ENTERPRISE CYBER SECURITY

THREAT THINKING

University of Glasgow

THREAT THINKING

- CAPEC
- STRIDE
- Attack Trees

COMMON ATTACK PATTERN ENUMERATION AND CLASSIFICATION (CAPEC)

COMMON ATTACK PATTERN ENUMERATION AND CLASSIFICATION (CAPEC)

- MITRE efforts similar to CVE and CWE.

- catalogue of **attack patterns** in a similar vain to software engineering patterns.

- MITRE advocates attack patterns as effective way to communicate attacker the perspective.

- distill from the consideration of software in the wild and aimed at strengthening systems.

COMMON ATTACK PATTERN ENUMERATION AND CLASSIFICATION (CAPEC)

- MITRE efforts similar to CVE and CWE.

- catalogue of **attack patterns** in a similar vain to software engineering patterns.

- MITRE advocates attack patterns as effective way to communicate attacker the perspective.

- distill from the consideration of software in the wild and aimed at strengthening systems.

ATTACK PATTERNS

- attack patterns can be classified in of architecture, artefact and external.

- **architecture** refers to the elements and connections itself, includes protocols and processes.

- **artefact** refers to actual source, platform and specifics of the actual system.

- **external** attack patterns can be considered a grab bag of attacks that exploit various aspects of architecture and artefacts, for example viruses and worms.

CAPEC ATTACK PATTERN

CAPEC ATTACK PATTERN

Example Attack Pattern

Name	HTTP Response Splitting
Typical Severity	High
Description	HTTP Response Splitting causes a vulnerable web server to respond to a maliciously crafted request by sending an HTTP response stream such that it gets interpreted as two separate responses instead of a single one. This is possible when user-controlled input is used unvalidated as part of the response headers. An attacker can have the victim interpret the injected header as being a response to a second dummy request, thereby causing the crafted contents to be displayed and possibly cached. To achieve HTTP Response Splitting on a vulnerable web server, the attacker: 1. Identifies the user-controllable input that causes arbitrary HTTP header injection. 2. Crafts a malicious input consisting of data to terminate the original response and start a second response with headers controlled by the attacker. 3. Causes the victim to send two requests to the server. The first request consists of maliciously crafted input to be used as part of HTTP response headers and the second is a dummy request so that the victim interprets the split response as belonging to the second request.
Attack Prerequisites	User-controlled input used as part of HTTP header Ability of attacker to inject custom strings in HTTP header Insufficient input validation in application to check for input sanity before using it as part of response header
Typical Likelihood of Exploit	Medium
Methods of Attack	Injection Protocol Manipulation
Examples-Instances	In the PHP 5 session extension mechanism, a user-supplied session ID is sent back to the user within the Set-Cookie HTTP header. Since the contents of the user-supplied session ID are not validated, it is possible to inject arbitrary HTTP headers into the response body. This immediately enables HTTP Response Splitting by simply terminating the HTTP response header from within the session ID used in the Set-Cookie directive. CVE-2006-0207
Attacker Skill or Knowledge Required	High - The attacker needs to have a solid understanding of the HTTP protocol and HTTP headers and must be able to craft and inject requests to elicit the split responses.
Resources Required	None
Probing Techniques	With available source code, the attacker can see whether user input is validated or not before being used as part of output. This can also be achieved with static code analysis tools If source code is not available, the attacker can try injecting a CR-LF sequence (usually encoded as %0d%0a in the input) and use a proxy such as Paros to observe the response. If the resulting injection causes an invalid request, the web server may also indicate the protocol error.
Indicators-Warnings of Attack	The only indicators are multiple responses to a single request in the web logs. However, this is difficult to notice in the absence of an application filter proxy or a log analyzer. There are no indicators for the client
Solutions and Mitigations	To avoid HTTP Response Splitting, the application must not rely on user-controllable input to form part of its output response stream. Specifically, response splitting occurs due to injection of CR-LF sequences and additional headers. All data arriving from the user and being used as part of HTTP

STRIDE

STRIDE

- **framework** for thinking, discussing and classify threats developed by Kohnfelder and Garg at Microsoft.

- designed with the aim of getting software developers to **consider common threats**.

- considering primarily the **software development lifecycle**.

- STRIDE can be considered an **elicitation** technique of the perceived threats, rather than specific discovery.

STRIDE

- spoofing
- tampering
- repudiation
- information disclosure
- denial of service
- elevation of privilege

SPOOFING

- spoofing refers to the concept of **masquerading** as something itself.

- an attacker could pretend to a process, file, machine or another person.

- consider a website that masquerades or pretends to be an official website.

- consider a social engineering phone call pretending to be an official or organisation.

SPOOFING

TAMPERING

- tampering can be consider an attack that **modifies** some data.
- modification could occur on the cyber system, both on disk or memory, as well as over the network.
- attacker could add additional nefarious packets to the network rather than alter existing ones.
- recall, many designs may start from just getting things working rather than what is optimal in terms of security.

TAMPERING

REPUDIATION

- repudiation refers to **rejection** of responsibility of actions.
- an interesting aspect of STRIDE as it more an **enterprise** issue, than a technology issue.
- **non-repudiation** is crucial to ensure another entity or individual cannot reject responsibility.
- transactions and actions require confidence between both parties.

INFORMATION DISCLOSURE

- information disclosure means that information was consumed or revealed to **unauthorised** parties.

- essentially meaning that an individual or entity was not meant or should not have access to the information.

- can consider this from very small to very large information disclosure.

- an error message revealing structure of system or even recovery implementations.

INFORMATION DISCLOSURE

DENIAL OF SERVICE

- denial of service attacks effectively **consume** resources to the detriment to others.

- such attacks can be considered **active** or **persistent** attacks.

- denial of service attacks can also be considered in terms of **amplification**.

DENIAL OF SERVICE

ELEVATION OF PRIVILEGE

- elevation of privileges is an entity executing at level that is not permitted.

- consider an entry-level individual executing processes on a cyber system restricted to administrators.

- an external entity with no privileges executing processes remotely on cyber systems.

ELEVATION OF PRIVILEGE

- **horizontal** escalation refers to accessing function available to other users on the same tier.

- name misleading, but essentially stealing username/password access similar functions.

- **vertical** escalation refers to accessing functions that are the preserve of entity with different privileges.

- consider iPhone unlocking, access administration rights for particular system etc.

ELEVATION OF PRIVILEGE

ATTACK TREES

ATTACK TREES

- 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

- 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

- 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

- **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

- **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

ACCESS MHC

ATTACK NODES

- 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

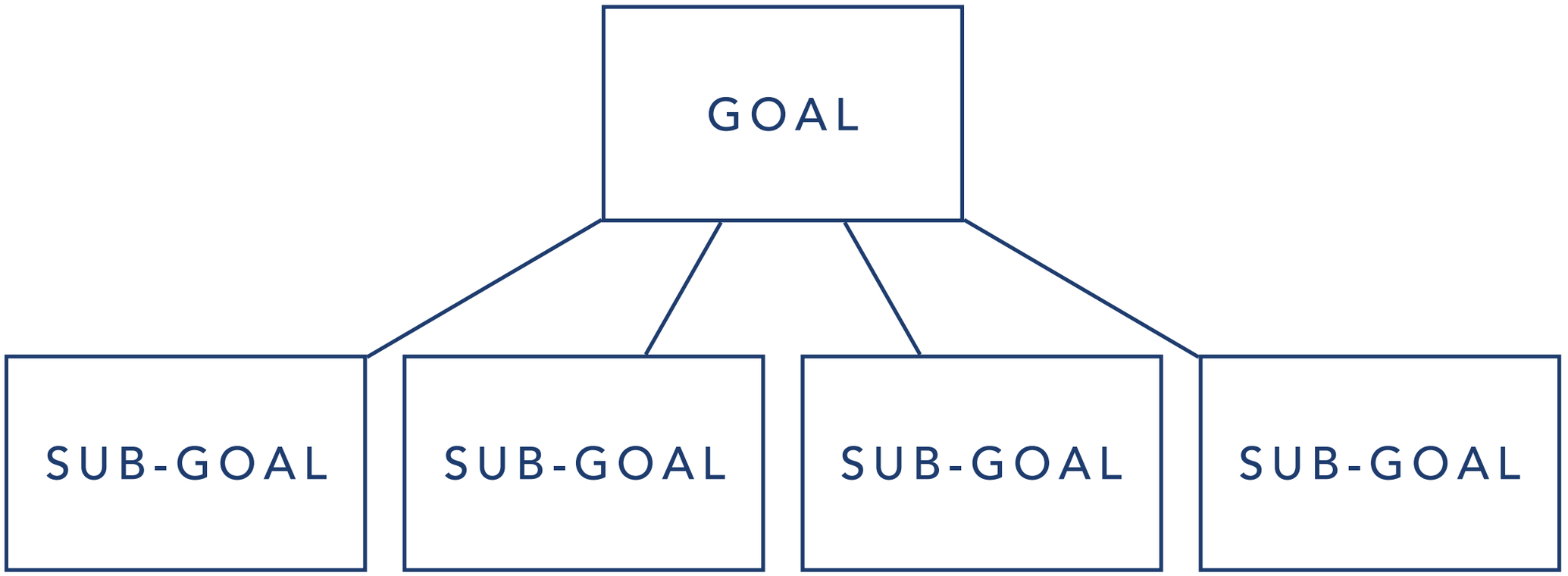
GOAL

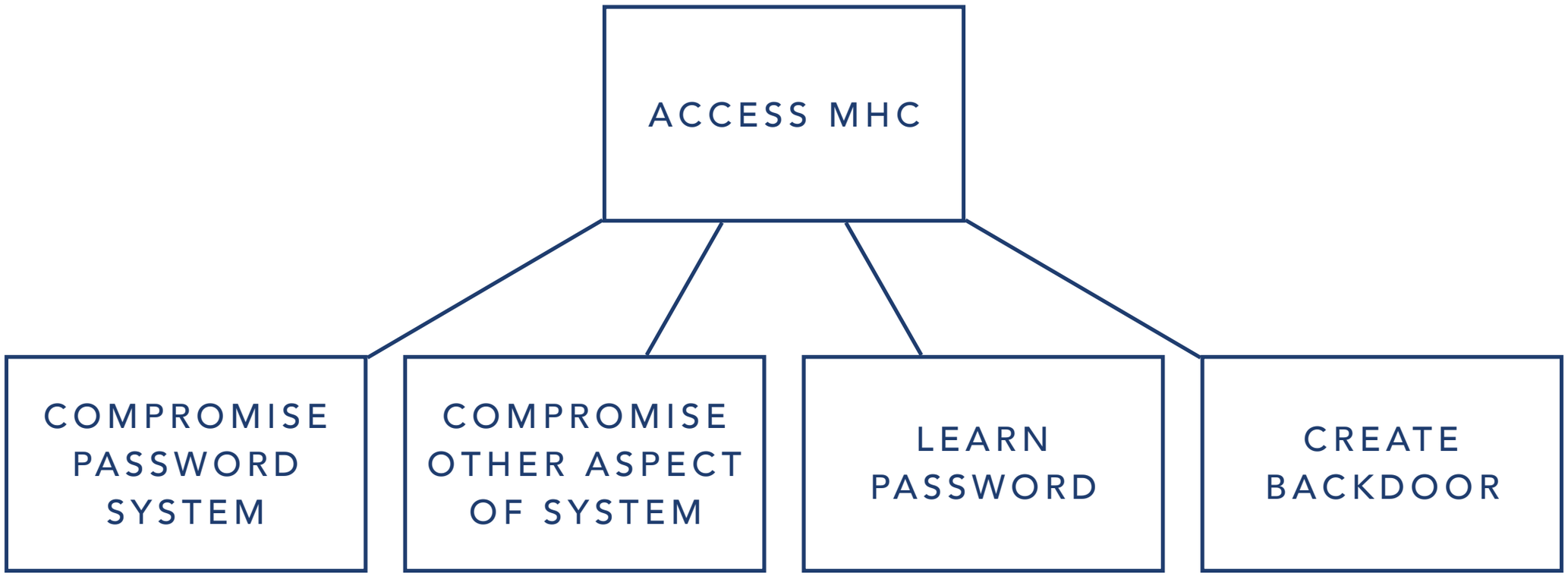
SUB-GOAL

SUB-GOAL

SUB-GOAL

SUB-GOAL


GOAL
SUB-GOAL
SUB-GOAL
SUB-GOAL
SUB-GOAL

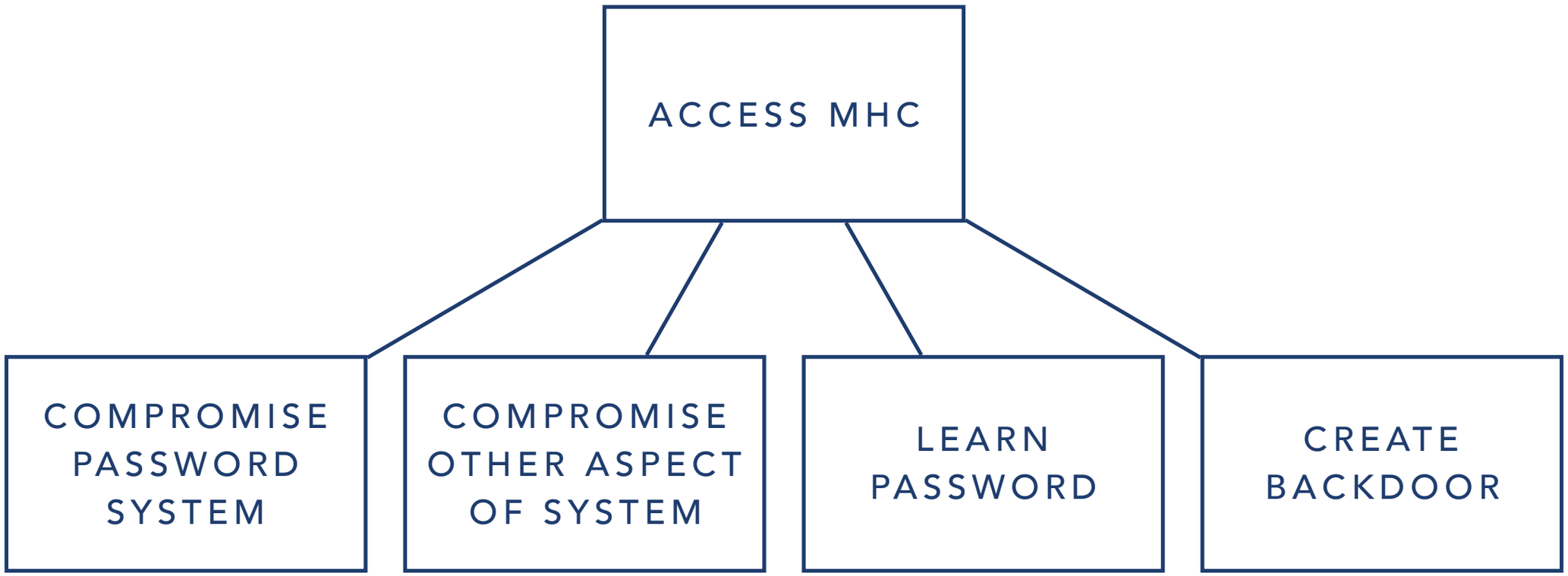

ACCESS MHC
COMPROMISE PASSWORD SYSTEM
COMPROMISE OTHER ASPECT OF SYSTEM
LEARN PASSWORD
CREATE BACKDOOR

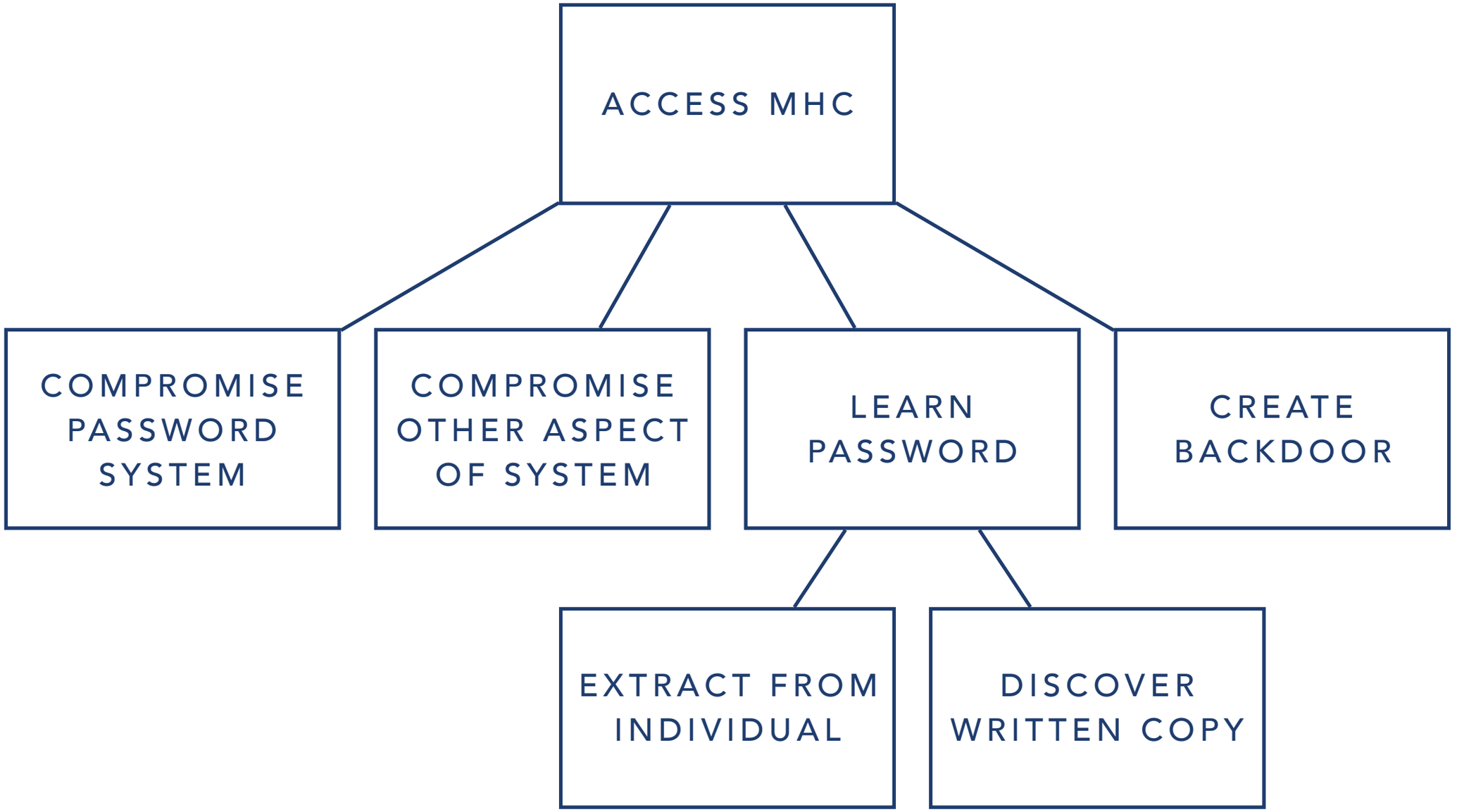
ATTACK NODES

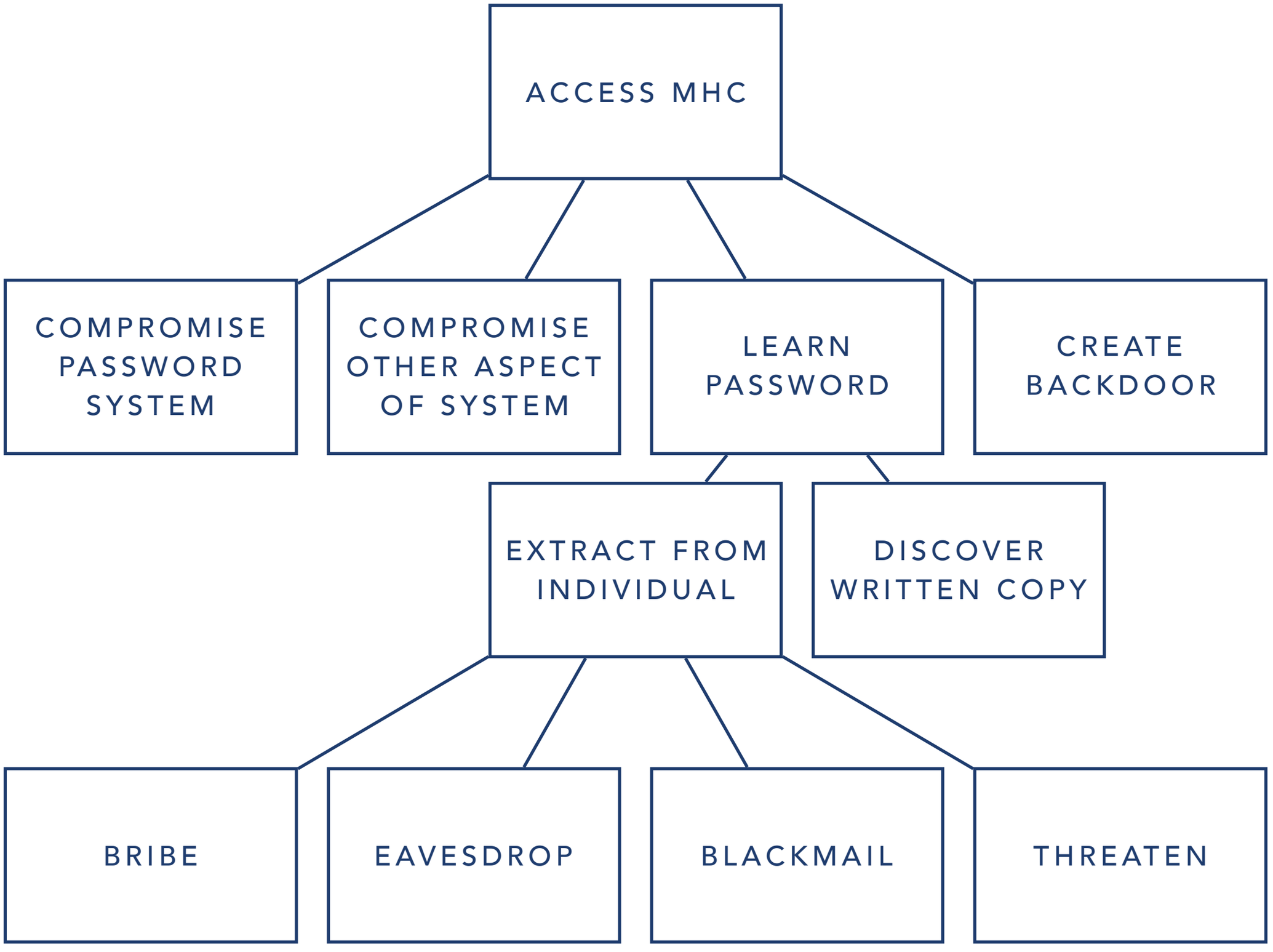
- can consider each attack node in turn as **sub-goals** of the adversary.

- 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.

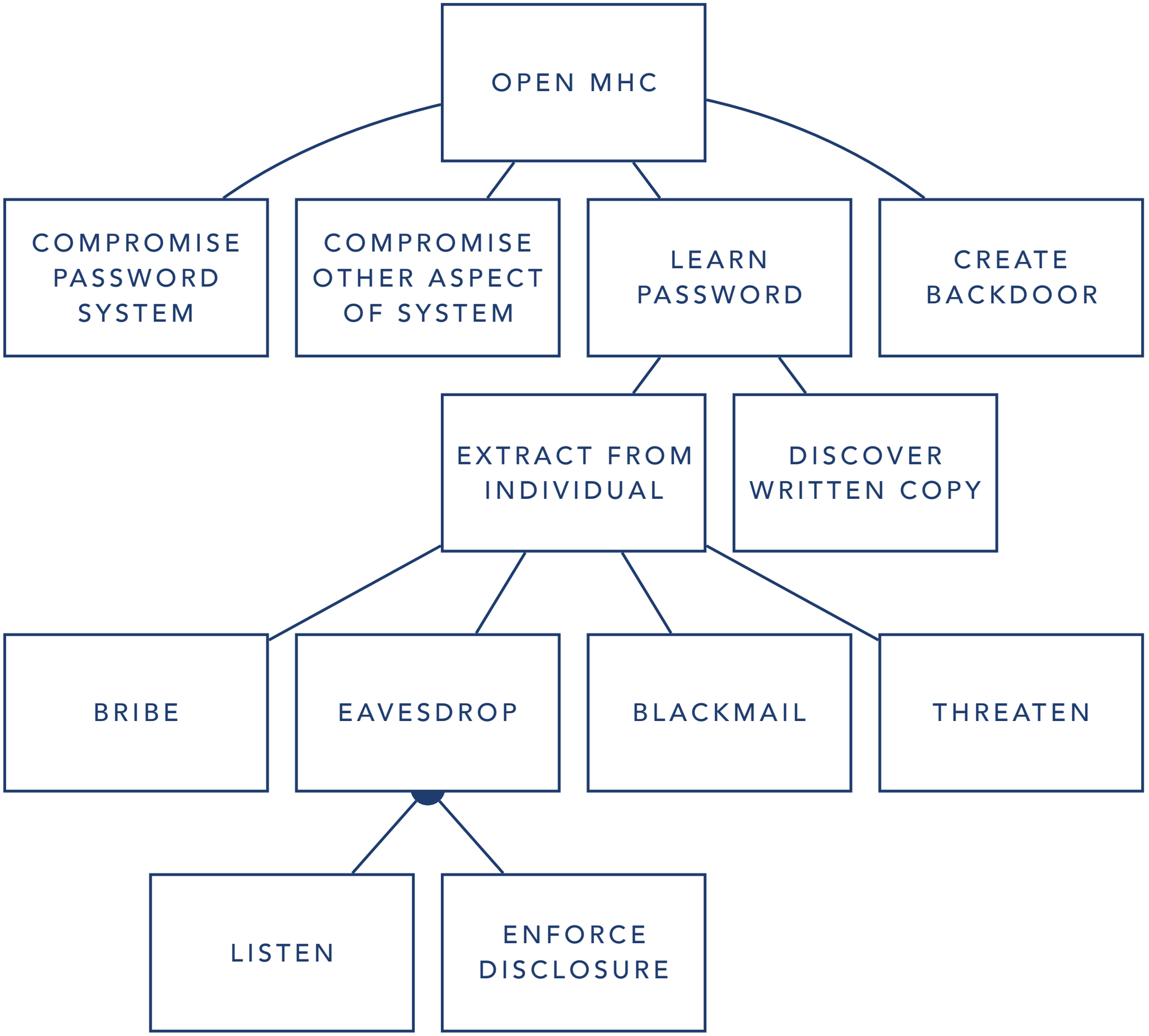

ACCESS MHC
COMPROMISE PASSWORD SYSTEM
COMPROMISE OTHER ASPECT OF SYSTEM
LEARN PASSWORD
CREATE BACKDOOR


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

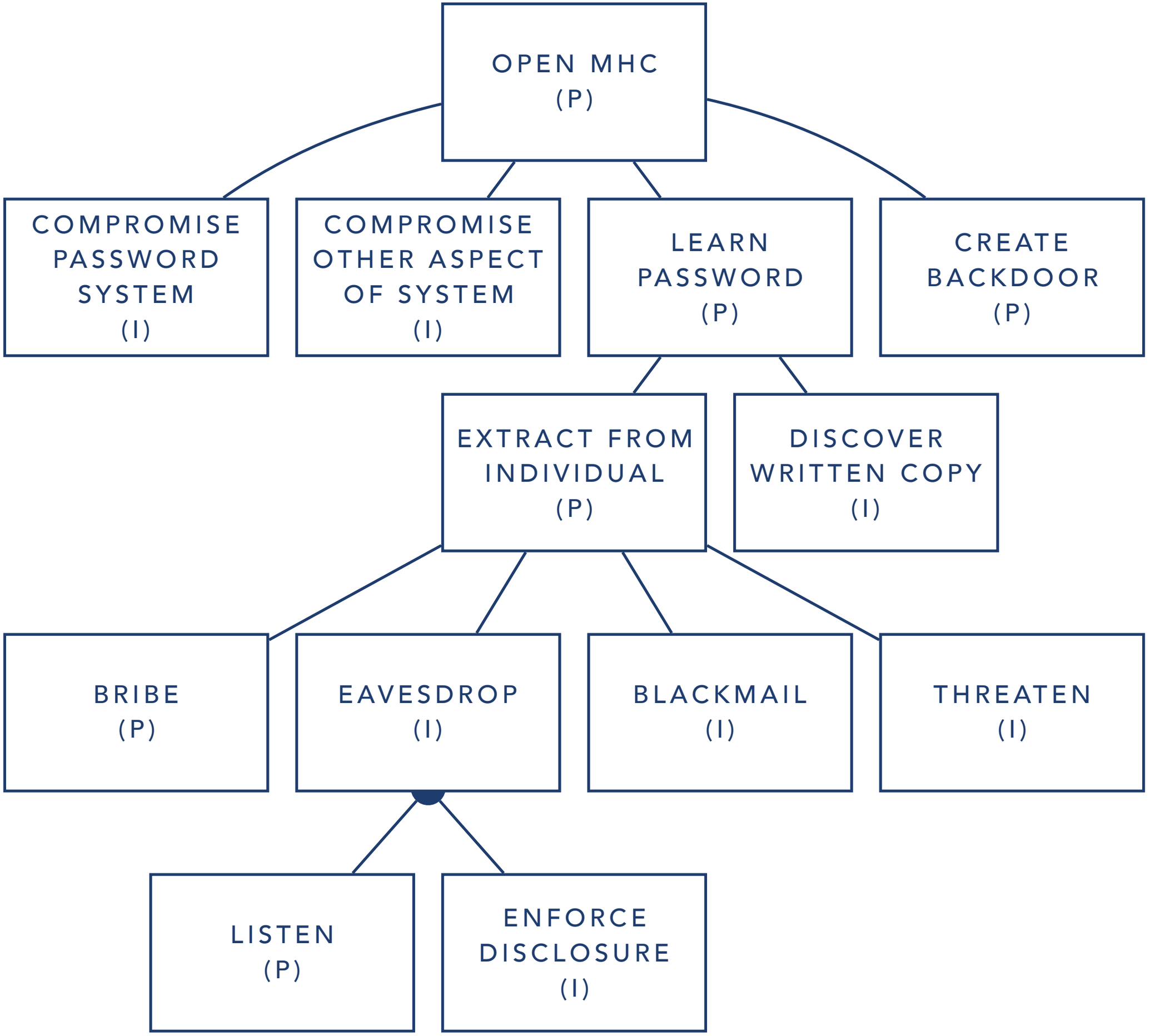
LOGIC

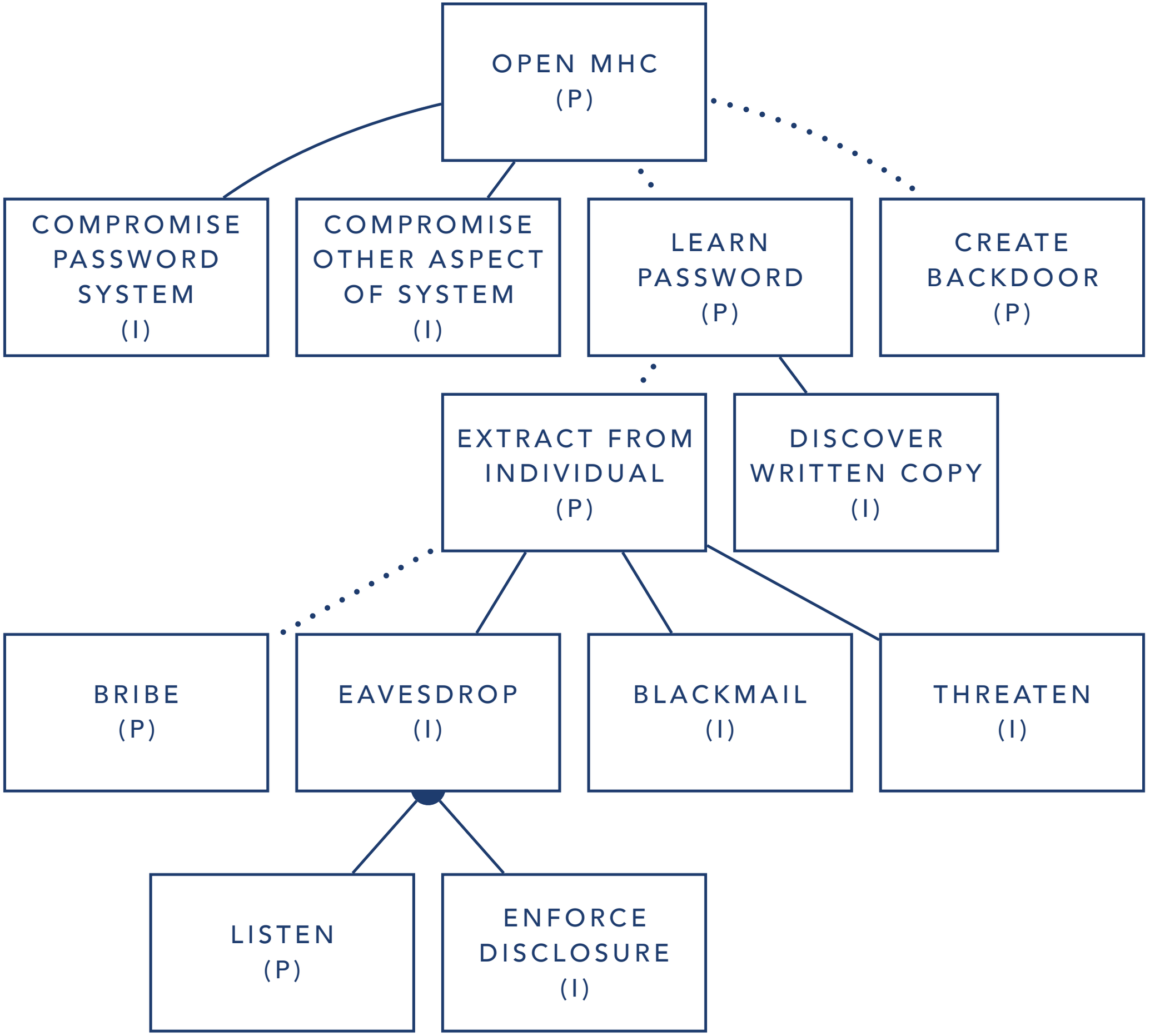
- attack nodes can be considered **AND** or **OR** attack nodes.
- **AND** as combinations that have to happen to achieve each goal.
- **OR** as options or alternatives to achieve each goal.


OPEN 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

- 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.


OPEN 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)


OPEN 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

- 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.

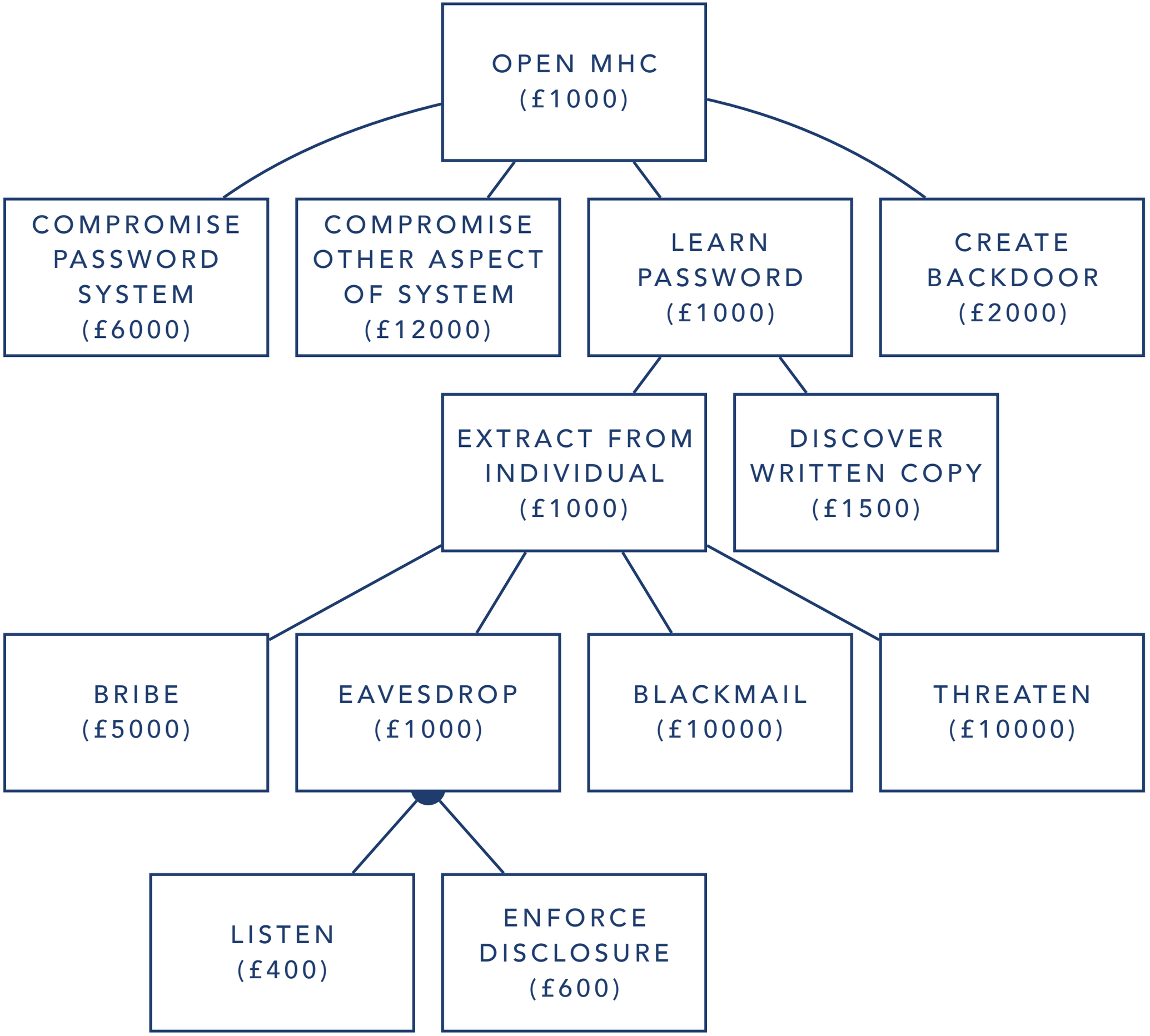
PERSPECTIVES

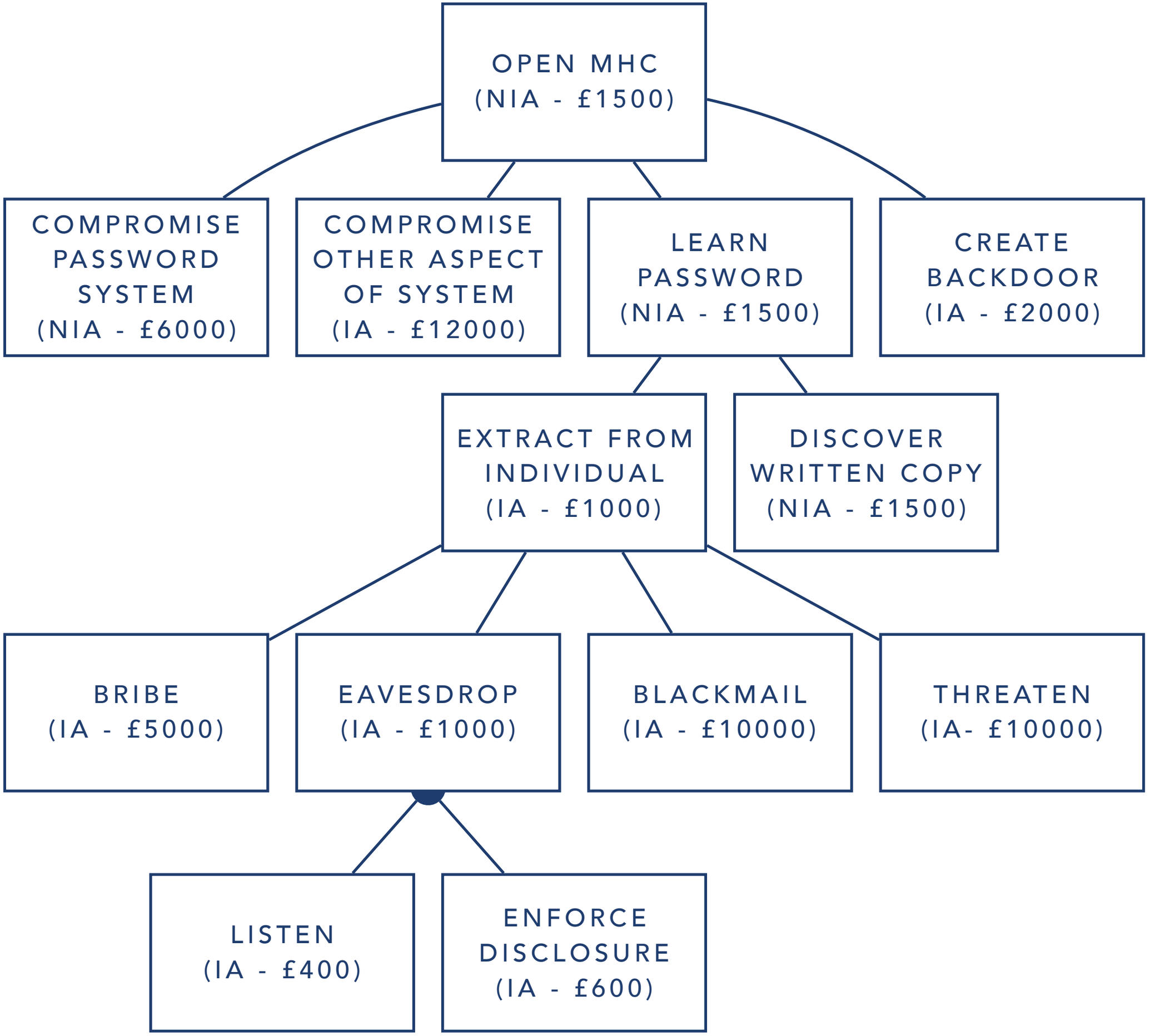
- multiple attack trees can be created to consider attacks from multiple adversaries.

- 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.


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


OPEN 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)

OUTLINE

COMPLETENESS

- research, evidence, literature survey
- attacker libraries
- STRIDE
- CAPEC
- pruning attack tree to ensure it is an accurate and efficient representation of what is being considered.

THREAT THINKING AND DELIVEROO

SMALL GROUP DISCUSSION

DELIVEROO

DELIVEROO

Technology

Deliveroo customers billed for unordered food

8 hours ago | Technology

Share

THREAT THINKING

- consider the context of Deliveroo.
- consider some potential threats for something like Deliveroo.
- consider one of the least expensive attacks for a hungry individual to mount against Deliveroo.

ENTERPRISE CYBER SECURITY

THREAT THINKING

University of Glasgow

GDPR IMPACT ON ENTERPRISES AND SUBSYSTEMS

SMALL GROUP DISCUSSION

CYBER SECURITY CONCERNS OF DEDUPLICATION FOR ENTERPRISES AND SUB-SYSTEMS

SMALL GROUP DISCUSSION