Daniele Spagnulo

Risk Assessment for Security Economics

Workshop on Security Frameworks "Security Assurance“ – 16th December 2005

Dipartimento di Matematica ed Informatica Università di Catania

What is IT?

IT : Short for ***I****nformation* ***T****echnology,* and pronounced as separate letters, the broad subject concerned with all aspects of managing and processing information, especially within a large organization or company. Because computers are central to information management, computer departments within companies and universities are often called *IT departments.*

Business requirements: preserve IT Systems Data from damages involved in

1. Integrity = *Unauthorized People cannot modifiy System's Information;*
2. Availability = *System is always operative and functional;*
3. Privacy = *Unauthorized People cannot approach System's Information;*

We could reach this aim through...

Security Risk Analysis:

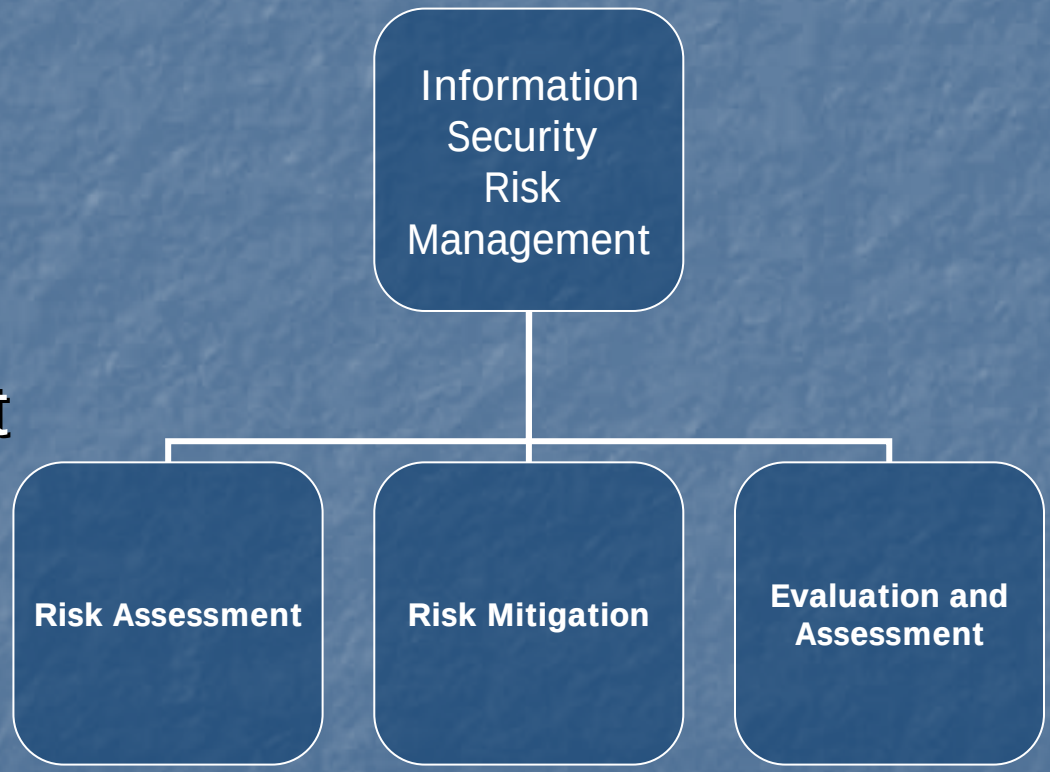
a process to ensure that the security controls for an IT system are fully commensurate with its risks.

Today's Main Topics...

- Information Security Risk Management;
- Risk Management Methodologies;
- Attack Trees, Vulnerability Trees, Fault Trees and Event Trees;
- Attack Scenery Analysis through Attack Trees ;

Information Security Risk Management

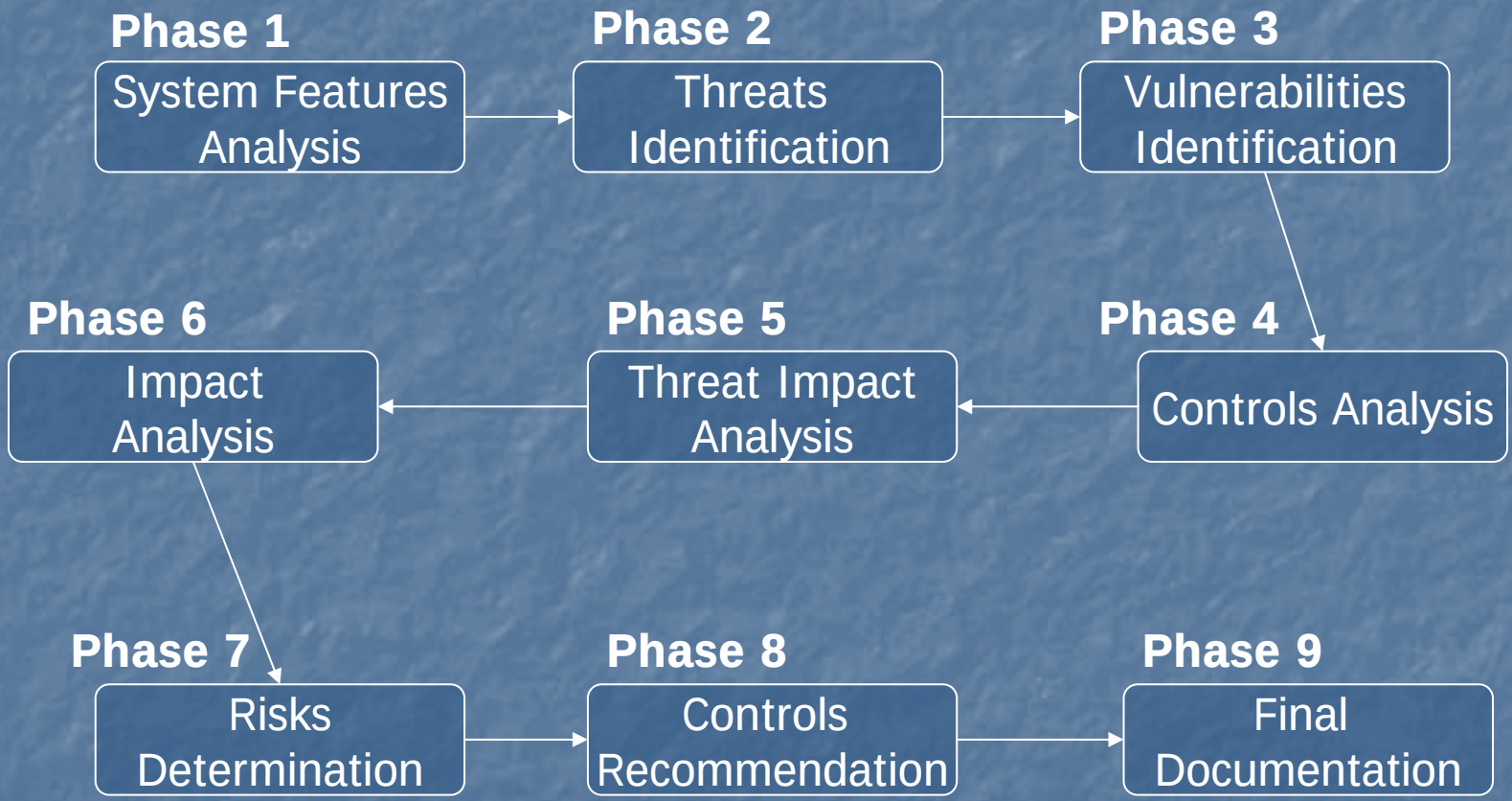
Aim: watching over business in order to identify IT risks and trying to managing them in order to cut down impact's consequences.



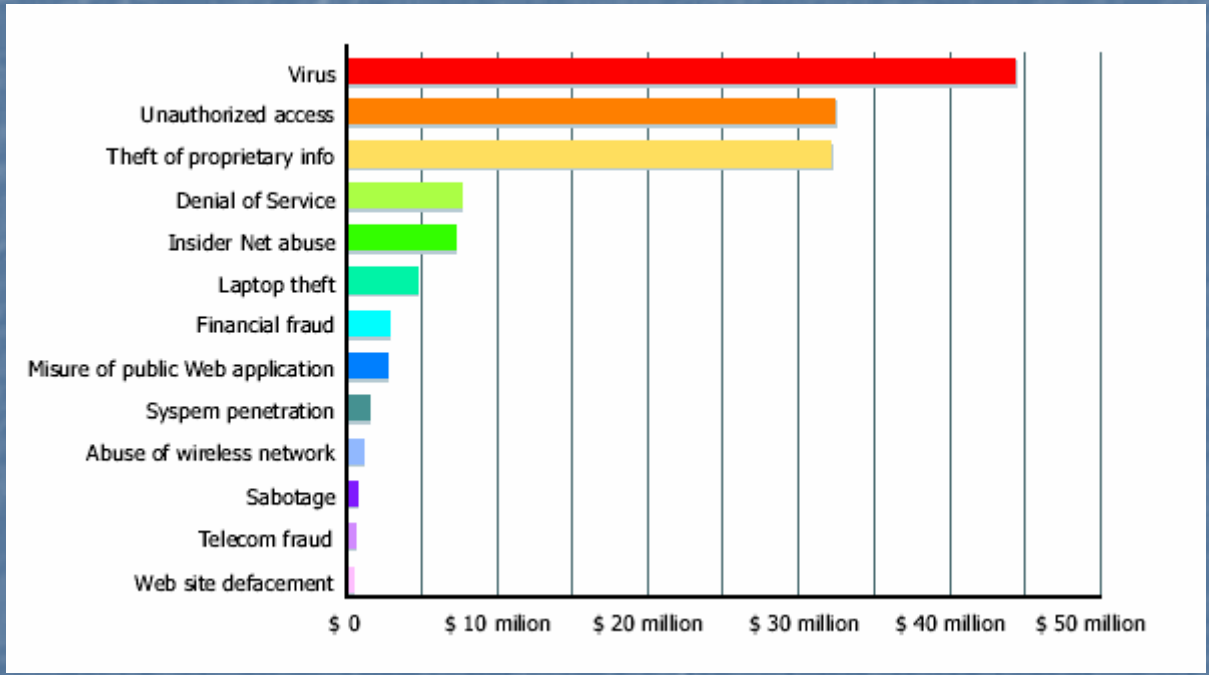
Risk Assessment

- Asset (def.): Any real or personal property, tangible or intangible, that a company or individual owns that can be given or assigned a monetary value. Intangible property includes things such as goodwill, proprietary information, and related property.

Risk Assessment



Risk Assessment: Sources of Threats



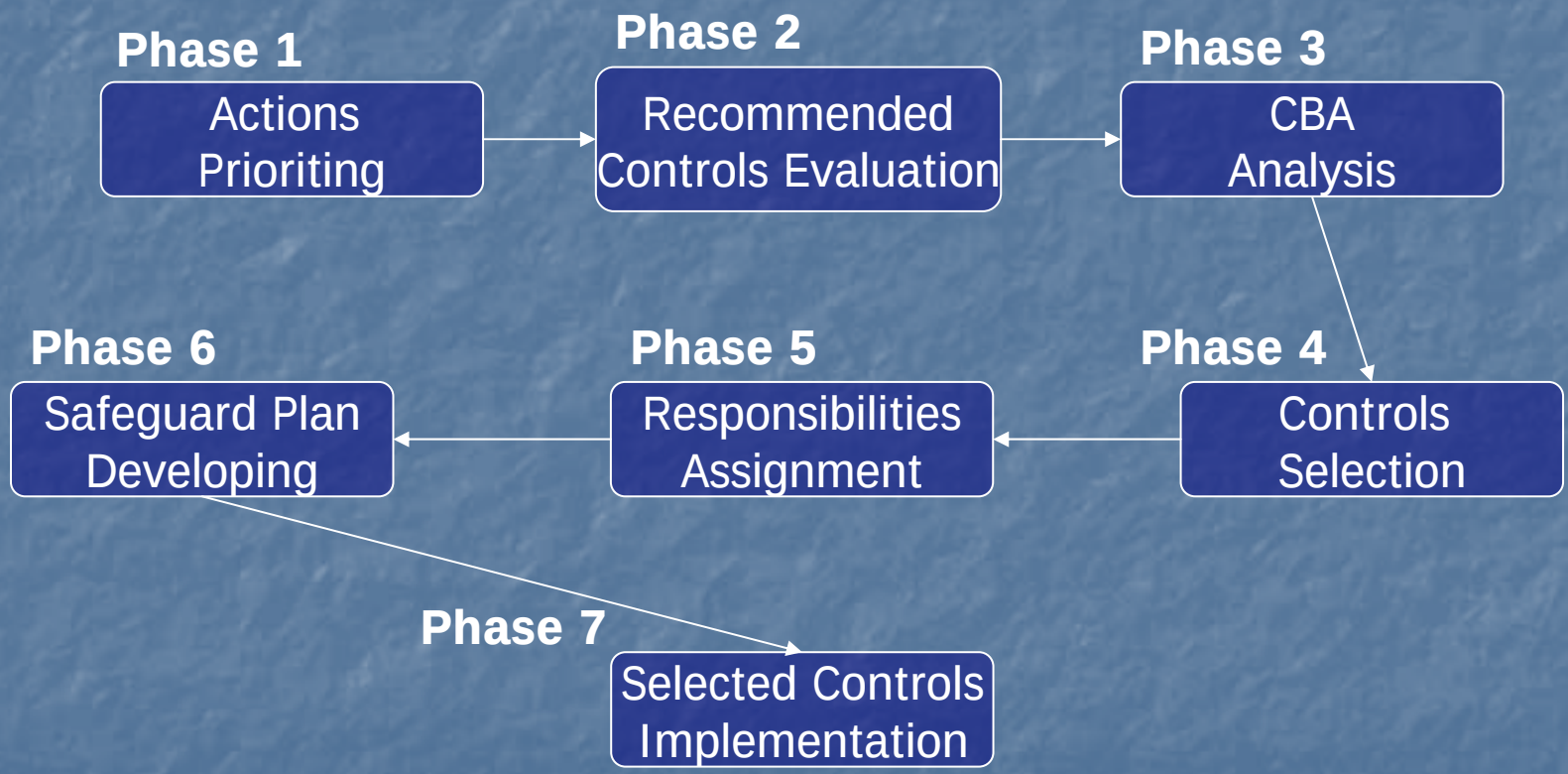
Risk Mitigation

(def.): *the process of evaluating and implementing recommended controls as a result of the previuous phase of Risk Assessment, giving necessary support to Management planning the budget and executing controls*

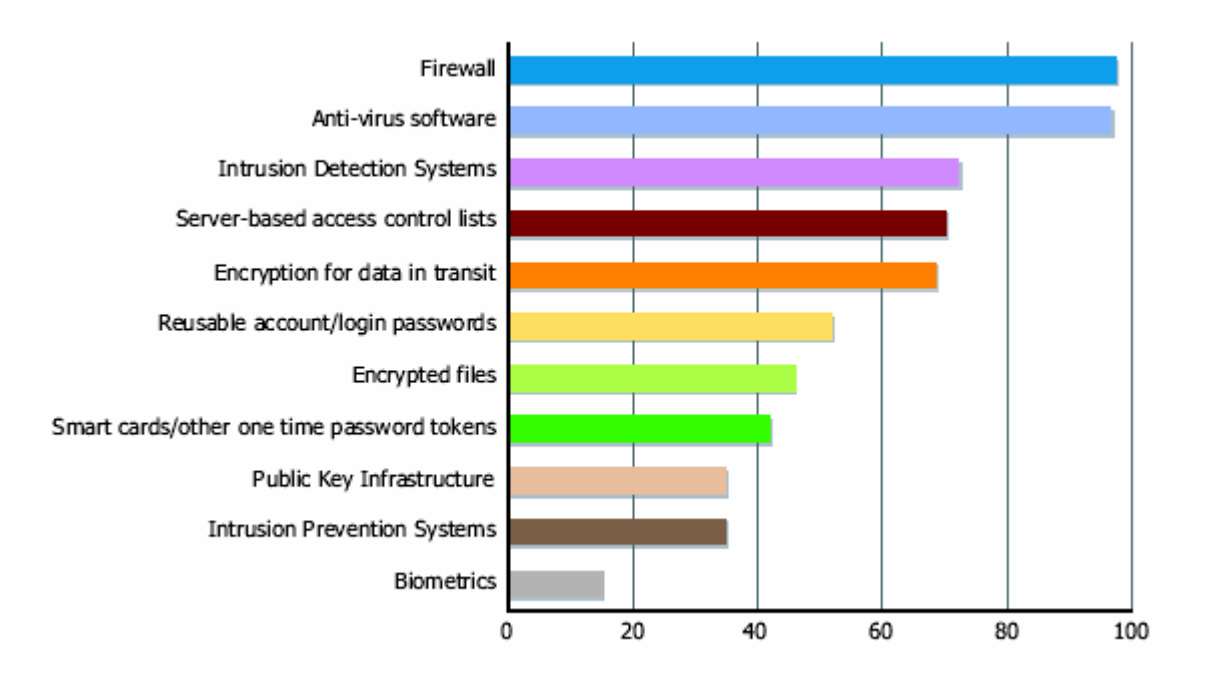
Risk mitigation possible strategies:

1. Risk Assumption;
2. Risk Elimination;
3. Risk Restriction;
4. Risk Planning;
5. Research And Comprehension;
6. Risk Transfer;

Risk Mitigation



Risk Mitigation: Most used Countermeasures



Risk Evaluation and Assessment

- IT Systems are often modified;
- System Conditions are changed;
- We need another Risk Assessment Process?...

NO!

We have just to evaluate periodically system risks in order to adapt necessary changes to applied countermeasures

Risk Management Methodologies

Three kind of approach:

- Qualitative ;
- Quantitative;
- Hybrid;

Qualitative Approach

- Simple and Flexible;
- No Technical Knowledge required;
- Use of Interviews to define value and risk run for each asset;
- Risk/Value → High,Medium,Low ;
- Useful tools: Risks Matrix

Final aim? → Outline possible attack sceneries

Quantitative Approach

- Numeric evaluation of assets;
- Technical Knowledge required;
- Use of indexes to define correct forecast inherent the system;
- Risk/Value → EF,SLE,ARO,ALE,ROSI,ROA, Cost/Benefits Analysis;

Final aim? → Outline possible attack sceneries

Quantitative Approach

- Exposure Factor (EF): The proportion of an asset's value that is likely to be destroyed by a particular risk, expressed as a percentage.
- Single Loss Expectancy (SLE): The Single Loss Expectancy (SLE) is the expected monetary loss every time a risk occurs. The Single Loss Expectancy, Asset Value (AV), and exposure factor (EF) are related by the formula:

$$SLE = AV * EF$$

Quantitative Approach

- Annualized Rate of Occurence (ARO): The probability that a risk will occur in a particular year.
- Annualized Loss Expectancy (ALE): The Annualized Loss Expectancy (ALE) is the expected monetary loss that can be expected for an asset due to a risk over a one year period. It is defined as:

  ALE = SLE * ARO

  where SLE is the Single Loss Expectancy and ARO is the Annualized Rate of Occurrence.

Quantitative Approach

asset	*asset* value	Threat	EF	SLE	ARO	ALE
Database	200.000 €	Virus	50%	100.000 €	0.65	65.000 €
File Server	12.000 €	Failure	100%	12.000 €	0.40	4.800 €
Product Plans	150.000 €	Disclosure	70%	105.000 €	0.65	68.250 €
Infrastructure	1.500.000 €	Fire	30%	450.000 €	0.10	45.000 €

Quantitative Approach

Costs/Benefits Analysis: It could be executed using three indexes

1. ALE (prior) : ALE before applying countermeasures;
2. ALE (post) : ALE with in force countermeasures;
3. Annualized Cost of Safeguard (ACS) : countermeasures total cost;

CBA = ALE (prior) – ALE (post) - ACS

Quantitative Approach

Return on Security Investment (ROI/ROSI): It's a gauge used to evaluate investment rendering and to compare other alternatives

ROI = CBA/ACS

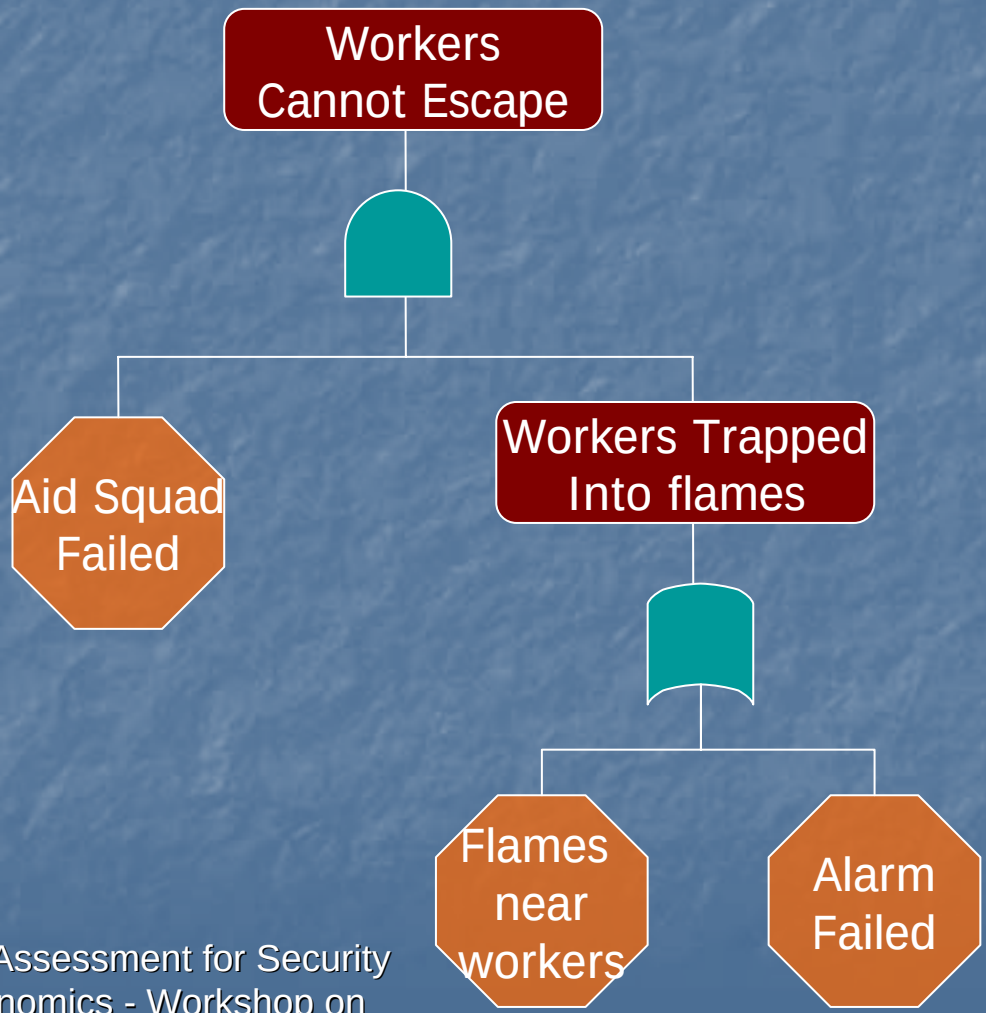
ROSI = (Risk Exposure * % Risk Mitigated) – SC/SC

Return on Attack (ROA): It's a gauge used from attackers to evaluate attacks' profit

ROA= gain from successful attack / cost before S + loss caused by S

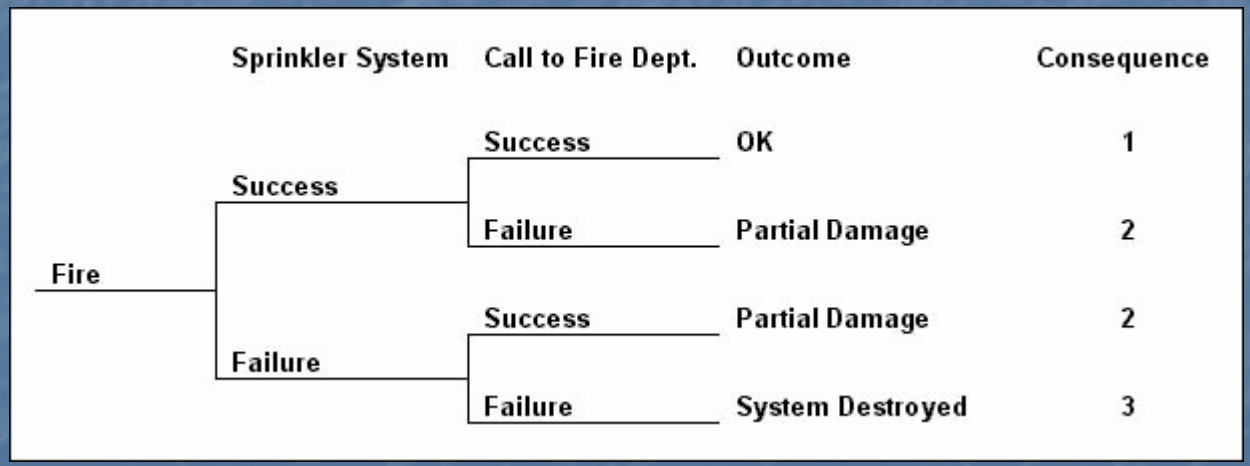
Fault Tree Analysis

fault tree analysis (a.k.a. fault analysis) offers the ability to focus on an event of importance, such as a highly critical safety issue, and work to minimize its occurrence or consequence. Fault tree analyses are performed using a top-down approach. The resulting fault tree diagram is a graphical representation of the chain of events in your system or process, built using events and logical gate configurations.



Event Trees

An event tree is a visual representation of all the events which can occur in a system. Event trees can be used to analyze systems in which all components are continuously operating, or for systems in which some or all of the components are in standby mode. The starting point (referred to as the initiating event) disrupts normal system operation. The event tree displays the sequences of events involving success and/or failure of the system components.

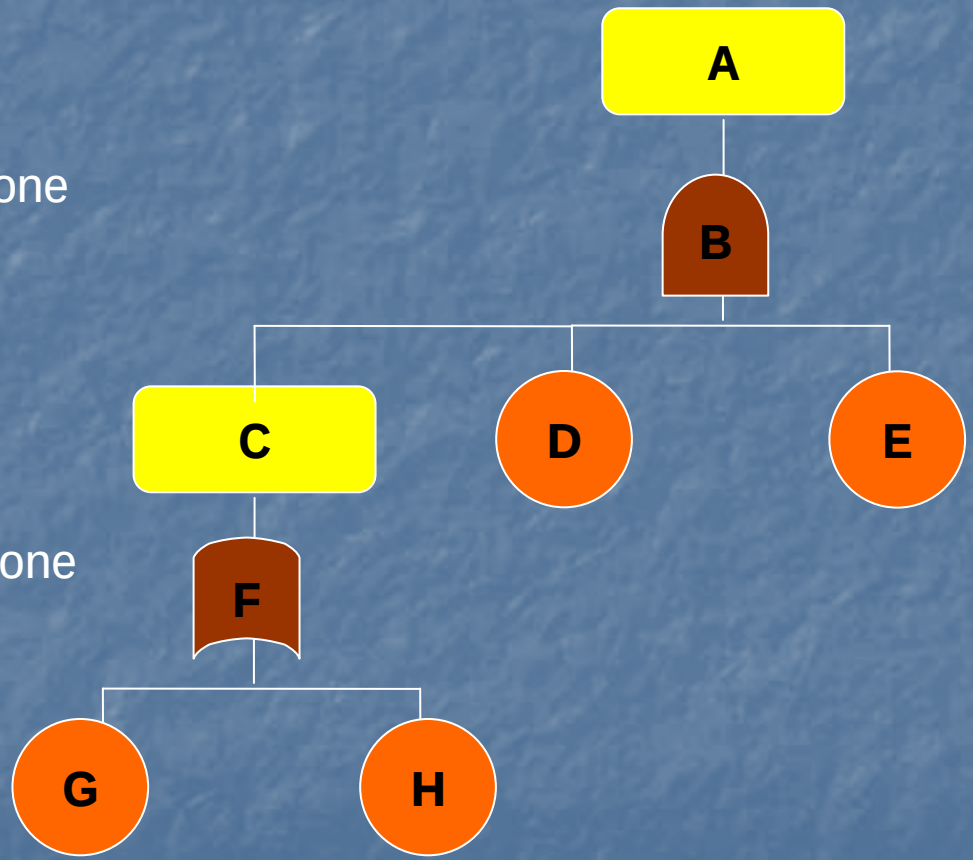


Vulnerability Trees

- Vulnerability trees are hierarchy trees constructed as a result of the relationship between one vulnerability and other vulnerabilities and/or steps;
- A threat agent has to carry out in order to reach the top of the tree;
- The top of the tree is known as the top vulnerability and we will symbolise it with a capital 'V'.
- There are a large number of ways that such a top vulnerability can be exploited. Each of these ways will constitute a branch of the tree.
- The branches will be constructed by child vulnerabilities.

"A" zone

"B" zone



Attack Trees

- Structured attack scenarios against a system organized in a tree structure;
- Root node represents a main goal, child nodes are subgoals that must be achieved to accomplish higher level goals;
- A given system is likely to have many attack trees associated with its operation; A set of attack trees is referred to as an attack forest;
- And/Or structure;

Attack Trees

Attack Trees

Attack Scenery Analysis

Analysing Sceneries Attack we'll follow these simple steps

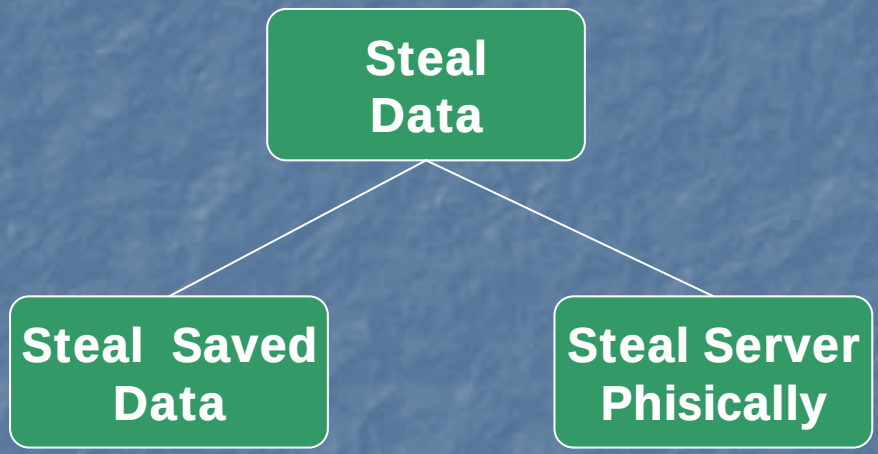
1. Attack Strategies Recognizing;
2. Countermeasures Recognizing;

While to examine various points of view analysing Attack Sceneries we'll folow these steps:

1. Attack Tree Labelling;
2. Countermeasures Labelling;

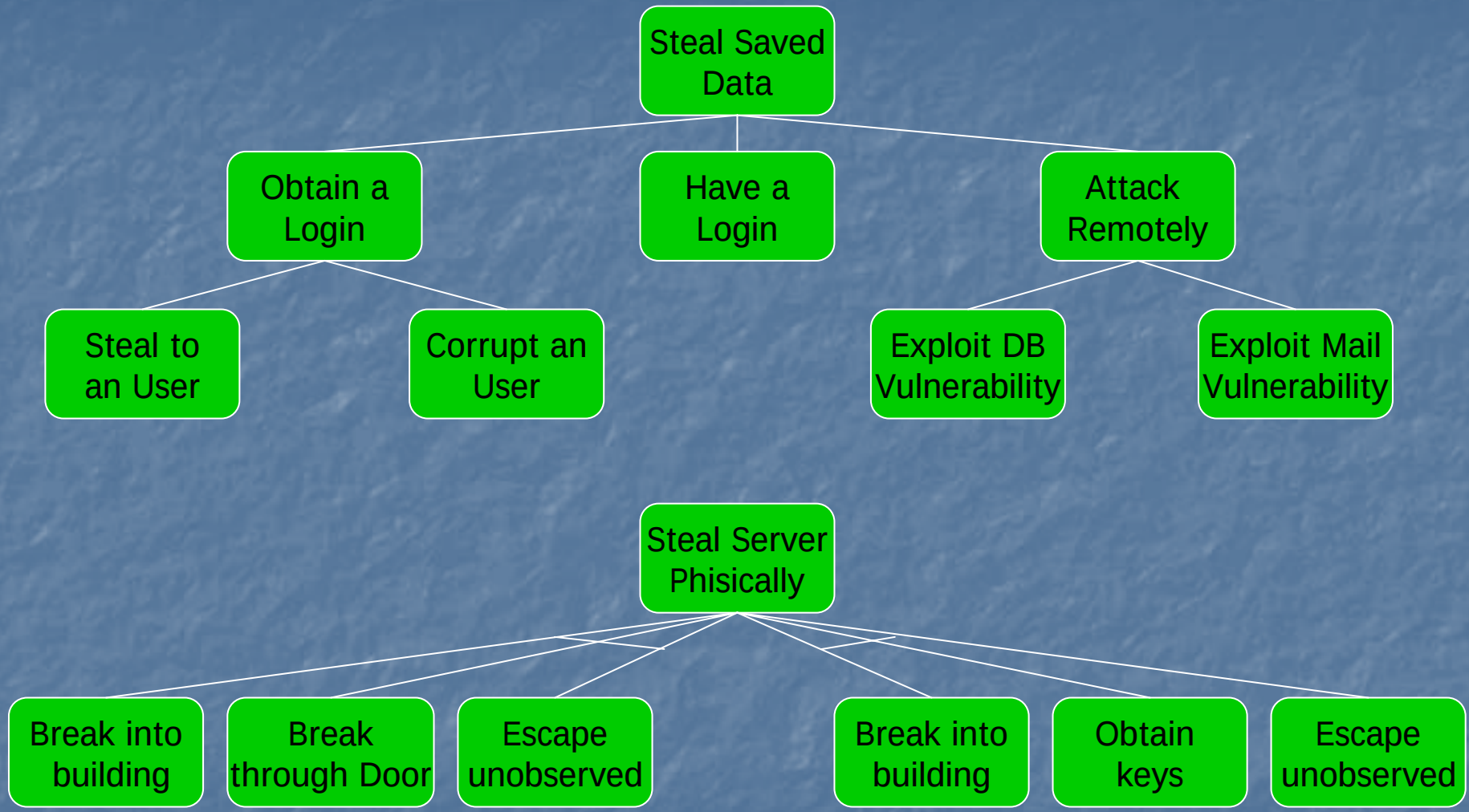
Attack Strategies Recognizing

Attacker's Aim: Steal data from a server

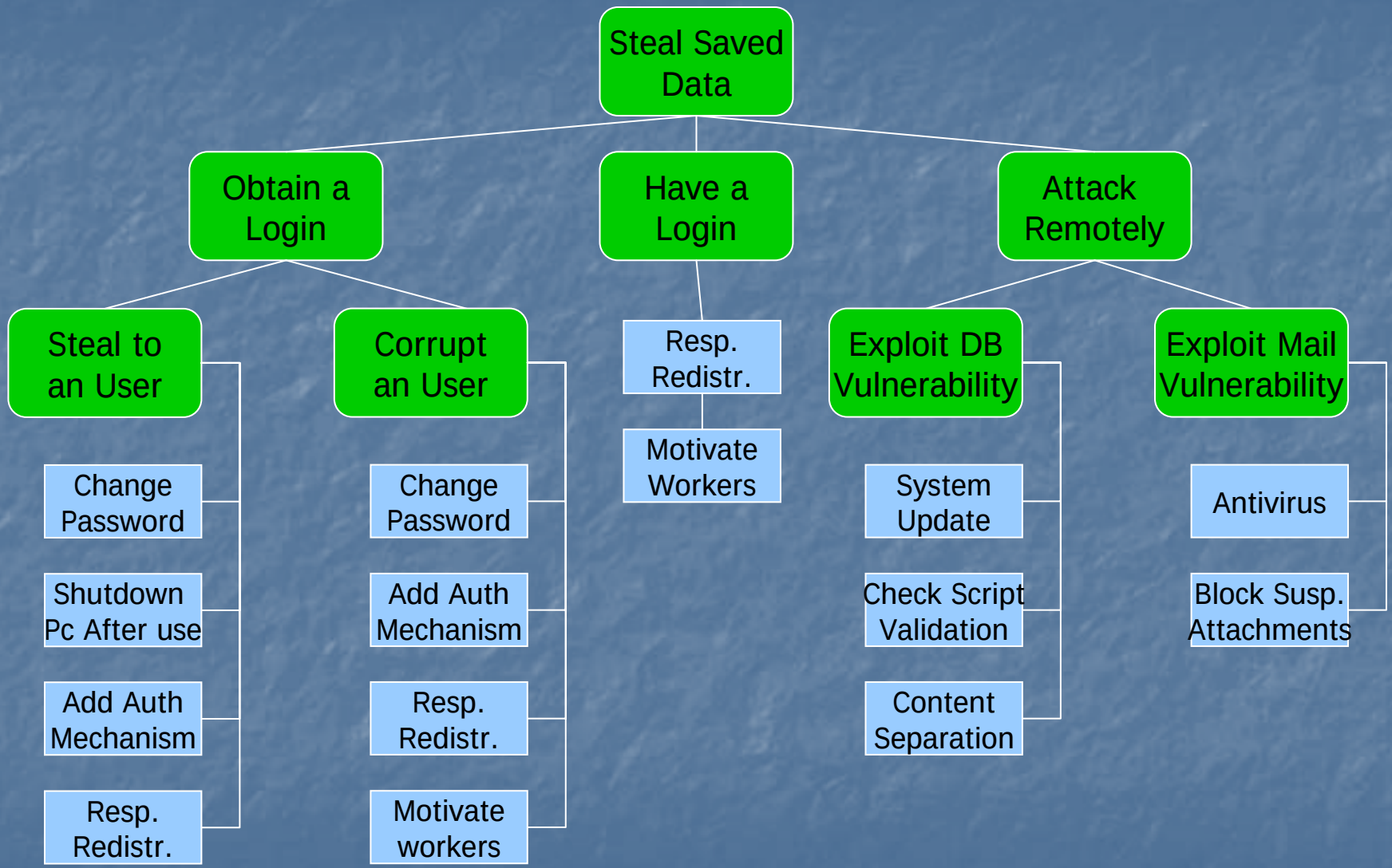


Let's develop separately these childs...

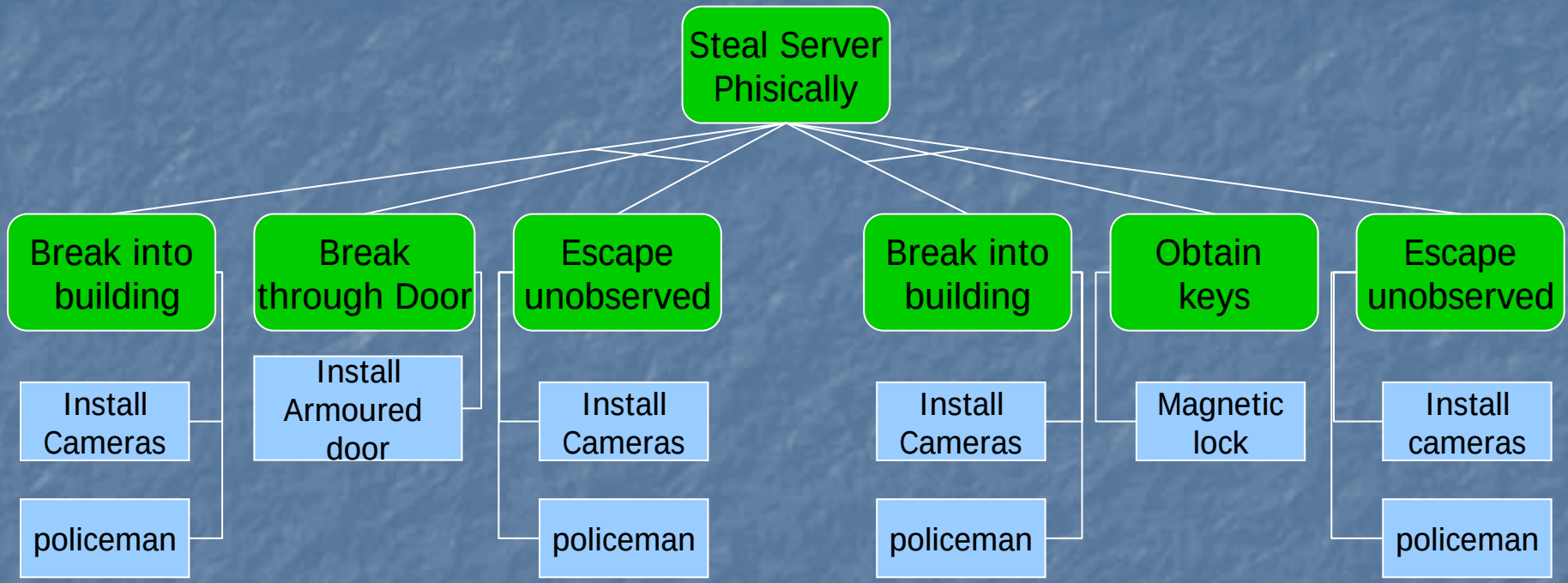
Attack Strategies Recognizing



Countermeasures Recognizing



Countermeasures Recognizing

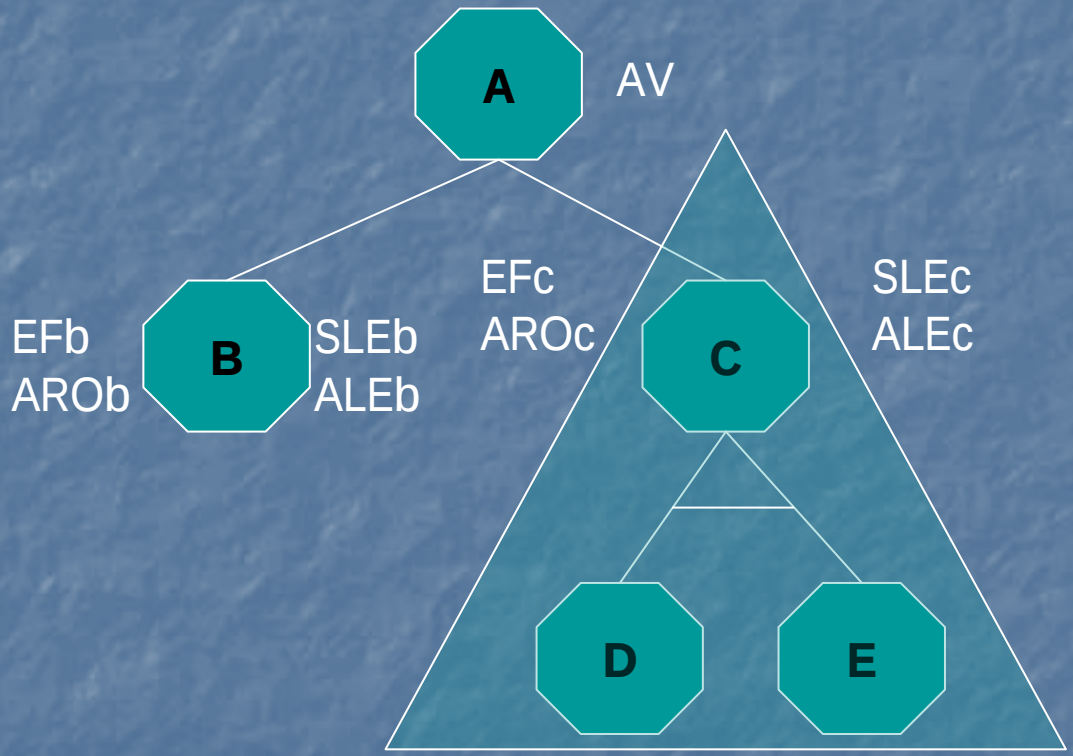


Business Point of View

Attack Tree Labelling:

1. Study tree in order to define best investments and to preserve assets;
2. Use of labels in order to evaluate tree in a quantitative way (AV,EF,ARO)
3. Attacks described by OR nodes: SLE and ALE calculations depends only on EF and ARO values involved in the node itself;
4. Attacks described by AND nodes: SLE and ALE calculations depends on EF and ARO values involved with the actions under the AND node;

Business Point of View



Business Point of View

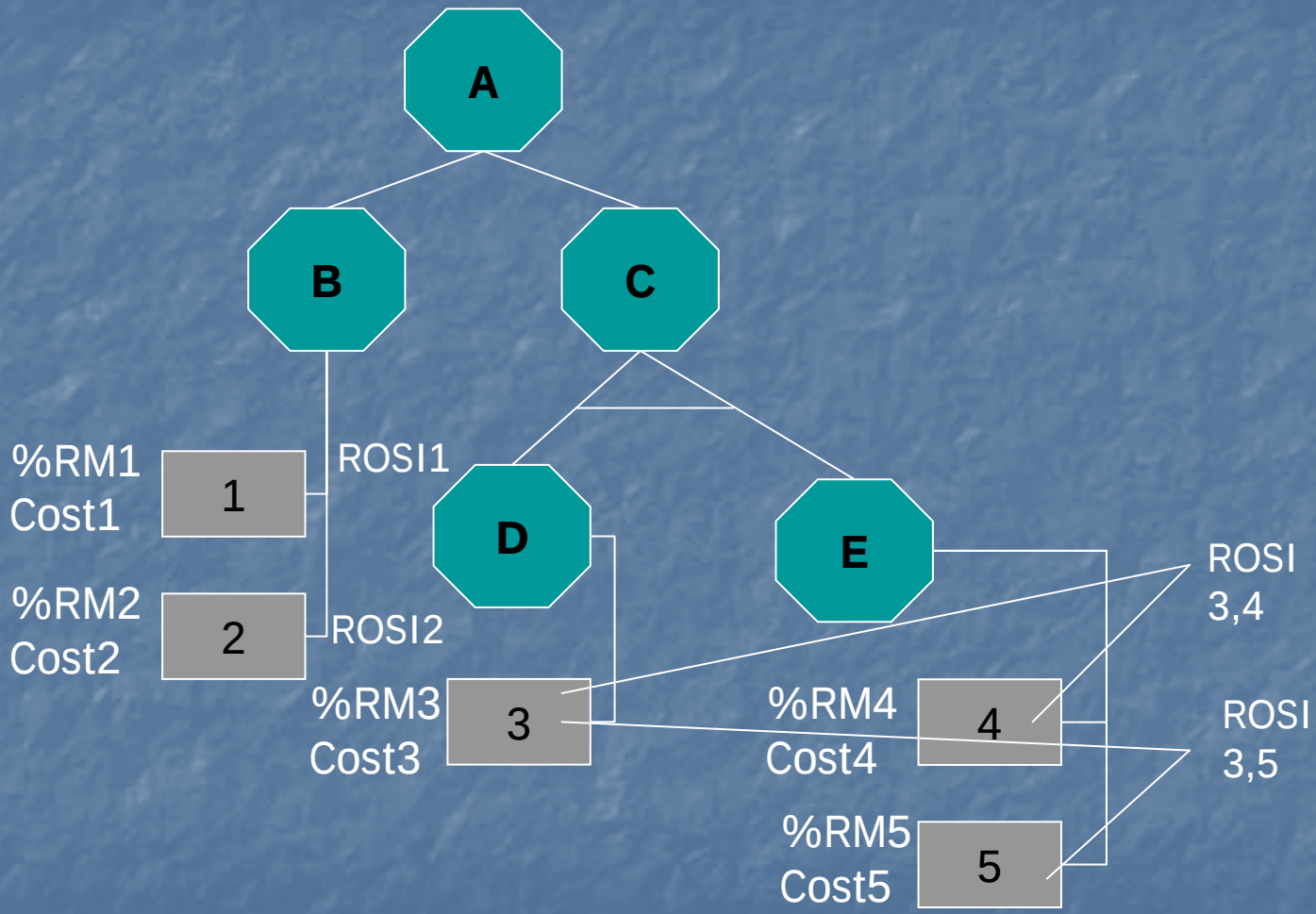
Attack	EF	ARO	SLE	ALE
Steal Data + Steal Root Perm.	100%	0,09	100.000€	9.000€
Steal Saved Data + Corrupt to gain Root Perm.	100%	0,09	100.000€	9.000€
Steal Saved Data + Root Perm.	100%	0,40	100.000€	40.000€
Steal Saved Data + Remote Attack (DB)	90%	0,08	90.000€	7.200€
Steal Saved Data + Remote Attack (DB)	85%	0,68	85.000€	57.800€

Business Point of View

Countermeasures Labelling:

1. Study tree in order to define best defense sceneries;
2. Use of labels in order to evaluate best countermeasures (% Risk Mitigated, Cost of Investment,ROSI);
3. Countermeasures described by OR nodes: ROSI is calculated for each countermeasure;
4. Countermeasures described by AND nodes: ROSI is calculated for each countermeasure's combination;

Business Point of View



Business Point of View

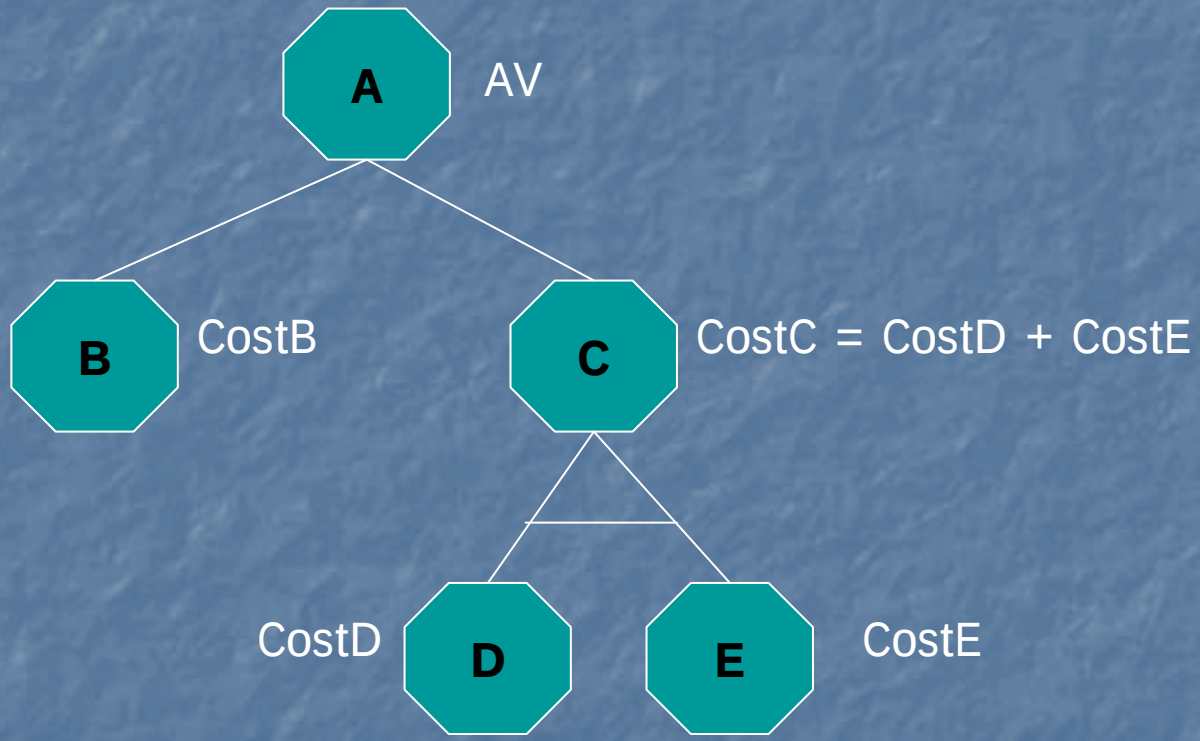
Countermeasure	ALE	%RM	Cost	ROSI
Change Password	9.000€	60%	500€	9,80
Shutdown Pc after use	9.000€	10%	100€	8,00
Responsibility Redistribution	40.000€	50%	15.000€	-0,70
System Update	7.200€	90%	2.500€	1,59
Antivirus	57.800€	80%	2.000€	22,10

Attacker Point of View

Attack Tree Labelling:

1. Study tree in order to define the expect profit gained from successful attacks;
2. Use of labels in order to evaluate Attack's cost (Gain,Cost)
3. Attacks described by OR nodes: Cost calculation depends only on Cost values involved in the node itself;
4. Attacks described by AND nodes: Cost calculation depends on Cost values involved with the composing nodes;

Attacker Point of View



Attacker Point of View

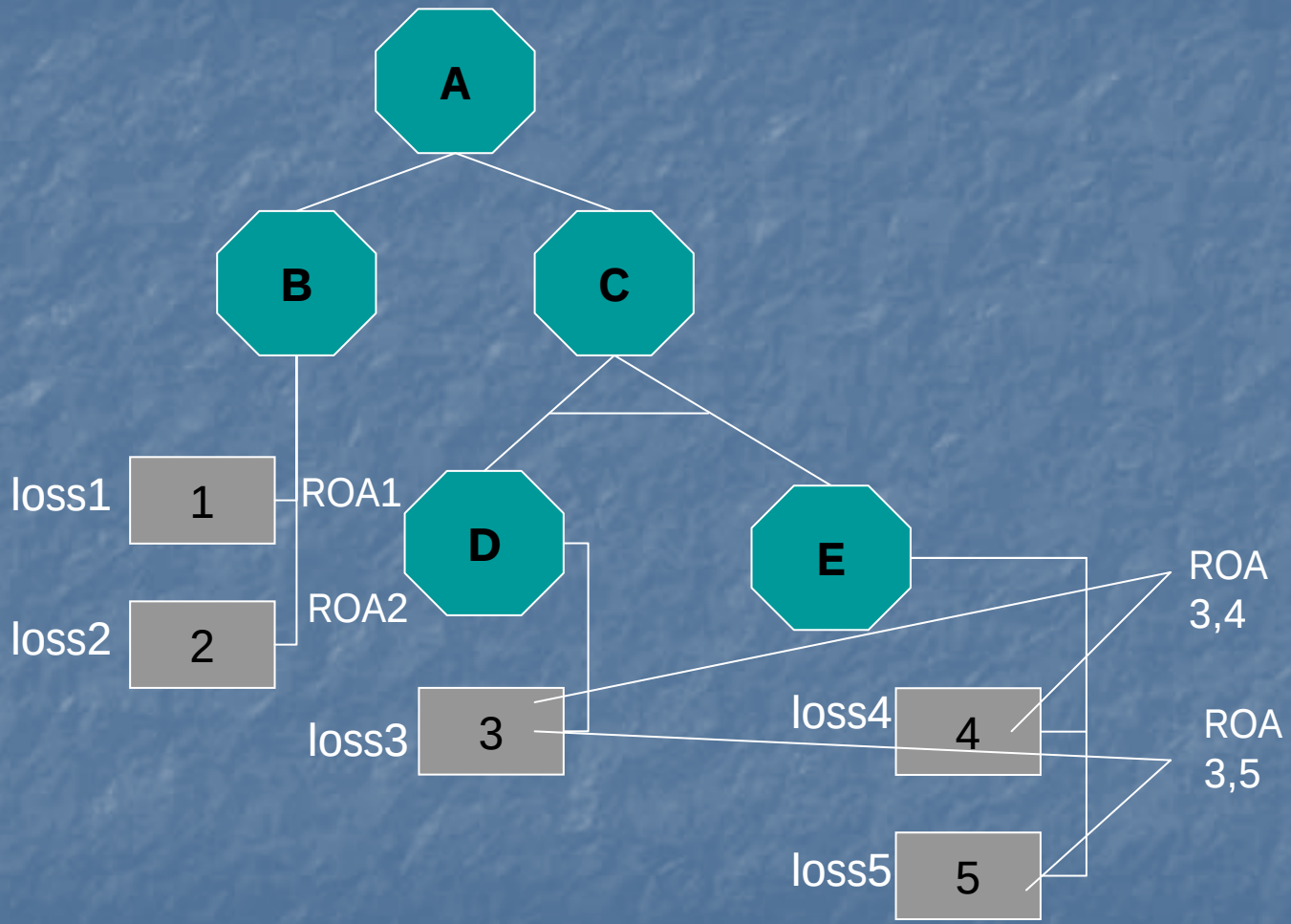
Attack	Cost
Steal Data + Steal Root Perm.	3.000€
Steal Saved Data + Corrupt to gain Root Perm.	10.000€
Steal Saved Data + Root Perm.	0€
Steal Saved Data + Remote Attack (DB)	2.000€
Steal Saved Data + Remote Attack (DB)	1.000€

Attacker Point of View

Countermeasures Labelling:

1. Study tree in order to define best attack strategies;
2. Use of labels in order to evaluate gain expected from a successful attack (loss,ROA);
3. Countermeasures described by OR nodes: ROA is calculated for each countermeasure;
4. Countermeasures described by AND nodes: ROA is calculated for each countermeasure's combination;

Attacker Point of View



Attacker Point of View

Countermeasure	Cost	Loss	ROA
Change Password	3.000€	1.000€	7,50
Add Authentication Mechanism	10.000€	1.500€	2,60
Responsibility Redistribution	0€	700€	42,85
System Update	2.000€	2.500€	6,67
Antivirus	1.000€	1.500€	12,00

Conclusions...

Possible future works:

1. Developing a new method involved with ARO evaluation;
2. Add a new index to ROA regarding a possible Attack Opposite Exposition;
3. Developing economical studies to underline the most exploited vulnerabilities;