Threat Modelling

CDT Threats & Risks: Session 1

Matthew Edwards

Oct. 10th, 2019

Section 1

This Module

Module Goals

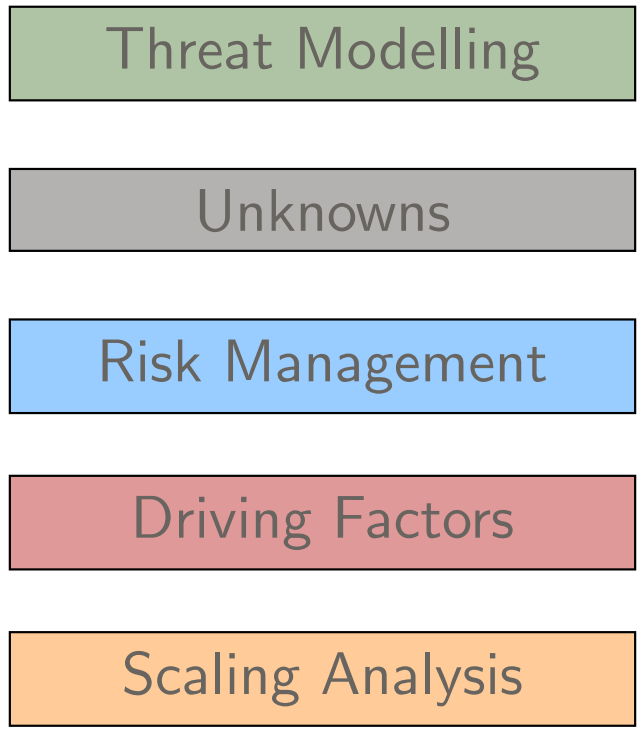
- Introduction to attack & threat modelling, reporting, and incident response methods.
- Risk management, risks in large-scale infrastructure.
- Unknowns, uncertainties and limitations of extant approaches.
- Scaling-up: information overload, analytics for security events.
- Factors driving adversarial behaviours, threats understood economically, ecologically and societally.

Background

This module draws upon four CyBOK knowledge areas:

1. Security Operations and Incident Management
2. Adversarial Behaviours
3. Human Factors
4. Risk Management & Governance

Structure: Fortnights



Structure: Fortnightly

Thursdays, 11:00 – 13:00

Taught Session	
Flipped Session	Request Session

Section 2

Today's Session

Goals

- Introduction to attack & threat modelling methods.
- Overview of security operations and incident response approaches.
- Frameworks for understanding threats, risks & vulnerabilities.
- Useful resources and pointers for further reading.

Terms

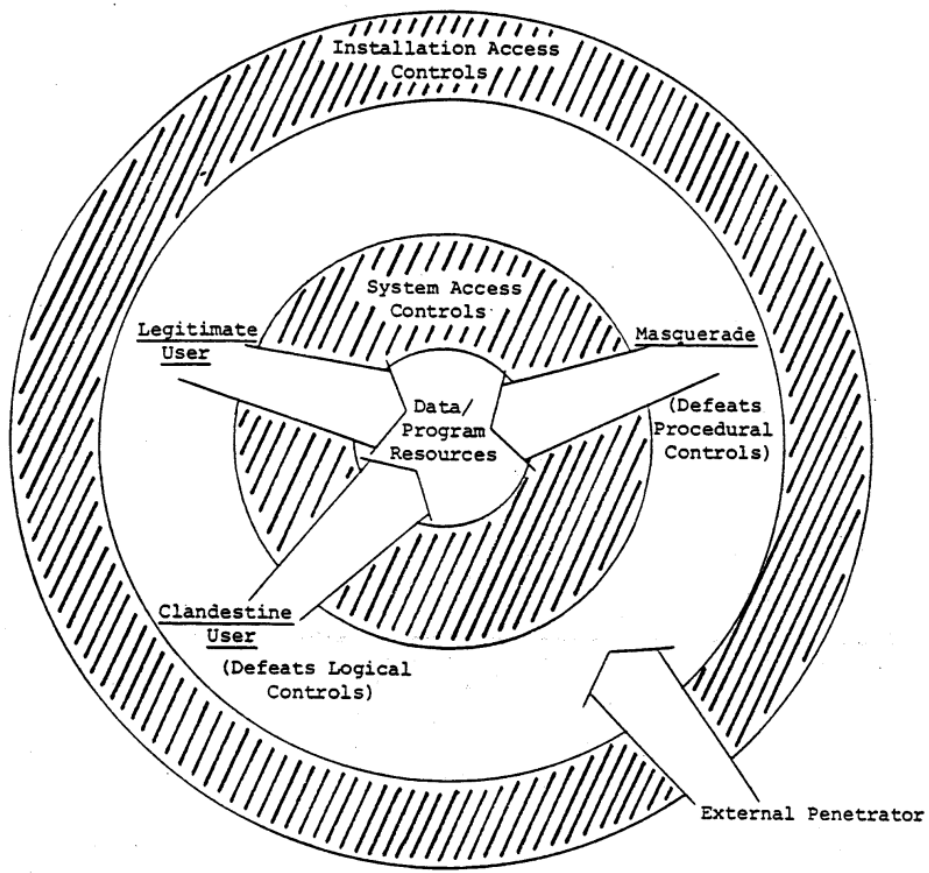
Threat	the possibility of a deliberate unauthorised attempt to violate **confidentiality**, **integrity**, or **availability** of information.
Vulnerability	a flaw in the design of a system protecting information.
Risk	the potential that a given threat will exploit vulnerabilities of an asset and thereby cause harm.
Attack	a specific formulation or execution of a plan to implement a threat.
Penetration	a successful attack.

Section 3

Security Operations

Security Operations

Problem: Full protection of infrastructure is impossible.[1]



[1] J. P. Anderson et al., "Computer security threat monitoring and surveillance," Technical report, James P. Anderson Company, Fort Washington, Pennsylvania, 1980.

Security Operations

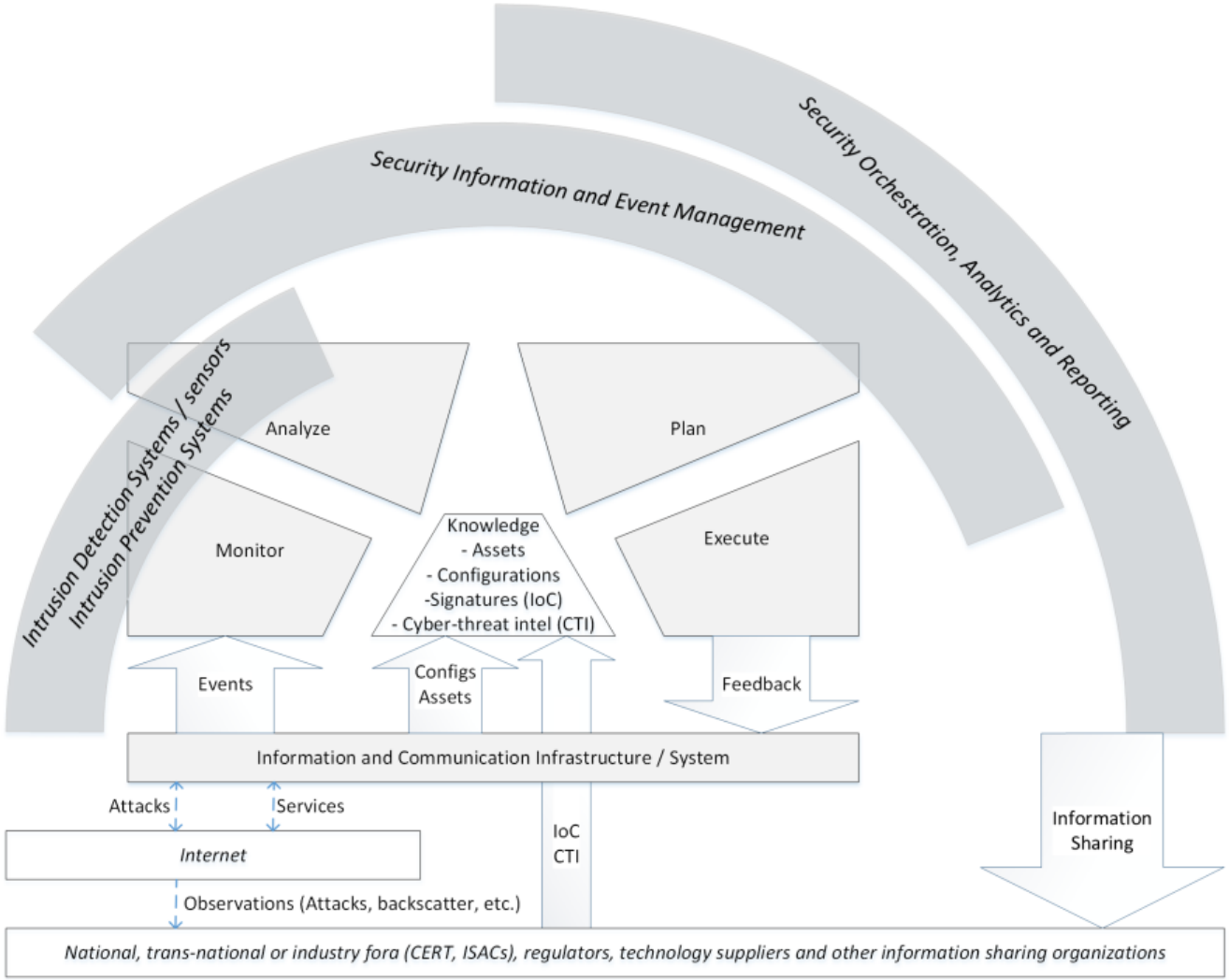
Solution: To complement protections, we should record system activity in order to detect and understand penetrations.

< Subject, Action, Object, Exception-Condition, Resource-Usage, Timestamp >[2]

[2] D. E. Denning, "An intrusion-detection model," IEEE Transactions on Software Engineering, no. 2, pp. 222–232, 1987.

Security Operations

Security operation as an **autonomic system**: MAPE-K.[3]



[3] H. Debar, "Security Operations & Incident Management Knowledge Area", CyBOK, 2019.

Security Operations: Monitor

Generally, monitoring is achieved through a combination of technical controls.

System	File access, system and kernel event logs, e.g., syslog.
Network	Highly granular (pcap) or aggregated (Netflow).
Application	Application-level (e.g., web server) logs.

Security Operations: Analyse

A huge literature ($\sim$ 1 million publications). Two general approaches:

Misuse Detection

Search for patterns matching **known malicious events** in the logs.

Anomaly Detection

Analyse logs for **anomalous deviations** from ordinary behaviour.

More on this in the **Scaling Analysis** block.

Analysis Task

Download and open the **SSH log file** provided.

timestamp	when the SSH connection was detected.
uid	unique identifier for this connection.
id.orig_h	IP address of the originating machine.
id.orig_p	Originating machine's port.
id.resp_h	IP address of the responding machine.
id.resp_p	Responding machine's port.
status	if the login was (guessed to be) a success or a failure.
direction	outbound or inbound connection.
client	software string from the client.
server	software string from the server.

Analysis Task Questions

1. How many failed connection attempts are there, as a proportion of all the data?
2. Which host is originating the most failed connection attempts?
3. Which host is *receiving* the most failed connection attempts? Where from?
4. Which origin hosts have attempted to connect to the most server IP addresses?
5. What is the UID for the most recent successful connection?
6. At what time of day did it occur?

Security Operations: Plan

Planning is supported in a **Security Information and Event Management** (SIEM) platform.

- Handles incoming alerts from **sensors** in a variety of formats.
- Correlates alerts from different sensors with each other and **situational information**.
- Measures the performance/ability of the **SOC** against benchmarks.

Information Security Indicators

`https://www.etsi.org`

Security Operations: Execute

A **detection system** controlling a gateway can become a **prevention system**.

Operations teams must also patch vulnerabilities.

Security configuration changes must be assessed to prevent the interruption of business. Commonly, this is carried out through **ticketing systems**.

Security Operations: Knowledge

CTI *Cyber Threat Intelligence*. Organisations that run **honeypots** and share information on threats and IoC between affected organisations.

IoC *Indicators of Compromise*. Patterns that indicate an ongoing, imminent or previous attack on your system.

CERT *Computer Emergency Response Team*. Share information on threats, but also best practices.

Common Vulnerabilities and Exposures

Most commonly referred to as **CVE**. Paired with **CVSS**, the *Common Vulnerability Scoring System*. Acts as a common dictionary for known software vulnerabilities.

At a higher level, the **CWE** describes weaknesses in software authorship that lead to vulnerabilities.

MITRE CVE Database

Accessible at `https://cve.mitre.org/`.

CAPEC

The **Common Attack Pattern Enumeration and Classification** framework. Classifies and describes attack patterns at a high level, with links to supporting weaknesses.

MITRE CAPEC Database

Accessible at `https://capec.mitre.org/`

ATT&CK

Reference framework for **Adversarial Tactics, Techniques and Common Knowledge** – describing the specific actions an attacker takes while operating in a network. Covers groups of ongoing concern to the security community.

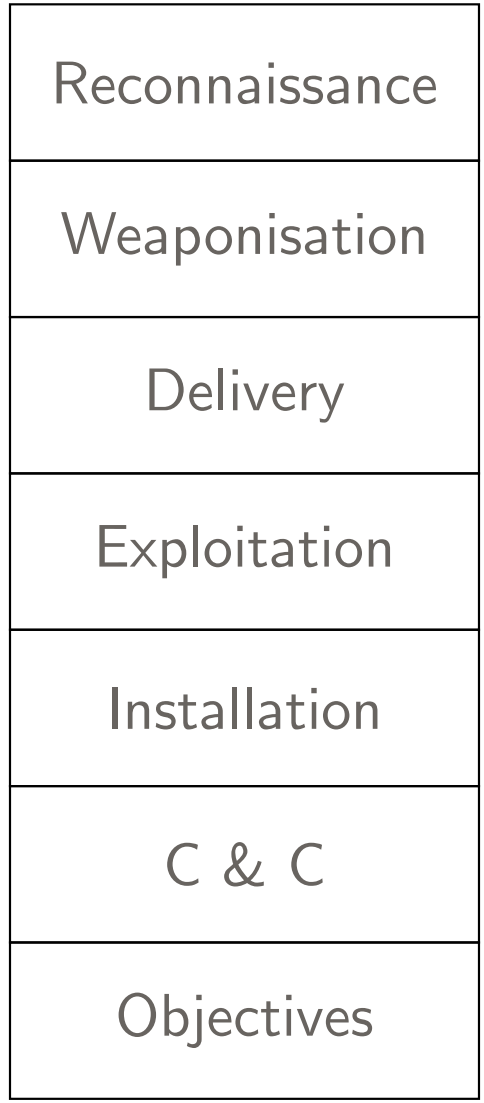
MITRE ATT&CK Database

Accessible at `https://attack.mitre.org/`

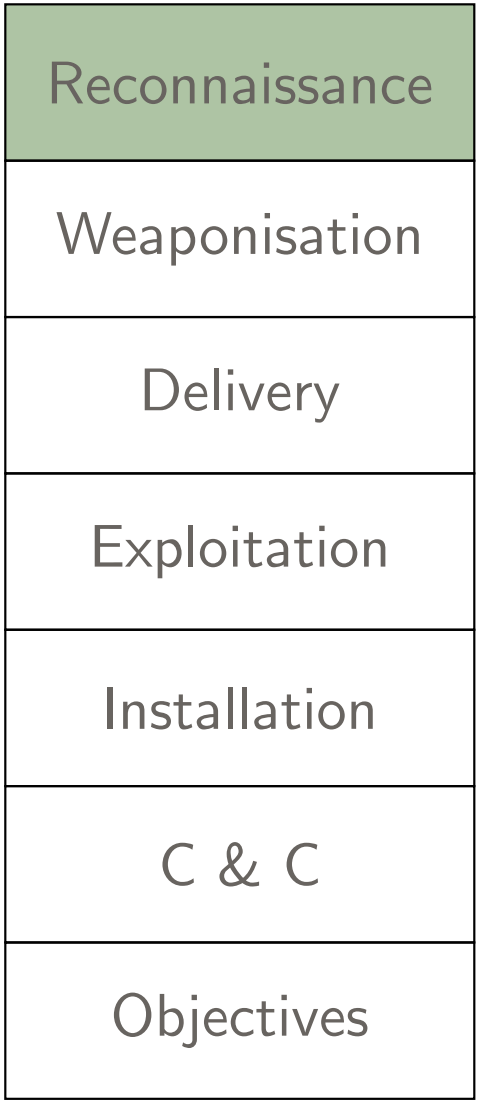
Section 4

Attack Modelling

The Killchain



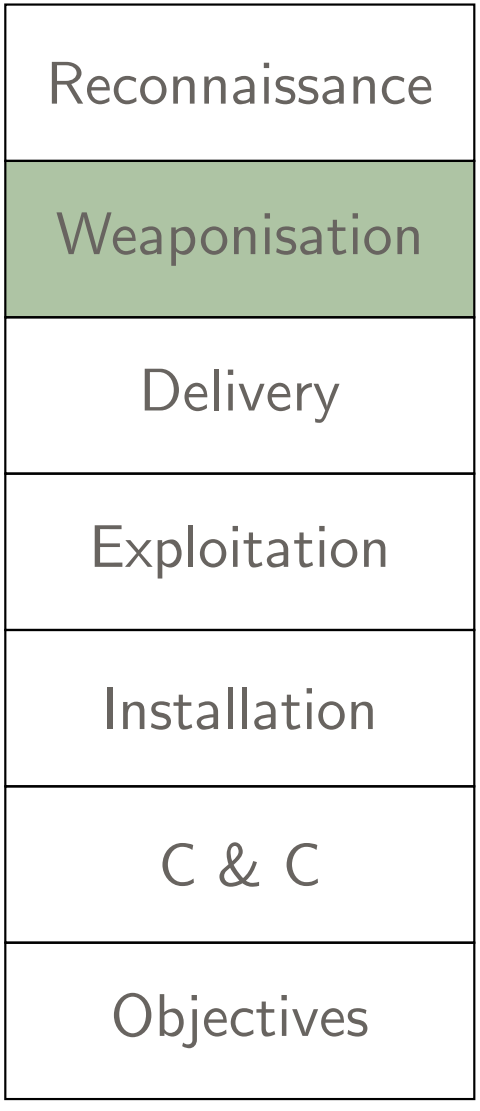
The Killchain: Reconnaissance



Attackers identify possible targets.

Detect	Web analytics
Deny	Firewall
Disrupt	CAPTCHA
Degrade	Report scan origins
Deceive	Pollution

The Killchain: Weaponisation



Attackers craft the exploit package.

Detect

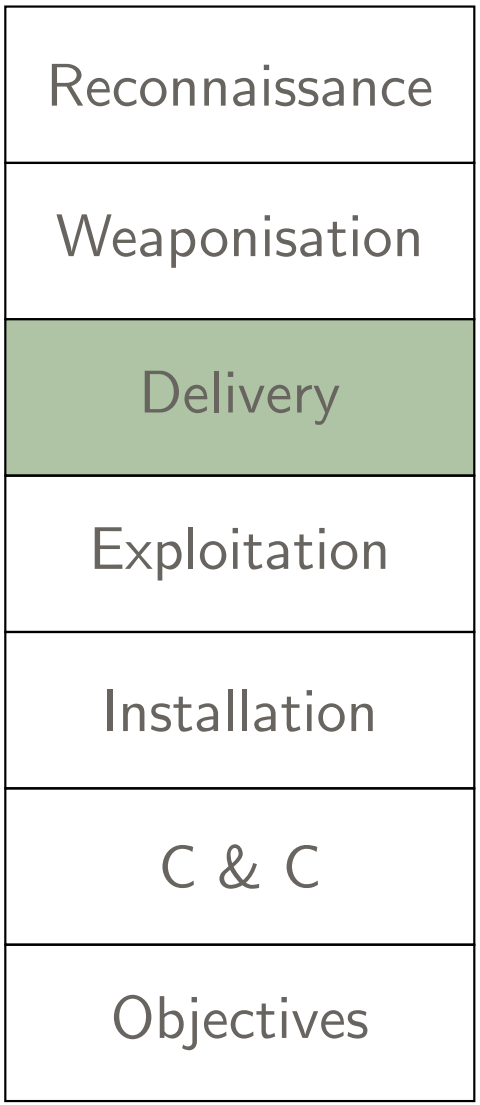
Deny

Disrupt

Degrade

Deceive

The Killchain: Delivery



Attackers transmit the exploit to the target.

Detect

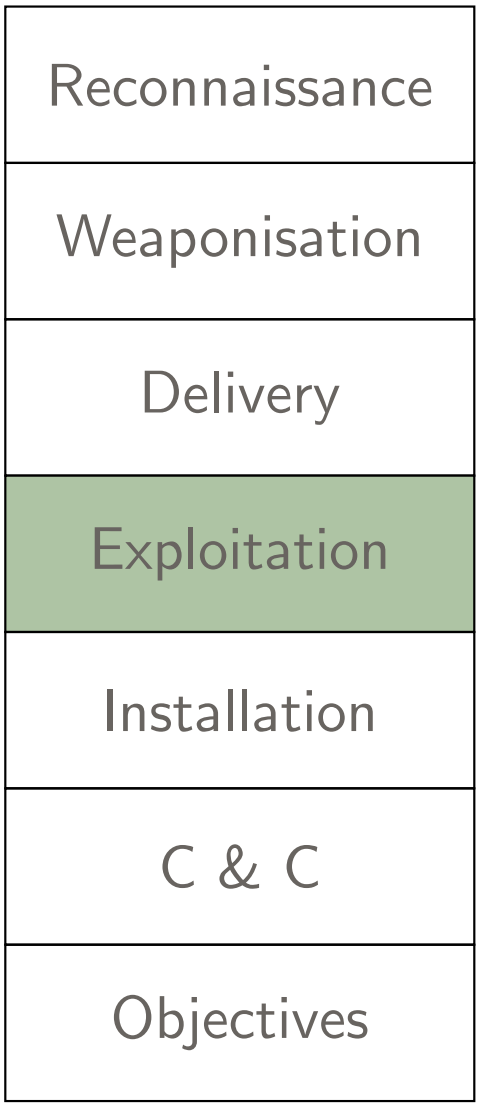
Deny

Disrupt

Degrade

Deceive

The Killchain: Exploitation



The exploit reaches and acts on the target's vulnerability.

Detect

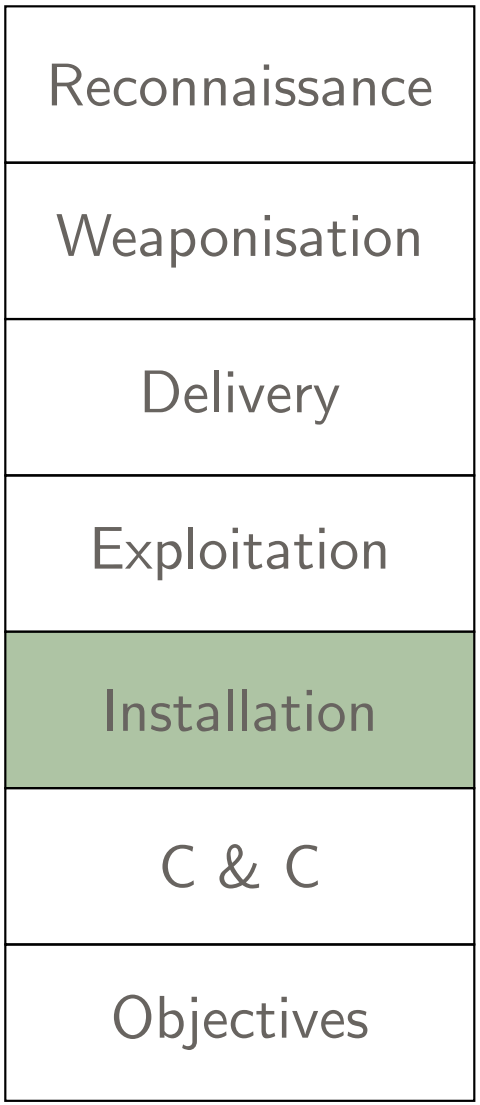
Deny

Disrupt

Degrade

Deceive

The Killchain: Installation



The exploit establishes persistent/necessary access.

Detect

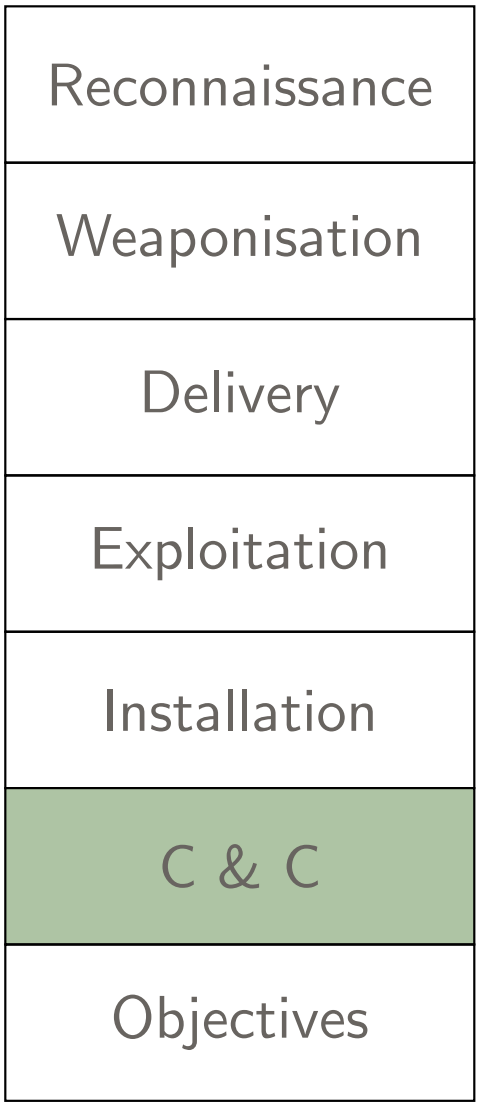
Deny

Disrupt

Degrade

Deceive

The Killchain: Command & Control



The exploit establishes communications with the attacker.

Detect

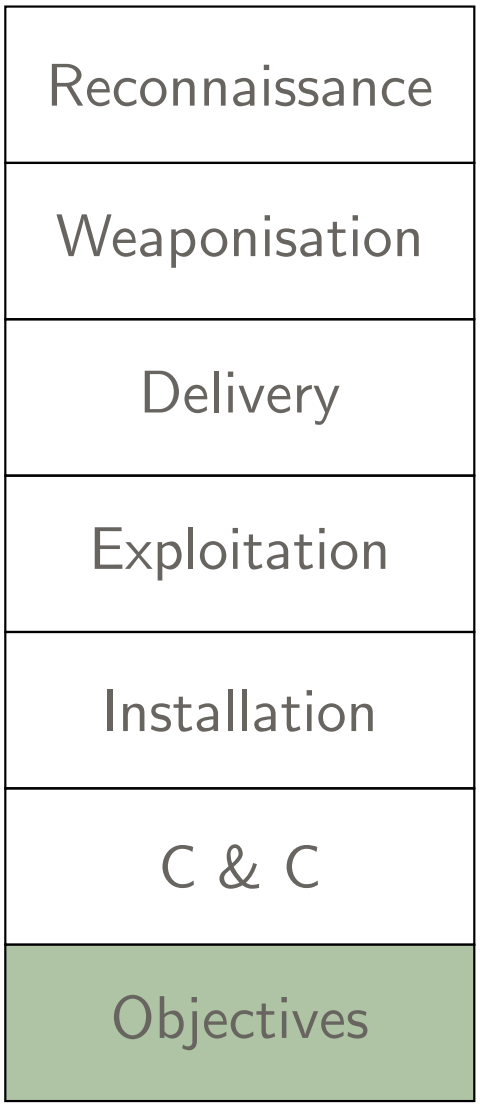
Deny

Disrupt

Degrade

Deceive

The Killchain: Actions on Objectives



The attacker's objectives in the system are realised.

Detect

Deny

Disrupt

Degrade

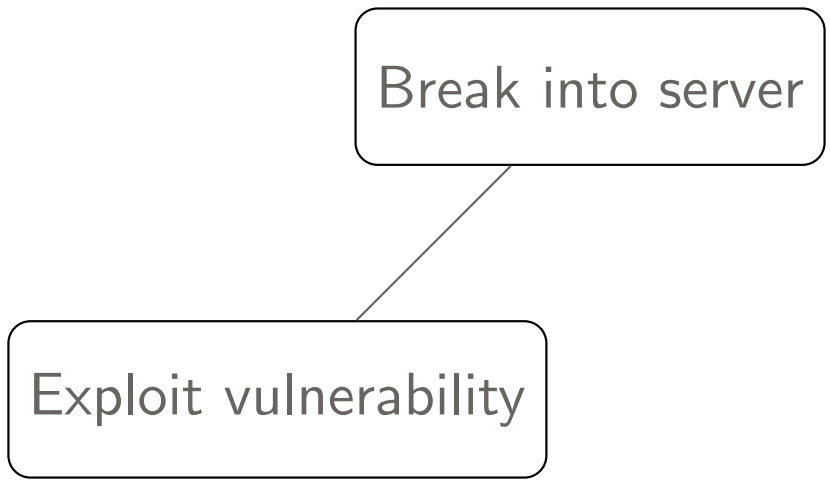
Deceive

Attack Trees

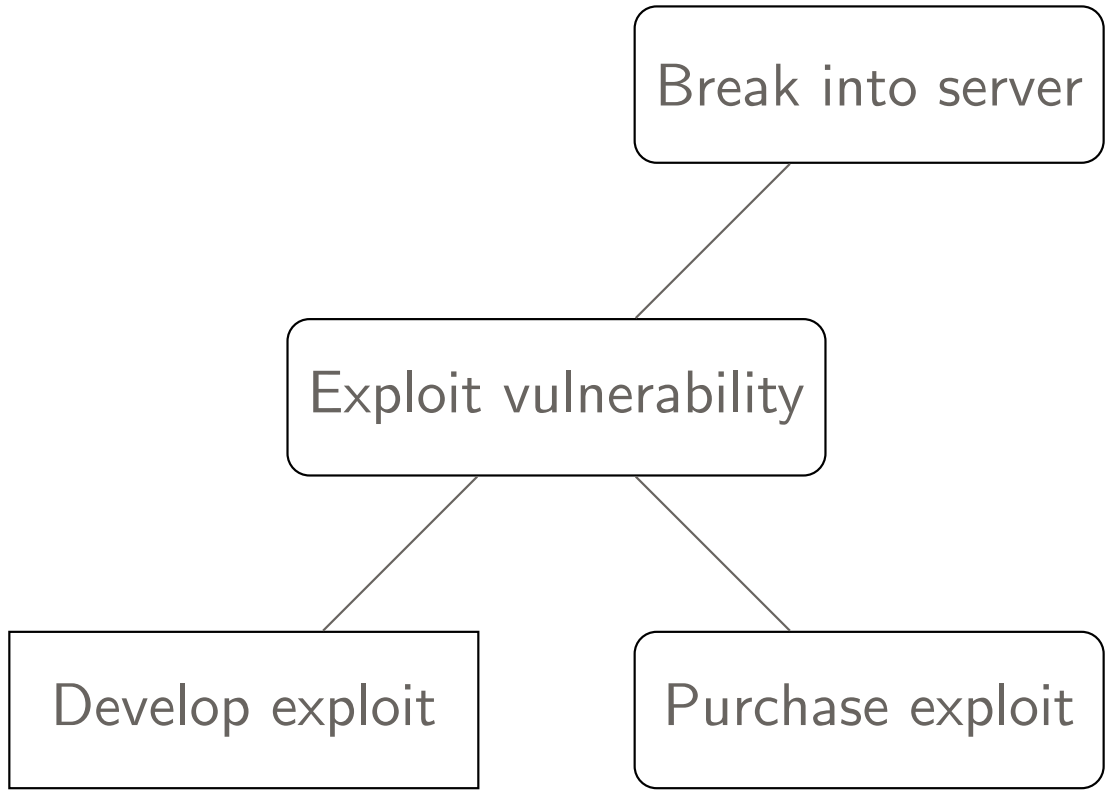
A formalised mechanism for visualising the paths to penetration. Start from an attacker's **goal** and work backwards through their method using a series of 'and' and/or 'or' nodes.

Attack Trees

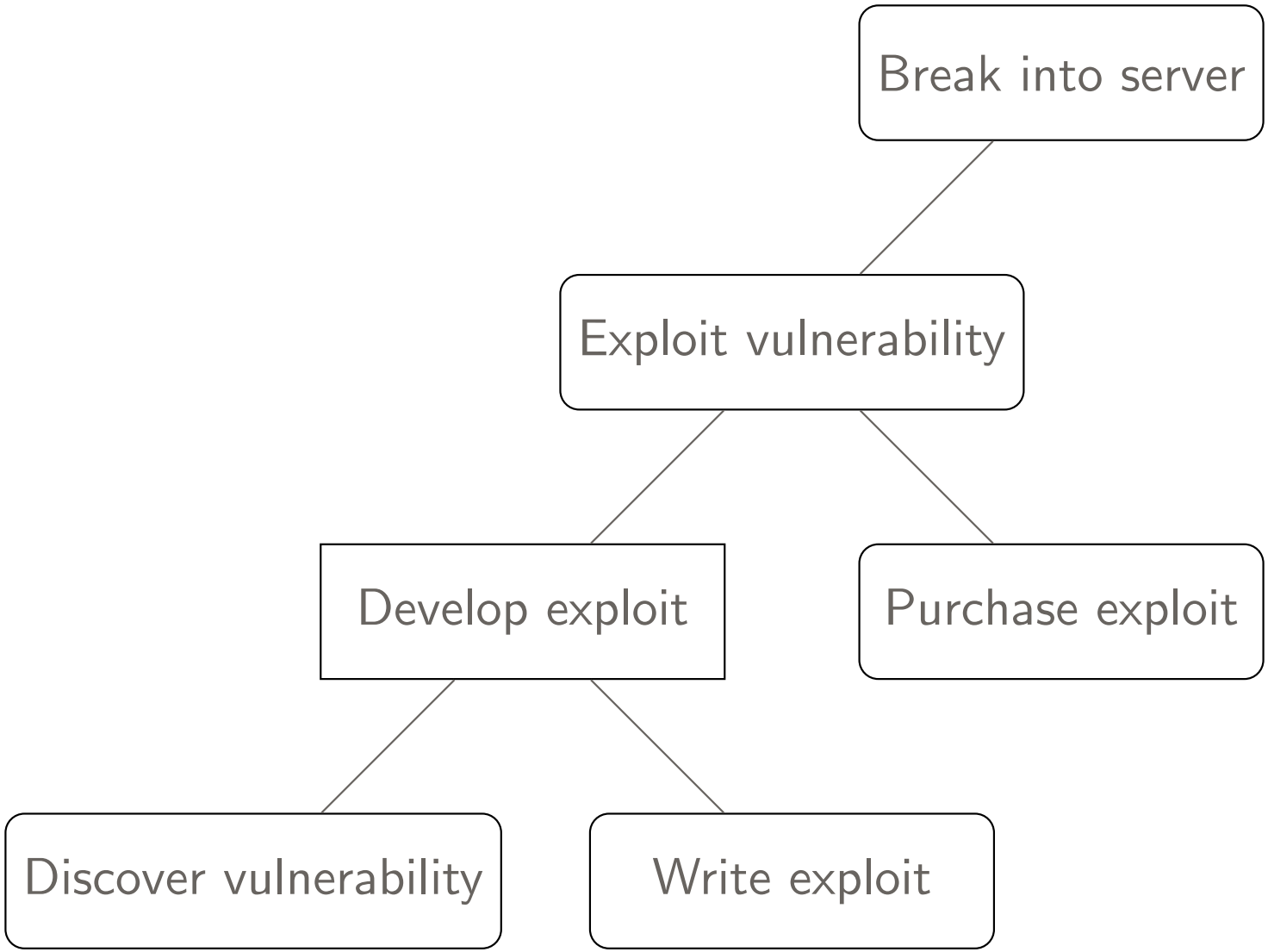
Attack Trees



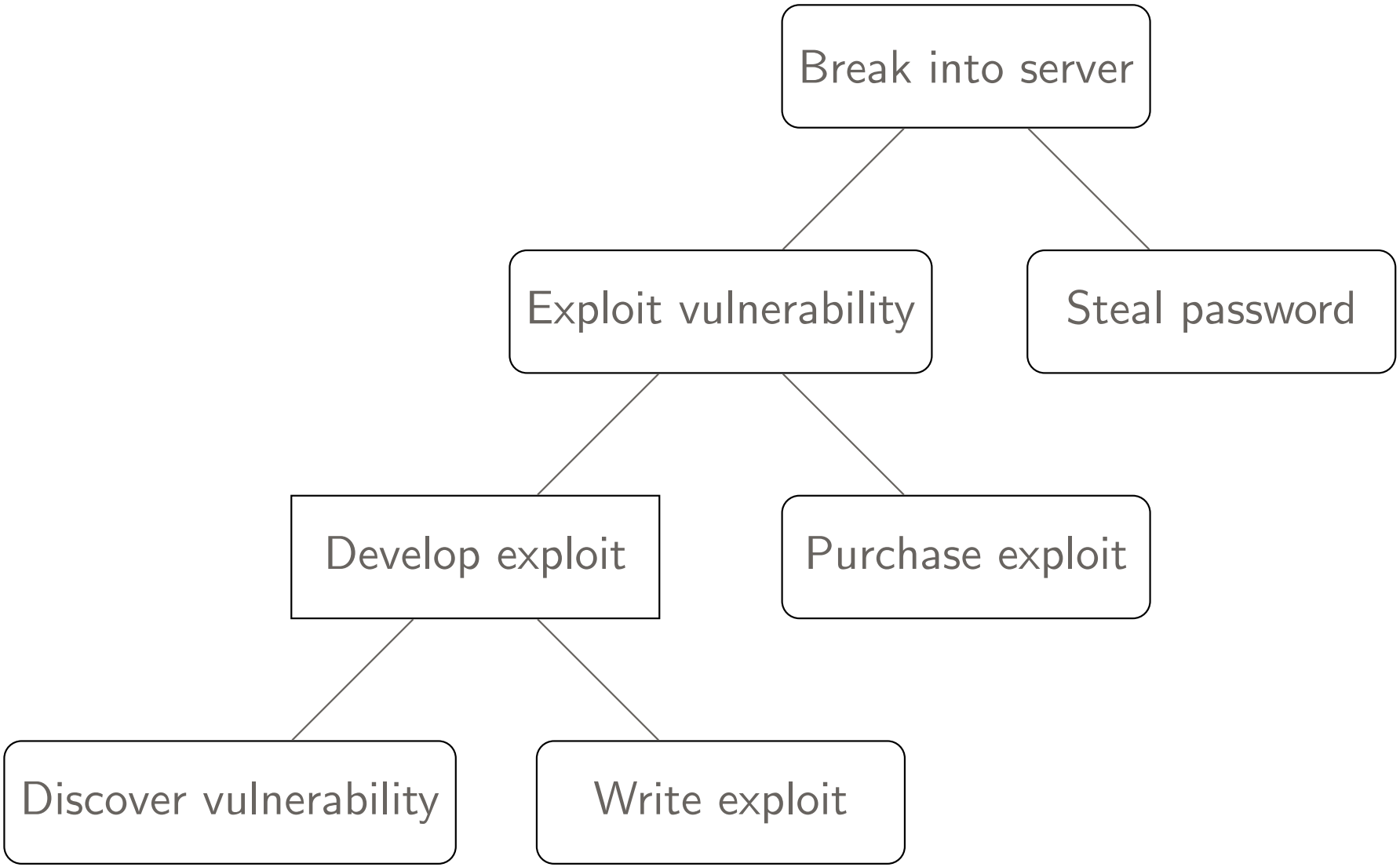
Attack Trees



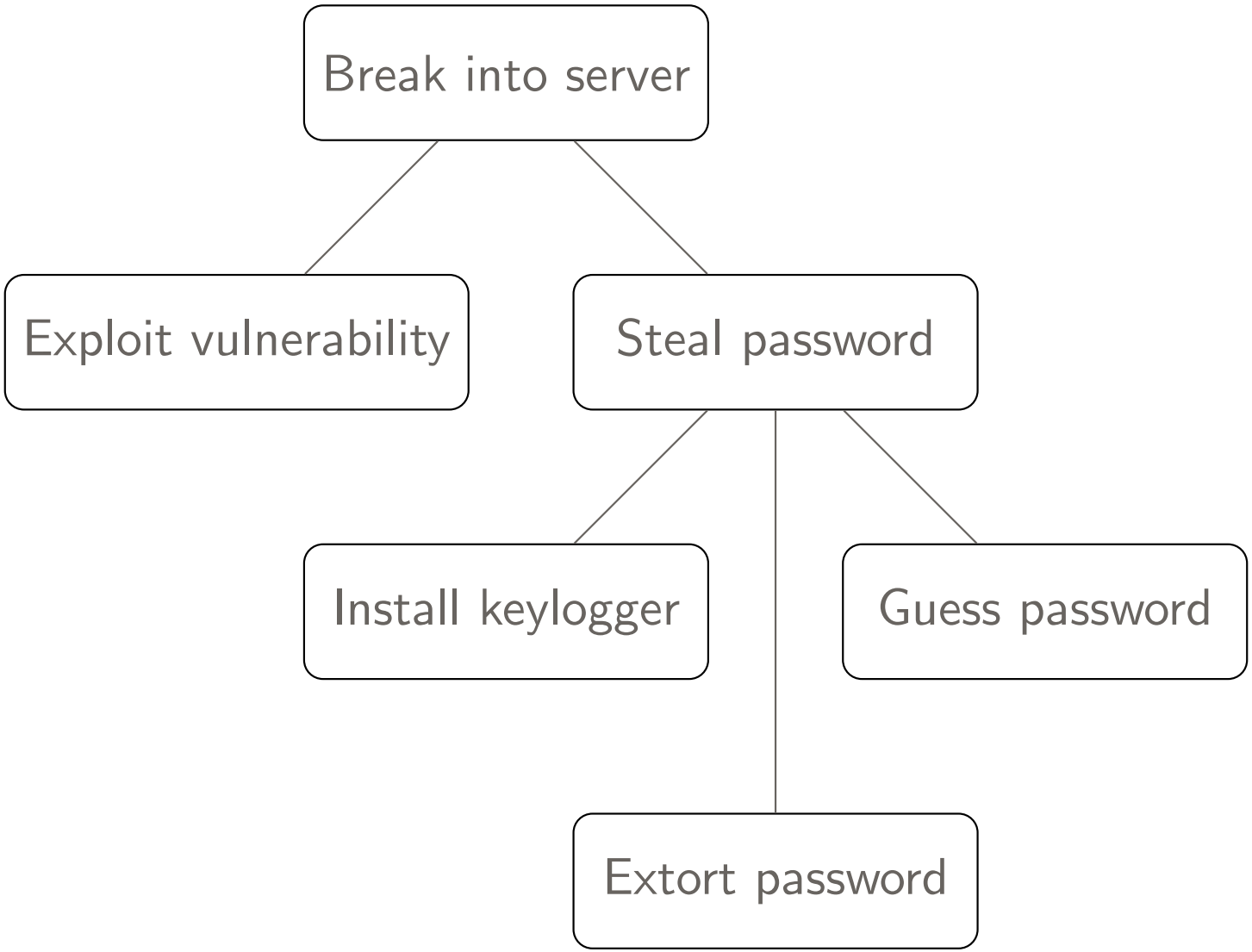
Attack Trees



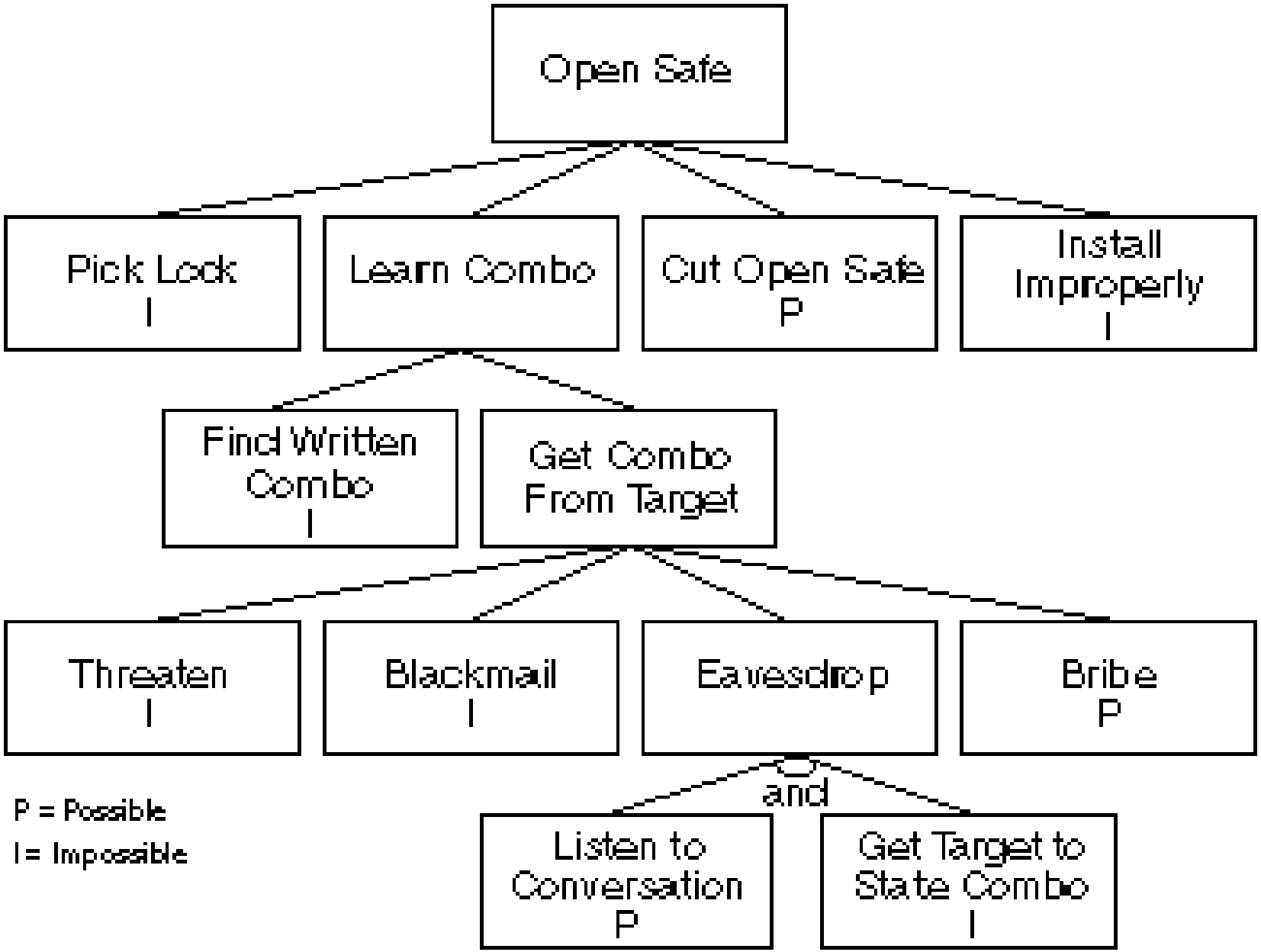
Attack Trees



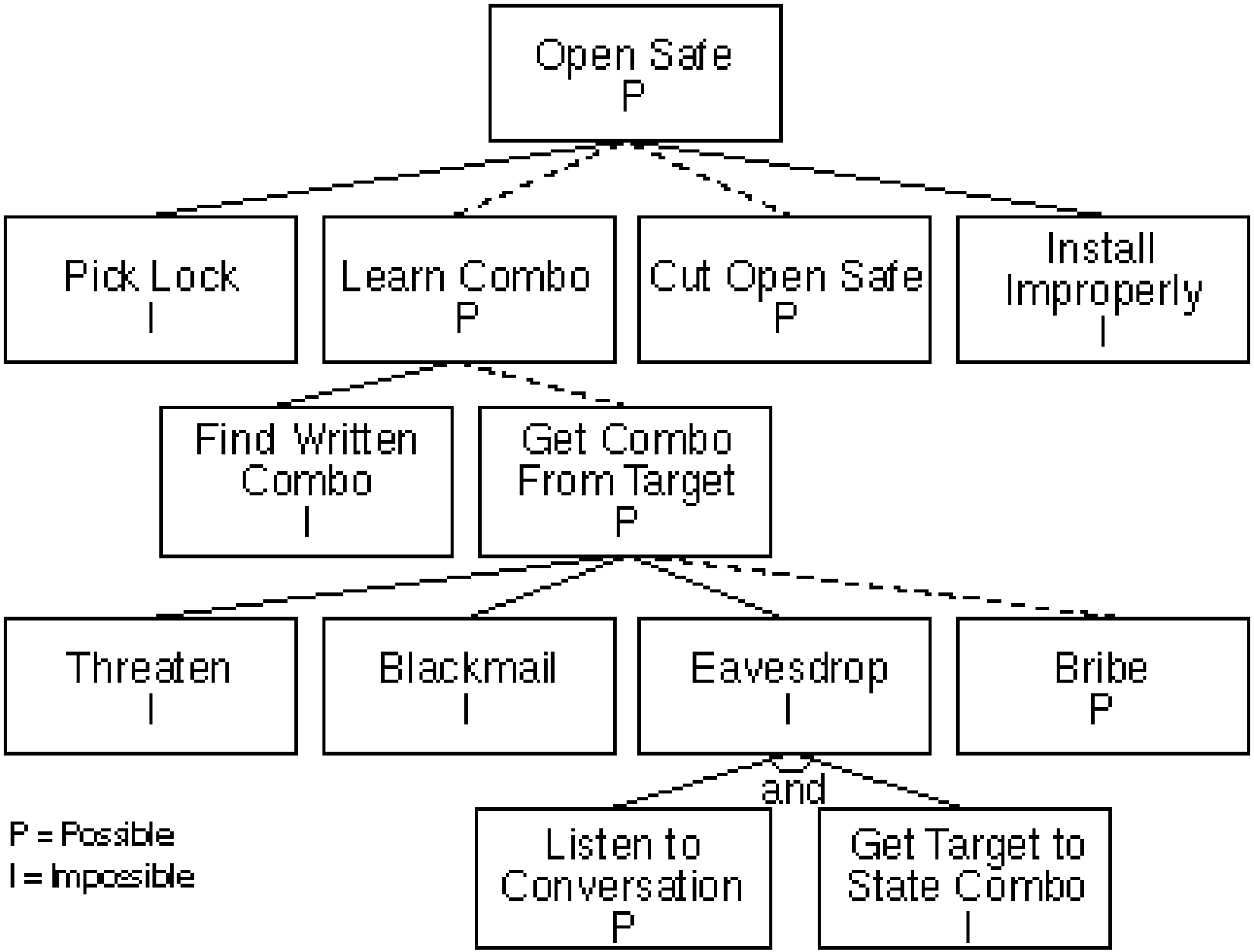
Attack Trees



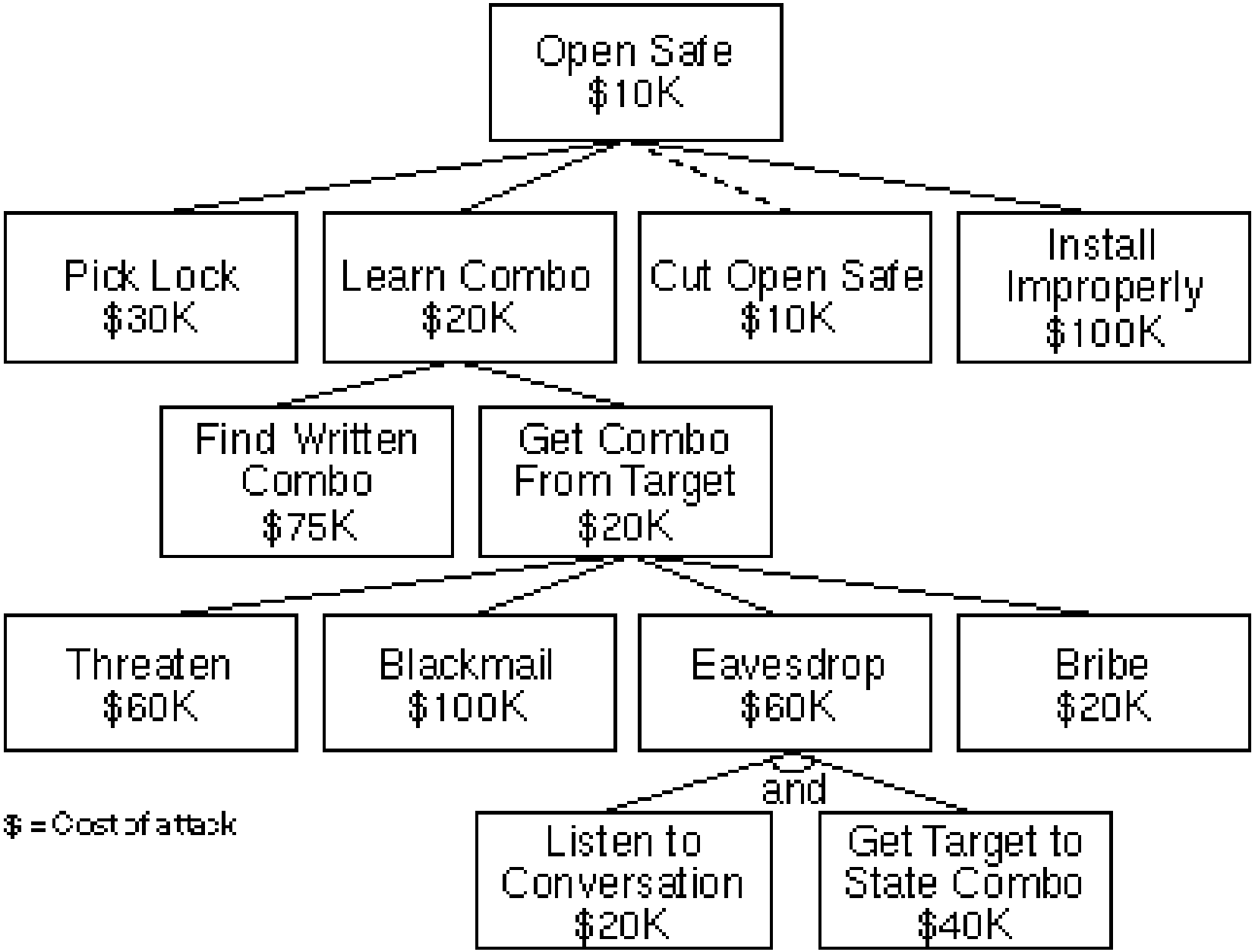
Attack Trees: Annotation



Attack Trees: Annotation



Attack Trees: Annotation



Attack Trees: Task

1. Generate an attack tree from your assigned root node and context organisation, exploring as many paths as deeply as possible (∼10 min.).
2. Swap with someone else and look for new paths. (∼10 min.)
3. Scoring system:
   - **10 points** for a new top-level path.
   - **5 points** for a new second-level path.
   - **2 points** for a new third-level path.
   - **1 point** for a new fourth-or-below path.

Attack Trees: Nodes & Context

	Goal	**Context**
Priyanka	Steal intellectual property	Pharmaceutical Org.
Hannah	Rig election	Foreign Government
Soo Yee	View exam solutions	University
Robert	Prevent bill passing	Houses of Parliament
Tobias	Extract money	Car Insurance Website
Manolis	Blow up pipeline	Oil & Gas Corp.

Section 5

Next Week

Flipped Session

In your assigned groups, prepare a 25-minute presentation on your group's assigned threat modelling framework. You should try to cover:

- What it is, what it does.
- The academic background; the context it is designed for.
- A demonstration of how the approach can be applied.
- Software support for the approach.
- What is known about uptake in industry; actual applications.
- Proposed extensions or modifications (if any).

Group 1: STRIDE

Priyanka, Soo Yee & Tobias

Starting points:

- https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)
- https://www.microsoft.com/en-us/download/details.aspx?id=49168

Group 2: TRIKE

Hannah, Robert & Manolis

Starting points:

- `http://trike.sourceforge.net/papers/`
- `http://www.octotrike.org/tools`

Request Session

Suggestions:

- Complementary session on PASTA?
- Deep-dive on particular threat actors?
- Hands-on session with OWASP Threat Dragon?
- ...