Risk Analysis?

https://iuk.one/1033-1005

Clemens H. **Cap**
ORCID: 0000-0003-3958-6136

Department of Computer Science
University of **Rostock**
Rostock,Germany
clemens.cap@uni-rostock.de

Version 2

Overview

1. Perspectives of Risk Analysis
2. The Absolute Position
3. Mathematics of Risk Analysis
4. Psychology of Risk Analysis
5. Methods of Risk Analysis

1. Perspectives of Risk Analysis

What are the possible goals of a risk analysis?

Absolute Position

Definition of the Absolute Position

Something **must not** happen, at any price.

Evaluation:

- Usually an unrealistic expectation.
- Truly reasonable only in an extremely small number of cases.
- Example: Launch of Nuclear Weapons.

Rational Position

Definition of the Rational Position

Minimize the total costs of all your decisions.

Evaluation:

- Easier said than done.
- Faces numerous difficulties.

Pragmatic Position

Definition of the Pragmatic Position

Extremely expensive risks: Try to avoid them at any price.

Medium risks which are well understood are evaluated according to statistics.

Smaller risks may be taken.

Cost-of-the-attacker Position

Definition of the Cost-of-the-attacker Position

Security attempts to raise the costs for an attacker to a level rendering the attack unattractive or impossible.

Evaluation:

- Reasoning in the costs and capabilities of the attacker is very effective.
- **Problem 1:** Need to know the cost factors of the attacker.
- **Problem 2:** Works only against a rational attacker.

2. The Absolute Position

Only suitable for extreme risks.
However, such risks do exist.
Position can teach us a lot about risk management.

Example: Launch of Nuclear Weapons (1)

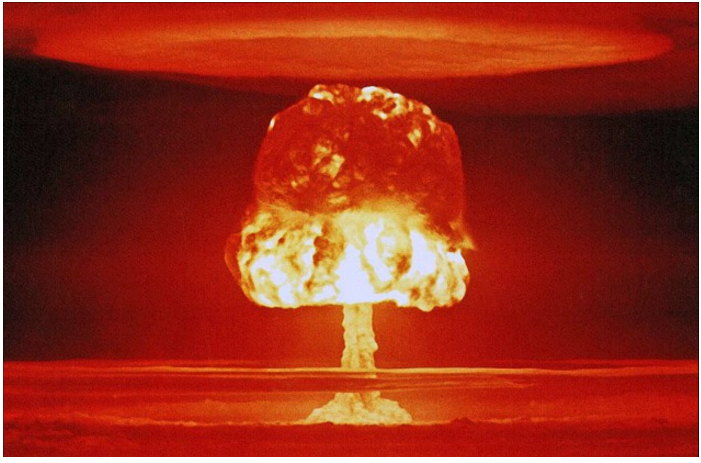

Fig. 1: Explosion of a Hydrogen Bomb © Rechtsnachweis siehe Anhang.

Example: Launch of Nuclear Weapons (2)

Solutions:

- Not much known about it.
- No real chance to authenticate the myths.
- Not the typical job assignment for Rostock alumni.

Evaluation: Problem is in fact unsolvable.

- **Aspect 1:** Distinction of intent and sanity of intent.
- **Aspect 2:** Human factor.

Distinction of Intent and Sanity of Intent (1)

Analysis:

- Security measures are concerned only with the identity of the president.
- It is very difficult to identify the sanity of an intent.

> *How can I know that an order I receive to launch my missiles came from a sane president.*
>
> Harold Hering, *1973. (Discharged from Air Force due to (t)his question)*

Distinction of Intent and Sanity of Intent (2)

Computers cannot distinguish intended from not-intended commands.

Warnings may only provide a hint as to the sanity of the intent.

```
hostname# cd /
hostname# cd /temp
sh: cd: /temp: No such file or directory
hostname# rm -rf *
.......
```

Src. 1: Terminal transcript, where intent is difficult to assess for a computer. However, a mild warning ("do you really want to delete all files of the root directory") might be in order.

Human Factor

Human mental capabilities sometimes do not measure up with the task.

Bill Clinton lost the nuclear codes for months.

Jimmy Carter sent the nuclear launch codes to the cleaner:

> *You do whatever you can and think you have an infallible system, but somehow someone always seems to find a way to screw it up.*
>
> *Statement on human factor in the nuclear launch codes by Henry Shelton, Chairman of the Joint Chiefs of Staff, in his autobiography.*

3. Mathematics of Risk Analysis

How would a mathematician approach a risk?

Cost Optimization

Look at the **total costs**:

- Costs D of all possible disasters plus
- Costs S of all security measures taken (includes security analysis).

To cope for **uncertainties:** Take the expectation value.

- Possible disasters: Weigh by degree of possibility p_i of cost C_i.
- Sum over all possible cases $i \in I$.

$$D = \sum_{i \in I} p_i \cdot C_i$$

Goal: Decide in a way to minimize the total costs $D + S$.

Problems of the Theory (1)

Problem 1: Practically, disaster probabilities are difficult to estimate.

- Eg: Probability of complete failure of Berlin power supply for more than 8 h?

Problem 2: Monetary valuation is difficult.

- Eg: What is the value in € of 10 dead people?

Problem 3: Risk expectation values are highly parameter sensitive to probability.

- We face a product of a
  1. very small number probability of a disaster
  2. very large number cost of that unlikely disaster
- If one factor is very large – what is the impact of an error in estimating the other?

Problems of the Theory (2)

Problem 4: Small probabilities are difficult to estimate.

- Eg: In 1 million cases we have 2 incidents
  and this is the only study we have on a rare phenomenon.
- What practical statement can be made on the probability?

Problem 5: Relative effects on small values are difficult to handle.

- Eg: An intervention changes 2 incidents out of 1 million to 1 incident out of 1 million.
- What can be said on the effectiveness of the intervention?

Example: Space Shuttle Risk Analysis

(1) According to management: 1:100.000
Method: Systematic evaluation and inclusion of every component.

(2) According to engineers: 1:50 to 1:200
Method: Guts feeling and estimations.

(3) According to Richard Feynman: 1:100
Method: Observe and think, when evaluating after first accident

(4) Reality: 2:135 = 1:67
Method: Evaluation after all flights had taken place.

Observe: The systematic method of the management produced an error of 3 orders of magnitude.

Task: Space Shuttle Risk Analysis

Calculate the expectation value of the costs of a space shuttle flight in $.

Use as costs the price of a space shuttle (web research), leaving aside the "costs" of astronaut lives.

Use as probability the different risk assessments of the previous slide.

Comment on the differences in the resulting costs.

Read the article on micromort.

Calculate the risk of taking part in one space shuttle flight in micromort and compare this with other dangerous activities. Comment again on the differences resulting from the assessments of the previous slide.

Task: A New Disease (1)

The year 2084 sees the new disease "Anorak".

It has a confirmed death risk of 1 in 1000 infected persons.

In the age group of Alice, the risk of an infection is 1 in 1000.

2097, company "Sinoca" produces a vaccine.

In 1 out of 2 cases the vaccine protects against an infection.

In a study on 1 million vaccinated persons in Northland, 2 persons die from "Rhombose".

In a study made in Northland in 2074 on 1 million people, 1 person died from "Rhombose".

In a study on 1 million vaccinated persons in Southland, 1 person dies from "Rhombose".

In a study made in Southland in 2071 on 1 million people, 2 persons died from "Rhombose".

In a study made in Southland in 2072 on 1 million people, no person died from "Rhombose".

Task: A New Disease (2)

All studies had exactly the same duration and further conditions such as age, health status etc.

No further facts are known.

Comment on the statement: The studies in Northland show that a vaccination raises the risk of death by "Rhombose" by 100%.

Comment on the statement: The studies in Southland show that a vaccination has no influence at all on the risk of death by "Rhombose".

Suppose Alice decides to get a vaccination.

- Estimate the risk that Alice dies from "Rhombose".
- Esitmate the risk that Alice dies from "Anorak".

Suppose Alice decides not to get a vaccination.

- Estimate the risk that Alice dies from "Rhombose".
- Estimate the risk that Alice dies from "Anorak".

Task: A New Disease (3)

Discuss the issues connected with small case numbers in risk scenarios!

Should Alice get a vaccination?

Comment on the methodical problems of the risk analysis.

Disclaimer:

- I am no medical doctor and I am not giving medical advice.
- The example and the provided numbers are completely fictional. They are presented only for illustrating some problems of practical risk analysis.
- The example reduces a very complex matter to an artificial, simplified textbook scenario.
- Medical decisions should not be made on the basis of simplified scenarios and require the consultation of a medical expert.
- In a community, decisions should also be based on the value of solidarity and not only on mathematical risk evaluations of a single individual.

4. Psychology of Risk Analysis

We understand why risk analysis is not so easy as the mathematicians of an insurance company claim it is.

Theoretical Result: Prospect Theory

According economic theory: Kahneman, Tversky: Prospect Theory: An analysis of decision under risk. Econometrica 47 (4), 263-291, doi: 10.2307/1914185. See: https://www.jstor.org/stable/1914185

Shorter: 🔗, W, W.

Important Result

Human beings are **not rationally** deciding agents
in the sense of maximizing benefits.

Example: Game of Balls in an Urn

Let's play a game of balls in an urn!

Rules of the game:

1. There are n balls in the urn.
2. **Exactly one** of the n balls is black.
3. You may draw one ball.
4. If you draw the black ball you get E euros.

Parameters of the game:

- Crucial question: What are n and E?

Example: Five Parameter Sets

	n	E
Game 1	1	1 million
Game 2	2	2 million
Game 3	10	10 million
Game 4	100	100 million
Game 5	1000	1 billion

Tab. 1: Five Parameter Sets for the Game.

Interpretation

- Game 1: You certainly become a millionaire. In **every** case! Cool!
- Game 2: In half of the cases you get nothing. Risky!
  In the other half you are double-millionaire. Double cool!
- Game 5: You win only in one out of 1.000 cases. Not so likely!
  But in this case you are billionaire. Crazy!!!

Example: Analysis of Five Parameter Sets

With regard to **expectation value**, all games are equal.
For each game: Expectation value of one round: 1 million €.

With regard to **probability**, there is a wide difference.

Compare:

- **Individual:** Only gets one or two shots at a game or risk.
- **Insurance company:** Plays game repeatedly.
- **Expectation values:** Are limits $\lim_{n\to\infty}$.

If you can repeat the games as often as you desire then all games are equal.

Example: Ask yourself!

If you are allowed to play only once:

- Which game would you play?
- Which game would Donald Trump play?

Ask yourself:

- What is one additional million for Trump?
- What is one additional million for you?

Explanation:

- Losses are felt more negatively than gains.
- Our sensitivity is logarithmic and not linear.
- For both facts, there are genetic reasons.

5. Methods of Risk Analysis

How can I do a systematic risk analysis?

Answer is always: Systematized, standardized checklists.

Basic Problem

Question: How would I know that I am aware of all possible attacks?

Solution:

- Find a semi-formal, systematic method which directs me to all possible weak spots.
- Evaluate the individual risks.
- Identify the most important ones and weight according to the taken perspective.

Important Approaches:

1. Threat Matrix
2. Attack Trees

This report of Carnegie Mellon University outlines 12 different methods!

Goal: Use a systematic method and a published standard / cook-book.

Threat Matrix

Two-dimensional analysis consisting of:

- **areas** which may get attacked (eg: components)
- **threats** which may be launched

Implementation:

- Areas as rows and threats as columns (or vice versa).
- In the intersection: Evaluation of likelihood and damage.
- May do quantitative or qualitative analysis.

Example: Threat Matrix

May be as small as:

Rows: Areas which may get attacked
Columns: Possible threats or attacks.

	Stolen	**Ransom Ware**
Laptop Computer	Small, 1.500 €	Small, 5.000 €
DSL-Modem	Small, 200€	Very small, 200€

Or as large as: https://www.usccu.us/documents/US-CCU Cyber-Security Matrix (Draft Version 2).pdf

Attack Trees

Tree:

- **Root:** Protection goal.
- **Node:** Intermediary goal in an attack.
  - **Conjunctive** node: All child goals must be reached by attacker.
  - **Disjunctive** node: At least one child goal must be reached by attacker.
- **Leaf:** Elementary step in an attack.
- **Path:** Detailed description of a particular attack variant.

Example: Threat Tree

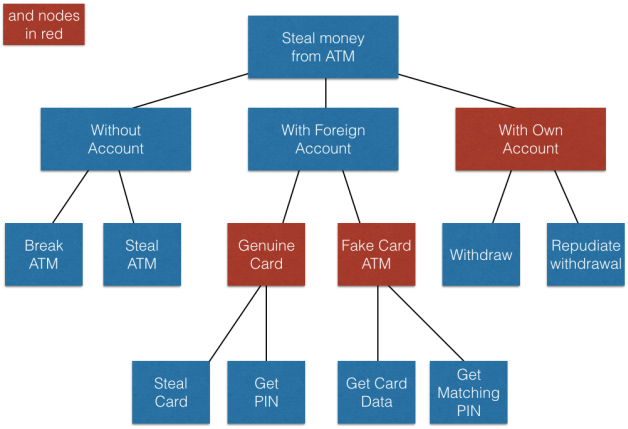

Fig. 2: Example of a threat tree for stealing money from an ATM

Example: Linearized Threat Tree

Linearized variant: Often the tree is too complex to be drawn.

- Then a textual, indented variant is used.

Steal money from ATM 1. Without Account
1.1 Break ATM
1.2 Steal ATM
2. With Foreign Account
2.1 With Genuine Card (AND Node)
2.1.1 Steal Card
2.1.2 Get PIN
2.2 With Fake Card (AND Node)
2.2.1 Get Card Data
2.2.1 Get Matching PIN
3. With Own Account (AND Node)
3.1 Withdraw
3.2 Repudiate withdrawal

Risk Evaluation in a Threat Tree

Risk Evaluation:

- Add attributes to the leafs.
- Use a metric, ordinal or nominal scale.

Mechanisms to **propagate risk** to the root node:

- **Leaf:** Direct evaluation of risk
- **And Nodes:** Risk of node is minimum of risk child nodes
- **Or Nodes:** Risk of node is maximum of risk of child nodes

Task: Attribute the ATM Threat Tree

Make assumptions on the linearized threat tree of the ATM scenario.

Provide attributes on the leafs.

Illustrate the propagation mechanism throughout the tree.

BSI IT-Grundschutz-Kompendium

BSI Bundesamt für Sicherheit in der Informationstechnik
German Federal Office for Information Security
https://www.bsi.bund.de/

- Has published the IT-Grundschutz-Handbuch (IT baseline protection)
- Standardized cook-book for IT security.
- Can be used as a systematic checklist.

Important parts:

- Struktur (structure)
- Elementare Gefährdungen (threats)
- Grundschutz-Bausteine (areas)

Note: There are also English versions of this document, but they are less up to date, less complete and less easy to be found.

Task

You are writing your Master thesis on the use of caches in multimedia data bases. You do simulations and write the document on your PC. The PC is located in your dormitory and is connected to the network of the university. You are worried about possible cyber security risks and conduct a threat analysis according to the BSI IT-Grundschutz-Kompendium.

Task 1: Which of the 47 threats ("elementare Gefährdungen") are important for you? Identify the five top-most risks. Why?

Task 2: Which areas ("IT-Grundschutz-Bausteine") are important for you? Why?

Task 3: Provide a short (2 page) risk analysis document for your use case!

Appendix

Contents of Appendix

List of Codes

List of Figures

List of Tables

List of Rights

Fig. 1 Source: https://commons.wikimedia.org/wiki/File:Castle_Romeo.jpg, as US government work it is in the public domain

Terms of Use (1)

Die hier angebotenen Inhalte unterliegen deutschem Urheberrecht. Inhalte Dritter werden unter Nennung der Rechtsgrundlage ihrer Nutzung und der geltenden Lizenzbestimmungen hier angeführt. Auf das Literaturverzeichnis wird verwiesen. Das Zitatrecht in dem für wissenschaftliche Werke üblichen Ausmaß wird beansprucht. Wenn Sie eine Urheberrechtsverletzung erkennen, so bitten wir um Hinweis an den auf der Titelseite genannten Autor und werden entsprechende Inhalte sofort entfernen oder fehlende Rechtsnennungen nachholen. Bei Produkt- und Firmennamen können Markenrechte Dritter bestehen. Verweise und Verlinkungen wurden zum Zeitpunkt des Setzens der Verweise überprüft; sie dienen der Information des Lesers. Der Autor macht sich die Inhalte, auch in der Form, wie sie zum Zeitpunkt des Setzens des Verweises vorlagen, nicht zu eigen und kann diese nicht laufend auf Veränderungen überprüfen.

Alle sonstigen, hier nicht angeführten Inhalte unterliegen dem Copyright des Autors, Prof. Dr. Clemens Cap, ©2020. Wenn Sie diese Inhalte nützlich finden, können Sie darauf verlinken oder sie zitieren. Jede weitere Verbreitung, Speicherung, Vervielfältigung oder sonstige Verwertung außerhalb der Grenzen des Urheberrechts bedarf der schriftlichen Zustimmung des Rechteinhabers. Dieses dient der Sicherung der Aktualität der Inhalte und soll dem Autor auch die Einhaltung urheberrechtlicher Einschränkungen wie beispielsweise Par 60a UrhG ermöglichen.

Die Bereitstellung der Inhalte erfolgt hier zur persönlichen Information des Lesers. Eine Haftung für mittelbare oder unmittelbare Schäden wird im maximal rechtlich zulässigen Ausmaß ausgeschlossen, mit Ausnahme von Vorsatz und grober Fahrlässigkeit. Eine Garantie für den Fortbestand dieses Informationsangebots wird nicht gegeben.

Die Anfertigung einer persönlichen Sicherungskopie für die private, nicht gewerbliche und nicht öffentliche Nutzung ist zulässig, sofern sie nicht von einer offensichtlich rechtswidrig hergestellten oder zugänglich gemachten Vorlage stammt.

Use of Logos and Trademark Symbols: The logos and trademark symbols used here are the property of their respective owners. The YouTube logo is used according to brand request 2-9753000030769 granted on November 30, 2020. The GitHub logo is property of GitHub Inc. and is used in accordance to the GitHub logo usage conditions https://github.com/logos to link to a GitHub account. The Tweedback logo is property of Tweedback GmbH and here is used in accordance to a cooperation contract.

Terms of Use (2)

Disclaimer: Die sich immer wieder ändernde Rechtslage für digitale Urheberrechte erzeugt für mich ein nicht unerhebliches Risiko bei der Einbindung von Materialien, deren Status ich nicht oder nur mit unverhältnismäßig hohem Aufwand abklären kann. Ebenso kann ich den Rechteinhabern nicht auf sinnvolle oder einfache Weise ein Honorar zukommen lassen, obwohl ich – und in letzter Konsequenz Sie als Leser – ihre Leistungen nutzen.

Daher binde ich gelegentlich Inhalte nur als Link und nicht durch Framing ein. Lt EuGH Urteil 13.02.2014, C-466/12 ist das unbedenklich, da die benutzten Links ohne Umgehung technischer Sperren auf im Internet frei verfügbare Inhalte verweisen.

Wenn Sie diese Rechtslage stört, dann setzen Sie sich für eine Modernisierung des völlig veralteten Vergütungssystems für urheberrechtliche Leistungen ein. Bis dahin klicken Sie bitte auf die angegebenen Links und denken Sie darüber nach, warum wir keine für das digitale Zeitalter sinnvoll angepaßte Vergütungssysteme digital erbrachter Leistungen haben.

Zu Risiken und Nebenwirkungen fragen Sie Ihren Rechtsanwalt oder Gesetzgeber.

Weitere Hinweise finden Sie im Netz hier und hier oder hier.

Citing This Document

If you use contents from this document or want to cite it,
please do so in the following manner:

Clemens H. Cap: Risk Analysis?. Electronic document. https://iuk.one/1033-1005 1. 5. 2021.

Bibtex Information: https://iuk.one/1033-1005.bib

```
@misc{doc:1033-1005,
   author       = {Clemens H. Cap},
   title        = {Risk Analysis?},
   year         = {2021},
   month        = {5},
   howpublished = {Electronic document},
   url          = {https://iuk.one/1033-1005}
}
```

Typographic Information:
Typeset on May 1, 2021
This is pdfTeX, Version 3.14159265-2.6-1.40.21 (TeX Live 2020) kpathsea version 6.3.2
This is pgf in version 3.1.5b
This is preamble-slides.tex myFormat©C.H.Cap

List of Slides

Legend:
continuation slide
slide without title header
image slide