Attack Trees

Adversarial Behaviours

Attack Trees

Adversarial Behaviours

- Origin of attack trees is **debatable**, NSA involved in development, Schneier evangelised.
- Conceptual diagrams for **considering and discussing** threats to systems.
- **Common technique** used across multiple domains and not restricted to computing science.
- Attacks trees can be considered a **formal** approach of organising, discussing and finding threats to systems.

Attack Trees

Adversarial Behaviours

- Afford designers to **capture**, **communicate** and **consider** various attacks at high-level.
- Act as **documentation** for systems of the consideration of particular attacks.
- Can construct **numerous** attack trees for multiple perspectives.
- Can create **library** of attack trees that can be reused in various instances.

Attack Trees

Adversarial Behaviours

- May reveal what is the **crucial attacks** to consider, rather than what is perceived.
- Concern that attack trees are **incomplete**, they always likely only represent what is known.
- Attack trees are a useful starting point, but the should be cemented with **research**, **investigation** and **peer-review.**

Root

Attack Trees

- **Ambiguity** about the root of an attack tree, can differ between approaches and assumptions by creators.
- Generally the root of an attack would be the **goal of the adversary** or high-impact action.
- **Motivation** for understanding the root influences the branches.

Root

Attack Trees

- **Adversary goal** we want to consider all the paths that are necessary to achieve the goal.
- **High-impact action**, then we should consider what would happen to cause the action to happen.
- These are the two perspectives restrict consideration around.
- Multiple perspectives and approaches can be adopted.

Goal

Attack Trees

Goal

Attack Trees

Attack Nodes

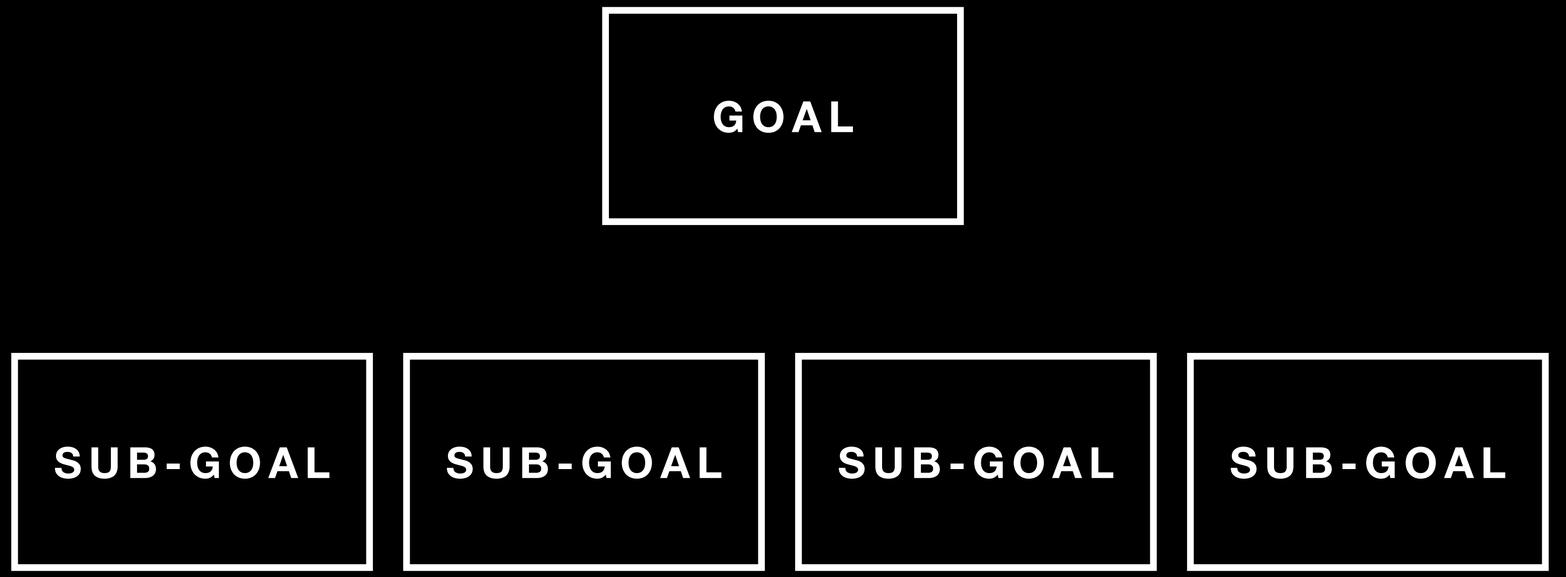
Attack Trees

- Common trees, may have similar **patterns** or predictable structure.
- Attacking system the first set of attack notes may be **physical access**, **compromise software** or **person**.
- **Attacking** a system via a people, process or technology.
- Attack system **during** its system, design, implementation, production etc.

Goal

Attack Trees

Sub-goal
Attack Trees



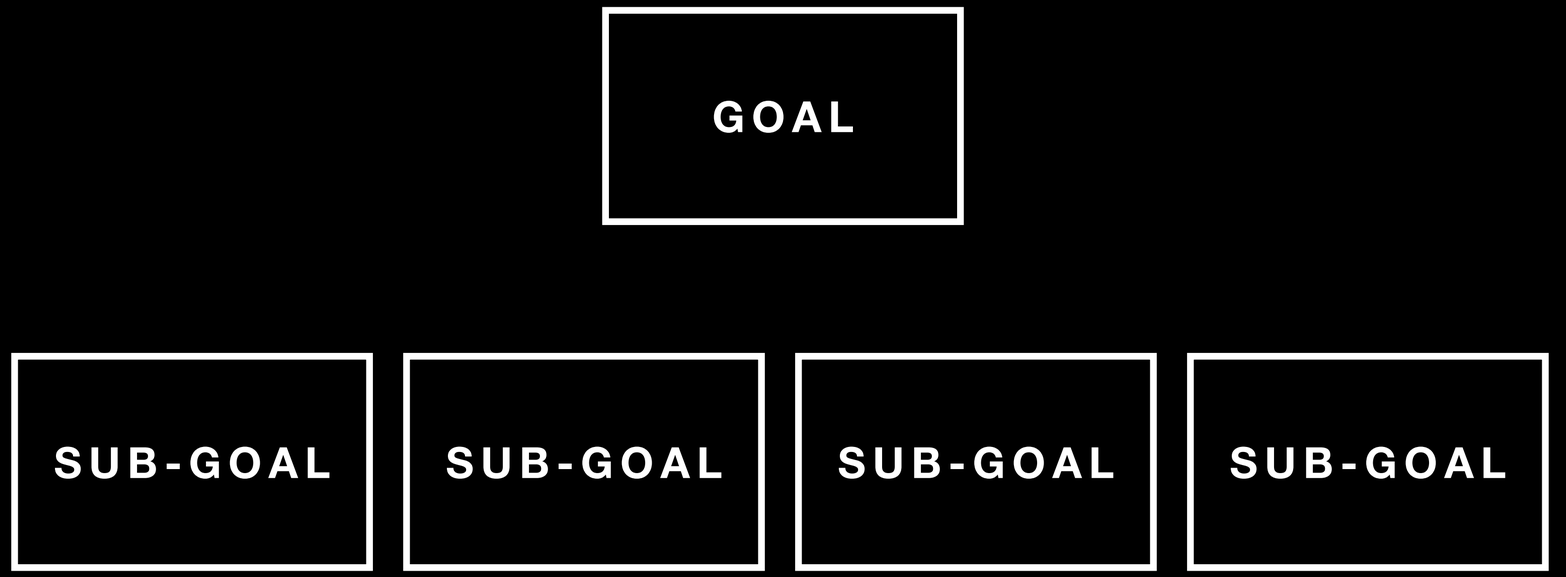
Sub-goal
Attack Trees

Sub-goal
Attack Trees

- Can consider each attack node in turn as **sub-goals** of the adversary.
- Each attack node can likely be **decomposed** into further sub-goals and so on and so forth.
- Each layer of sub-goals and can be considered another level when considering the attack.

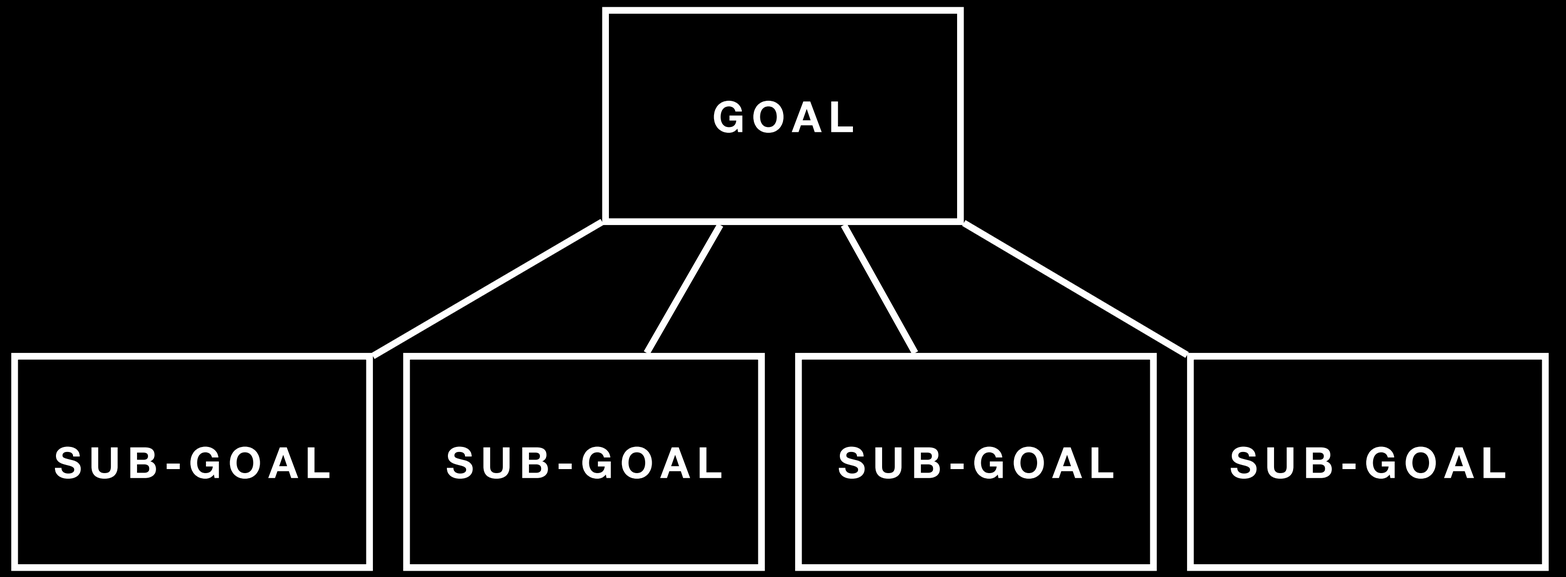
Sub-goal
Attack Trees

Sub-goal
Attack Trees



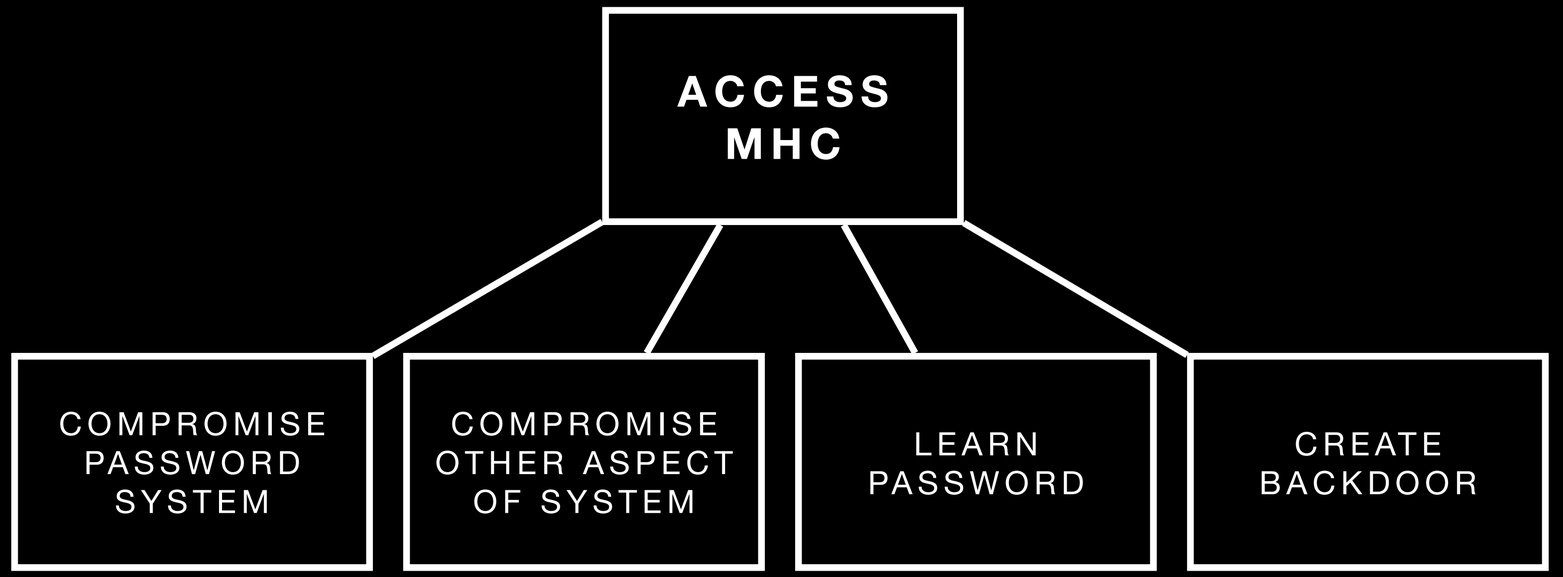
Achieving Goal

Attack Trees



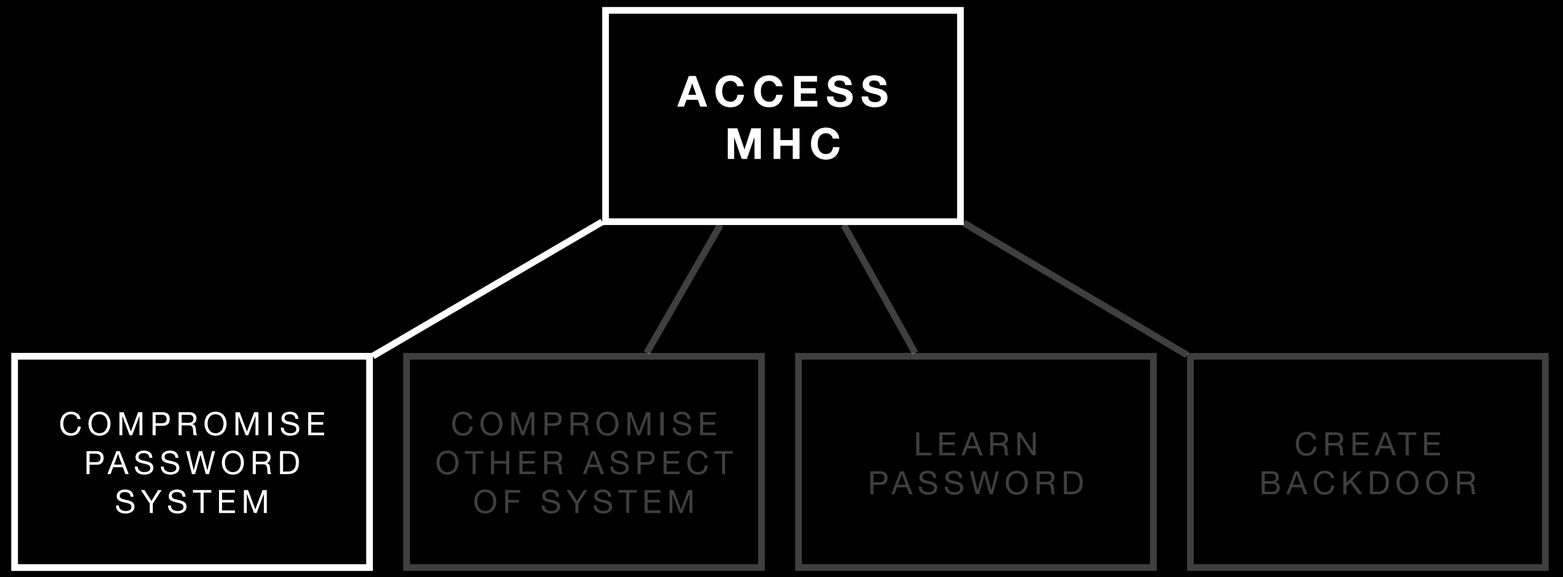
Achieving Goal

Attack Trees



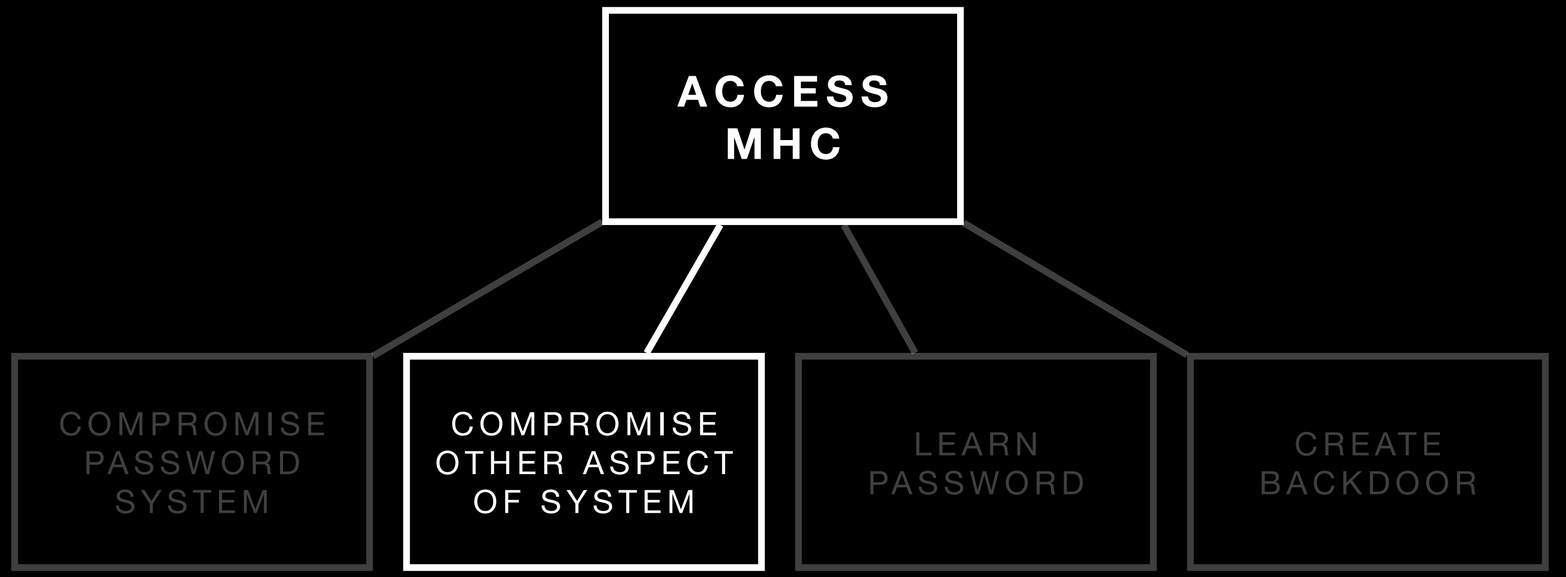
Achieving Goal

Attack Trees



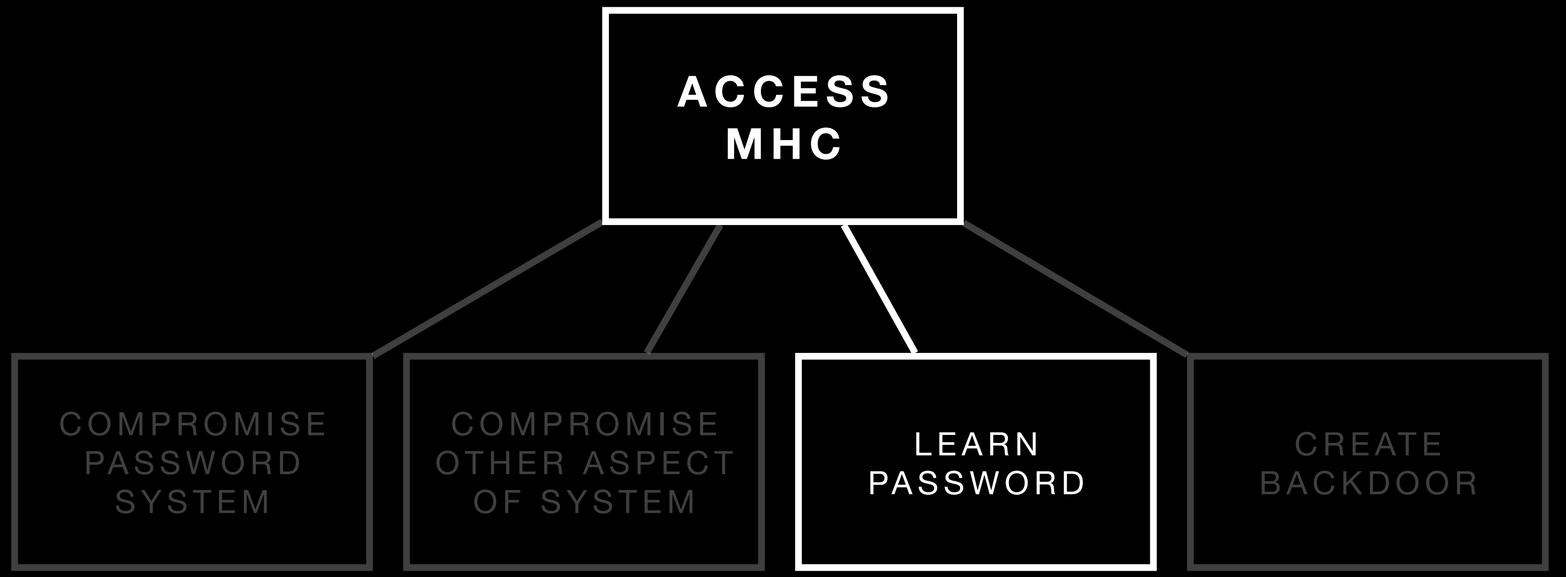
Achieving Goal

Attack Trees



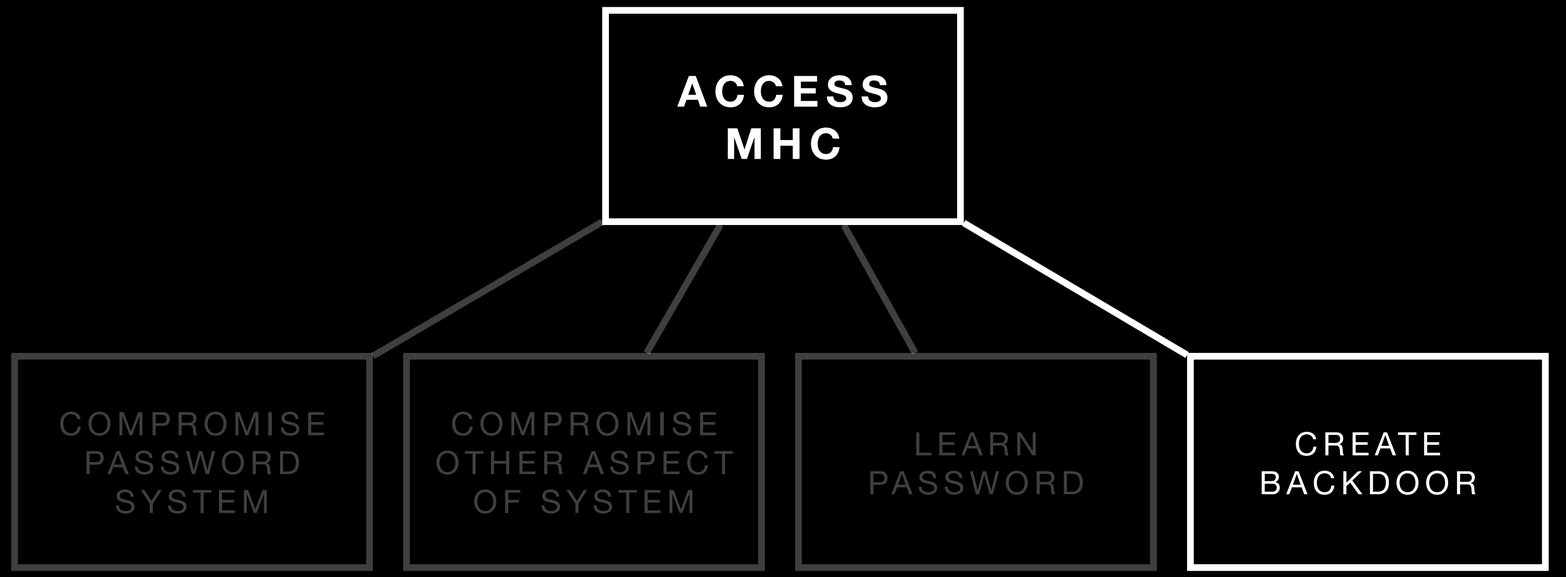
Achieving Goal

Attack Trees



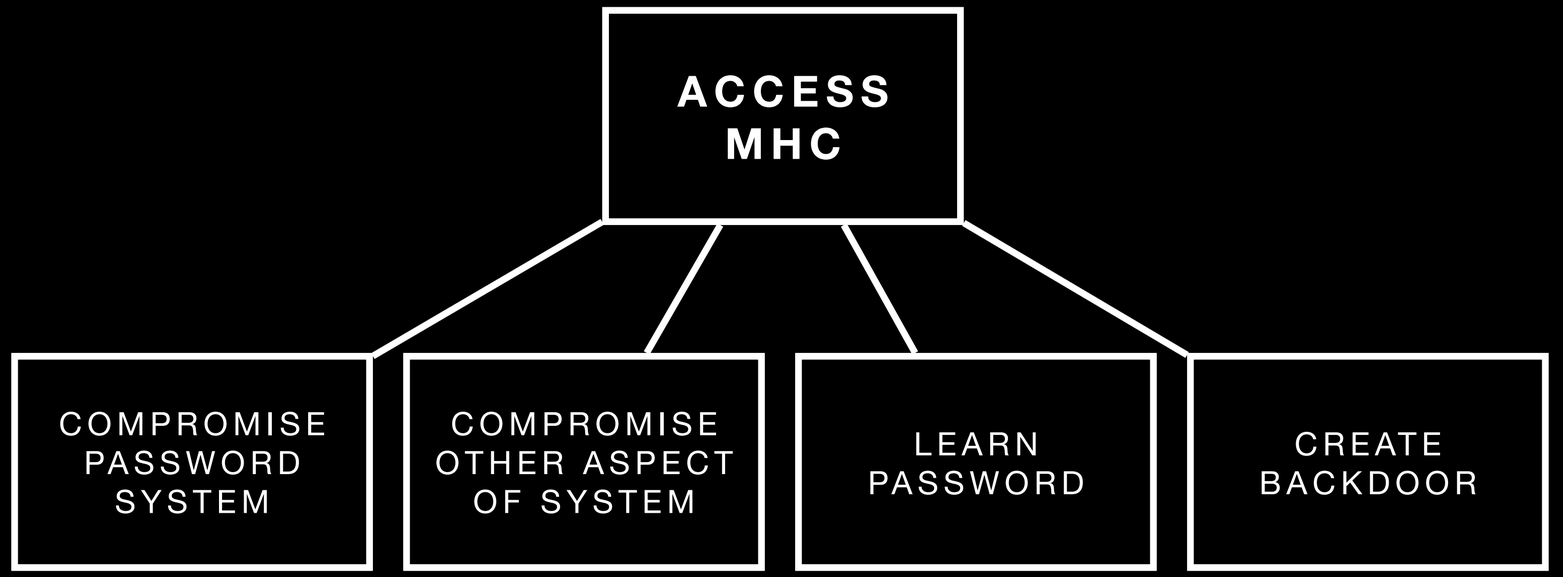
Achieving Goal

Attack Trees



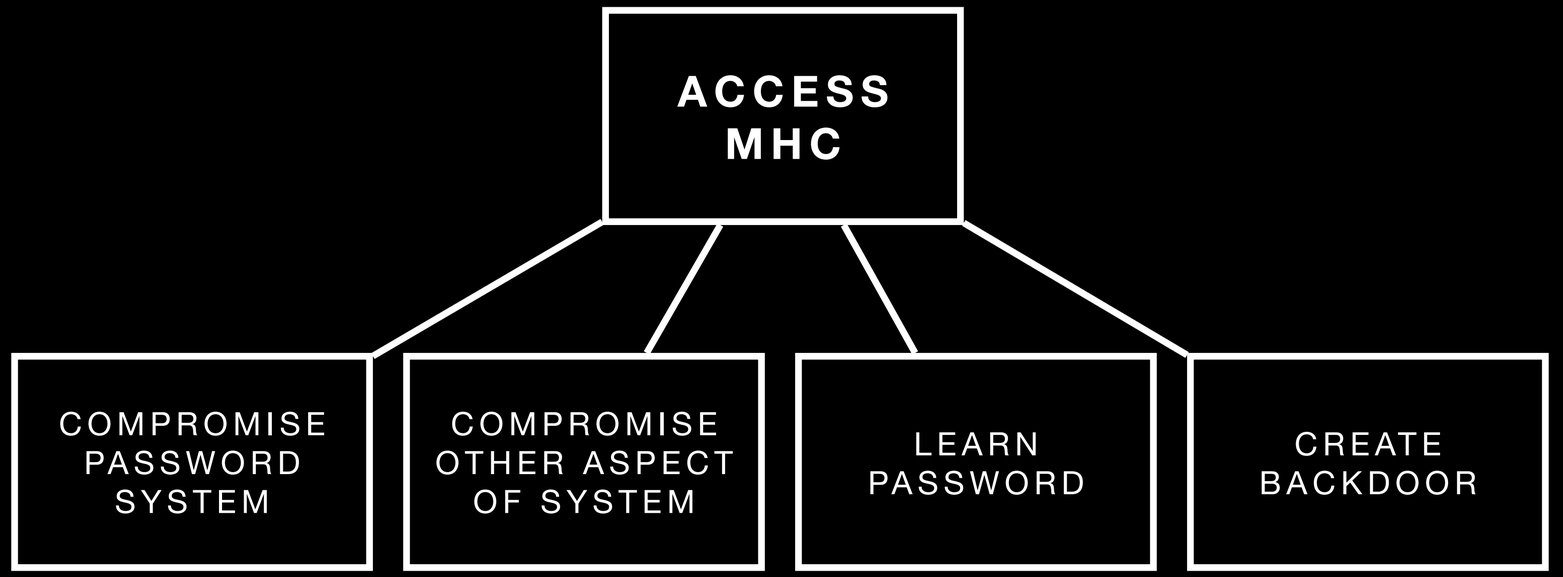
Achieving Goal

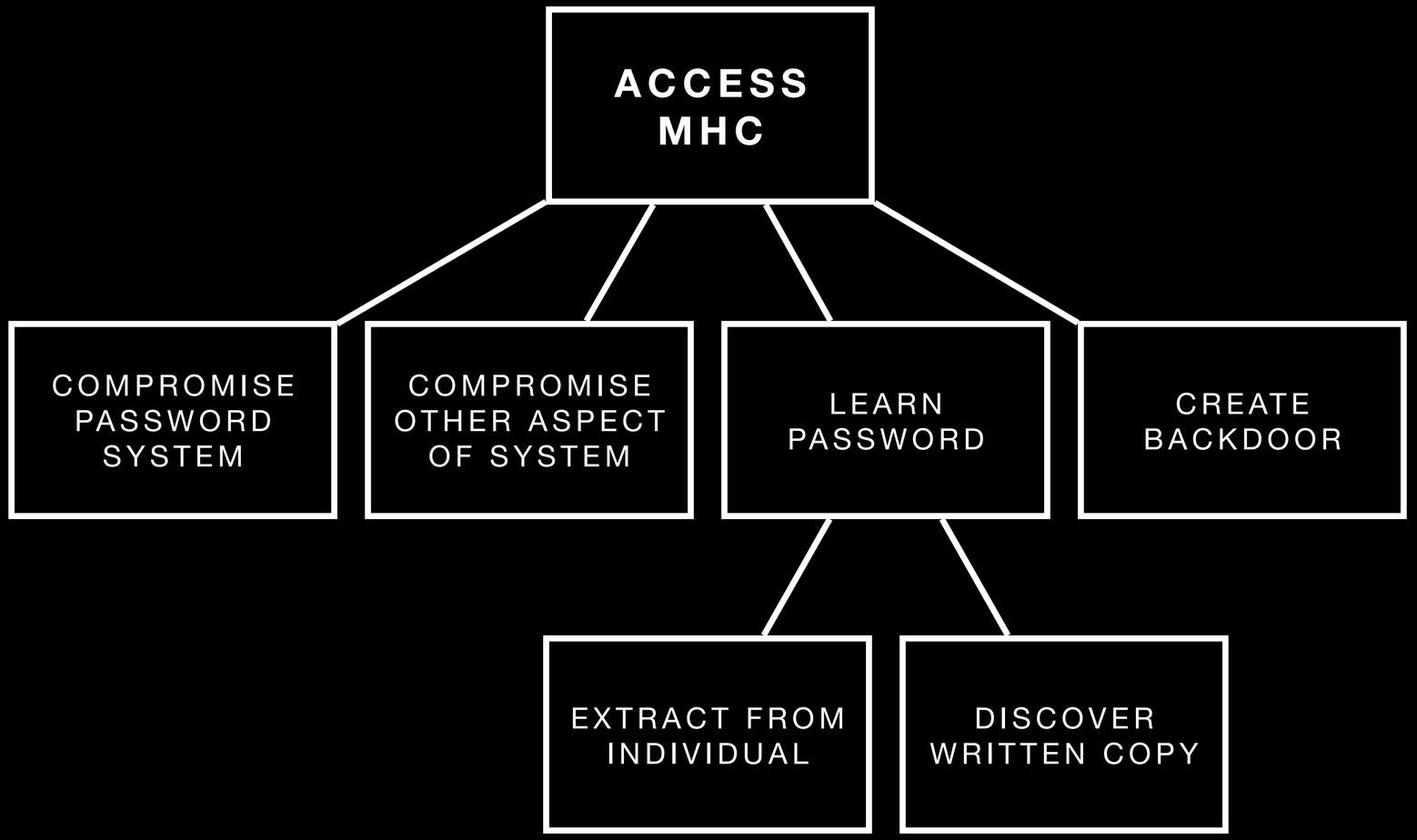
Attack Trees

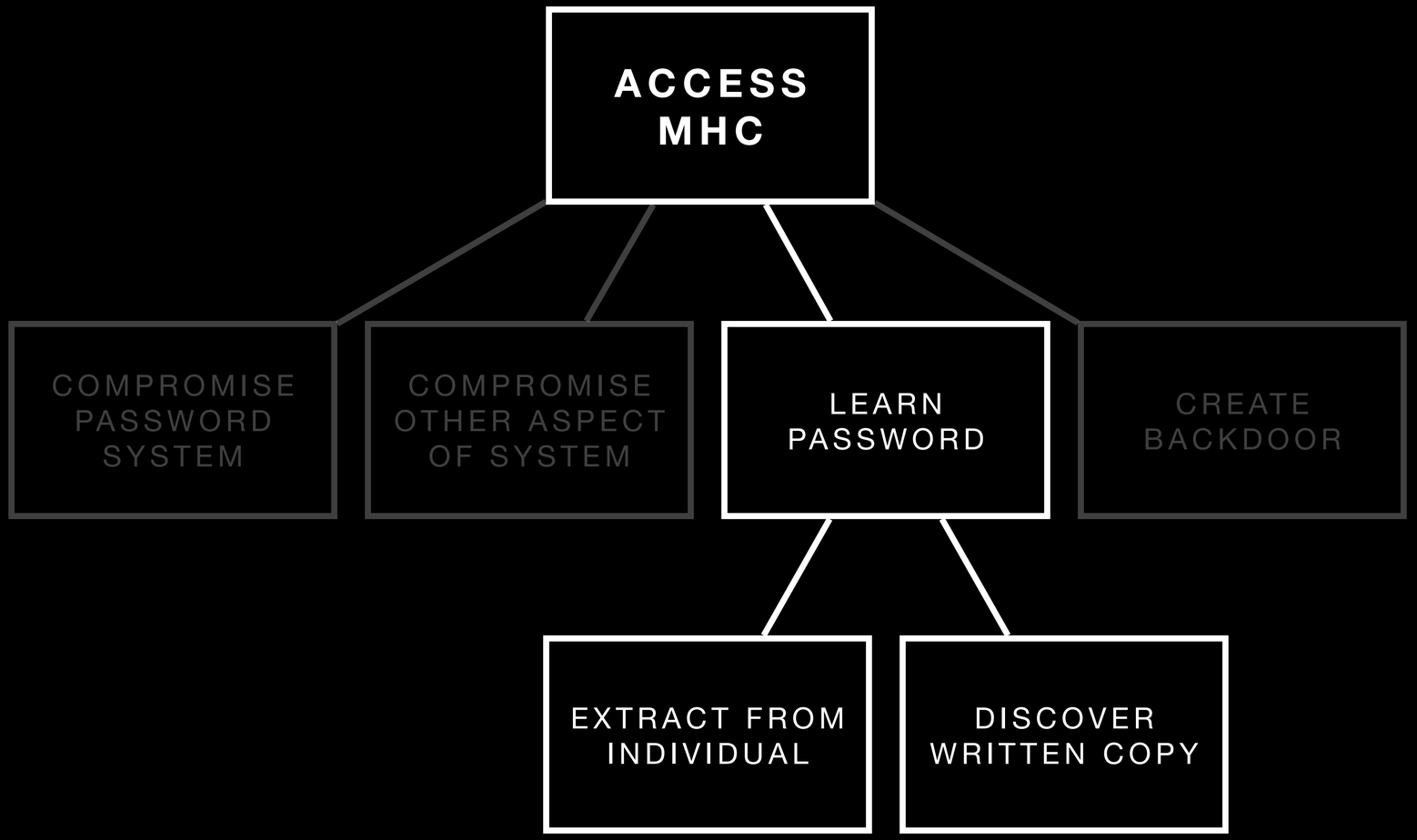


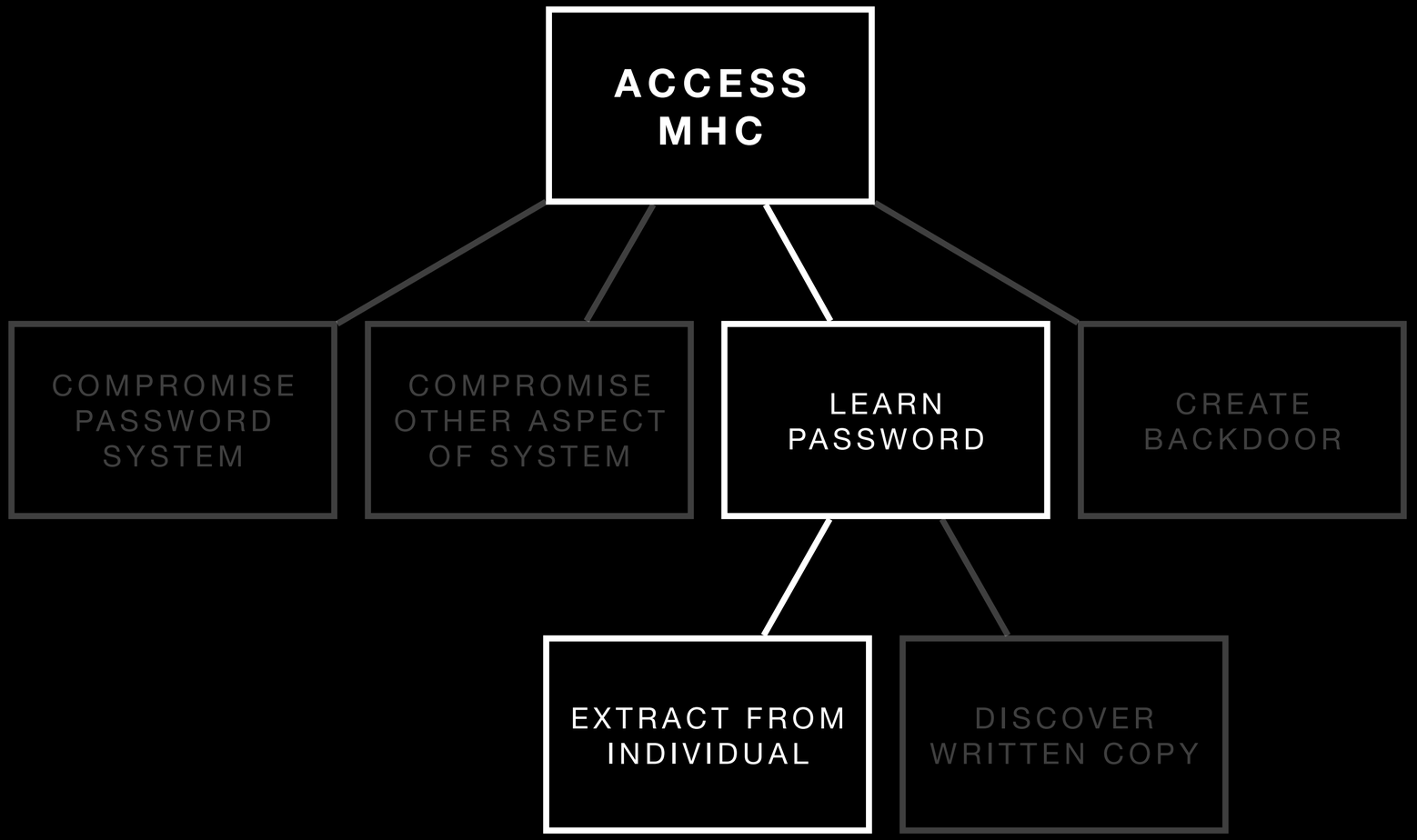
Achieving Goal

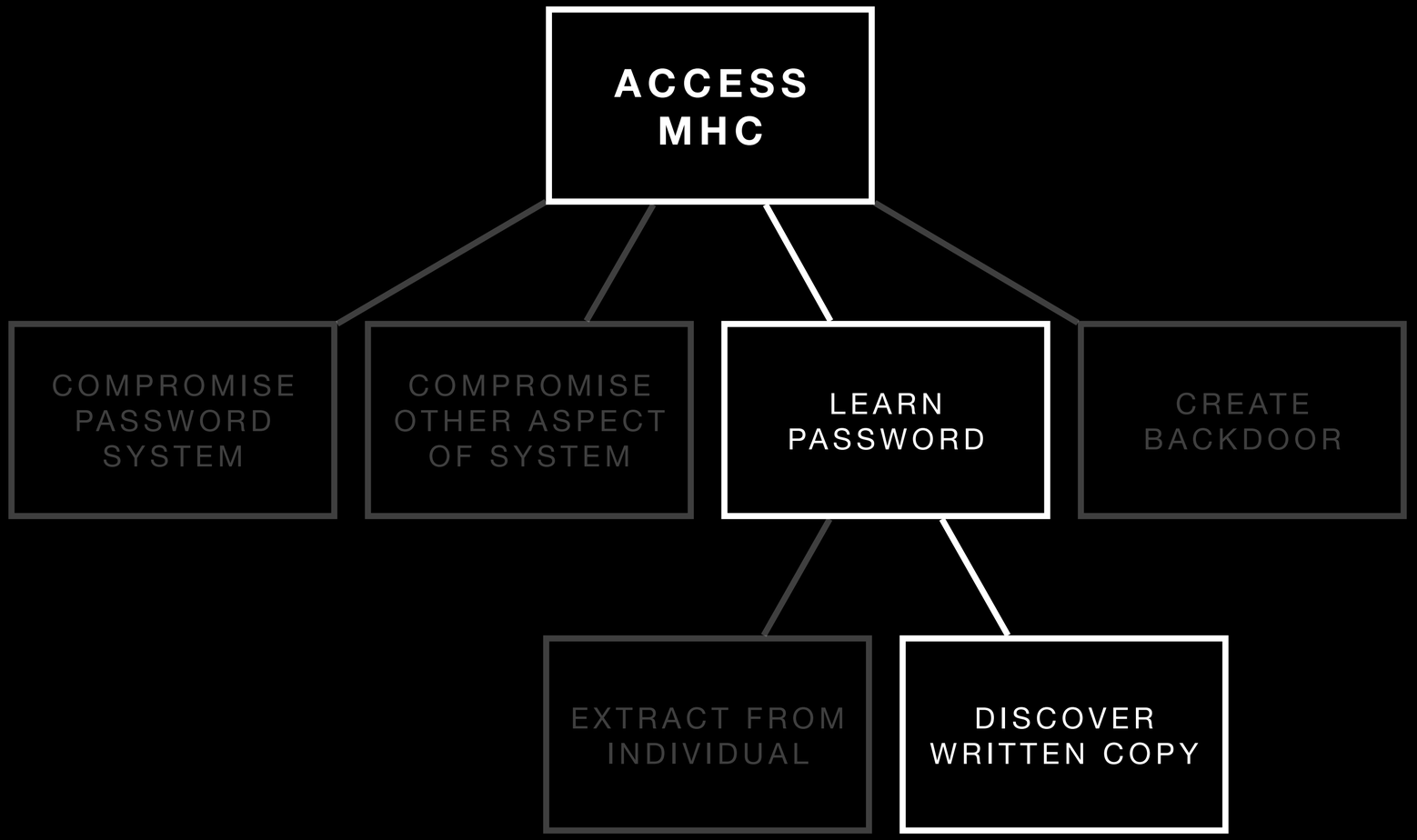
Attack Trees

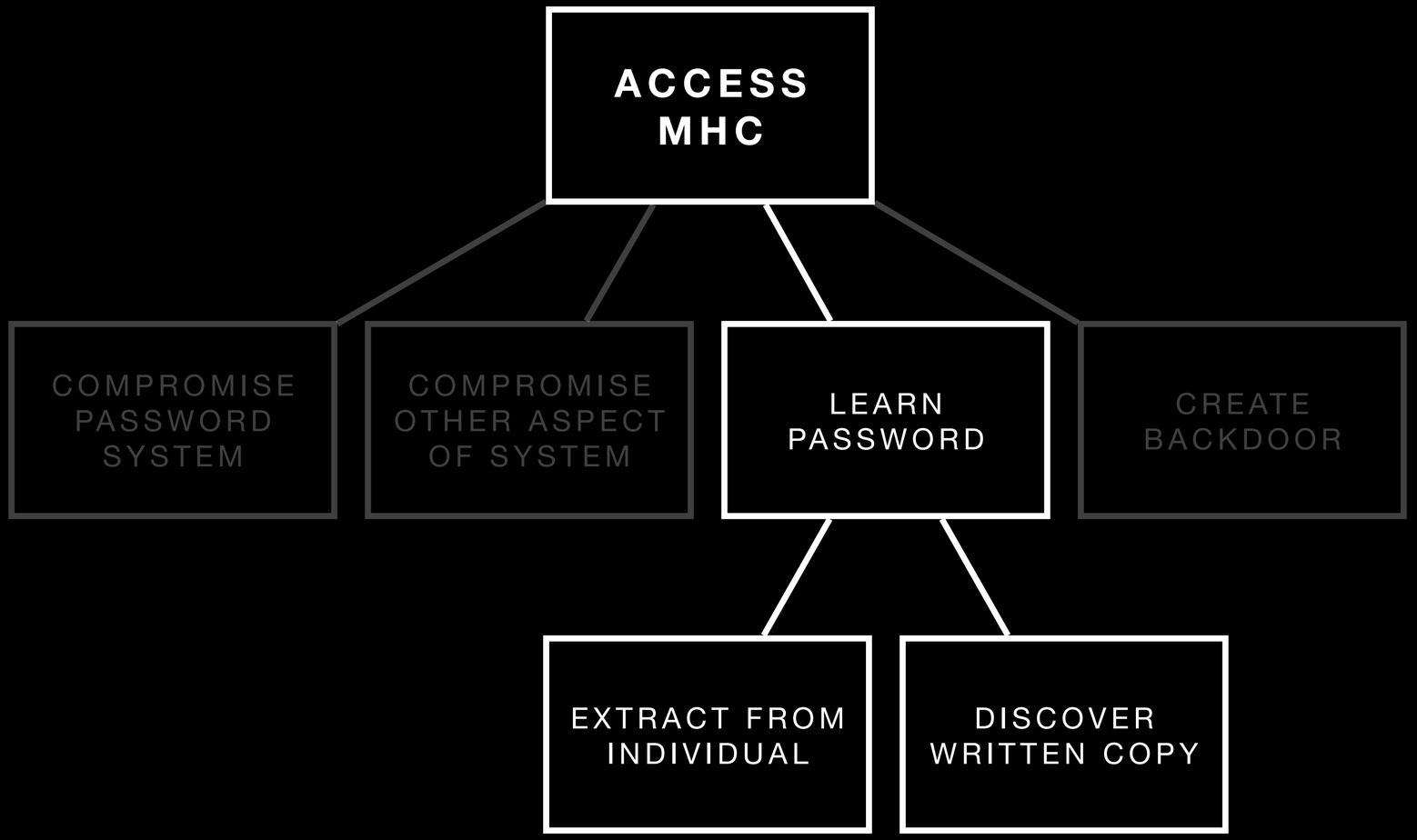


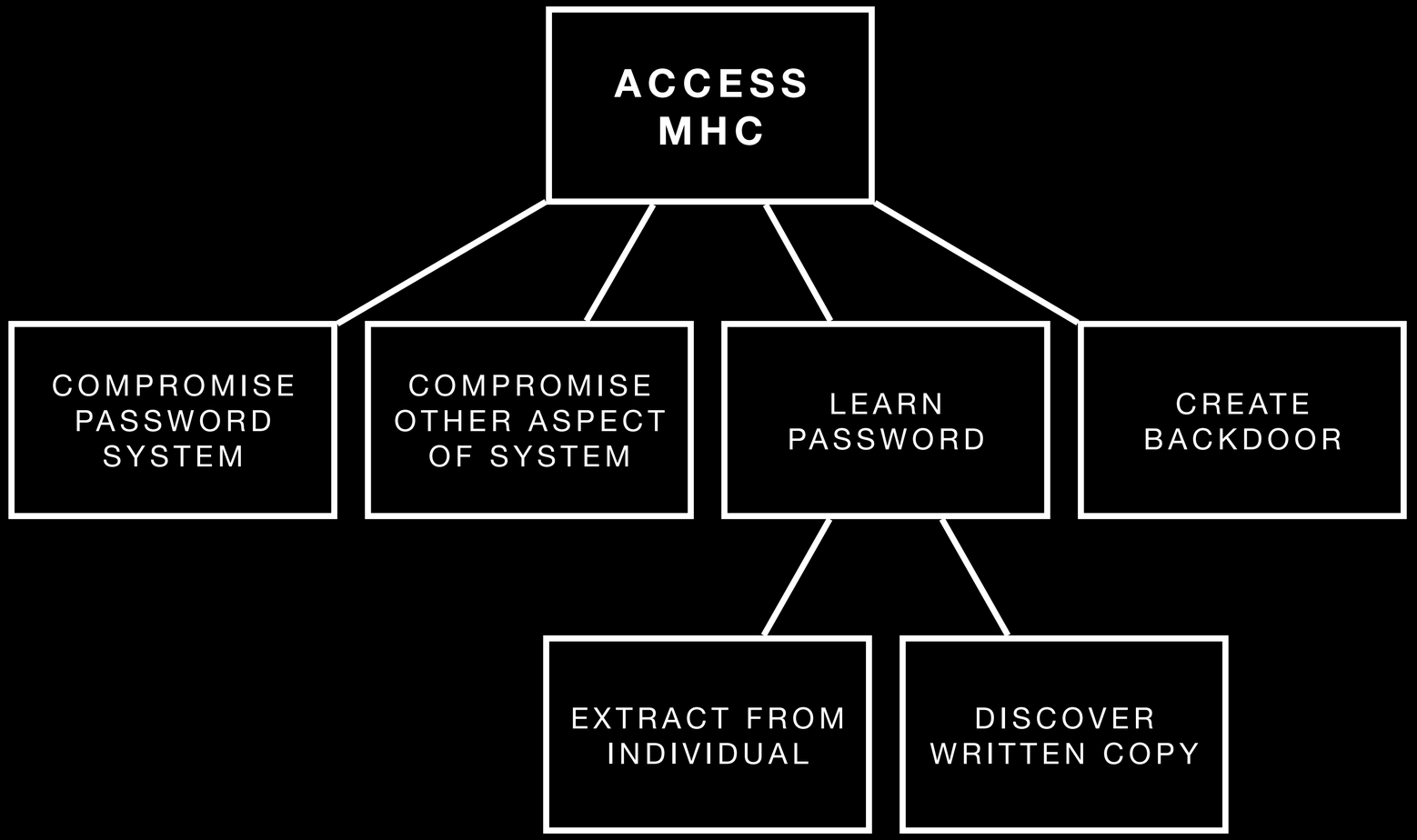

ACCESS MHC
COMPROMISE PASSWORD SYSTEM
COMPROMISE OTHER ASPECT OF SYSTEM
LEARN PASSWORD
CREATE BACKDOOR
EXTRACT FROM INDIVIDUAL
DISCOVER WRITTEN COPY

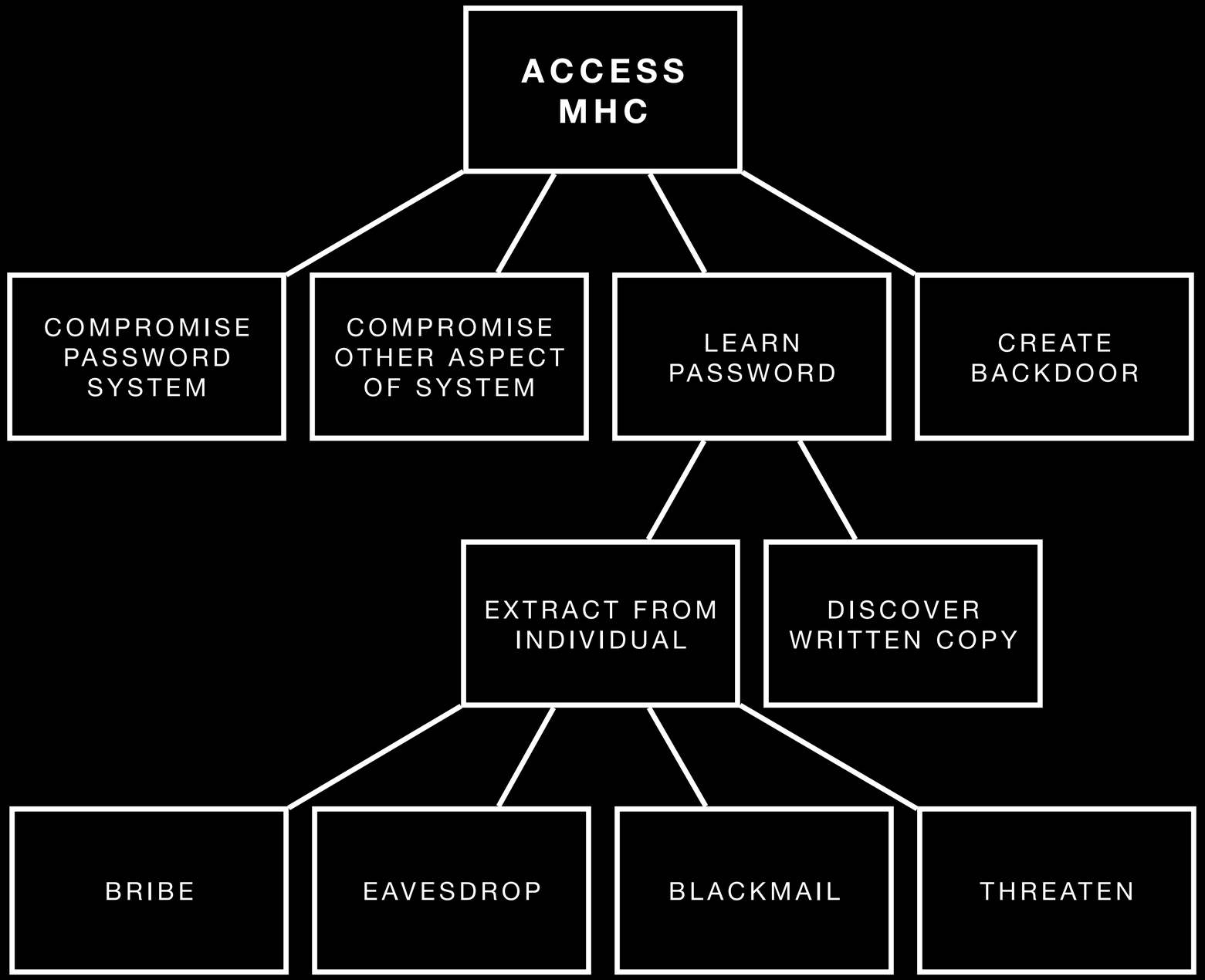

ACCESS MHC
COMPROMISE PASSWORD SYSTEM
COMPROMISE OTHER ASPECT OF SYSTEM
LEARN PASSWORD
CREATE BACKDOOR
EXTRACT FROM INDIVIDUAL
DISCOVER WRITTEN COPY

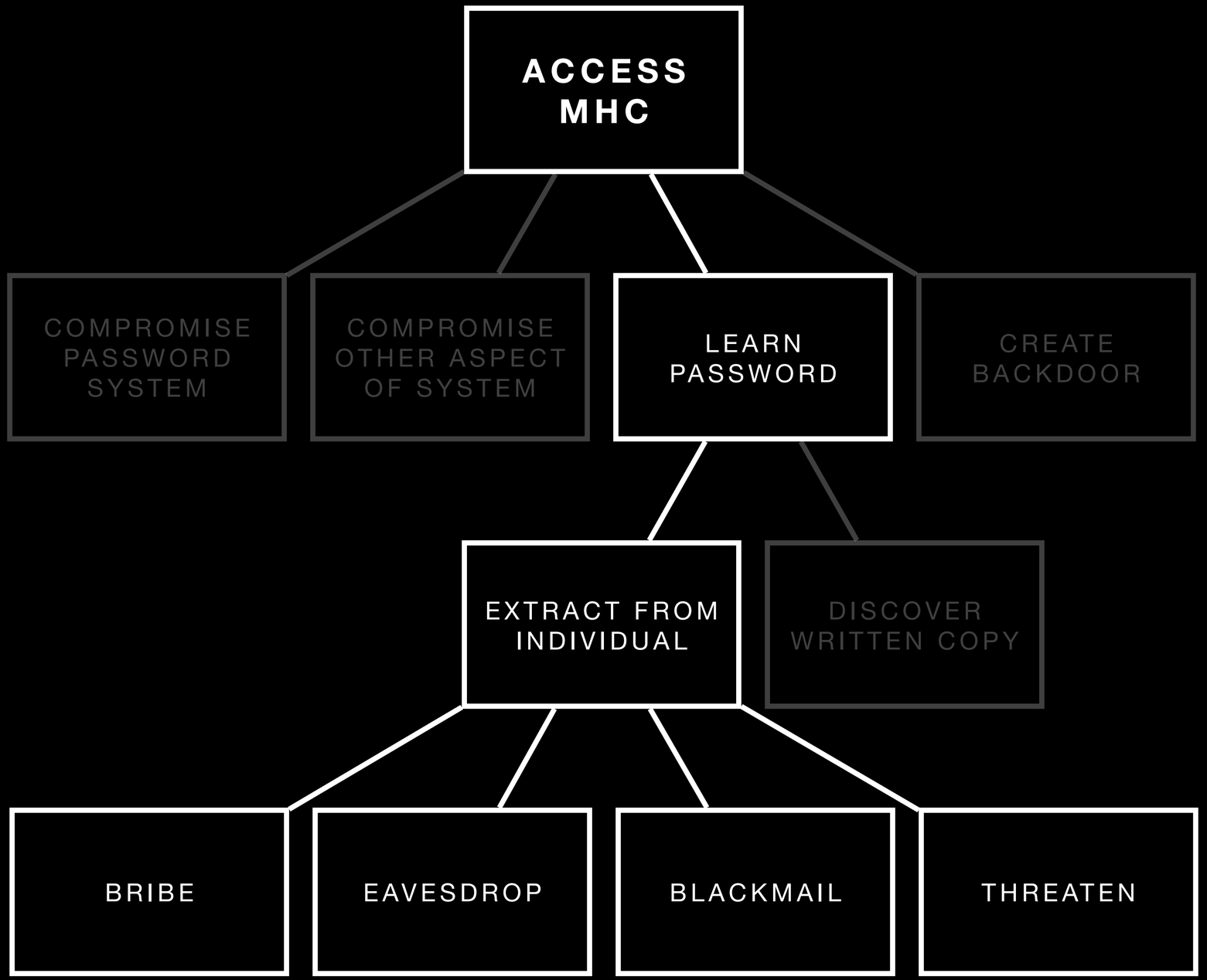

ACCESS MHC
COMPROMISE PASSWORD SYSTEM
COMPROMISE OTHER ASPECT OF SYSTEM
LEARN PASSWORD
CREATE BACKDOOR
EXTRACT FROM INDIVIDUAL
DISCOVER WRITTEN COPY

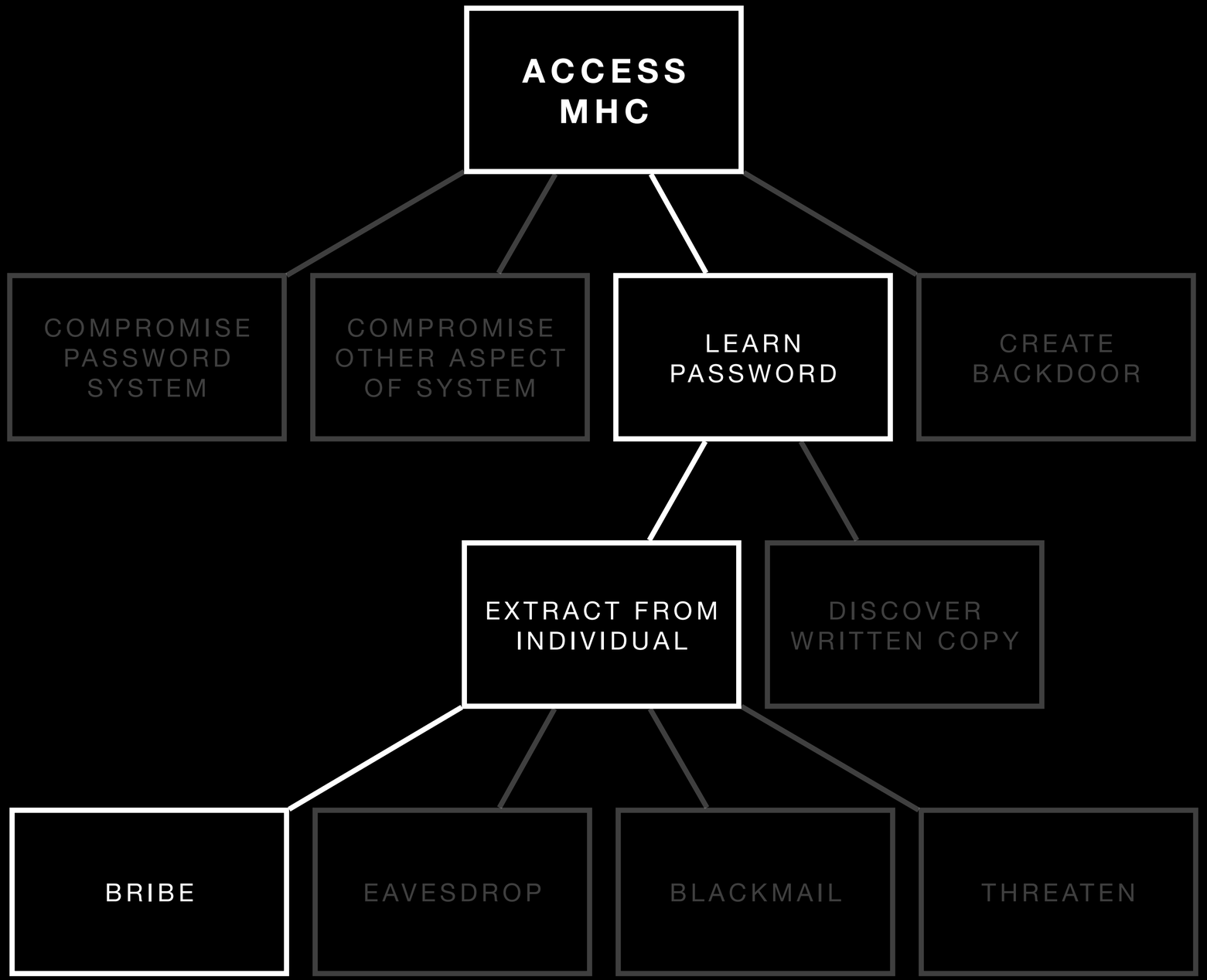

ACCESS MHC
COMPROMISE PASSWORD SYSTEM
COMPROMISE OTHER ASPECT OF SYSTEM
LEARN PASSWORD
CREATE BACKDOOR
EXTRACT FROM INDIVIDUAL
DISCOVER WRITTEN COPY

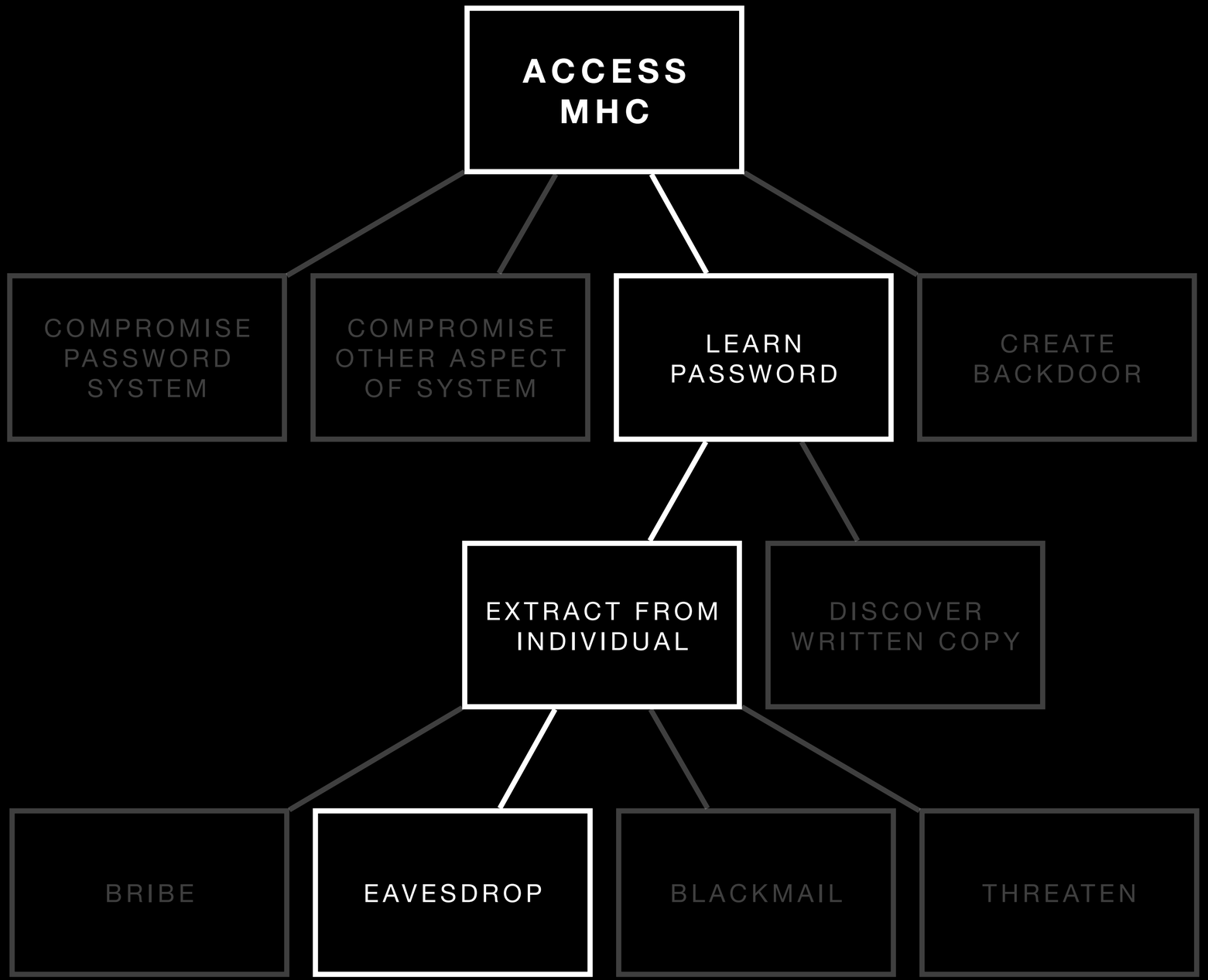

ACCESS MHC
COMPROMISE PASSWORD SYSTEM
COMPROMISE OTHER ASPECT OF SYSTEM
LEARN PASSWORD
CREATE BACKDOOR
EXTRACT FROM INDIVIDUAL
DISCOVER WRITTEN COPY

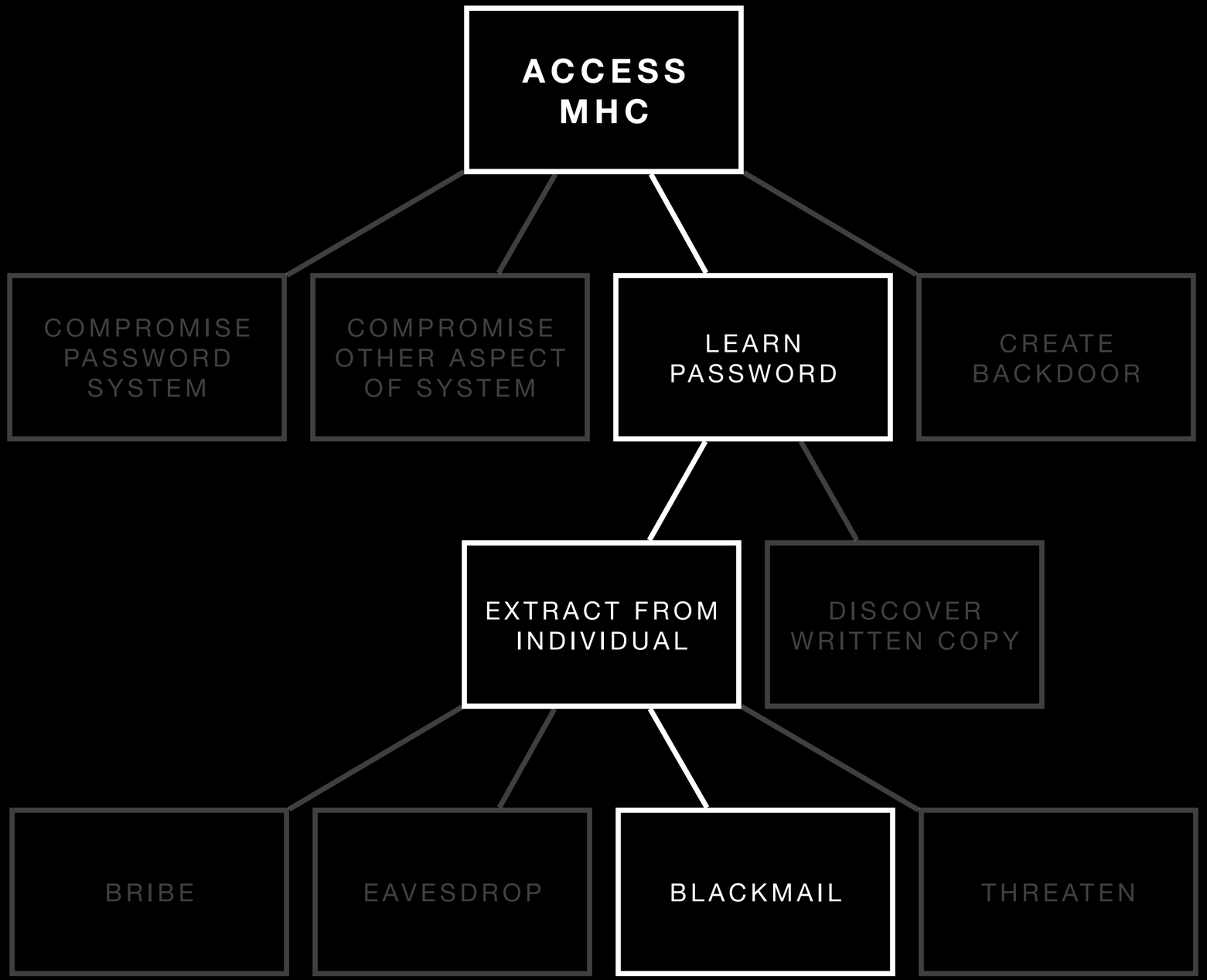

ACCESS MHC
COMPROMISE PASSWORD SYSTEM
COMPROMISE OTHER ASPECT OF SYSTEM
LEARN PASSWORD
CREATE BACKDOOR
EXTRACT FROM INDIVIDUAL
DISCOVER WRITTEN COPY

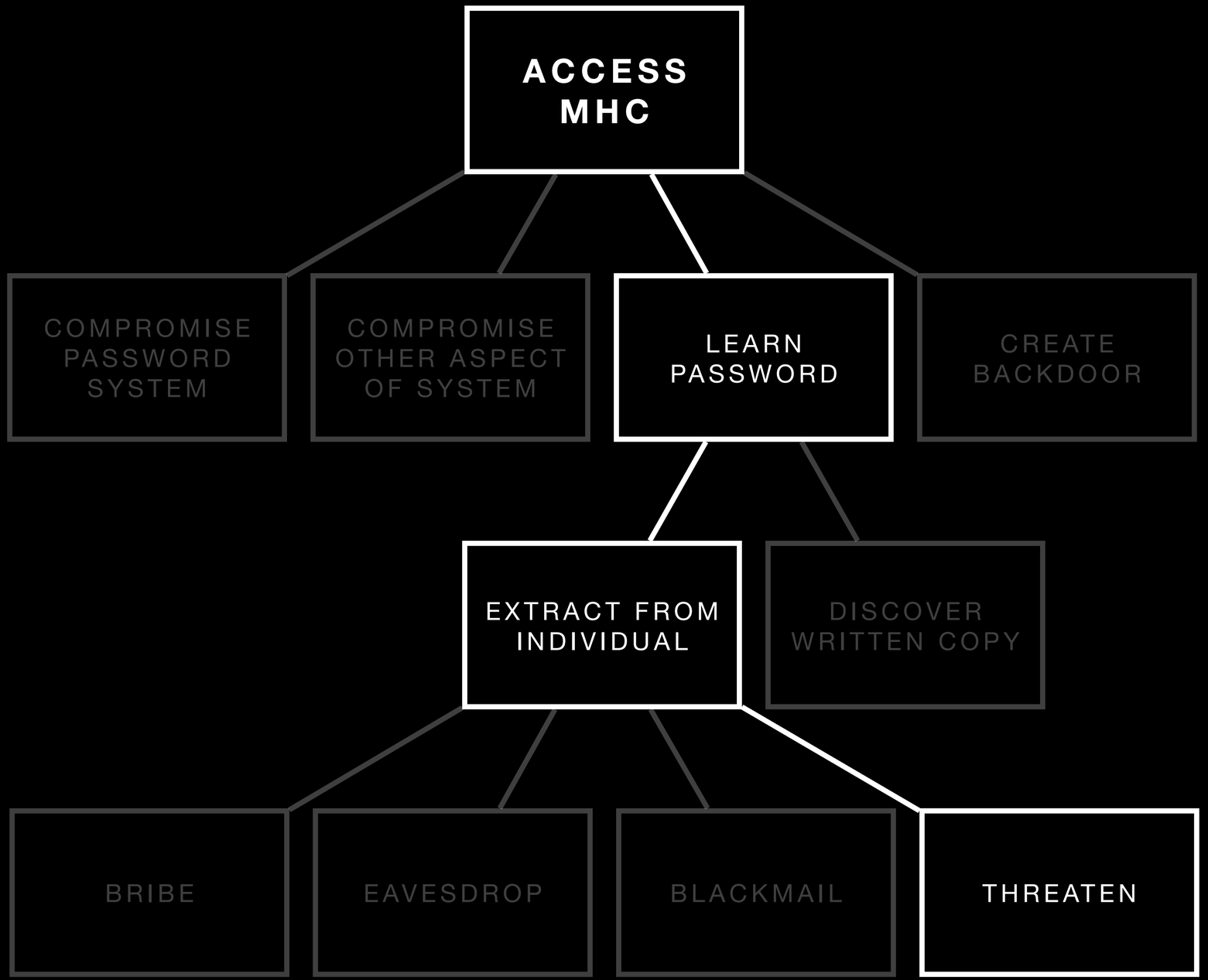

ACCESS MHC
COMPROMISE PASSWORD SYSTEM
COMPROMISE OTHER ASPECT OF SYSTEM
LEARN PASSWORD
CREATE BACKDOOR
EXTRACT FROM INDIVIDUAL
DISCOVER WRITTEN COPY
BRIBE
EAVESDROP
BLACKMAIL
THREATEN

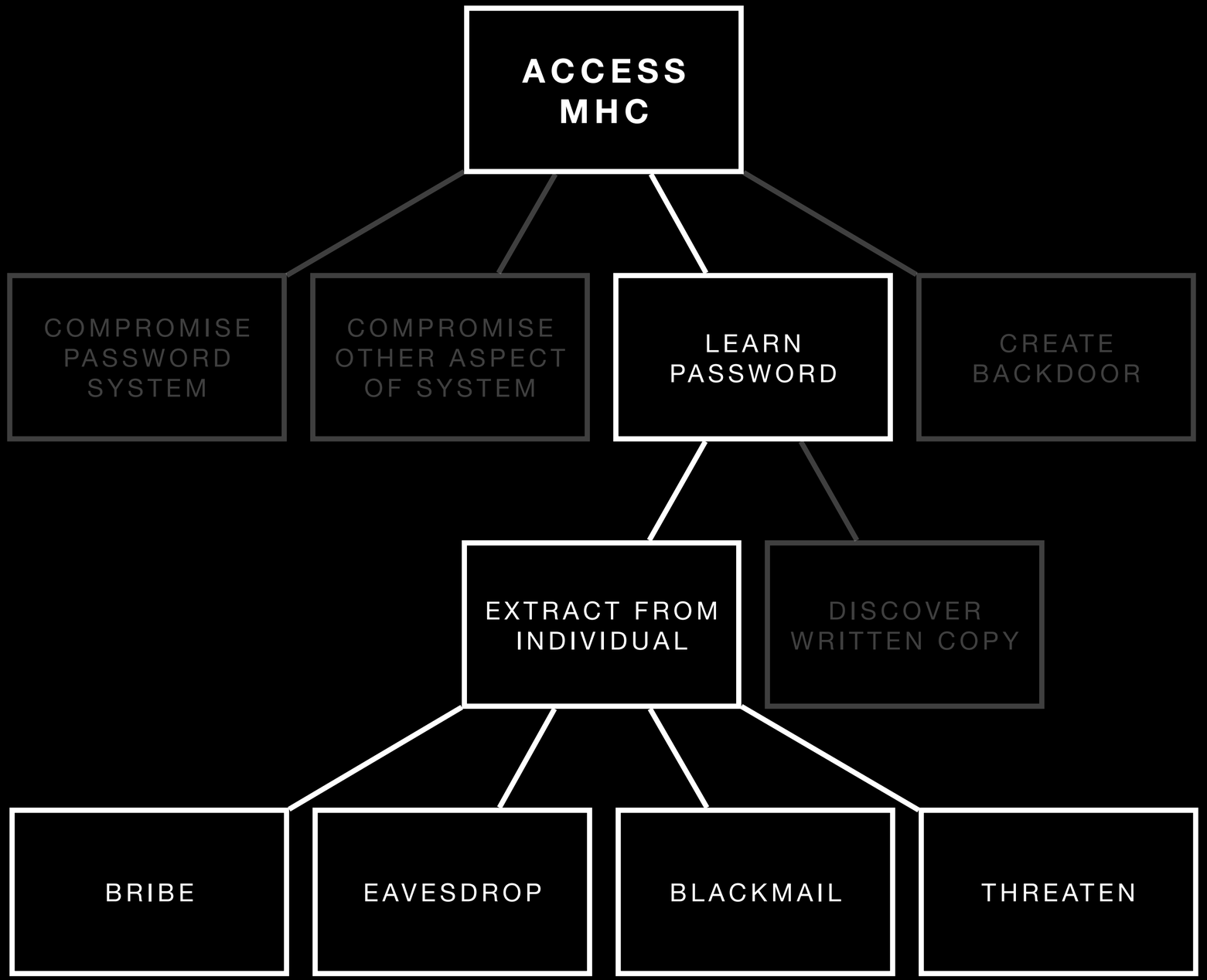

ACCESS MHC
COMPROMISE PASSWORD SYSTEM
COMPROMISE OTHER ASPECT OF SYSTEM
LEARN PASSWORD
CREATE BACKDOOR
EXTRACT FROM INDIVIDUAL
DISCOVER WRITTEN COPY
BRIBE
EAVESDROP
BLACKMAIL
THREATEN

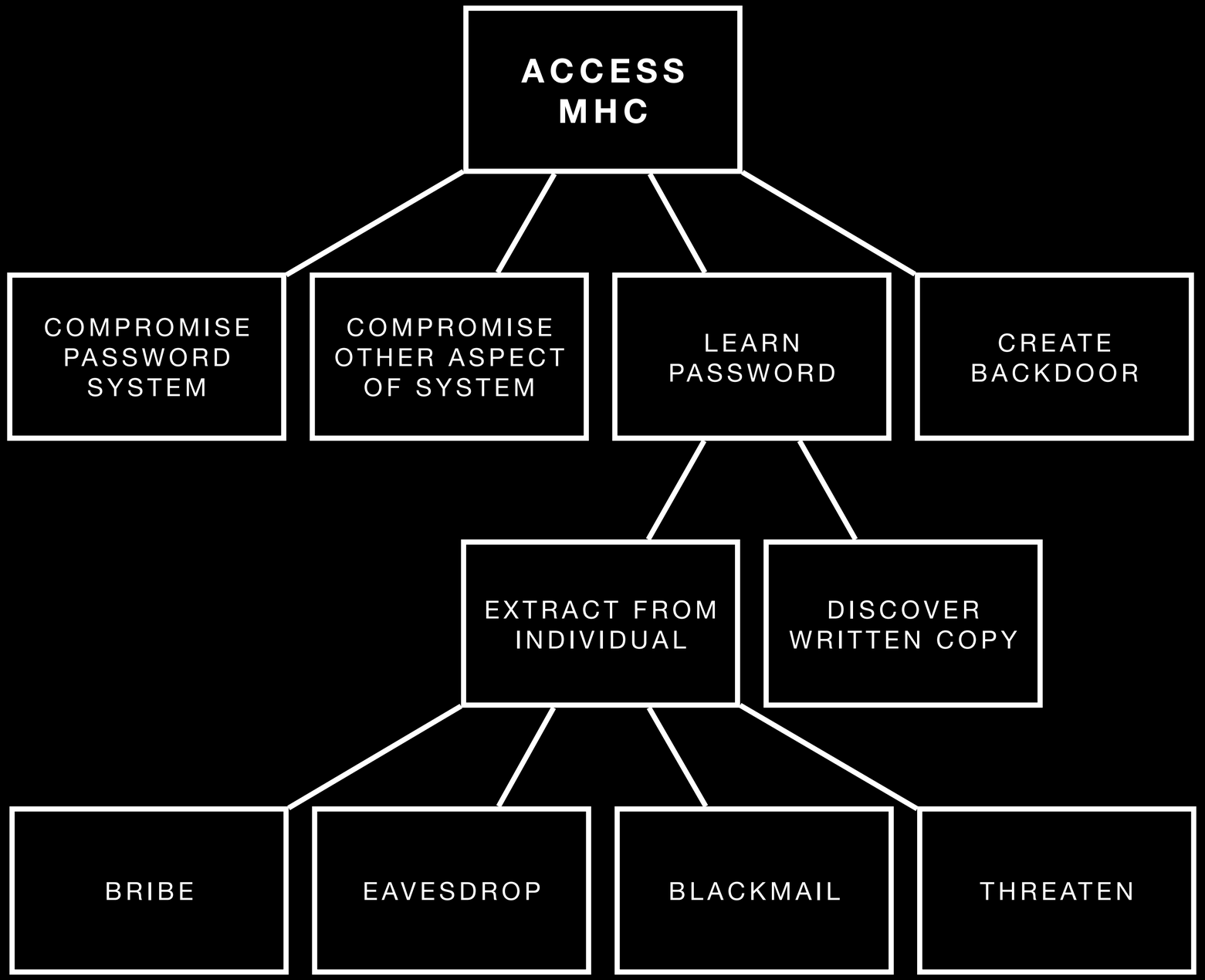

ACCESS MHC
COMPROMISE PASSWORD SYSTEM
COMPROMISE OTHER ASPECT OF SYSTEM
LEARN PASSWORD
CREATE BACKDOOR
EXTRACT FROM INDIVIDUAL
DISCOVER WRITTEN COPY
BRIBE
EAVESDROP
BLACKMAIL
THREATEN


ACCESS MHC
COMPROMISE PASSWORD SYSTEM
COMPROMISE OTHER ASPECT OF SYSTEM
LEARN PASSWORD
CREATE BACKDOOR
EXTRACT FROM INDIVIDUAL
DISCOVER WRITTEN COPY
BRIBE
EAVESDROP
BLACKMAIL
THREATEN


ACCESS MHC
COMPROMISE PASSWORD SYSTEM
COMPROMISE OTHER ASPECT OF SYSTEM
LEARN PASSWORD
CREATE BACKDOOR
EXTRACT FROM INDIVIDUAL
DISCOVER WRITTEN COPY
BRIBE
EAVESDROP
BLACKMAIL
THREATEN

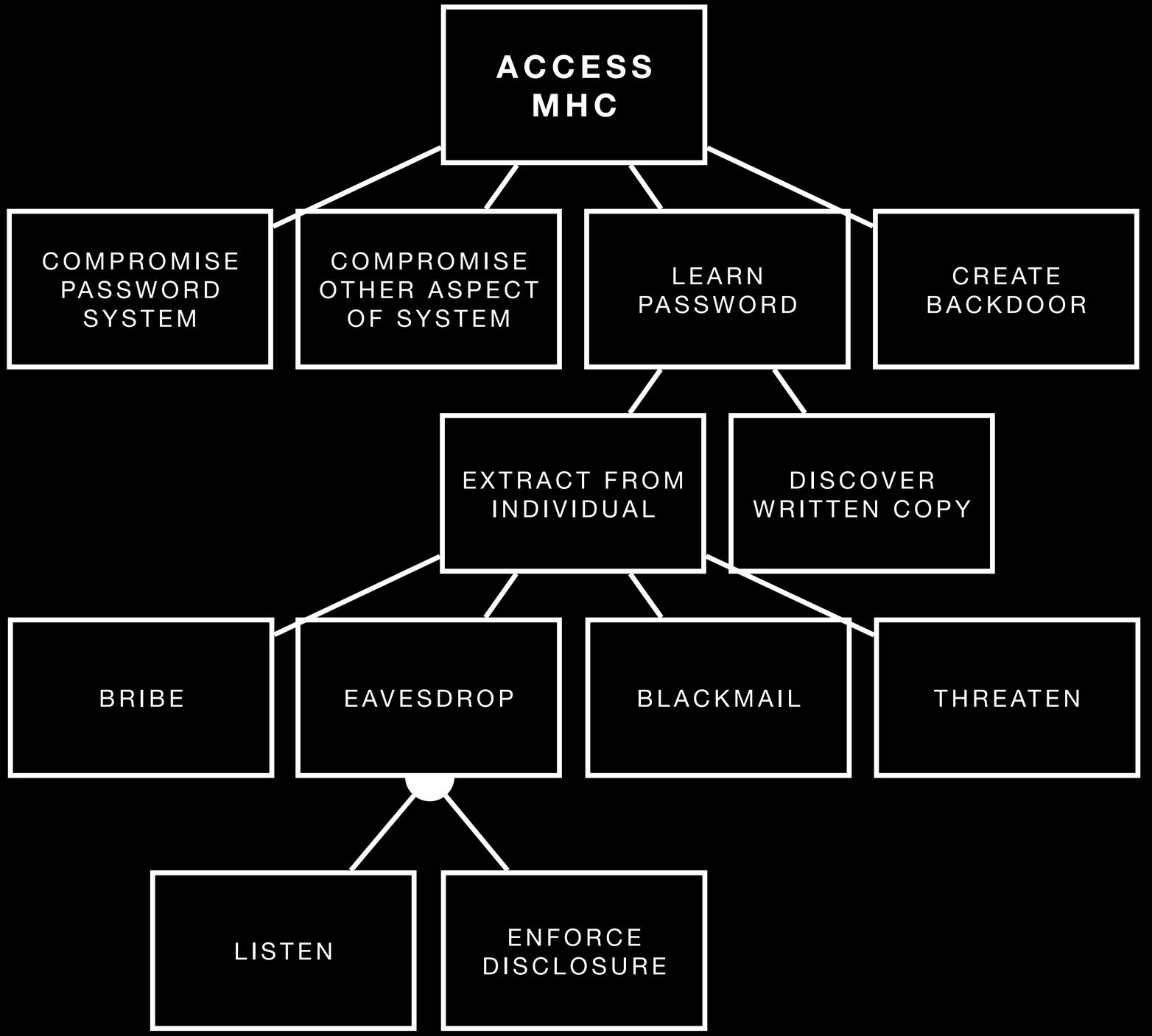

ACCESS MHC
COMPROMISE PASSWORD SYSTEM
COMPROMISE OTHER ASPECT OF SYSTEM
LEARN PASSWORD
CREATE BACKDOOR
EXTRACT FROM INDIVIDUAL
DISCOVER WRITTEN COPY
BRIBE
EAVESDROP
BLACKMAIL
THREATEN

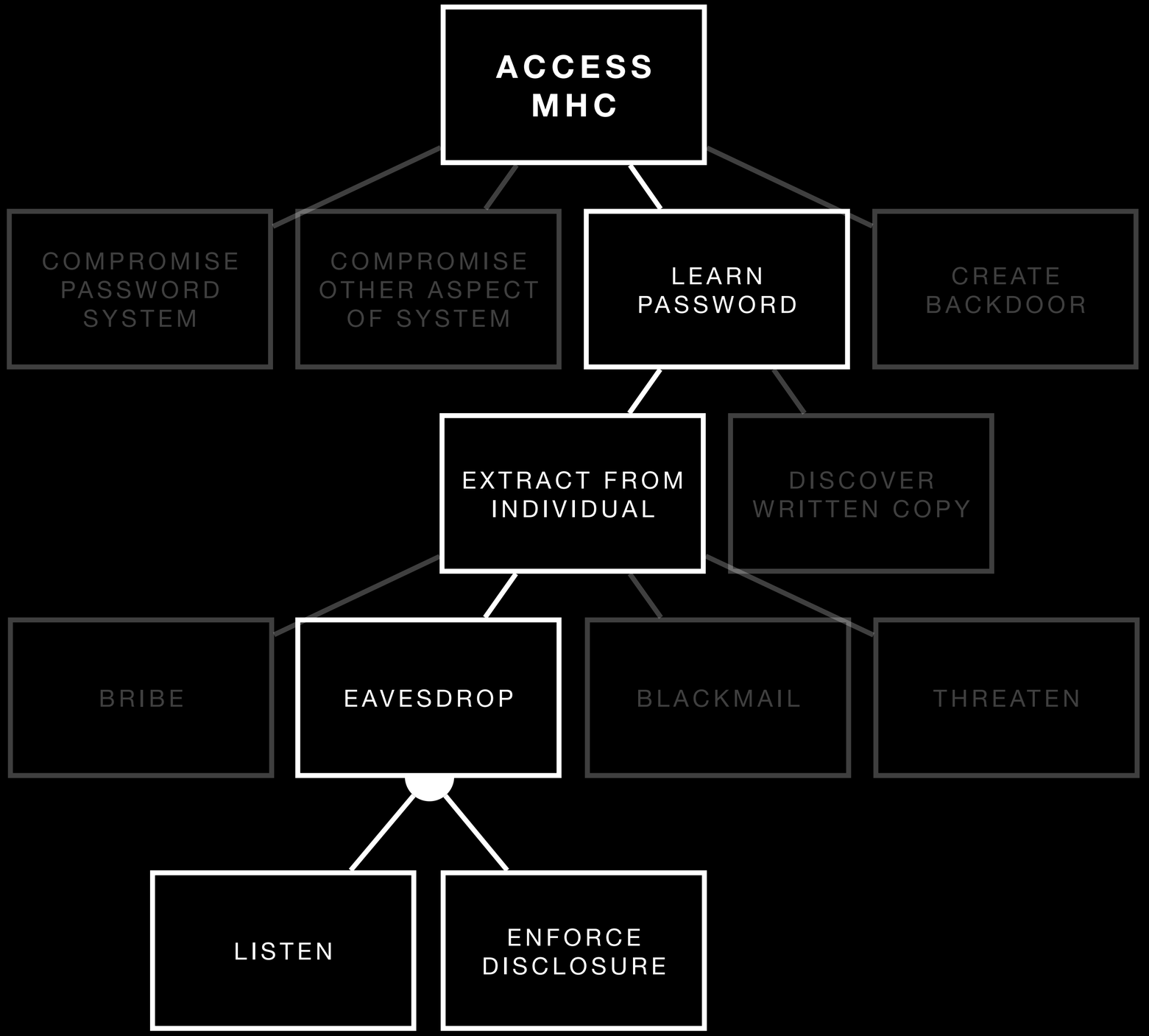

ACCESS MHC
COMPROMISE PASSWORD SYSTEM
COMPROMISE OTHER ASPECT OF SYSTEM
LEARN PASSWORD
CREATE BACKDOOR
EXTRACT FROM INDIVIDUAL
DISCOVER WRITTEN COPY
BRIBE
EAVESDROP
BLACKMAIL
THREATEN

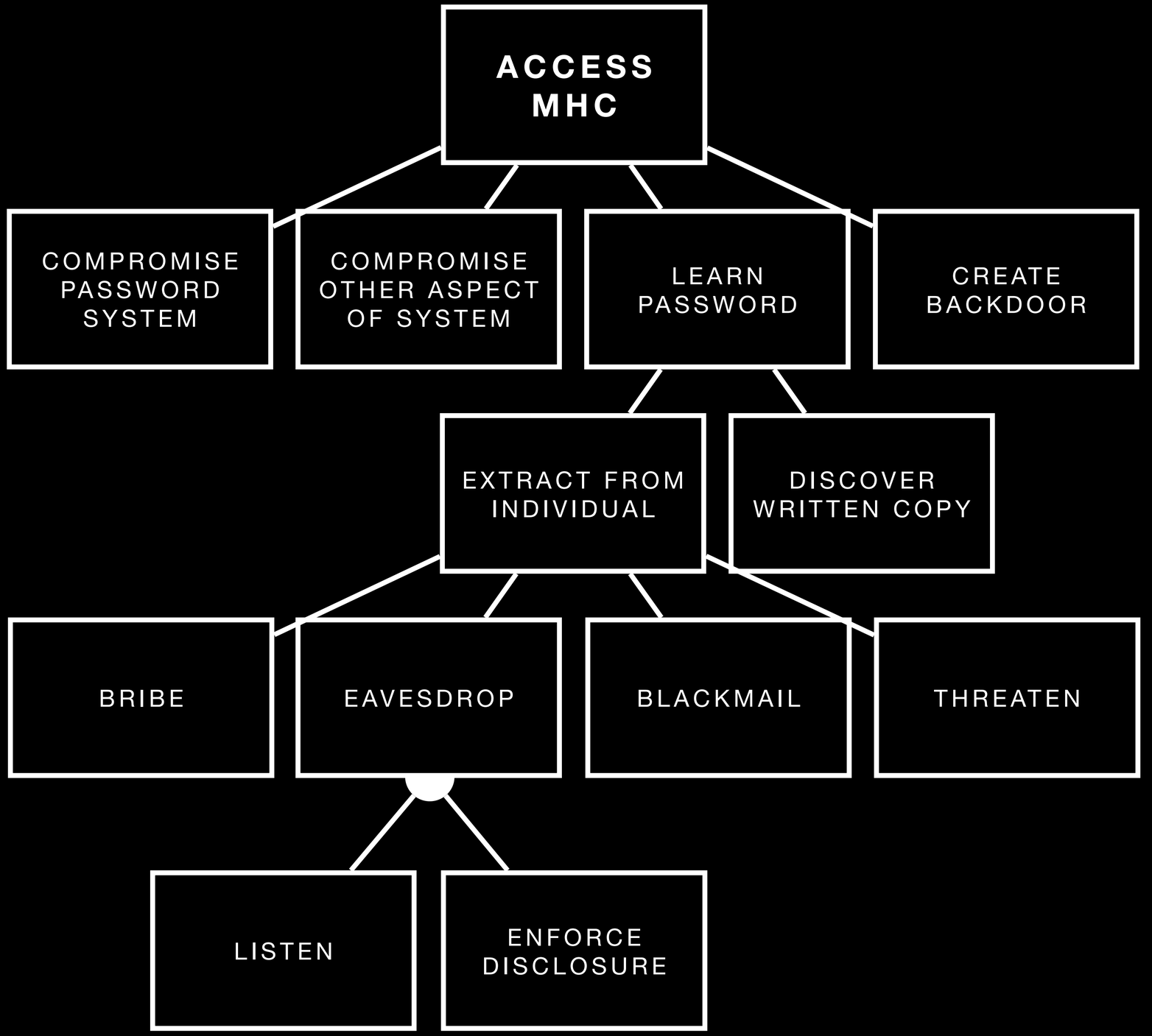

ACCESS MHC
COMPROMISE PASSWORD SYSTEM
COMPROMISE OTHER ASPECT OF SYSTEM
LEARN PASSWORD
CREATE BACKDOOR
EXTRACT FROM INDIVIDUAL
DISCOVER WRITTEN COPY
BRIBE
EAVESDROP
BLACKMAIL
THREATEN

Logic
Attack Trees

- Attack nodes can be considered **AND** or **OR** attack nodes.
- **AND** as combinations that have to happen to achieve each goal.
- **OR** as options or alternatives to achieve each goal.


ACCESS MHC
COMPROMISE PASSWORD SYSTEM
COMPROMISE OTHER ASPECT OF SYSTEM
LEARN PASSWORD
CREATE BACKDOOR
EXTRACT FROM INDIVIDUAL
DISCOVER WRITTEN COPY
BRIBE
EAVESDROP
BLACKMAIL
THREATEN
LISTEN
ENFORCE DISCLOSURE

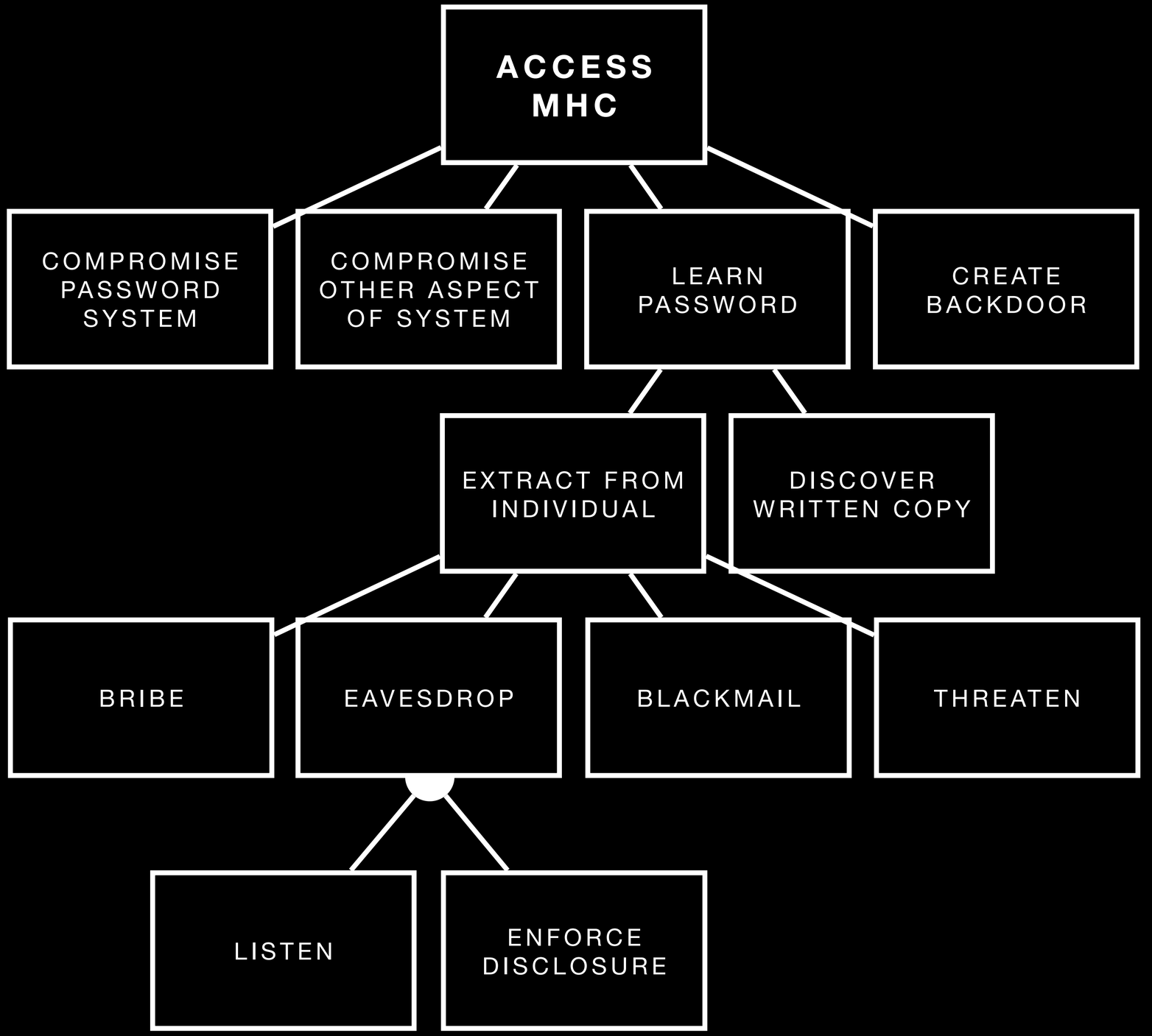

ACCESS MHC
COMPROMISE PASSWORD SYSTEM
COMPROMISE OTHER ASPECT OF SYSTEM
LEARN PASSWORD
CREATE BACKDOOR
EXTRACT FROM INDIVIDUAL
DISCOVER WRITTEN COPY
BRIBE
EAVESDROP
BLACKMAIL
THREATEN
LISTEN
ENFORCE DISCLOSURE

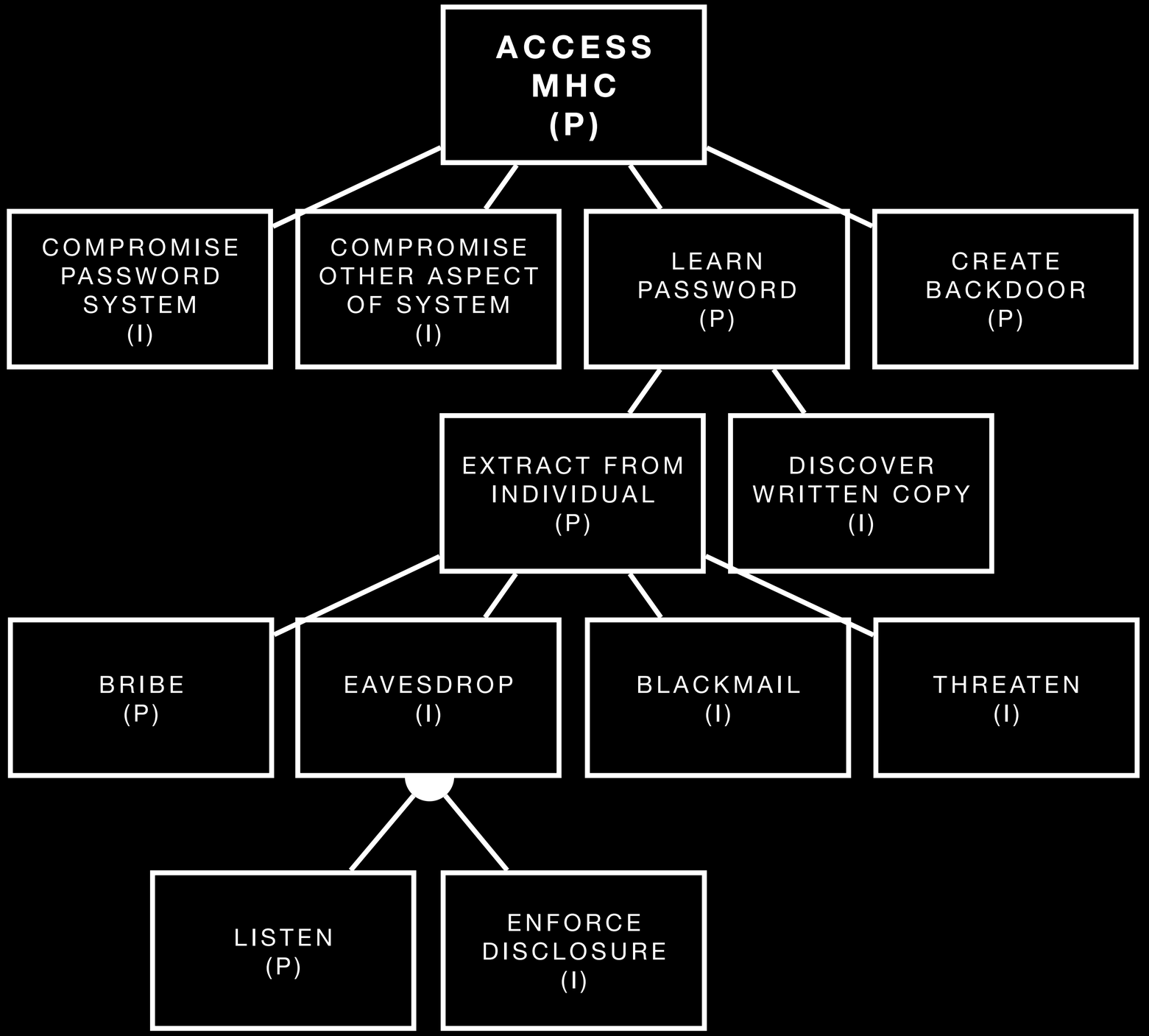

ACCESS MHC
COMPROMISE PASSWORD SYSTEM
COMPROMISE OTHER ASPECT OF SYSTEM
LEARN PASSWORD
CREATE BACKDOOR
EXTRACT FROM INDIVIDUAL
DISCOVER WRITTEN COPY
BRIBE
EAVESDROP
BLACKMAIL
THREATEN
LISTEN
ENFORCE DISCLOSURE

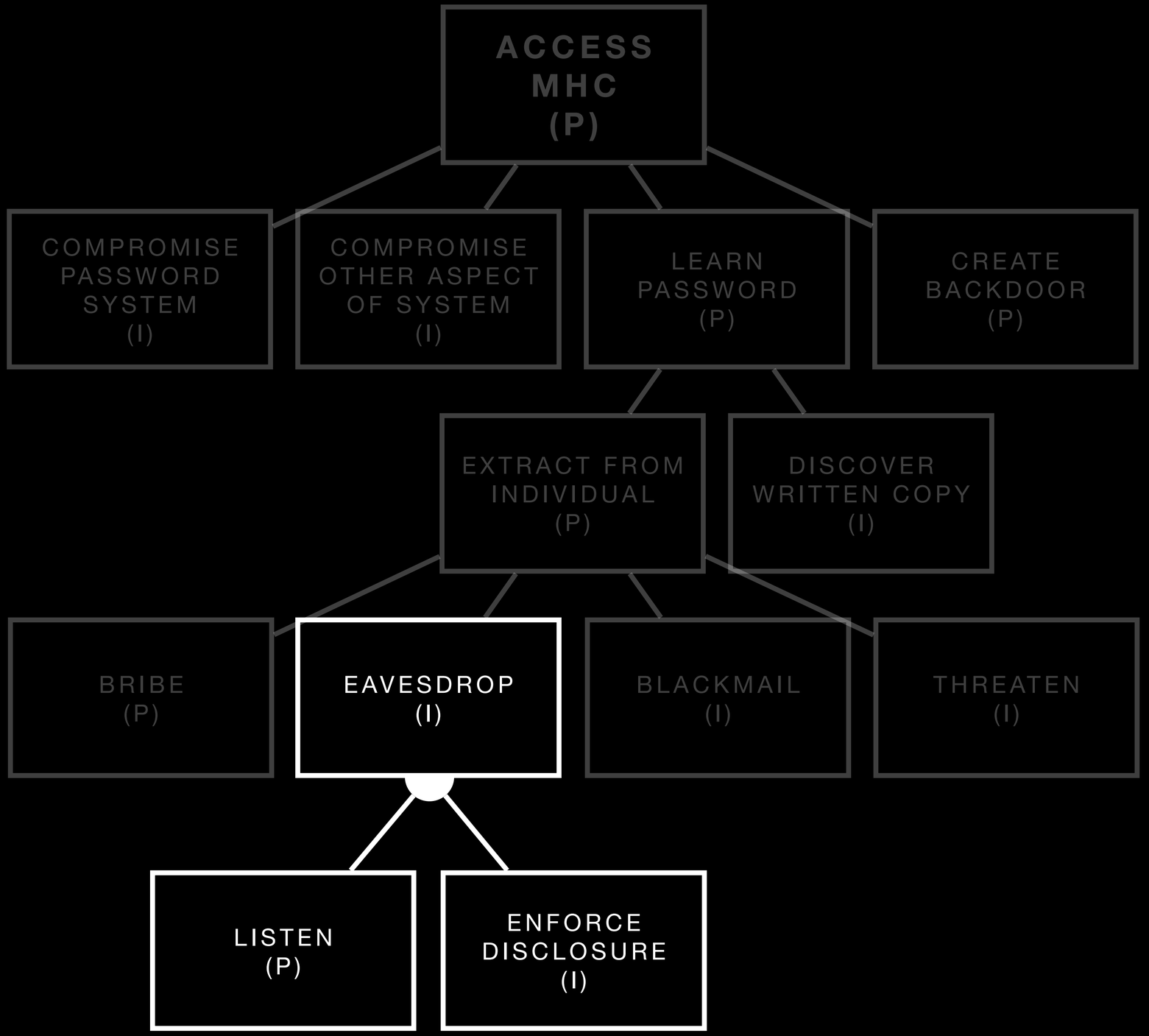
Impossible vs Possible

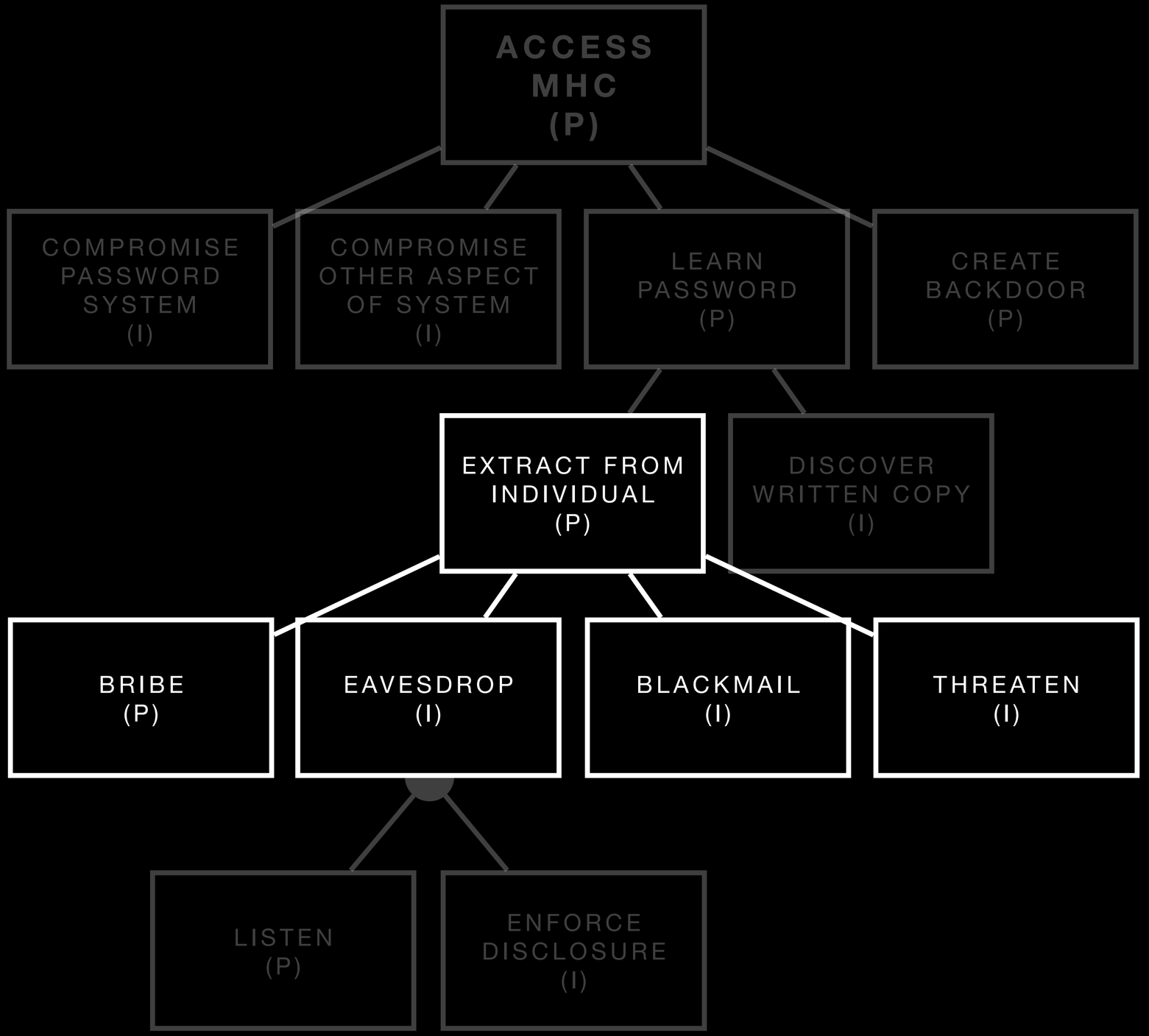
Attack Trees

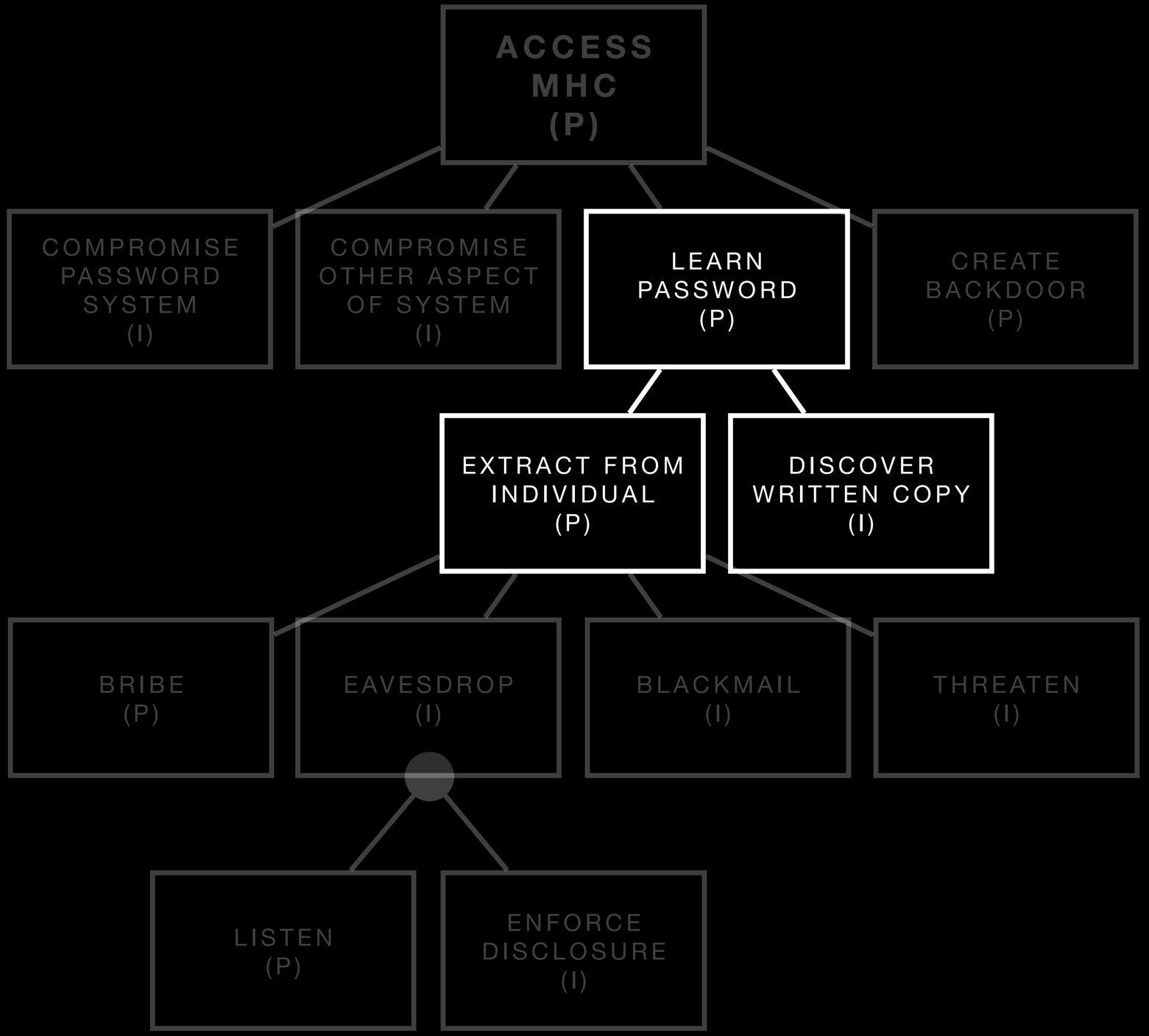
- Constructed simple attack tree, consider the possibility of each attack node.
- Some attack nodes after research may be deemed impossible.
- Alternatively after some consideration some attack notes may be considered possible.
- Label attack tree to indicate whether an attack node can be considered possible or impossible.

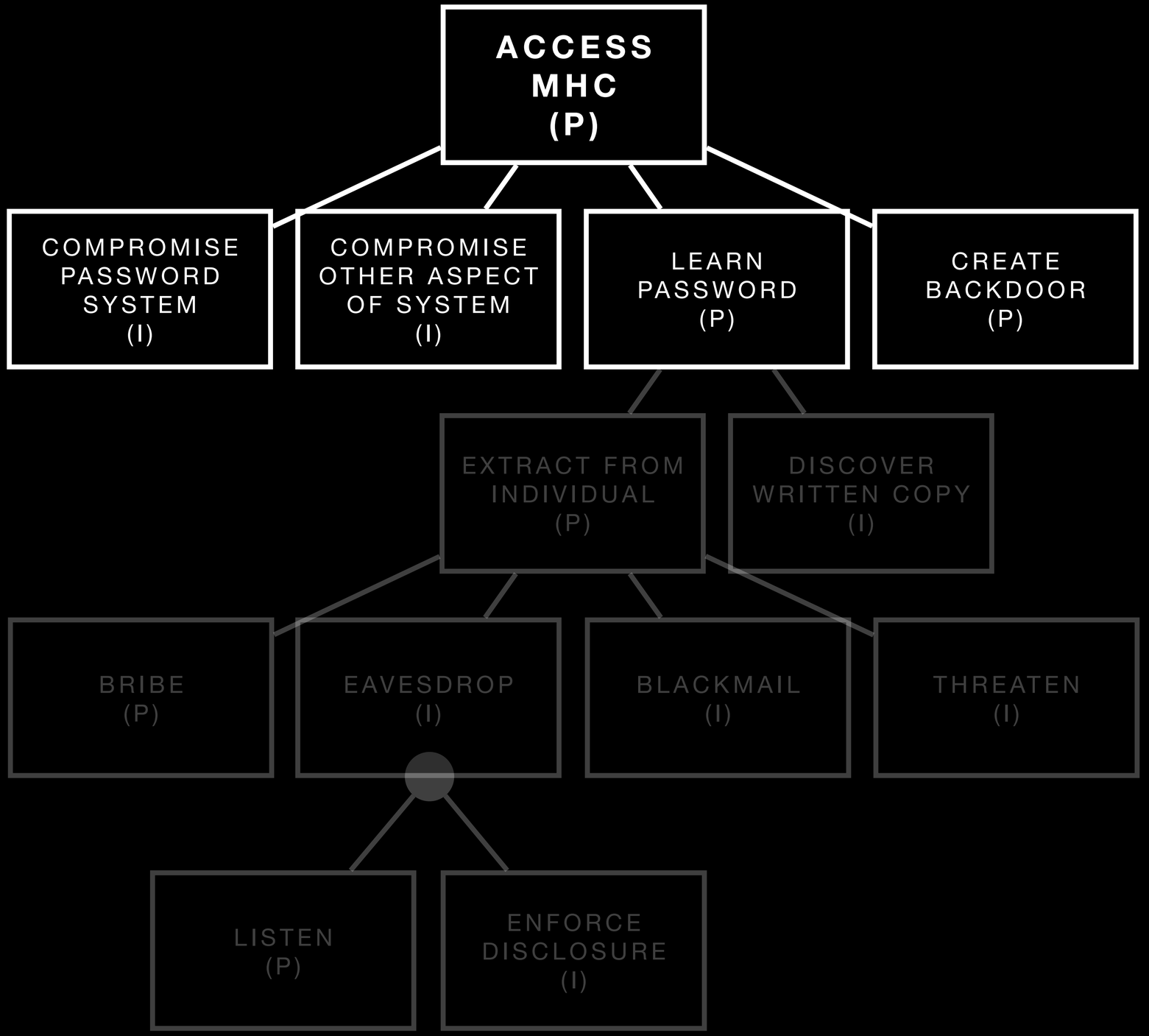

ACCESS MHC
COMPROMISE PASSWORD SYSTEM
COMPROMISE OTHER ASPECT OF SYSTEM
LEARN PASSWORD
CREATE BACKDOOR
EXTRACT FROM INDIVIDUAL
DISCOVER WRITTEN COPY
BRIBE
EAVESDROP
BLACKMAIL
THREATEN
LISTEN
ENFORCE DISCLOSURE

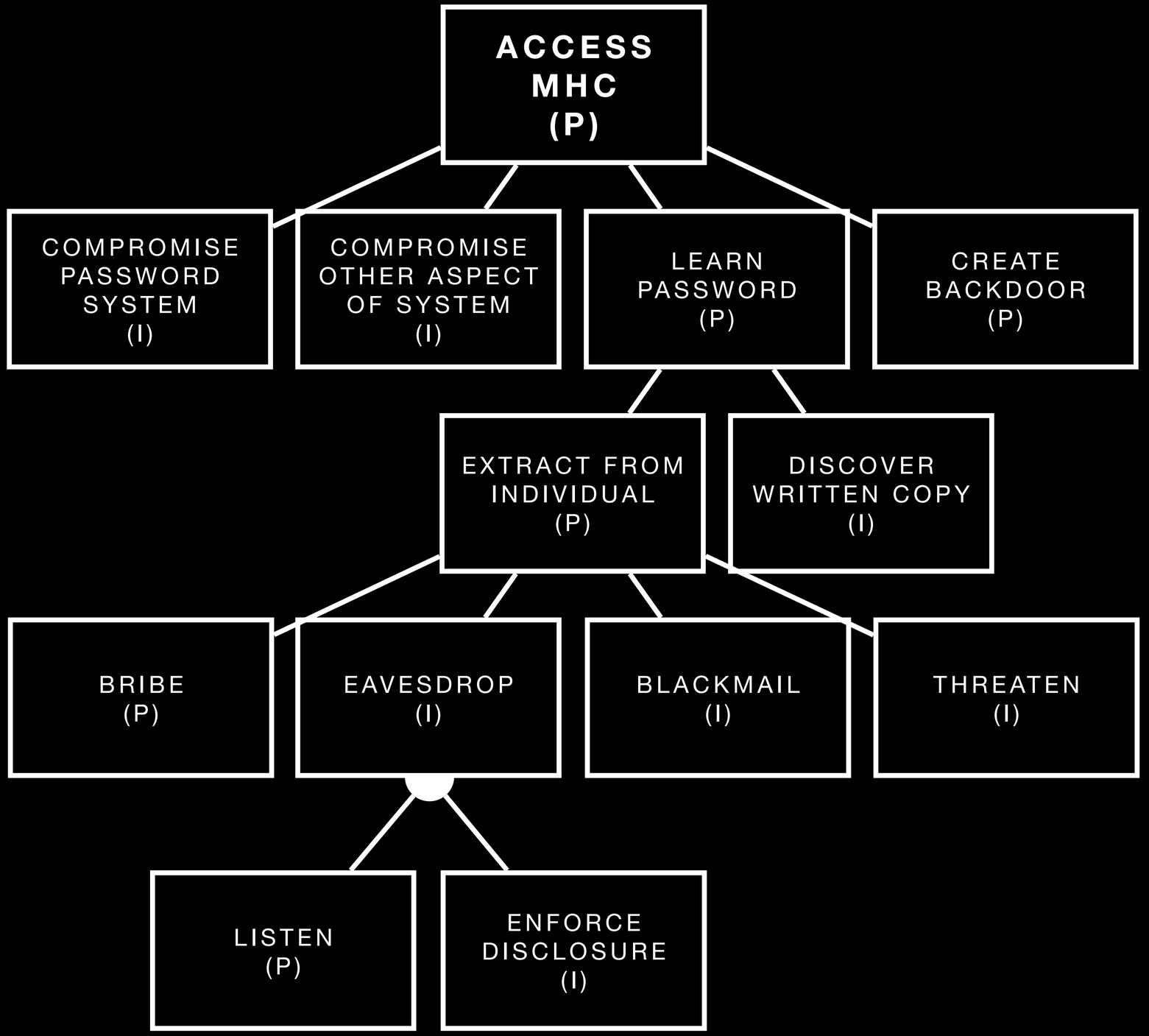

ACCESS MHC (P)
COMPROMISE PASSWORD SYSTEM (I)
COMPROMISE OTHER ASPECT OF SYSTEM (I)
LEARN PASSWORD (P)
CREATE BACKDOOR (P)
EXTRACT FROM INDIVIDUAL (P)
DISCOVER WRITTEN COPY (I)
BRIBE (P)
EAVESDROP (I)
BLACKMAIL (I)
THREATEN (I)
LISTEN (P)
ENFORCE DISCLOSURE (I)

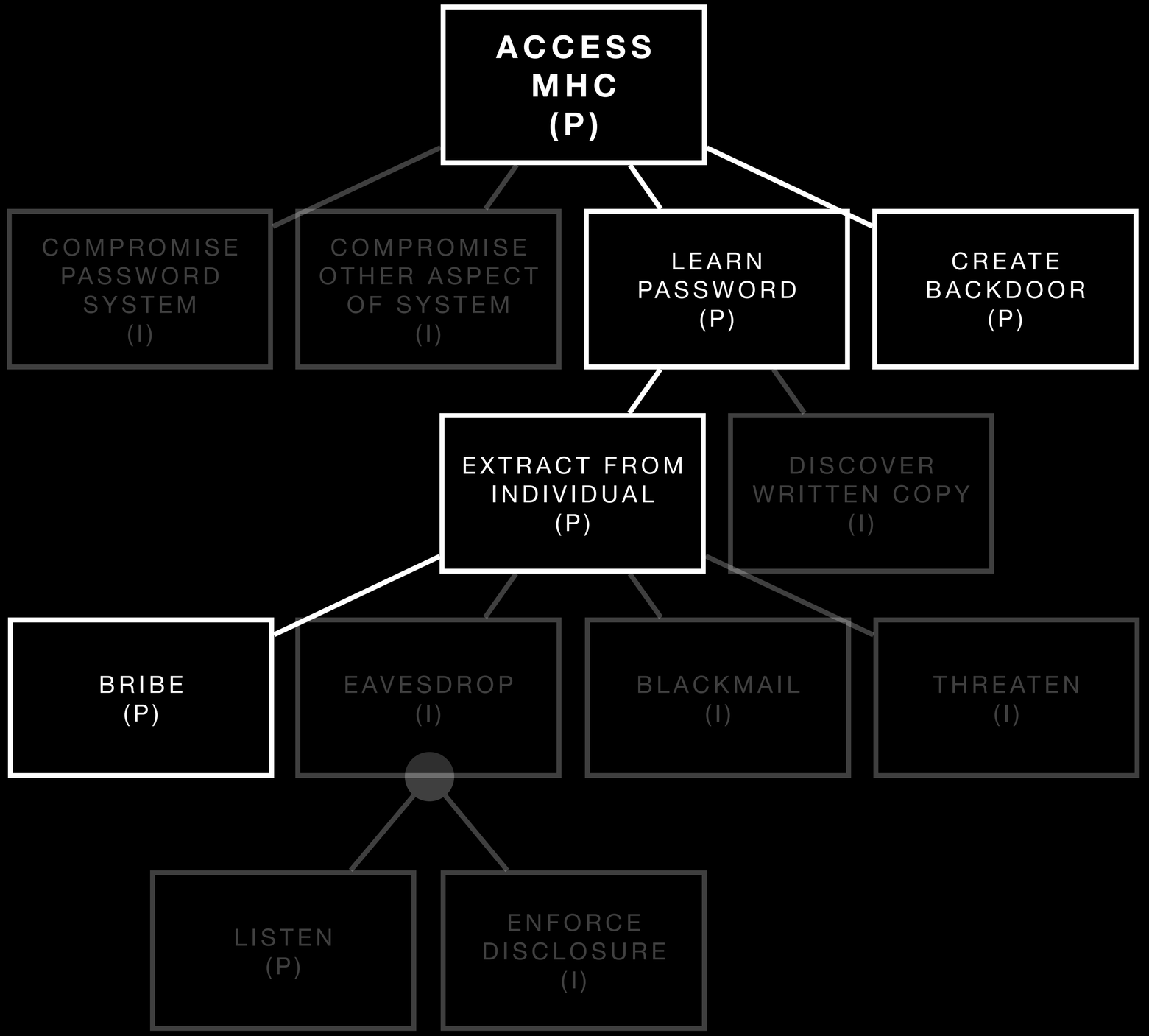

ACCESS MHC (P)
COMPROMISE PASSWORD SYSTEM (I)
COMPROMISE OTHER ASPECT OF SYSTEM (I)
LEARN PASSWORD (P)
CREATE BACKDOOR (P)
EXTRACT FROM INDIVIDUAL (P)
DISCOVER WRITTEN COPY (I)
BRIBE (P)
EAVESDROP (I)
BLACKMAIL (I)
THREATEN (I)
LISTEN (P)
ENFORCE DISCLOSURE (I)


ACCESS MHC (P)
COMPROMISE PASSWORD SYSTEM (I)
COMPROMISE OTHER ASPECT OF SYSTEM (I)
LEARN PASSWORD (P)
CREATE BACKDOOR (P)
EXTRACT FROM INDIVIDUAL (P)
DISCOVER WRITTEN COPY (I)
BRIBE (P)
EAVESDROP (I)
BLACKMAIL (I)
THREATEN (I)
LISTEN (P)
ENFORCE DISCLOSURE (I)


ACCESS MHC (P)
COMPROMISE PASSWORD SYSTEM (I)
COMPROMISE OTHER ASPECT OF SYSTEM (I)
LEARN PASSWORD (P)
CREATE BACKDOOR (P)
EXTRACT FROM INDIVIDUAL (P)
DISCOVER WRITTEN COPY (I)
BRIBE (P)
EAVESDROP (I)
BLACKMAIL (I)
THREATEN (I)
LISTEN (P)
ENFORCE DISCLOSURE (I)


ACCESS MHC (P)
COMPROMISE PASSWORD SYSTEM (I)
COMPROMISE OTHER ASPECT OF SYSTEM (I)
LEARN PASSWORD (P)
CREATE BACKDOOR (P)
EXTRACT FROM INDIVIDUAL (P)
DISCOVER WRITTEN COPY (I)
BRIBE (P)
EAVESDROP (I)
BLACKMAIL (I)
THREATEN (I)
LISTEN (P)
ENFORCE DISCLOSURE (I)


ACCESS MHC (P)
COMPROMISE PASSWORD SYSTEM (I)
COMPROMISE OTHER ASPECT OF SYSTEM (I)
LEARN PASSWORD (P)
CREATE BACKDOOR (P)
EXTRACT FROM INDIVIDUAL (P)
DISCOVER WRITTEN COPY (I)
BRIBE (P)
EAVESDROP (I)
BLACKMAIL (I)
THREATEN (I)
LISTEN (P)
ENFORCE DISCLOSURE (I)


ACCESS MHC (P)
COMPROMISE PASSWORD SYSTEM (I)
COMPROMISE OTHER ASPECT OF SYSTEM (I)
LEARN PASSWORD (P)
CREATE BACKDOOR (P)
EXTRACT FROM INDIVIDUAL (P)
DISCOVER WRITTEN COPY (I)
BRIBE (P)
EAVESDROP (I)
BLACKMAIL (I)
THREATEN (I)
LISTEN (P)
ENFORCE DISCLOSURE (I)

Impossible vs Possible

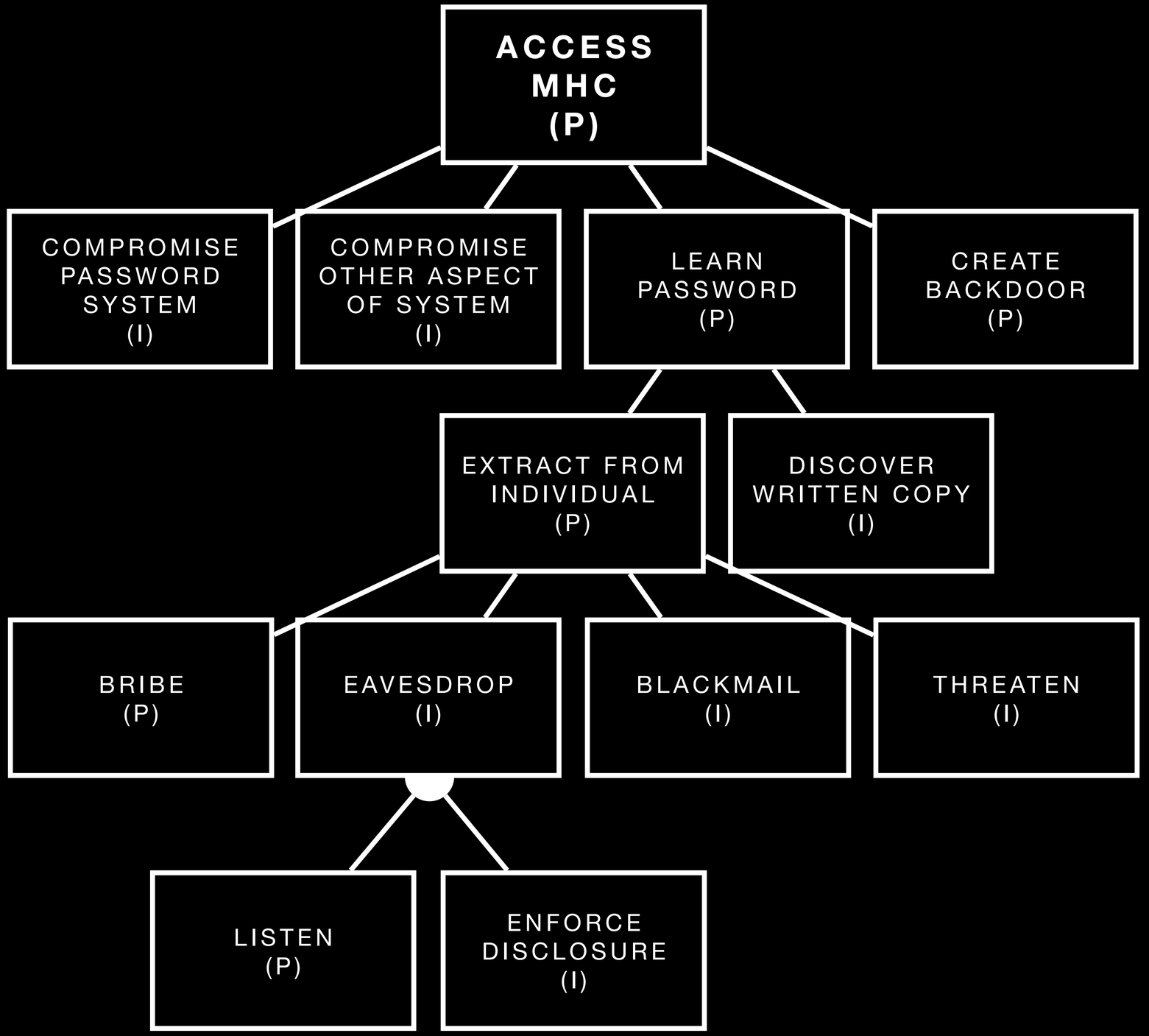
Attack Trees

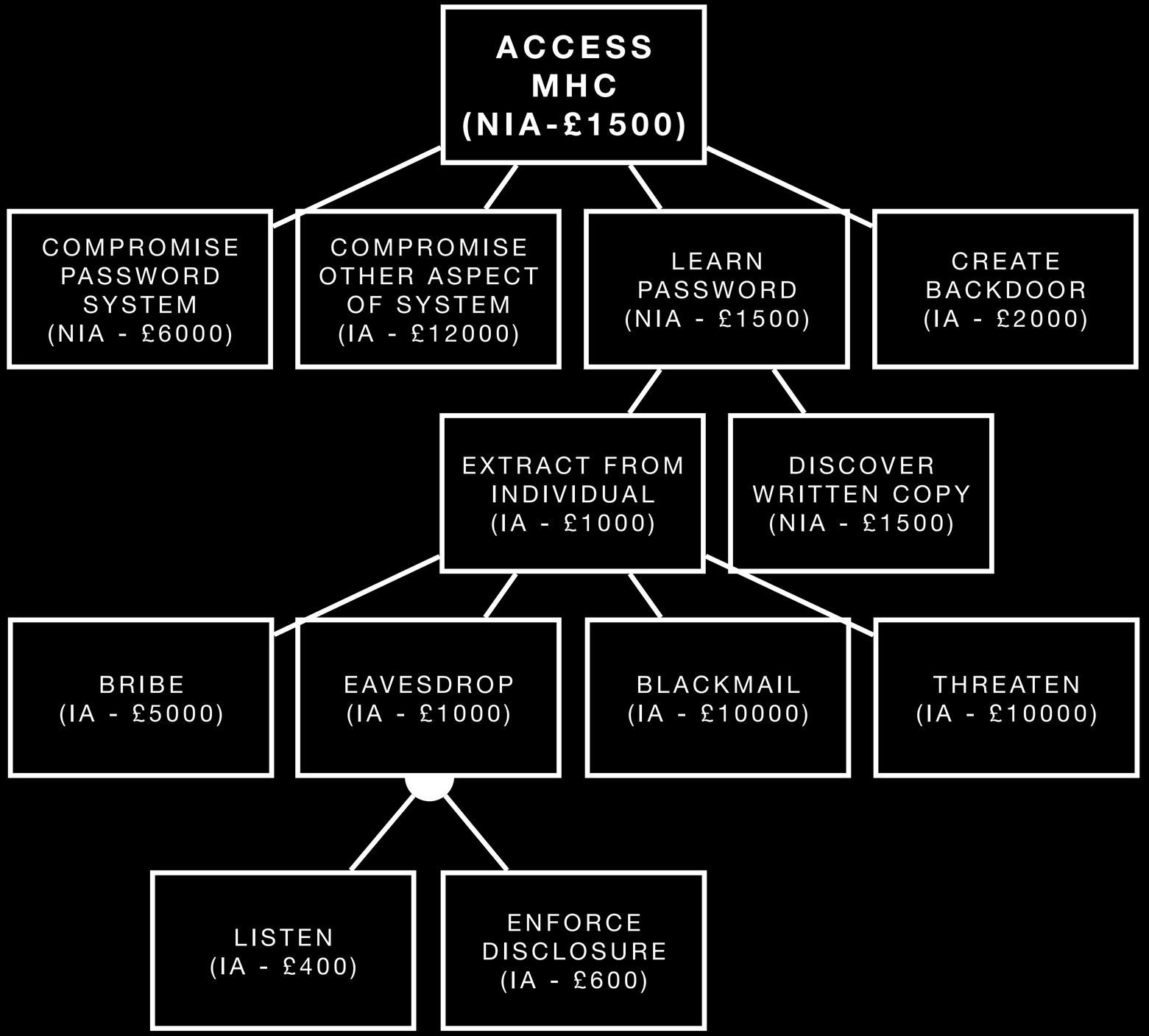
- Labelling attack nodes as impossible or possible is relatively simplistic, but is easy to communicate and comprehend.
- Can adopt alternative boolean values, labels or construct multiple attack tress with various different labels or values.
- Possible attack tree could assign actual monetary expense and assessment could be determined using these values.

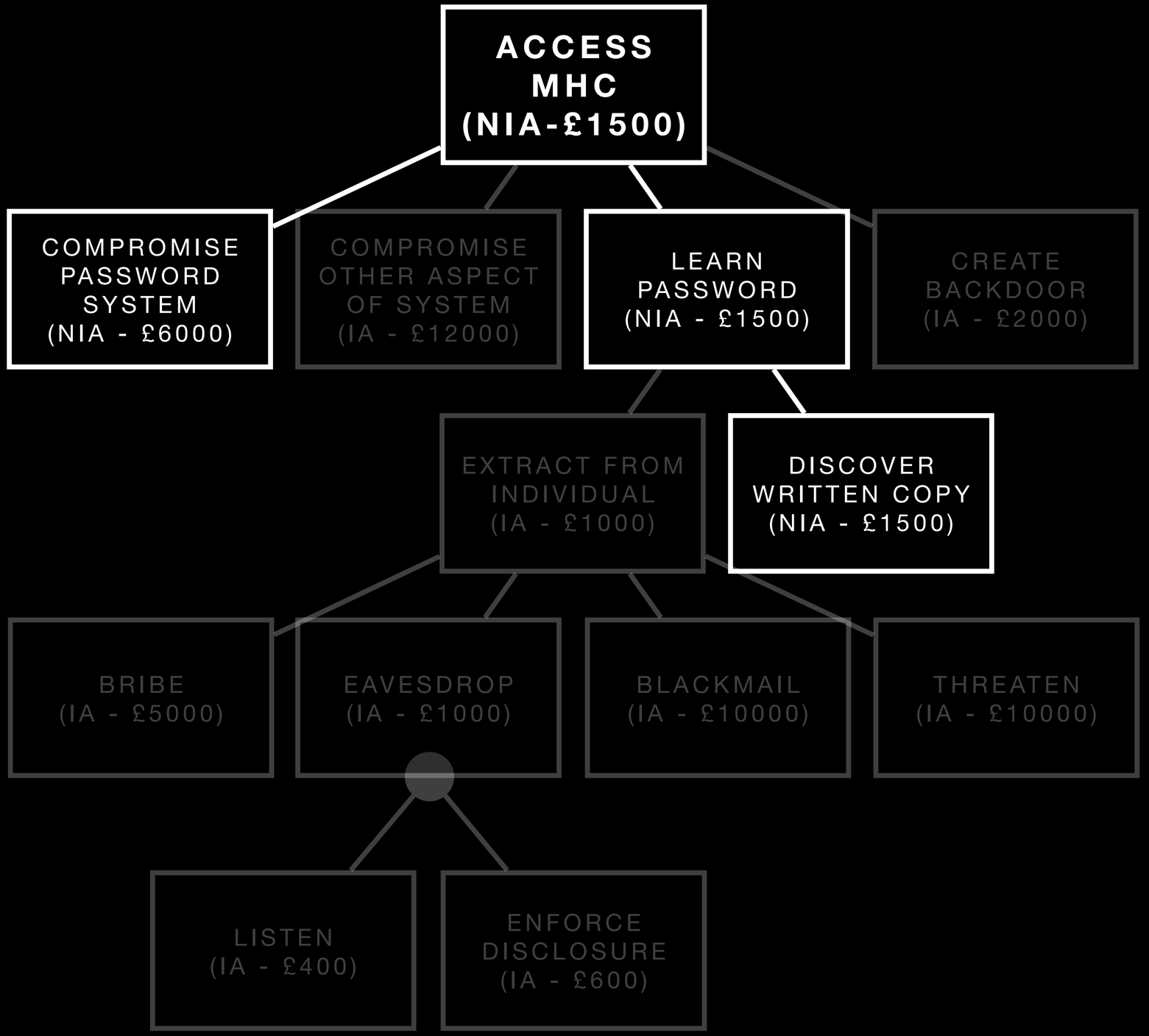
Perspectives

Attack Trees

- Multiple attack trees can be created to consider attacks from multiple adversaries.
- Recall, potential threats really are limited by the capability of the attacker.
- Organisation or company may be interested in the least expensive attack a hungry individual could mount.
- Similar, they may be more interested in threats from highly capable sources.


ACCESS MHC (P)
COMPROMISE PASSWORD SYSTEM (I)
COMPROMISE OTHER ASPECT OF SYSTEM (I)
LEARN PASSWORD (P)
CREATE BACKDOOR (P)
EXTRACT FROM INDIVIDUAL (P)
DISCOVER WRITTEN COPY (I)
BRIBE (P)
EAVESDROP (I)
BLACKMAIL (I)
THREATEN (I)
LISTEN (P)
ENFORCE DISCLOSURE (I)


ACCESS MHC (NIA-£1500)
COMPROMISE PASSWORD SYSTEM (NIA - £6000)
COMPROMISE OTHER ASPECT OF SYSTEM (IA - £12000)
LEARN PASSWORD (NIA - £1500)
CREATE BACKDOOR (IA - £2000)
EXTRACT FROM INDIVIDUAL (IA - £1000)
DISCOVER WRITTEN COPY (NIA - £1500)
BRIBE (IA - £5000)
EAVESDROP (IA - £1000)
BLACKMAIL (IA - £10000)
THREATEN (IA - £10000)
LISTEN (IA - £400)
ENFORCE DISCLOSURE (IA - £600)


ACCESS MHC (NIA-£1500)
COMPROMISE PASSWORD SYSTEM (NIA - £6000)
COMPROMISE OTHER ASPECT OF SYSTEM (IA - £12000)
LEARN PASSWORD (NIA - £1500)
CREATE BACKDOOR (IA - £2000)
EXTRACT FROM INDIVIDUAL (IA - £1000)
DISCOVER WRITTEN COPY (NIA - £1500)
BRIBE (IA - £5000)
EAVESDROP (IA - £1000)
BLACKMAIL (IA - £10000)
THREATEN (IA - £10000)
LISTEN (IA - £400)
ENFORCE DISCLOSURE (IA - £600)

Attack Trees

Adversarial Behaviours

- Attack trees can be considered a **formal** approach of organising, discussing and finding threats to systems.
- Attack trees can be valuable in appreciating security **during an attack** and allow many different stakeholders to consider security.
- Attack trees can become complex and wide fast, making it difficult to consider large-scale attacks or campaigns.
- Attack trees are also often not complete, often considering known attacks and less optimal at unknown attacks.
- Pruning is important to ensure important attacks are considered.

Attack Trees

Adversarial Behaviours