STRIDE Threat Modelling

Learning Outcomes

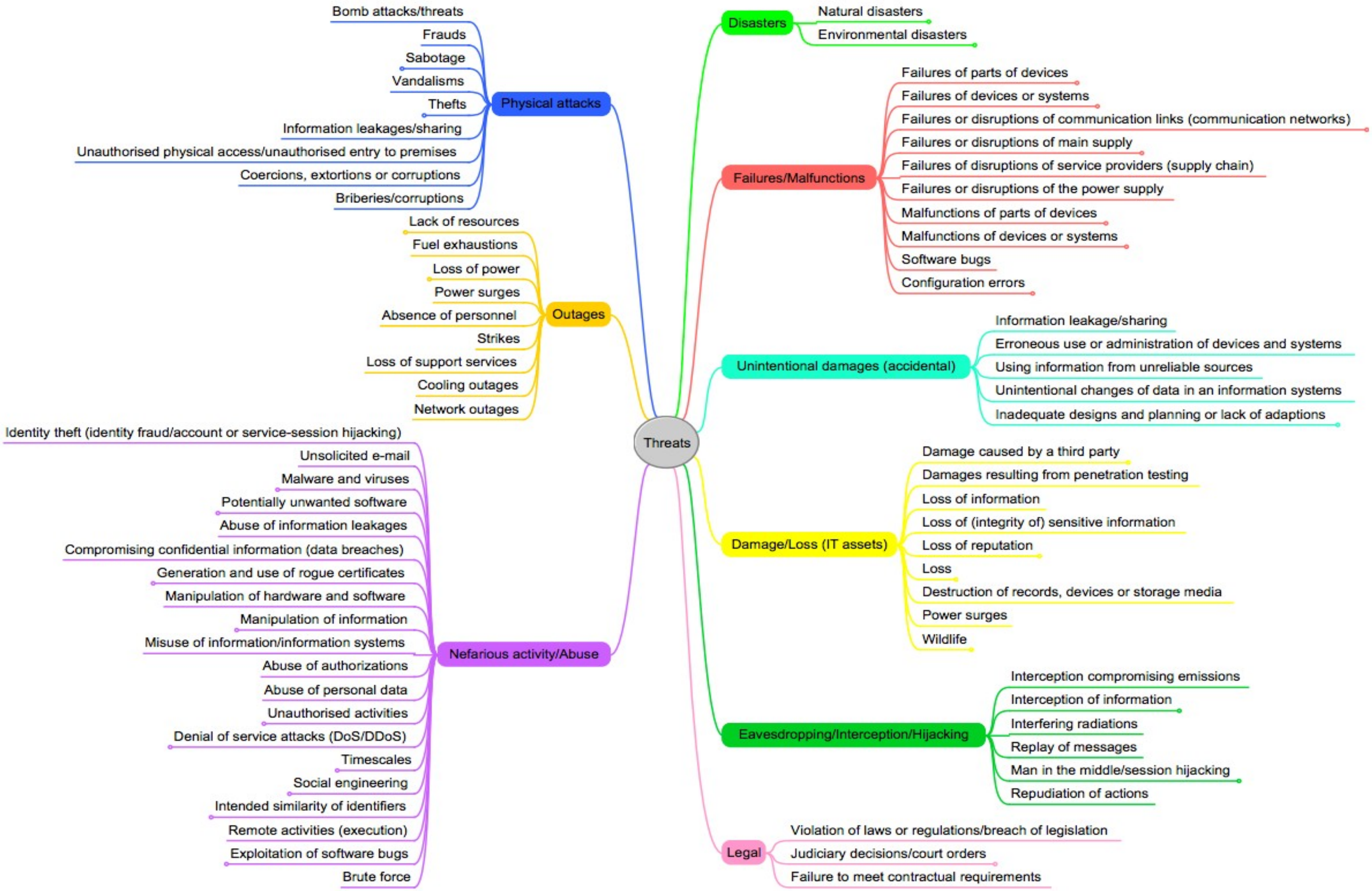
- Threat Landscape
- Identifying Threats with STRIDE
- Elements of STRIDE
- Properties of STRIDE

What is the current status?

THE THREAT LANDSCAPE

Overview

1. **The Threat Landscape**
2. Threat Actors
3. Attack Vectors
4. Stride and Threat



Threats

- Physical attacks
  - Bomb attacks/threats
  - Frauds
  - Sabotage
  - Vandalisms
  - Thefts
  - Information leakages/sharing
  - Unauthorised physical access/unauthorised entry to premises
  - Coercions, extortions or corruptions
  - Briberies/corruptions
- Outages
  - Lack of resources
  - Fuel exhaustions
  - Loss of power
  - Power surges
  - Absence of personnel
  - Strikes
  - Loss of support services
  - Cooling outages
  - Network outages
- Nefarious activity/Abuse
  - Identity theft (identity fraud/account or service-session hijacking)
  - Unsolicited e-mail
  - Malware and viruses
  - Potentially unwanted software
  - Abuse of information leakages
  - Compromising confidential information (data breaches)
  - Generation and use of rogue certificates
  - Manipulation of hardware and software
  - Manipulation of information
  - Misuse of information/information systems
  - Abuse of authorizations
  - Abuse of personal data
  - Unauthorised activities
  - Denial of service attacks (DoS/DDoS)
  - Timescales
  - Social engineering
  - Intended similarity of identifiers
  - Remote activities (execution)
  - Exploitation of software bugs
  - Brute force
- Disasters
  - Natural disasters
  - Environmental disasters
- Failures/Malfunctions
  - Failures of parts of devices
  - Failures of devices or systems
  - Failures or disruptions of communication links (communication networks)
  - Failures or disruptions of main supply
  - Failures of disruptions of service providers (supply chain)
  - Failures or disruptions of the power supply
  - Malfunctions of parts of devices
  - Malfunctions of devices or systems
  - Software bugs
  - Configuration errors
- Unintentional damages (accidental)
  - Information leakage/sharing
  - Erroneous use or administration of devices and systems
  - Using information from unreliable sources
  - Unintentional changes of data in an information systems
  - Inadequate designs and planning or lack of adaptions
- Damage/Loss (IT assets)
  - Damage caused by a third party
  - Damages resulting from penetration testing
  - Loss of information
  - Loss of (integrity of) sensitive information
  - Loss of reputation
  - Loss
  - Destruction of records, devices or storage media
  - Power surges
  - Wildlife
- Eavesdropping/Interception/Hijacking
  - Interception compromising emissions
  - Interception of information
  - Interfering radiations
  - Replay of messages
  - Man in the middle/session hijacking
  - Repudiation of actions
- Legal
  - Violation of laws or regulations/breach of legislation
  - Judiciary decisions/court orders
  - Failure to meet contractual requirements

What is Threat Landscape?

- The *threat landscape* is a list of threats and the associated threat actors and attack vectors.
    - threats
    - attack methods (vectors)
    - threat actors
    - exploits
    - vulnerabilities

Factors leading to a change?

- Exploitable vulnerabilities
- Assets value
- Threat actors capabilities
  - skills
  - tools
  - resources
  - motivation
- Introduction of new technology

The Threat Landscape & Risk Landscape

- A threat landscape contains …
    - vulnerabilities, assets, threats, countermeasures.
- A risk landscape
    - is more comprehensive
    - is based on a threat landscape
    - impact, likelihood
    - mitigation controls for the potential threats

Overview

1. The Threat Landscape
2. **Threat Actors**
3. Attack Vectors
4. Stride and Threat

Threat Actor

- Definition
  - *threat actor* indicates an individual or group that can manifest a threat [OWASP].
    - Internal
    - External
  - Capabilities + Intentions + Past Activities.

* OWASP - Open Web Application Security Project is an online community which creates freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security.

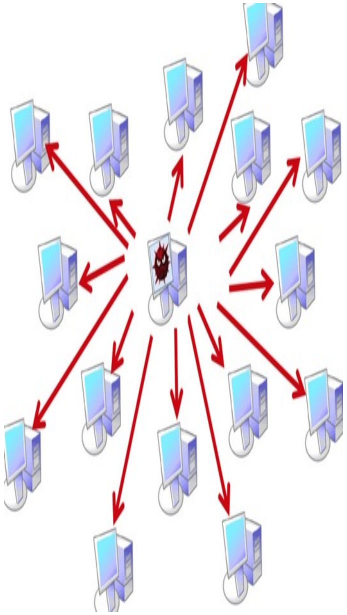
Threat Actors – Who are they?

- Cybercriminals
- Online Social Hackers
- Hacktivists
- Nation States
- Corporations
- Employees
- Cyber Fighters
- Cyber Terrorists

Overview

1. The Threat Landscape
2. Threat Actors
3. **Attack Vectors**
4. Stride and Threat

Attack vectors



- Definition
  - a path or a tool that a threat actor uses to gain access to a system in order to deliver a malicious outcome.
  - “how” to achieve a successful attack?
  - e.g. malicious emails, attachments, web pages, deception, code injection, etc.

How to describe a Cyber Attack?

- A generic description of the attack
  - an asset
  - its weakness/vulnerability
  - the techniques
  - the consequences
- Description format
  - a threat actor applies … techniques to exploit the vulnerabilities of the… system/assets, thus gaining access to achieve their … goals. This has resulted in the consequences of …

Overview

1. The Threat Landscape
2. Threat Actors
3. Attack Vectors
4. **Stride and Threat**

Background

- Developed by Praerit Garg and Loren Kohnfelder @ Microsoft

- Defines security threats into 6 categories

- Process of threat modelling

Identifying Threats Using Stride

Element	Description	Security Property
S		
T		Integrity
R		
I		Confidentiality
D		Availability
E		

Identifying Threats Using Stride

Element	Description	Security Property
S		Authentication
T		Integrity
R		Non-repudiability
I		Confidentiality
D		Availability
E		Autorisation

Identifying Threats Using Stride

Element	Description	Security Property
S	Spoofing – Attacker or program successfully identifies as another by falsifying data	Authentication
T		Integrity
R		Non-repudiability
I		Confidentiality
D		Availability
E		Autorisation

Identifying Threats Using Stride

Element	Description	Security Property
S	Spoofing – Attacker or program successfully identifies as another by falsifying data	Authentication
T	Tampering - Attacker attempts to modify data that’s exchanged between system components or component & user	Integrity
R		Non-repudiability
I		Confidentiality
D		Availability
E		Autorisation

Identifying Threats Using Stride

Element	Description	Security Property
S	Spoofing – Attacker or program successfully identifies as another by falsifying data	Authentication
T	Tampering - Attacker attempts to modify data that’s exchanged between system components or component & user	Integrity
R	Repudiation - Attacker performs an action with the system or component that is not attributable	Non-repudiability
I		Confidentiality
D		Availability
E		Autorisation

Non-repudiation

Definition:

A property achieved through a method to protect against an individual or entity falsely denying having performed a particular action related to data.

Extended Definition:

Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message.

Identifying Threats Using Stride

Element	Description	Security Property
S	Spoofing – Attacker or program successfully identifies as another by falsifying data	Authentication
T	Tampering - Attacker attempts to modify data that's exchanged between system components or component & user	Integrity
R	Repudiation - Attacker performs an action with the system or component that is not attributable	Non-repudiability
I	Information disclosure - Attacker is able to read the private data that the system is transmitting or storing	Confidentiality
D		Availability
E		Autorisation

Identifying Threats Using Stride

Element	Description	Security Property
S	Spoofing – Attacker or program successfully identifies as another by falsifying data	Authentication
T	Tampering - Attacker attempts to modify data that’s exchanged between system components or component & user	Integrity
R	Repudiation - Attacker performs an action with the system or component that is not attributable	Non-repudiability
I	Information disclosure - Attacker is able to read the private data that the system is transmitting or storing	Confidentiality
D	Denial of service - An attacker can prevent the passengers or system components from accessing each other	Availability
E		Autorisation

Identifying Threats Using Stride

Element	Description	Security Property
S	Spoofing – Attacker or program successfully identifies as another by falsifying data	Authentication
T	Tampering - Attacker attempts to modify data that's exchanged between system components or component & user	Integrity
R	Repudiation - Attacker performs an action with the system or component that is not attributable	Non-repudiability
I	Information disclosure - Attacker is able to read the private data that the system is transmitting or storing	Confidentiality
D	Denial of service - An attacker can prevent the passengers or system components from accessing each other	Availability
E	Elevation of privilege - Gain elevated access to resources that are normally protected from an application or user	Autorisation

Identifying Threats Using Stride

Element	Description	Security Property
S	Spoofing	Authentication
T	Tampering	Integrity
R	Repudiation	Non-repudiability
I	Information disclosure	Confidentiality
D	Denial of service	Availability
E	Elevation of privilege	Autorisation

How to identify threats using stride

- At all levels: networks, devices… ask how each of the attack forms might occur
- Record your assumptions too, how might they be broken?
- Detailed designs create additional attack surface
- Assess them
- Build in defences
- Security controls
- Security is an “arms race”: defences create their own attack surfaces

How do you know what could go wrong?

- Think like an attacker?

  May be hard. Can you think like a professional chef?

  Implies making assumptions which may prove incorrect

  Implies knowing motivation

- Or can we do it systematically, not requiring a single brilliant guru?

Trust Boundaries

- Everywhere where trust assumptions change
- Between principals
- Do all subsystems trust each other?
- Is there a network involved?
- Semi-permeable: firewalls, air gaps, policies, access control (hard!)

Security shouldn’t be an afterthought

(but it is… most of the time!)

Finding out problems afterwards, harder to fix

- Static check of code – line by line
- Pen testing – takes time
- Await bug reports – what about the current system state?

Rather:

- Describe system to be built (in complete detail)
- What could possibly go wrong/ be attacked? (map all attack surfaces)
- What defences to include (SPoF? Defence in Depth, think outside the box)
- Iterate and evaluate

Threat Modelling and Attack Trees

Threat Modelling

- Security doesn’t have meaning unless you know specifics
    - Secure from who?
    - Secure for how long?
- We need a way to model threats against our secure systems to help:-
    - Understand the many ways in which a system can be attacked
    - Understand who the attackers are as well as their abilities, motivations, and goals
    - To install proper countermeasures to deal with these threats

Threat Modeling Overview

- Vulnerabilities are unmitigated threats *Here’s our opportunity!*

• Threat modeling consists of Assets, Threats and Attacks • Assets are what you want to protect
• Threats live forever; they are the attacker’s goal
• Attacks are how an attacker can realize a threat
• Vulnerabilities are design or implementation errors that allow an attack to succeed
• Very hard to write secure solutions unless you understand your Assets, Threats and Attacks • If done right, provides more ROI than any other security activity

What is Threat Modeling?

•A powerful way to identify potential threats, visualize risk and understand the security of the software system

•Multi-disciplinary effort in which all team members think about and address threats •A way for architects to realize and mitigate design problems

•A road map for developer to write secure code

•A starting point to create robust security minded test plans

•The most reliable way to:

•Understand the security implications of system architecture •Find business-process and system-level security issues •Ensure you get the most impact for your security investment

Why Threat Model?

- Creates a common understanding amongst technical and management stakeholders
- Ensures design and code is written to protect critical assets •Allows organizations to:
- Make better decisions throughout development
- Prioritize security efforts according to true risk
- Understand your organization’s weaknesses
- Weigh security designs against functional design goals •Step into the mind of an attacker and identify attack vectors

A World *Without* Threat Modeling

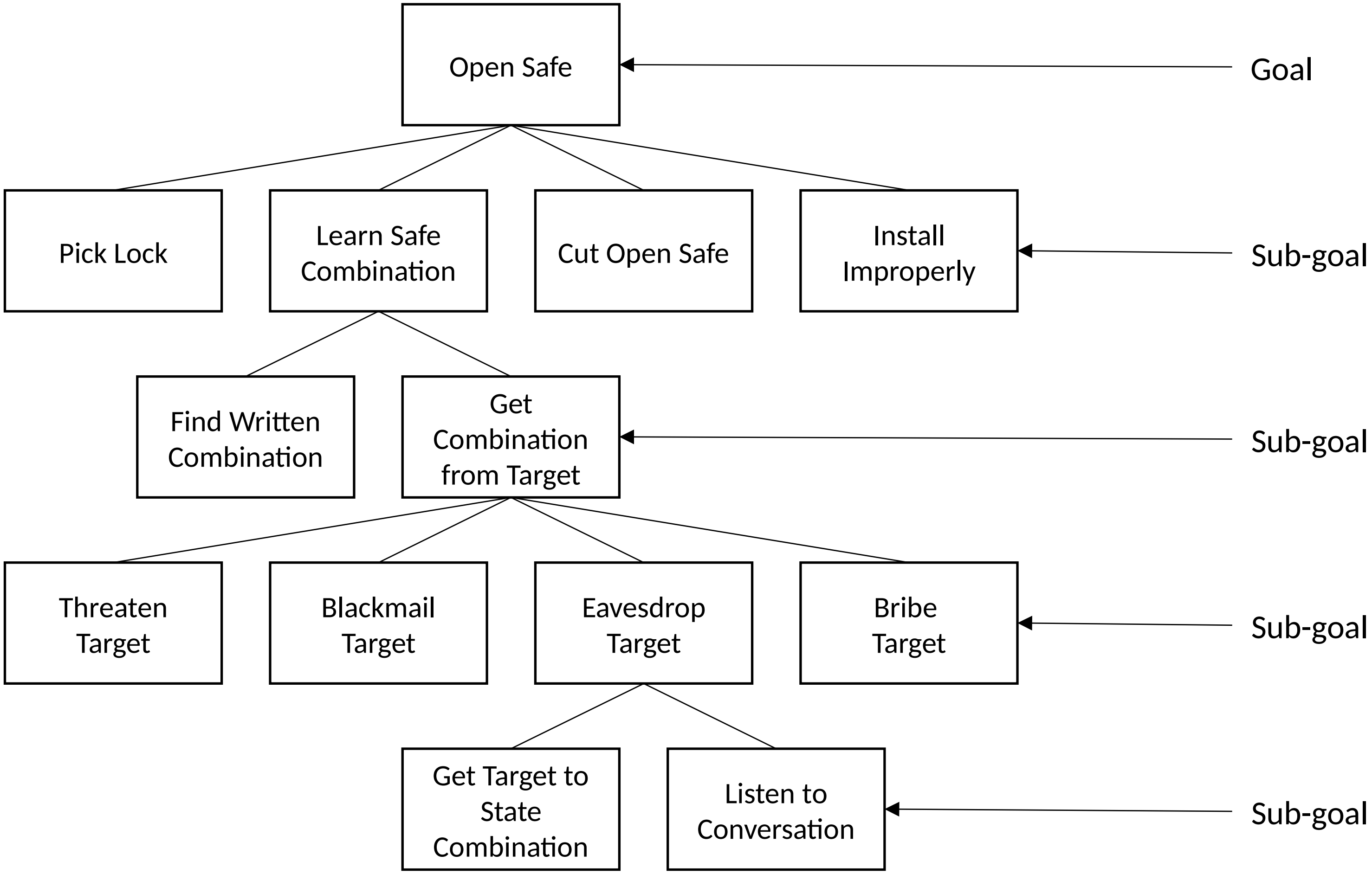
•Important assets are left unprotected •Many assets aren’t even identified
•Team doesn’t understand key threats to the system •Developers code defensively but leave gaps
•Mitigations are in place but they block the wrong attacks •Low risk areas are well protected, high risk areas left open •Testing is conducted with a one-size-fits-all solution
•Reliance on scanning tools and vendors with canned test plans

What a Threat Model Isn’t

- A representation of how an attacker approaches a system
- Represents system security, not an attacker model
- A test plan
- Test plans should be based on a TM, but a TM offers more than just test planning •A formal proof of system security
- This is not achievable on complex systems
- A design review
- Design review is the next level of action after the Threat Model is completed

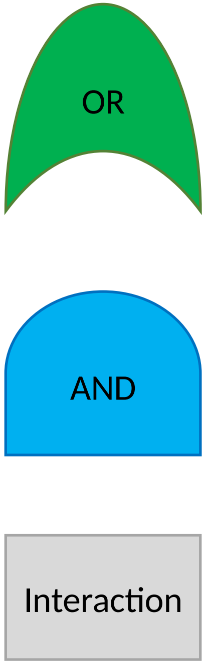
Attack Trees

- Provide a formal, methodical way of describing system security based on varying attacks
- We do this by representing an attack against a system in a tree like structure
- We start with the goal as the root node
- We list the different ways of achieving that goal as leaf nodes


Open Safe
Goal
Pick Lock
Learn Safe Combination
Cut Open Safe
Install Improperly
Sub-goal
Find Written Combination
Get Combination from Target
Sub-goal
Threaten Target
Blackmail Target
Eavesdrop Target
Bribe Target
Sub-goal
Get Target to State Combination
Listen to Conversation
Sub-goal

Attack Tree Nodes

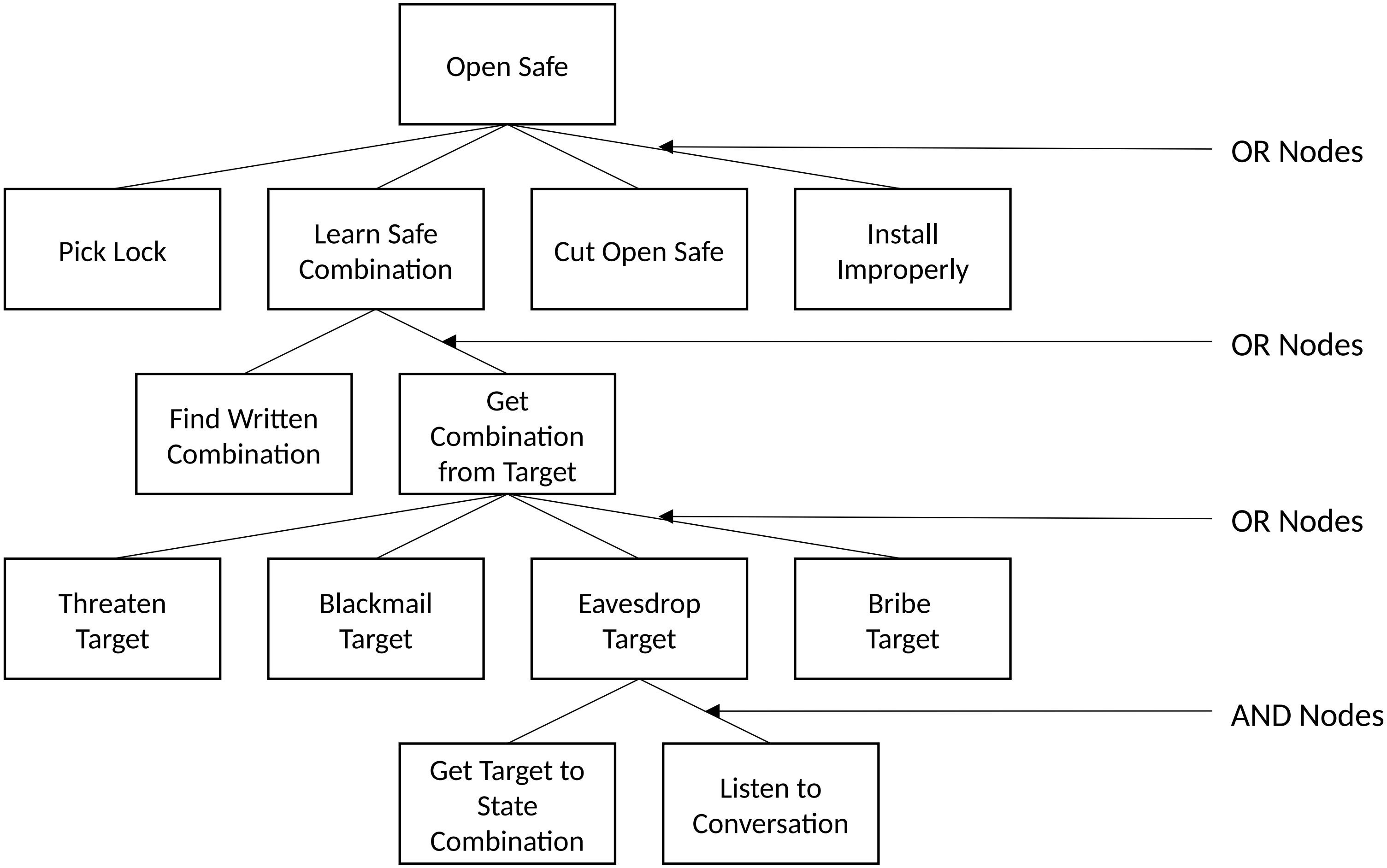
- Green nodes represent alternative ways in which the node can be realised (OR nodes)
- Blue nodes depict processes or procedures for accomplishing the node (AND)
- Grey rectangles are leaf nodes
  - Leaf nodes are the points of interaction between the adversary and the target



OR

AND

Interaction



Open Safe

Pick Lock

Learn Safe Combination

Cut Open Safe

Install Improperly

OR Nodes

Find Written Combination

Get Combination from Target

OR Nodes

Threaten Target

Blackmail Target

Eavesdrop Target

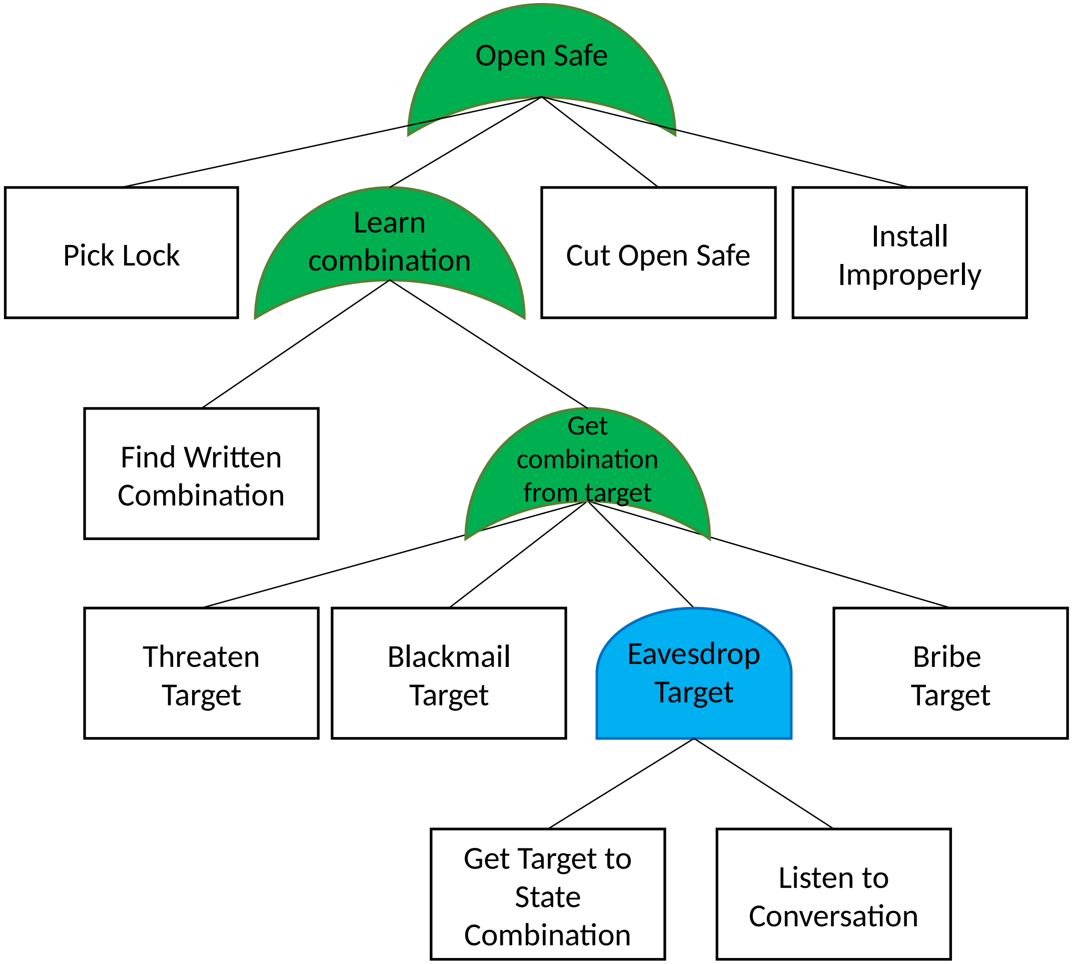
Bribe Target

OR Nodes

Get Target to State Combination

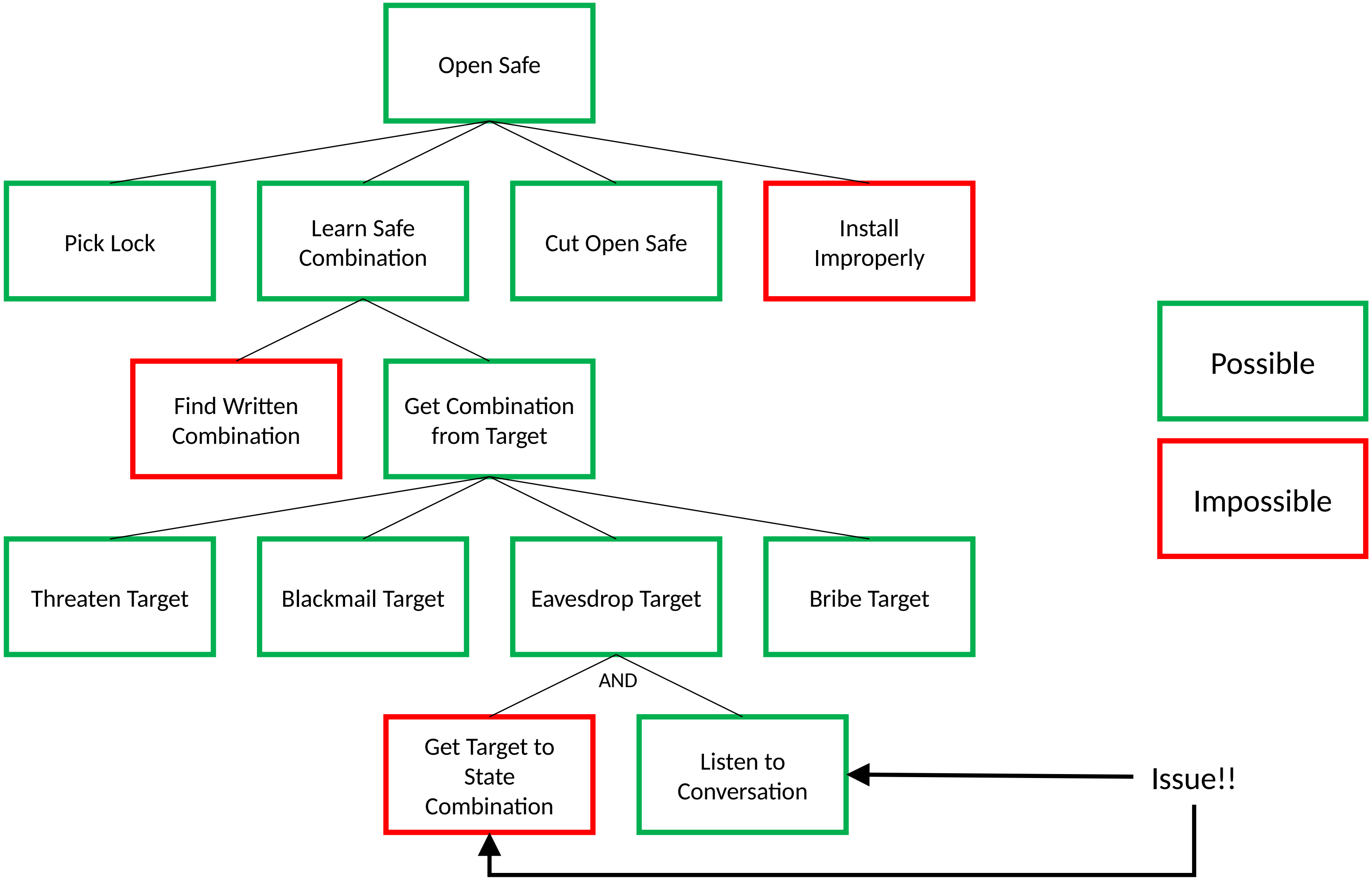
Listen to Conversation

AND Nodes


Open Safe
Pick Lock
Learn combination
Cut Open Safe
Install Improperly
Find Written Combination
Get combination from target
Threaten Target
Blackmail Target
Eavesdrop Target
Bribe Target
Get Target to State Combination
Listen to Conversation

Attack Tree Node Possibilities

- Assign possibility to leaf nodes
- Impossible – action cannot be accomplished under any circumstance
- Possible – action is possible depending upon other factors
- Assigning values depend on
  - Specific knowledge of target
  - General knowledge of target
- An OR node is possible if **ANY** of its leaf nodes are possible
- An OR node is impossible if **ALL** of its leaf node are impossible
- An AND node is possible only if **ALL** leaf node are possible
- An AND node is impossible only if **AT LEAST ONE** leaf node is impossible



Open Safe

Pick Lock

Learn Safe Combination

Cut Open Safe

Install Improperly

Find Written Combination

Get Combination from Target

Threaten Target

Blackmail Target

Eavesdrop Target

Bribe Target

AND

Get Target to State Combination

Listen to Conversation

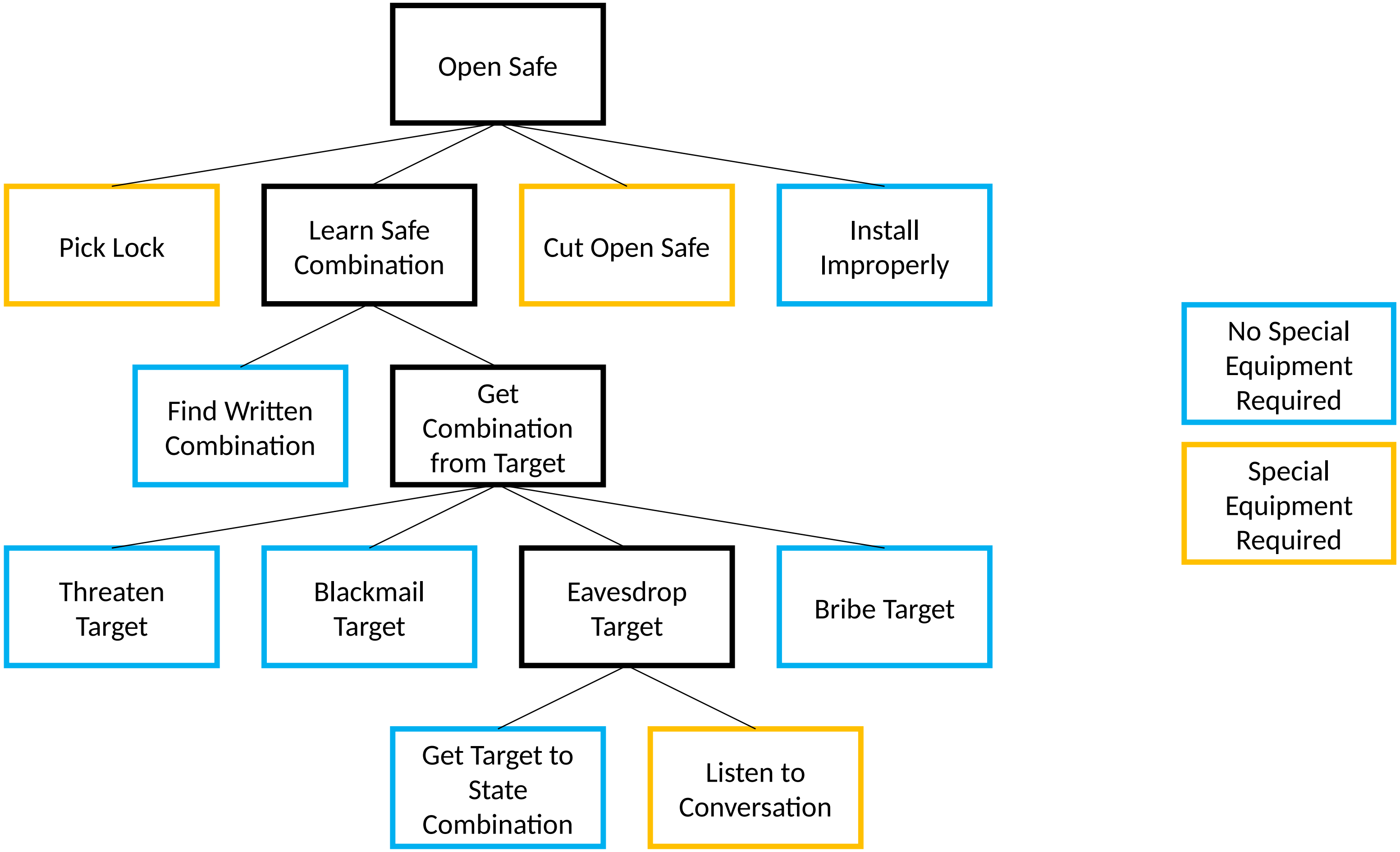
Issue!!

Possible

Impossible

Attack Tree Node Specialist Equipment

- Depending on the target and specific node determines if any special equipment is required
- Specialist equipment could include
  - Electronic Hardware
  - Software
  - Services
  - Specialist tools
- Specialist equipment will influence likelihood of attack as well as attack cost
- A stage requiring specialist equipment may make that stage impossible depending upon attackers resources



Open Safe

Pick Lock

Learn Safe Combination

Cut Open Safe

Install Improperly

Find Written Combination

Get Combination from Target

Threaten Target

Blackmail Target

Eavesdrop Target

Bribe Target

Get Target to State Combination

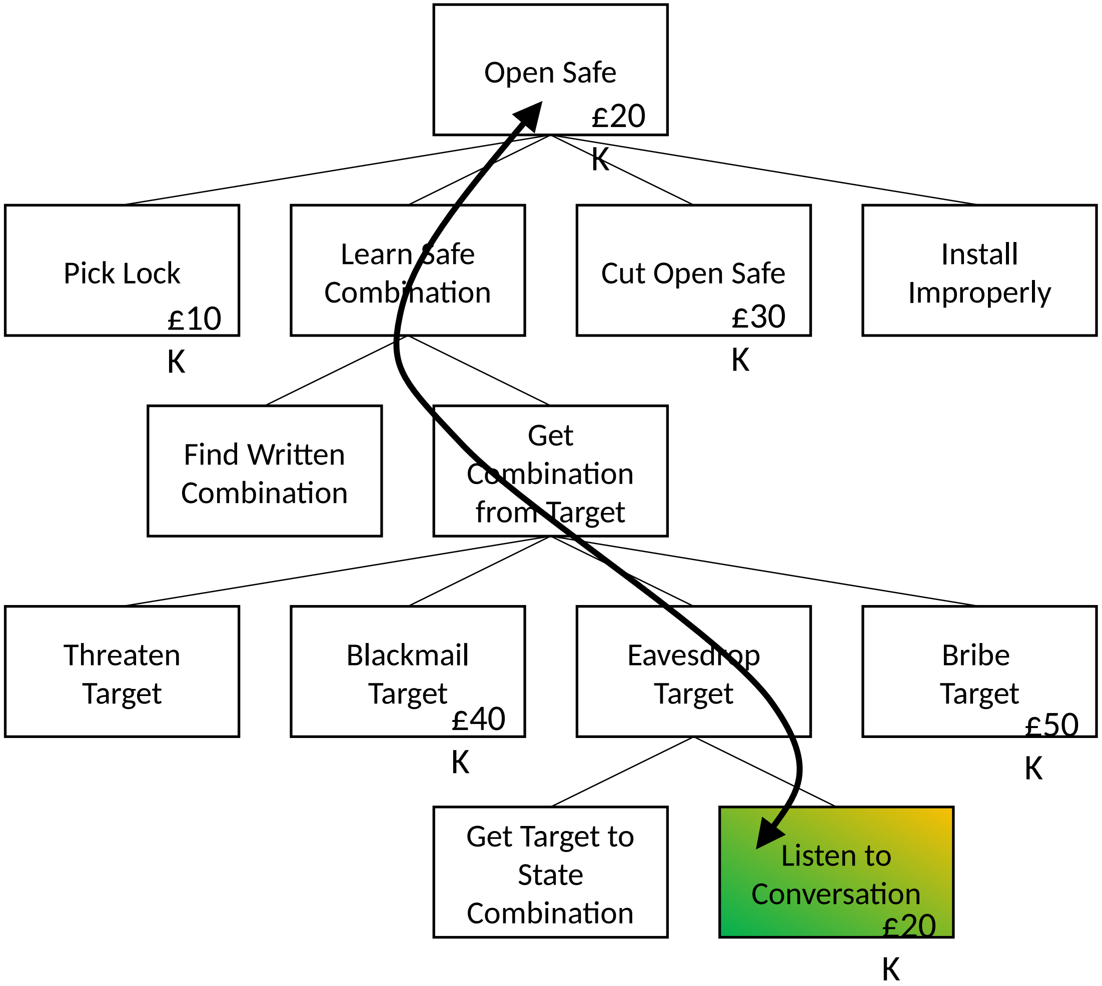
Listen to Conversation

No Special Equipment Required

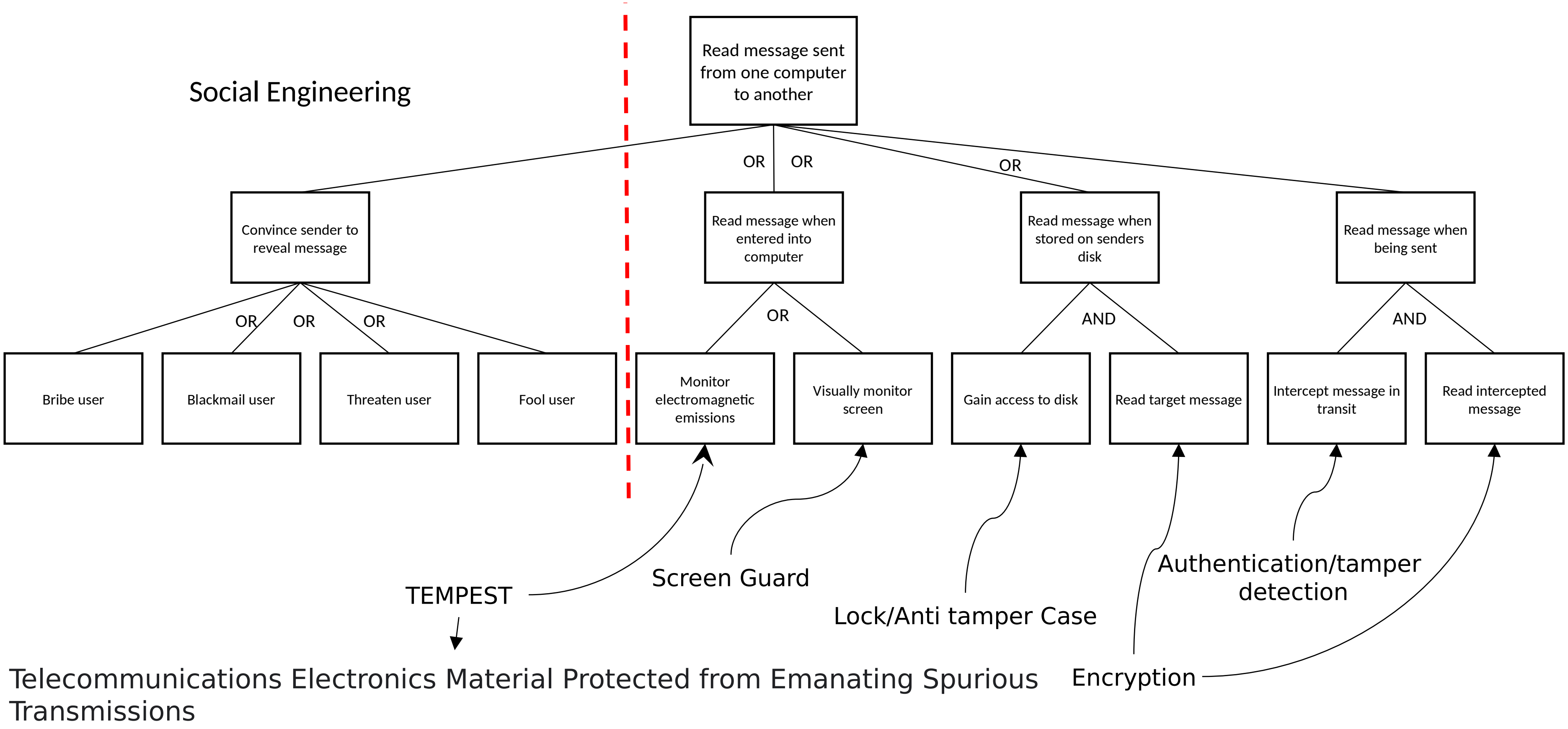
Special Equipment Required

Attack Tree Node Costs and Countermeasures

- Nodes will often vary in importance
- All attacks will have associated cost
- Assigning costs to nodes can determine the expense in that particular attack
- High costs may reduce the likelihood of an attack
- A low cost attack will thus increase the likelihood
- Countermeasures can be put in place to mitigate a potential attack
- Cost of attack can influence costs of countermeasures


Open Safe
£20 K
Pick Lock
£10 K
Learn Safe Combination
Cut Open Safe
£30 K
Install Improperly
Find Written Combination
Get Combination from Target
Threaten Target
Blackmail Target
£40 K
Eavesdrop Target
Bribe Target
£50 K
Get Target to State Combination
Listen to Conversation
£20 K

Attack Tree Example with Countermeasures



Social Engineering

Read message sent from one computer to another

OR

OR

OR

Convince sender to reveal message

Read message when entered into computer

Read message when stored on senders disk

Read message when being sent

OR

OR

OR

OR

AND

AND

Bribe user

Blackmail user

Threaten user

Fool user

Monitor electromagnetic emissions

Visually monitor screen

Gain access to disk

Read target message

Intercept message in transit

Read intercepted message

TEMPEST

Screen Guard

Lock/Anti tamper Case

Authentication/tamper detection

Encryption

Telecommunications Electronics Material Protected from Emanating Spurious Transmissions