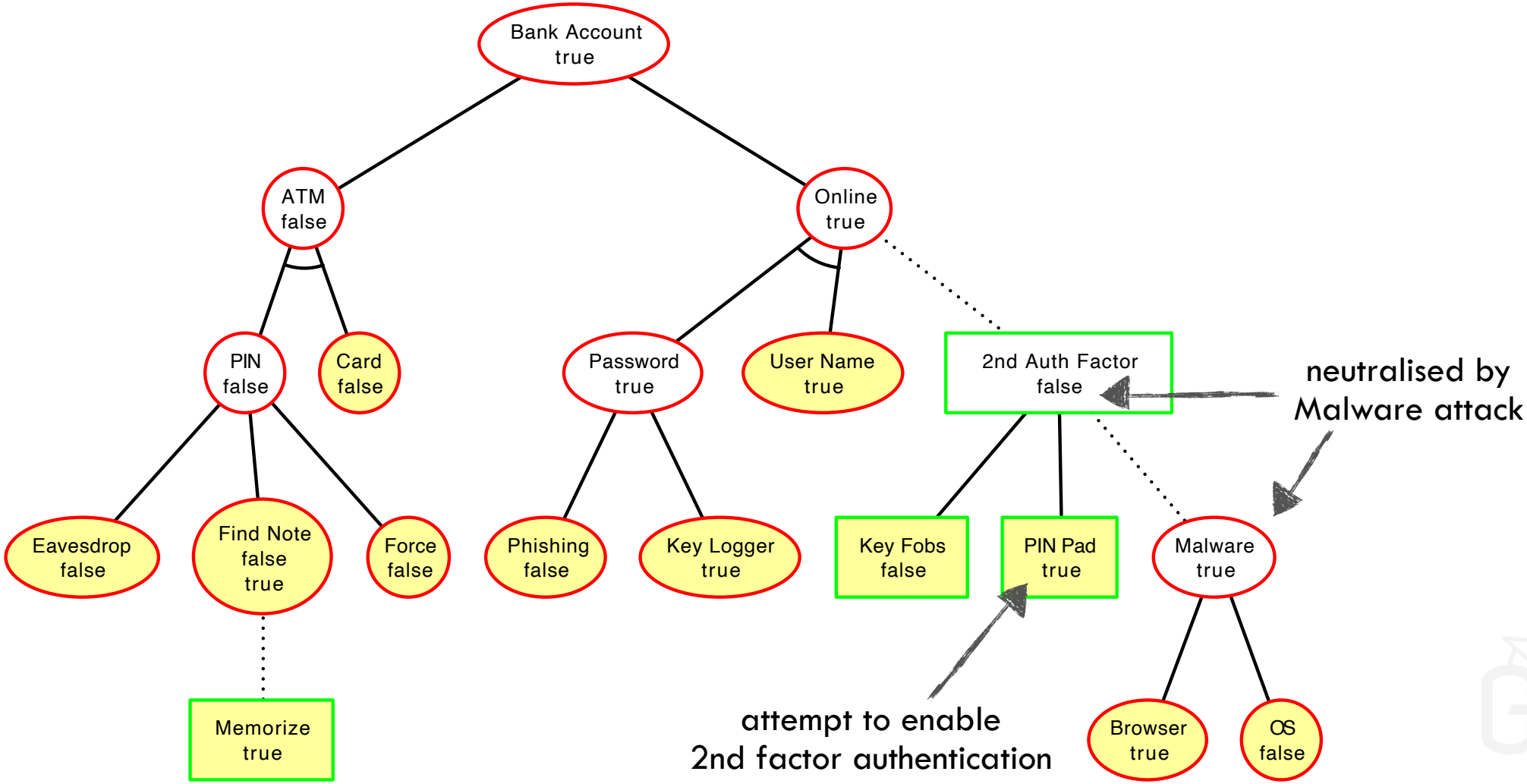
Feasibility Analysis



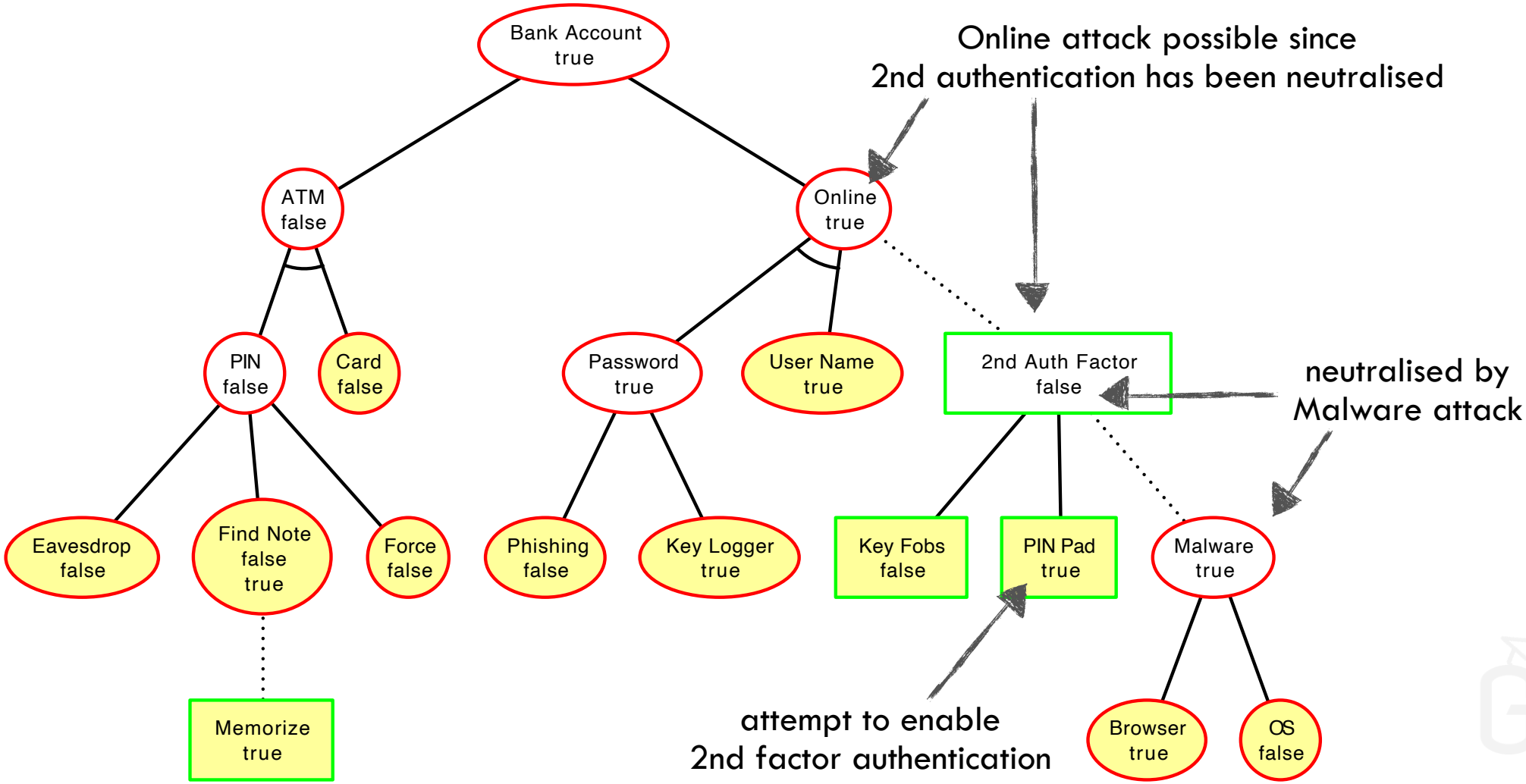
Feasibility Analysis



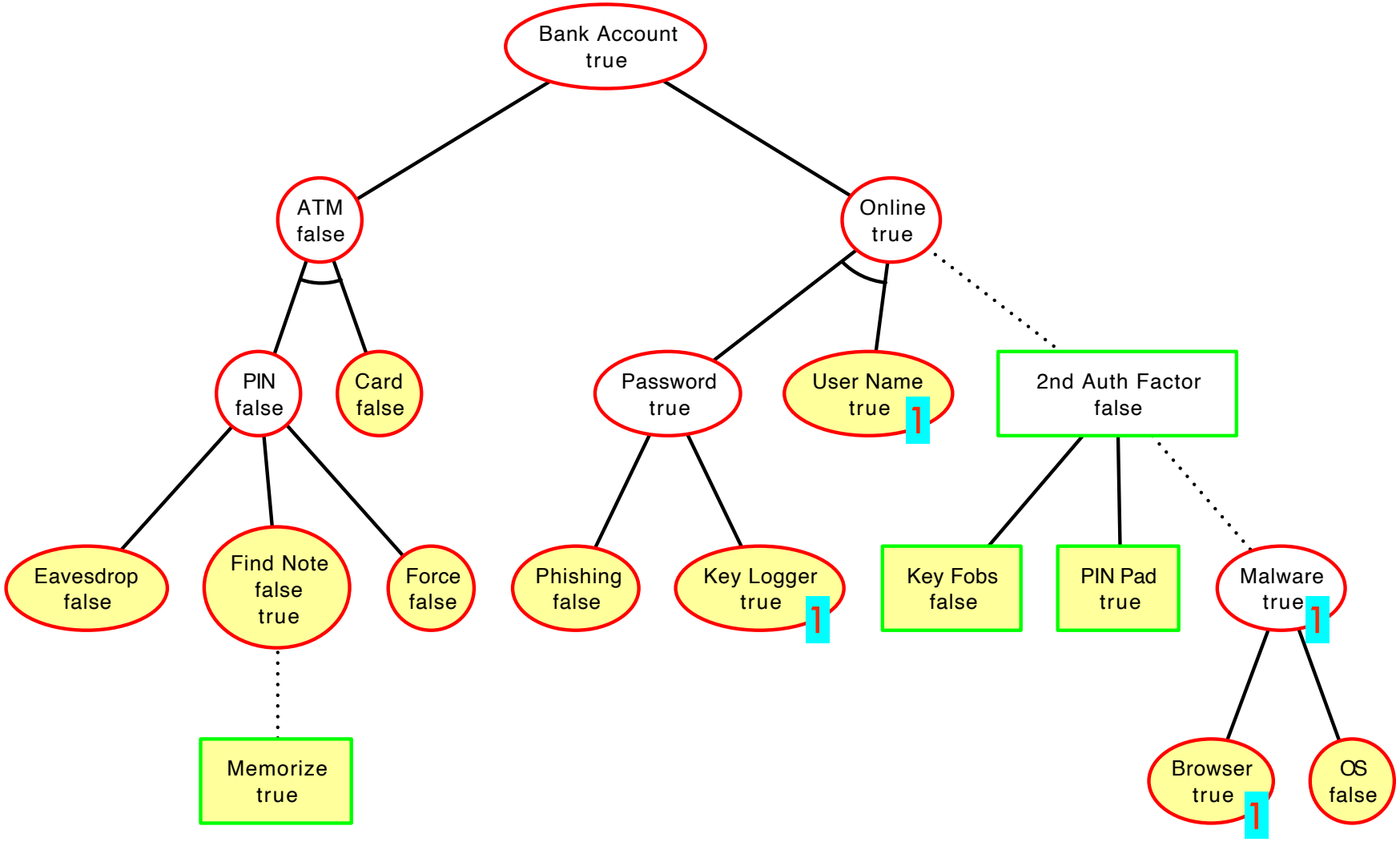
Feasibility Analysis



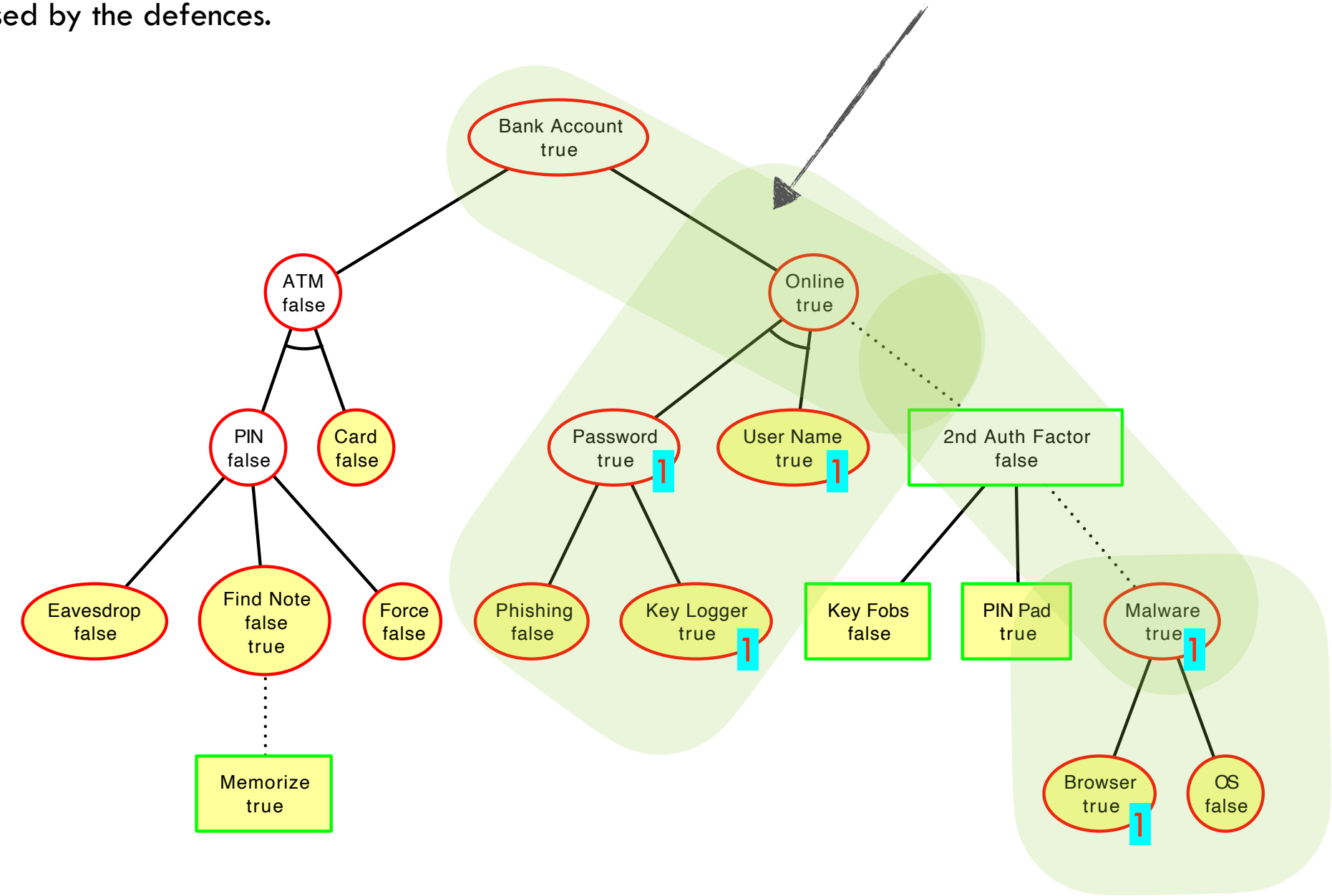
Feasibility Analysis



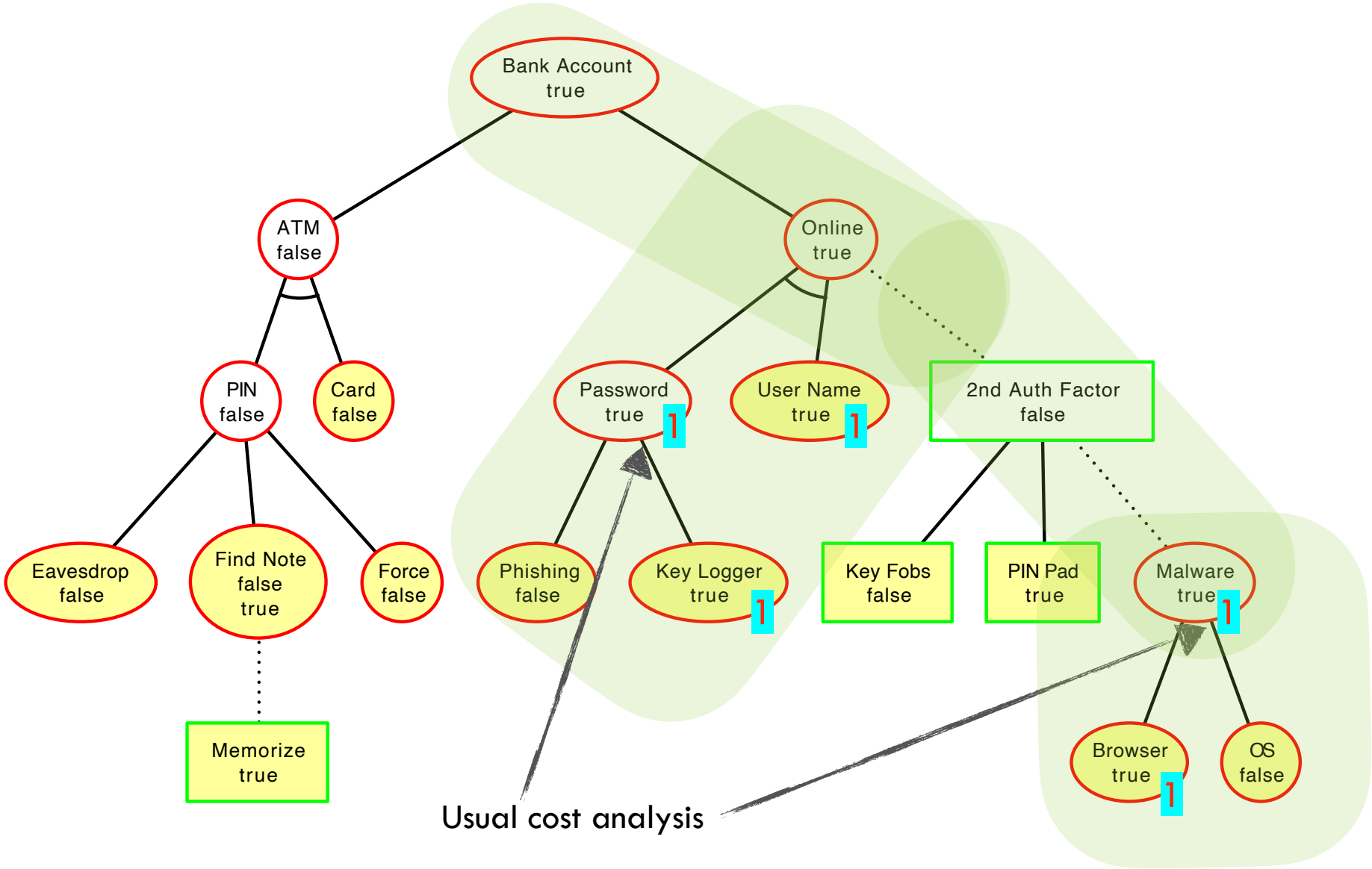
We can perform the minimal cost analysis on the attack tree obtained by removing the unfeasible attacks, as neutralised by the defences.



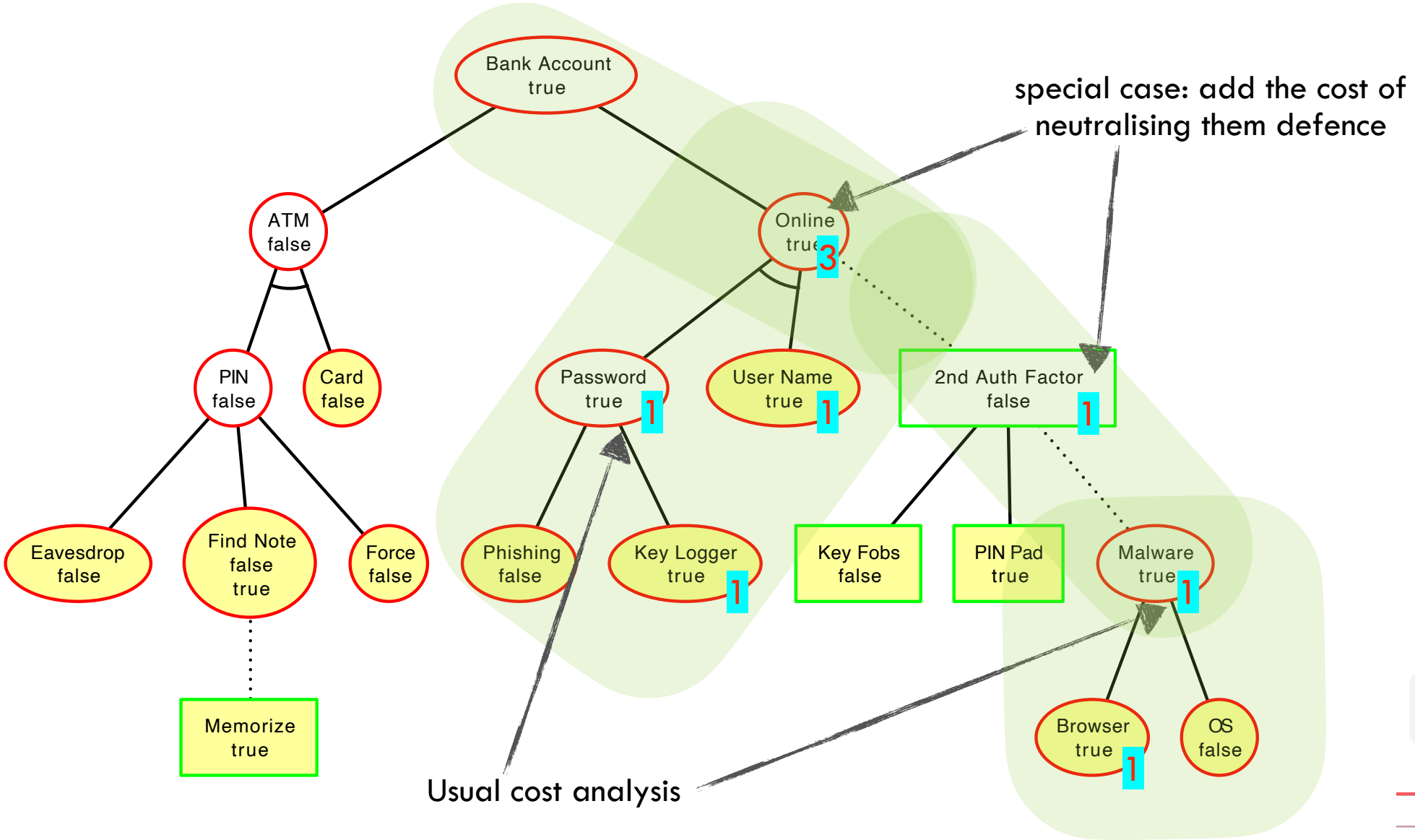
We can perform the minimal cost analysis on the attack tree obtained by removing the unfeasible attacks, as neutralised by the defences.



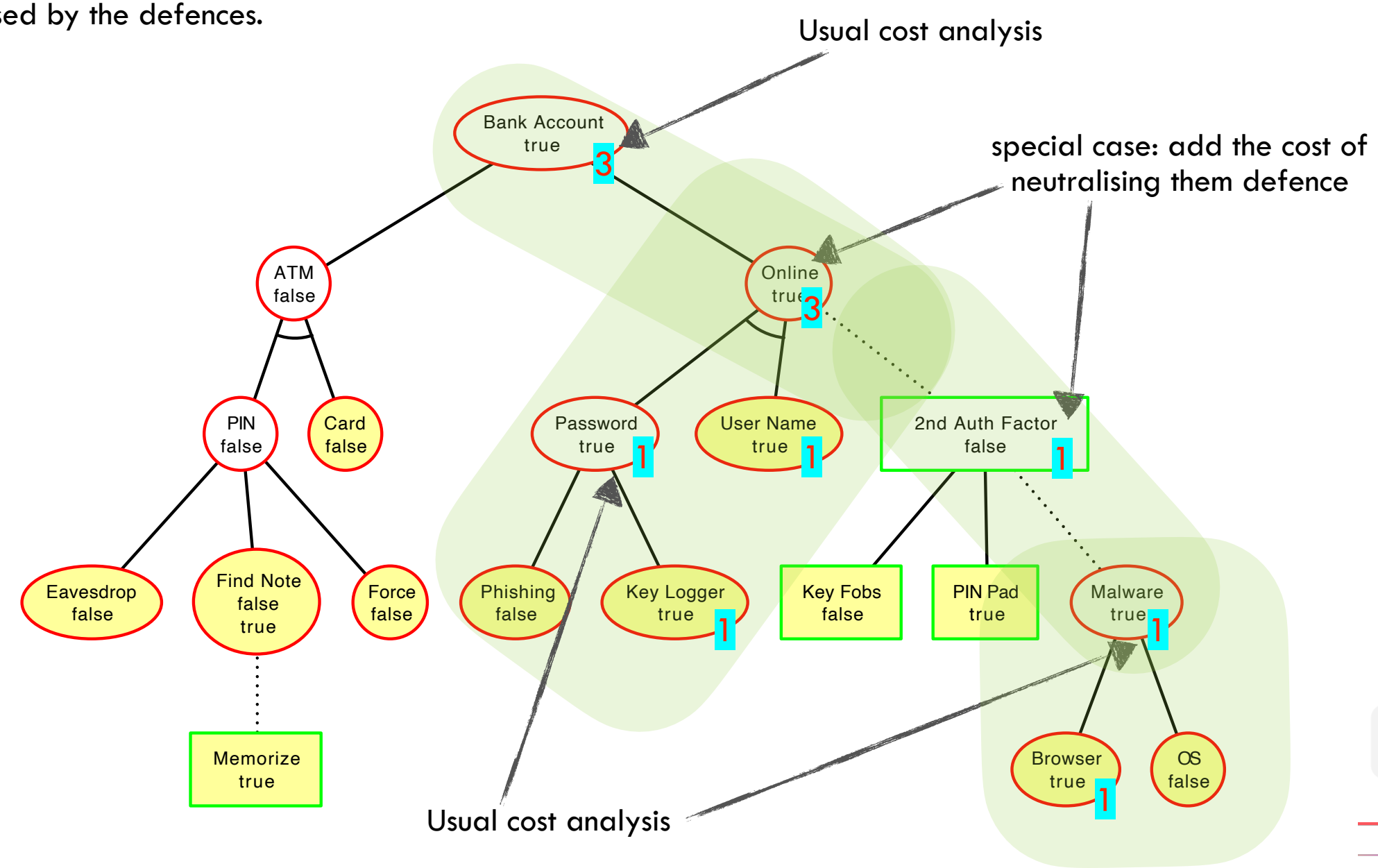
We can perform the minimal cost analysis on the attack tree obtained by removing the unfeasible attacks, as neutralised by the defences.



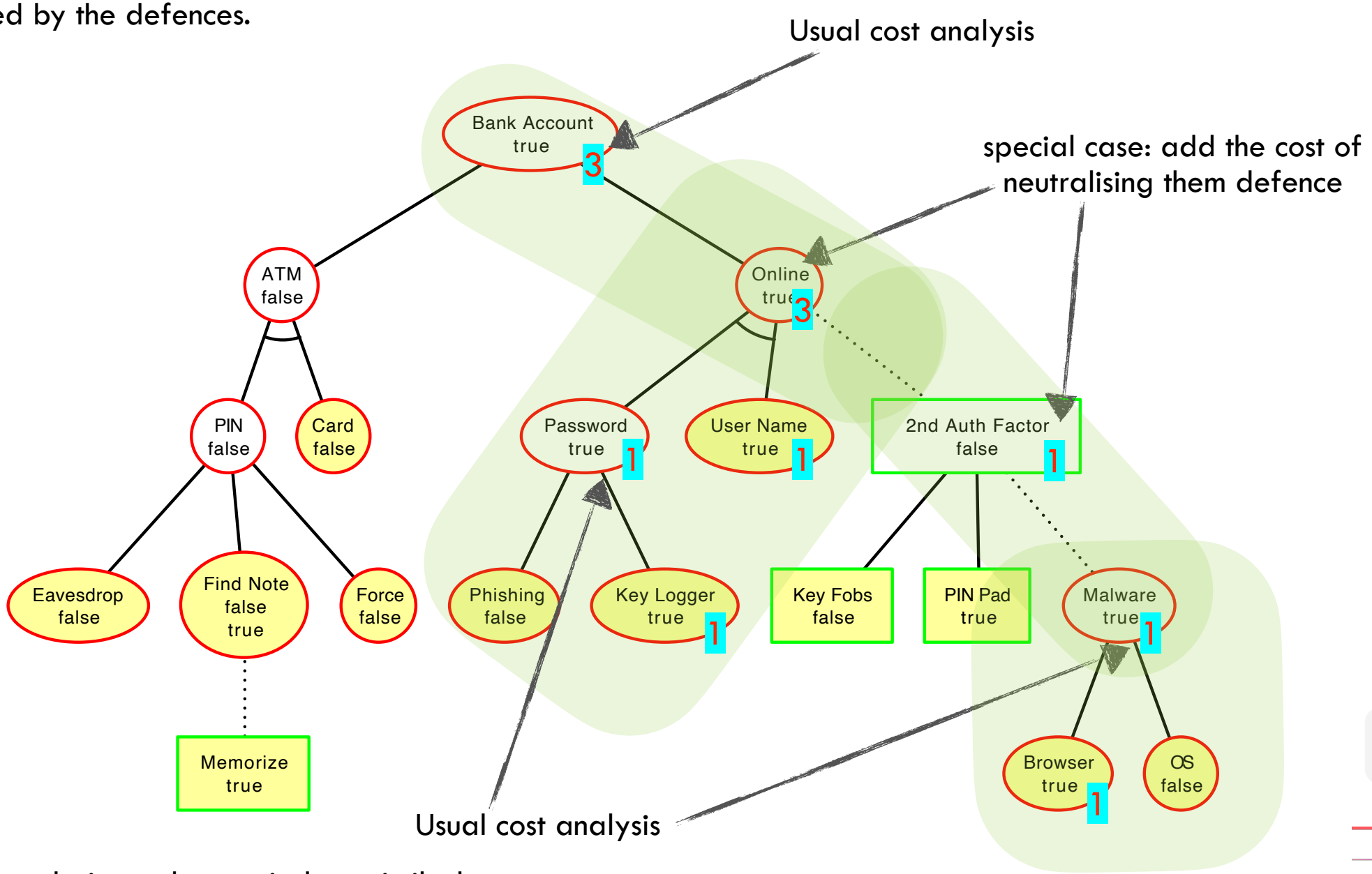
We can perform the minimal cost analysis on the attack tree obtained by removing the unfeasible attacks, as neutralised by the defences.



We can perform the minimal cost analysis on the attack tree obtained by removing the unfeasible attacks, as neutralised by the defences.



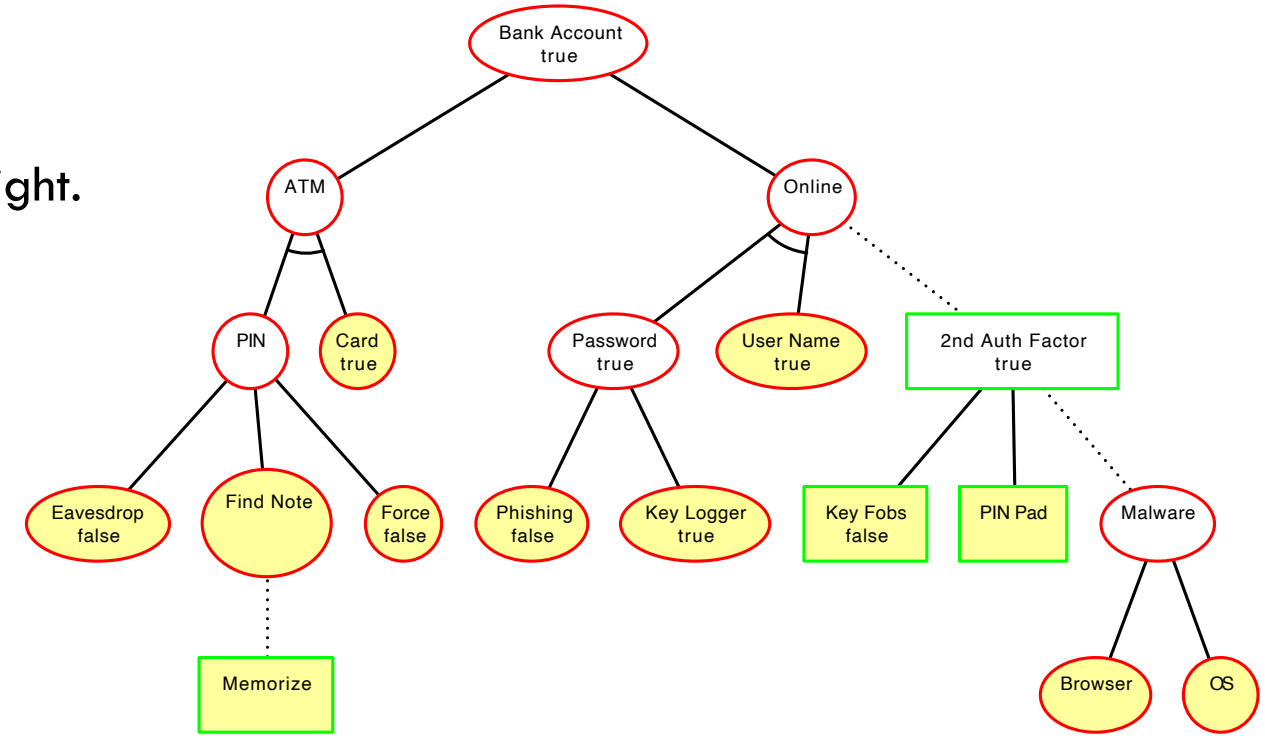
We can perform the minimal cost analysis on the attack tree obtained by removing the unfeasible attacks, as neutralised by the defences.



Likelihood analysis can be carried out similarly

EXERCISES

Consider the example Attack Tree on the right.



Exercise D.1. Complete the Attack Tree by adding the missing boolean annotations.

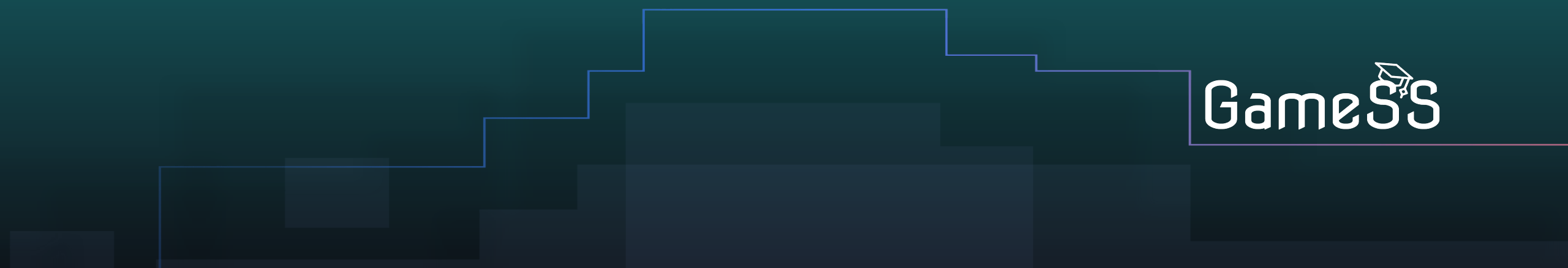
Exercise D.2. Which is the cheapest attack now? Which is the attack with highest probability of success?

Exercise D.3. True or False?

a) A defence action that is not neutralised will neutralise all attack nodes on the way to the root.
b) An attack action that is not neutralised will neutralise all defence nodes on the way to the root.
c) If all internal attack nodes have a corresponding countermeasure (defence action) then we can neutralise all attacks.

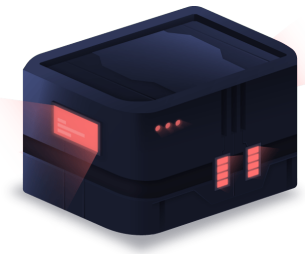
Hint: use ADTool to check your solutions. Solutions are provided at the end of the slide deck.

Summary



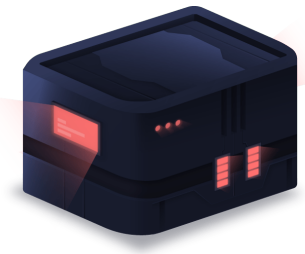
WHAT ARE THE MAIN TAKEAWAYS FOR THIS CONTENT?

- Attack Trees provide a structured methodology to threat modelling, supported by solid theories and effective tools.
- Attack Trees provide a visual representation of possible actions an attacker might take in order to compromise a system, and the defensive measures that a defender can employ to protect the system.
- Attack Trees can model several aspects of interests such as feasibility of attacks, probability of attack success and failure, effectiveness of countermeasures, and cost of attacks and countermeasures.
- Attack Tree tools such as ADTool can be used to automatise the assessment of Attack Trees.



FURTHER READING

- Barbara Kordy, Ludovic Pièvre-Cambacédès, Patrick Schweitzer: DAG-based attack and defense modeling: Don't miss the forest for the attack trees. Comput. Sci. Rev. 13-14: 1-38 (2014)
- Wojciech Widel, Maxime Audinot, Barbara Fila, Sophie Pinchinat: Beyond 2014: Formal Methods for Attack Tree-based Security Modeling. ACM Comput. Surv. 52(4): 75:1-75:36 (2019)
- Attack Trees, B. Schneier, Dr. Dobb's Journal, December 1999



Alberto Lluch Lafuente

Technical University of Denmark

FIND OUT MORE

https://gamess.dk/

albl@dtu.dk

linkedin.com/in/albertolluch

imm.dtu.dk/~albl/

GameSS

WHO IS BEHIND GameSS

Partners behind the project

SDU

DTU

IT UNIVERSITY OF CPH

AALBORG UNIVERSITET

Happy 42

Collaborators

ERHVERVSAKADEMI AARHUS

kea
KØBENHAVNS ERHVERVSAKADEMI

Dania
ERHVERVSAKADEMI

UCN

UCL Erhvervsakademi og Professionshøjskole

Supported by

Uddannelses- og Forskningsministeriet

Ministry of Higher Education and Science Denmark

WHO IS BEHIND GameSS

Partners behind the project

SDU

DTU

IT UNIVERSITY OF CPH

AALBORG UNIVERSITET

Happy 42

Collaborators

ERHVERVSAKADEMI AARHUS

kea
KØBENHAVNS ERHVERVSAKADEMI

Dania
ERHVERVSAKADEMI

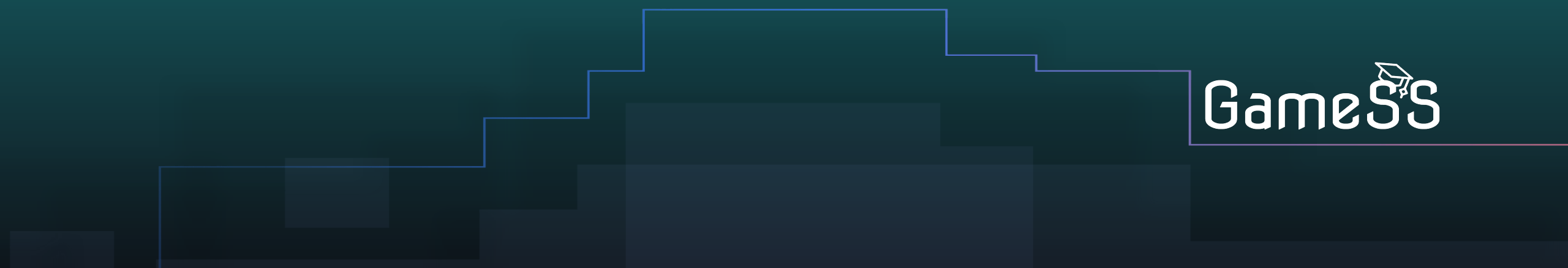
UCN

Erhvervsakademi og Professionshøjskole

Uddannelses- og Forskningsministeriet

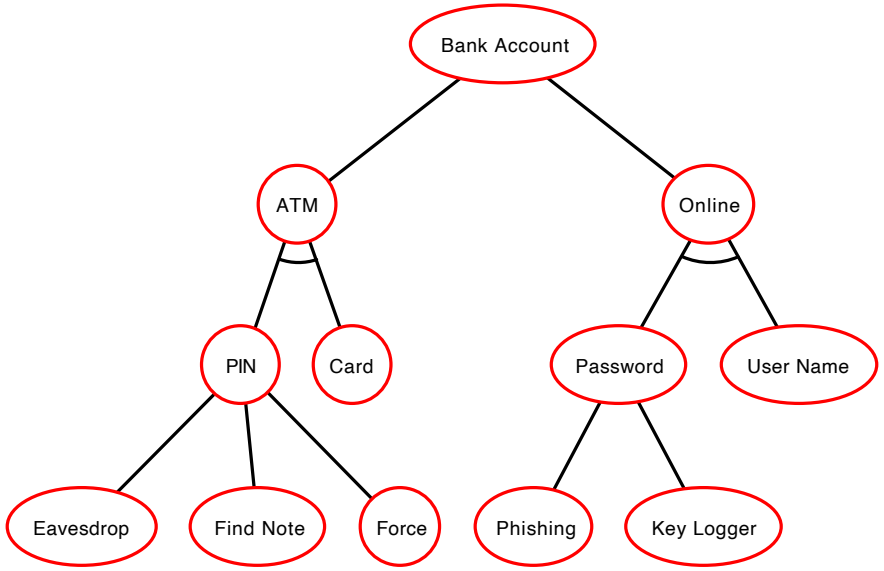
Ministry of Higher Education and Science Denmark

Solutions



SOLUTIONS

Consider our example Attack Tree.



Exercise A.1. Consider the following sets of attack actions:

a) {Eavesdrop, Find Note, Card} FEASIBLE
b) {Eavesdrop, Card} FEASIBLE
c) {Eavesdrop, Phishing} NOT FEASIBLE
d) {Keylogger, User Name} FEASIBLE

For each set, determine if it constitutes a feasible attack.

Exercise A.2. List all possible minimal attacks. {Eavesdrop, Card} , {Find Note, Card} , {Force, Card} , {Phising, User Name} , {Key Logger, User Name}

Exercise A.3. True or False?

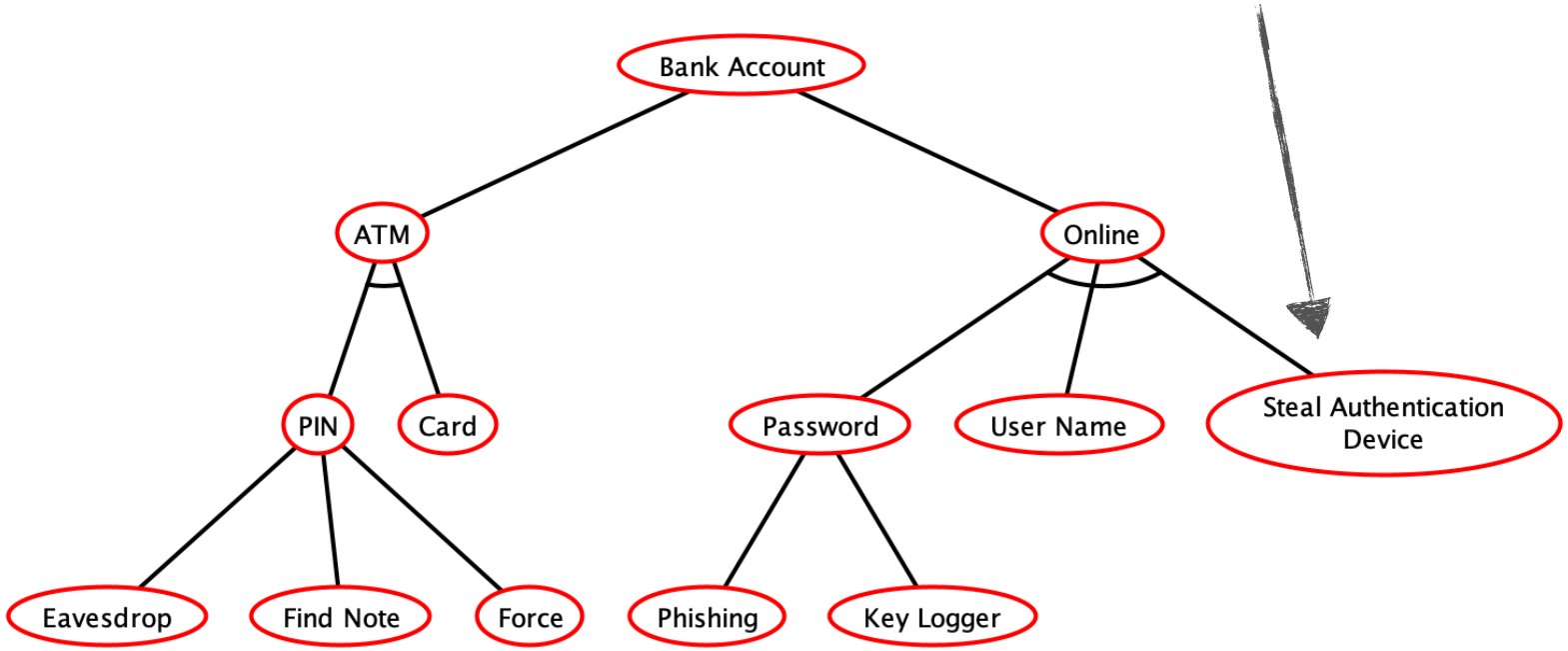
a) Every feasible attack including action "Phishing" includes also the action "User Name". FALSE, for example {Force, Card, Phishing} is a feasible attack.
b) Every minimal feasible attack including action "Phishing" includes also the action "User Name". TRUE, as seen from the solution to Exercise 2.
c) Every minimal feasible attack including action "User Name" includes also the action "Phishing". FALSE, as seen from the solution to Exercise 2.

SOLUTIONS

Consider our example Attack Tree.

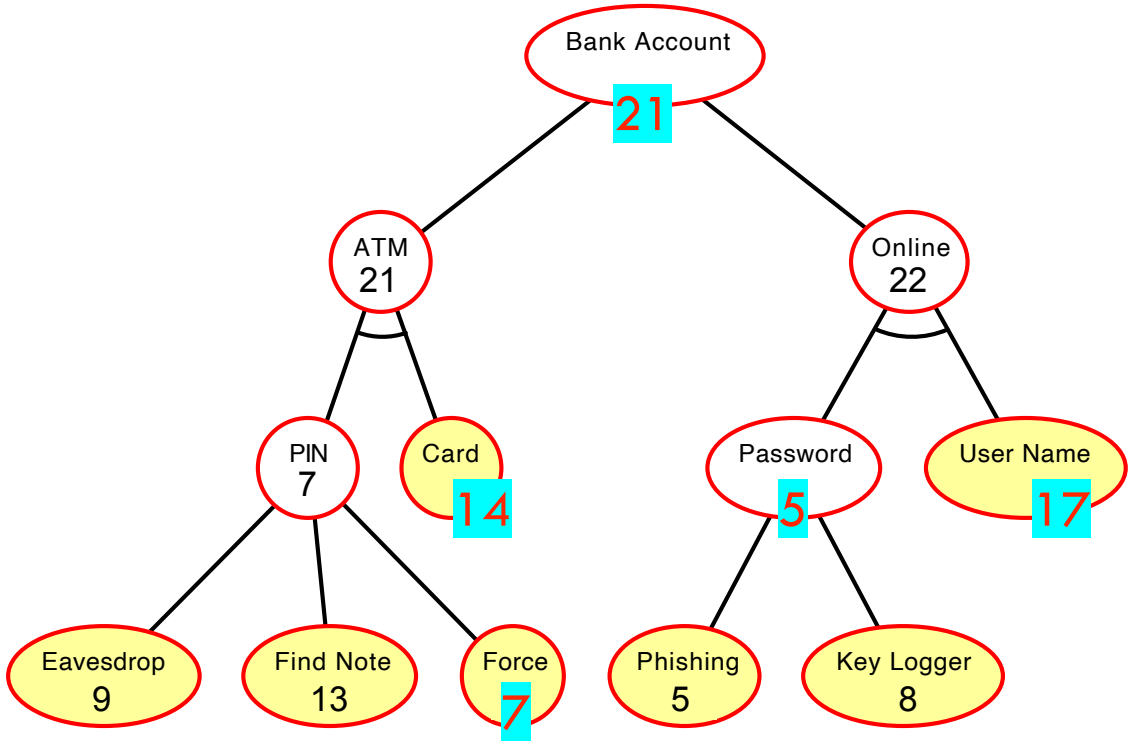
Exercise A.4. Let us assume that the bank decides to implement a second factor authentication as part of the online access. The set of actions {Password, User Name} does not constitute a feasible attack any more. The attacker also needs to perform additional actions. Modify the Attack Tree accordingly.

This is an open question and there are several valid answers. A simple one could be do add child to "Online" representing the stealing of the second factor authentication device.



SOLUTIONS

Consider the example Attack Tree on the right.



Exercise B.1. Complete the Attack Tree by adding the missing costs.

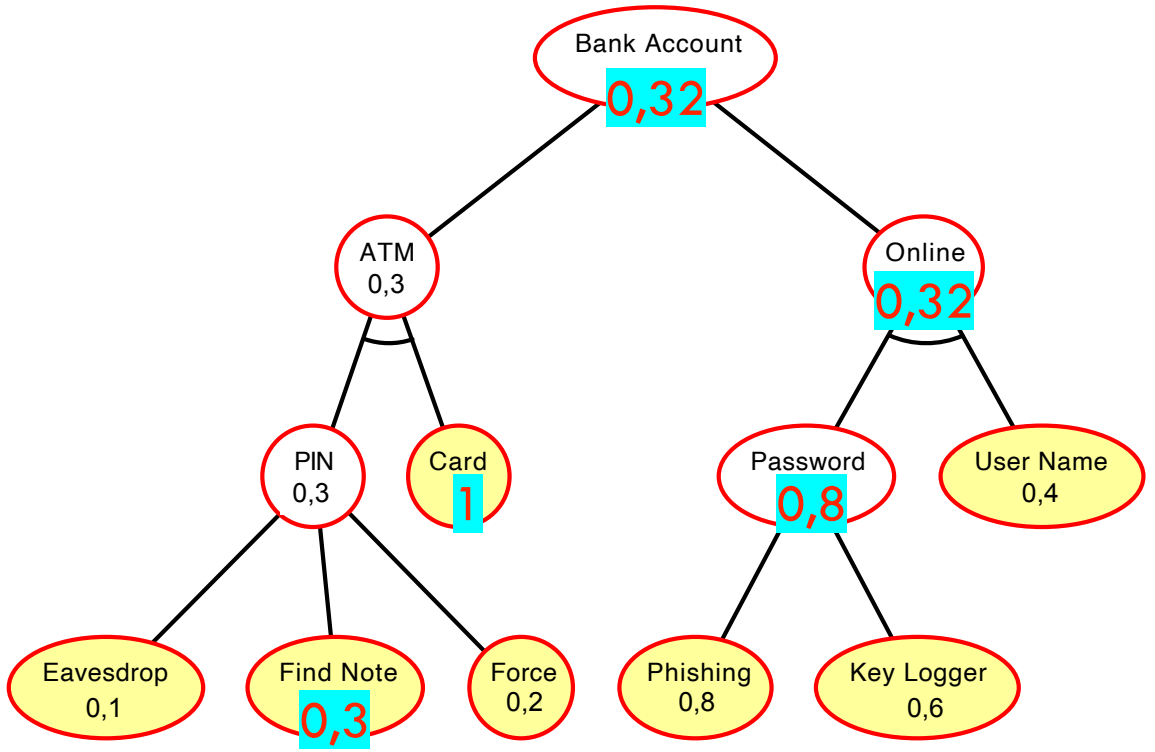
Exercise B.2. Which is the cheapest attack? {Force, Card}

Exercise B.3. True or False?

a) Every Attack Tree has exactly one cheapest attack. FALSE
b) In general, the cost of a feasible attack is greater than the most costly action in the tree. FALSE
c) In general, the cost of a feasible attack is greater than the most costly action in the attack. FALSE. First, an attack could consist of single action. Even if there are more actions they could have cost 0.
d) In general, the cheapest attack is cheaper than the sum of all attack actions. FALSE, for the same reasons as before.

SOLUTIONS

Consider the example Attack Tree on the right.



Exercise C.1. Complete the Attack Tree by adding the missing probabilities.

Exercise C.2. Which is most likely attack? {Phishing, User Name}

Exercise C.3. True or False?

a) The most likely attack and the least likely attack are always different. FALSE, there could be just one single attack in a tree.

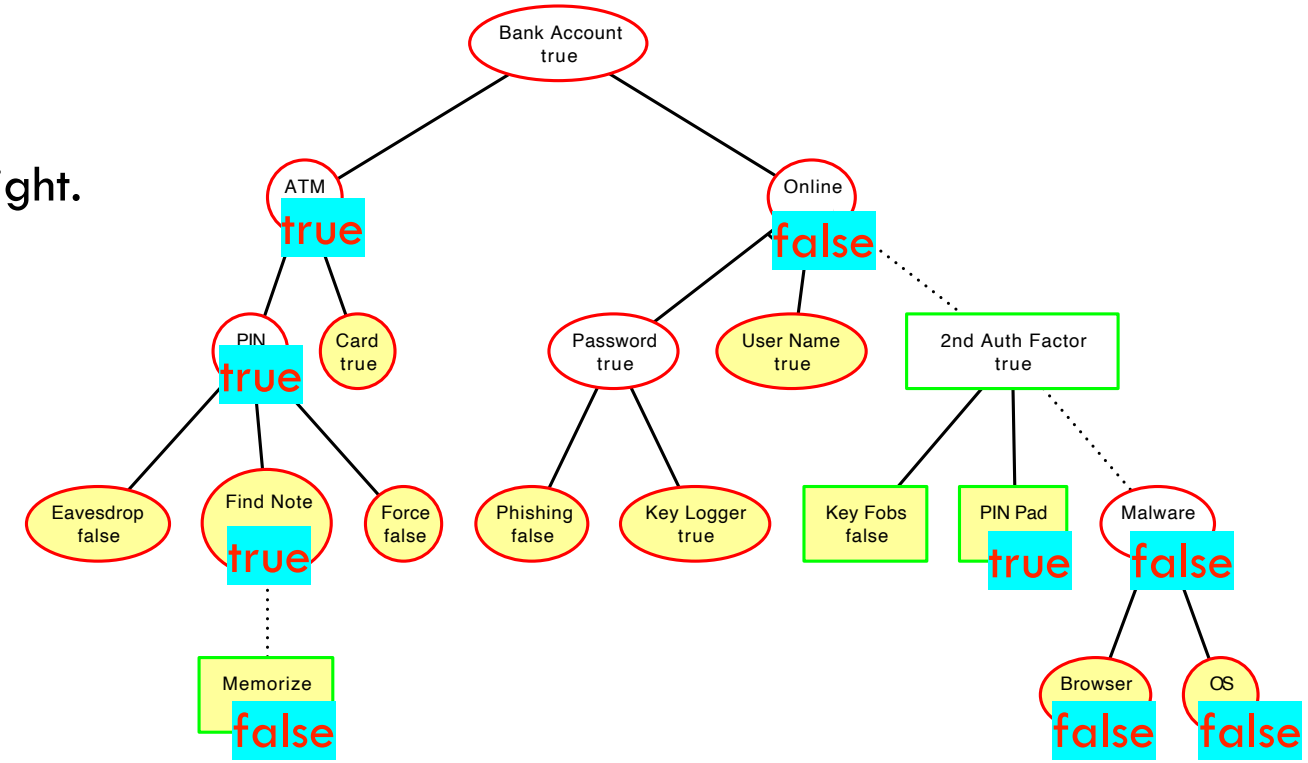
b) When comparing two attacks, the one with the most likely attack action will be the most likely attack. FALSE, we can see an example in the tree above, where Card has probability 1.

c) The probability of an attack is smaller than the product of all its attack actions. FALSE. An attack could consist of single action, have attacks with probability 1, combine them with OR, etc.

d) The probability of an attack is smaller than the probability of its most likely attack action. FALSE, for similar reasons as in (c).

SOLUTIONS

Consider the example Attack Tree on the right.



Exercise D.1. Complete the Attack Tree by adding the missing boolean annotations.

Exercise D.2. Which is the cheapest attack now? {Find Note, Card}
Which is the attack with highest probability of success? {Find Note, Card}

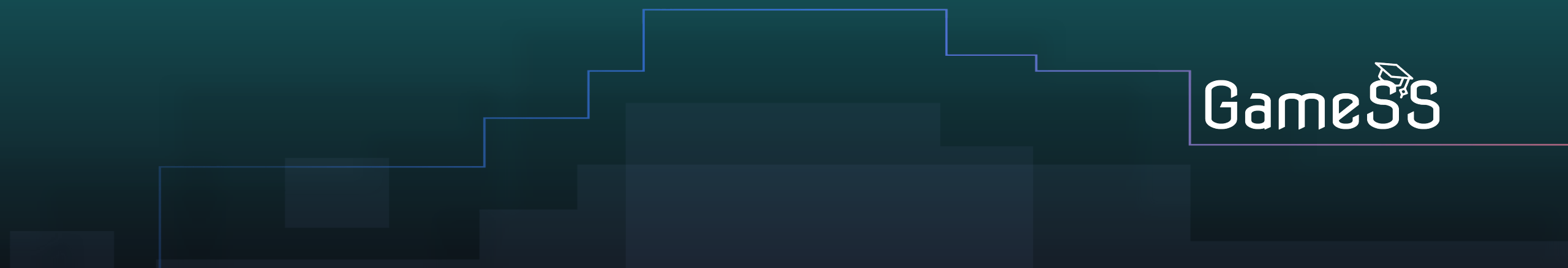
Exercise D.3. True or False?

a) A defence action that is not neutralised will neutralise all attack nodes on the way to the root. FALSE. For example, it could be not enabled or not acting on attack nodes on upper levels.

b) An attack action that is not neutralised will neutralise all defence nodes on the way to the root. FALSE, for similar reasons as above.

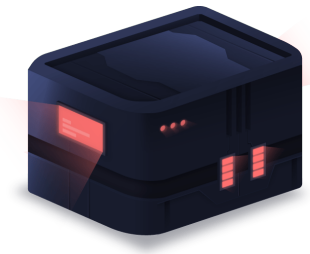
c) If all internal attack nodes have a corresponding countermeasure (defence action) then we can neutralise all attacks. TRUE

Challenges



CHALLENGES

- Challenges can be similar to the the exercises in the slides: given attack tree and partial assignment, complete assignment.
  - This can be done for Boolean, Costs and Probabilities
  - Input: Attack tree with partial assignment
  - Output: assignment in lexicographical order
  - Test of submission: just string matching
  - Example
    - Input: A = B or C, A = true, C = false
    - Question: Specify assignment for B
    - Output: B = true
- Other options that can be tested just via string matching:
  - Given attack tree, find out the smallest/cheapest/most likely attack
- Other options that could be more challenging to implement: given attack tree modify it to achieve some property.
  - Example: given attack tree and one feasible attack, introduce an optimal set of defences to prevent the attack



CHALLENGE #1

- Consider the “RFID Dos Attack” Attack Tree provided in ADTool (File > Load Example Tree).
- A preliminary evaluation has determined that the following attacks are unfeasible: Enter through Loading Dock, Pose as a Truck Driver, Distract Dog with Rats, Spray Pepper, Come as Visitor, Threaten, Blackmail, Disable Tag, Overload Tag, Disable Reader, Disable Backend, DoS in network, Blocker Reader, Blocker Tag.
- Moreover, the following defensive action is unfeasible: Attach with Stranger Adhesive.
- The possible defensive actions are hence given by this list: Barbed Wire, Monitor With BioMetric Sensors, Monitor with Security Cameras, Employ Guards, SnifferDog , Sniffer Dog, Escort Visitors, Register in Visitor's Log, Attend Visitor's Log, Presence Detectors on Premise, Attended Visitor's Log, Background Check, Security Awareness Training , Threaten to Fire Employees, Attach with Stronger Adhesive, Authenticate Tag, Secure Warehouse, Secure Warehouse, Faraday Around Tag and Reader.
- Your goal is to select the smallest set of defences to activate, so that any possible attack (not including the unfeasible actions above) is prevented.
- Once you have done so, you have to provide your solution as a list of defensive actions in the same order given in the above list. In other words, you have to provide the smallest sub-list that prevents all possible attacks.
- Answer format:
  - Defence names as they are provided above, use commas to separate, one blank space after the comma
  - Example: “Barbed Wire, Monitor With BioMetric Sensors”

Ideas to adapt & expand the teaching material

GameSS

IDEAS TO ADAPT & EXPAND THE TEACHING MATERIAL

- Group activities on discussing threats and countermeasures for a given system (e.g. a smart lock), using Attack Tree to guide the discussion.
- Finding examples of Attack Trees in scientific papers, discuss them, code them into ADTool and run various analyses.
- Present other threat modelling methodologies such as (STRIDE, Mitre ATT&CK…) and discuss their interplay with Attack Trees. How can they be used in a complementary way?
- Introduce formal semantics of Attack Trees, and formal definition of the various analyses for Attack Trees.
- Try out other Attack Tree tools, discuss their differences, pros/cons.

