Security as a Game

Decisions under uncertainty in risk management

Stefan Rass
Associate Professor @ Alpen-Adria Universität Klagenfurt
Institute of Applied Informatics – System Security
stefan.rass@aau.at

Keynote @ NetWare 2018

Motivation 1

- IT security - often a dilemma
  - Ideal case: Security mechanisms work transparently (unnoticed)
  - Worst Case: noticeable damage due to absence or failure of security measures

  In any case: only damage is perceived, no "noticeable" benefit

Security is like an immune system (and just as important)

- This raises a variety of problems/questions:
  - "Why more safety? Everything's going well right now!"
  - "The majority of our experts are of the opinion that we have no problem. So why do we need more security than we already have?"
  - "This problem is so unlikely, we don't need to worry about it!"
  - …

Motivation 2

Source: https://blog.mailfence.com

Advanced Persistent Threats

- Characteristics
  - targeted
  - unnoticed
  - slowly and over a long period (weeks... months)
  - specific ("tailor-made" malware)
  - too late to avert damage if symptoms become visible
- Procedure (model)

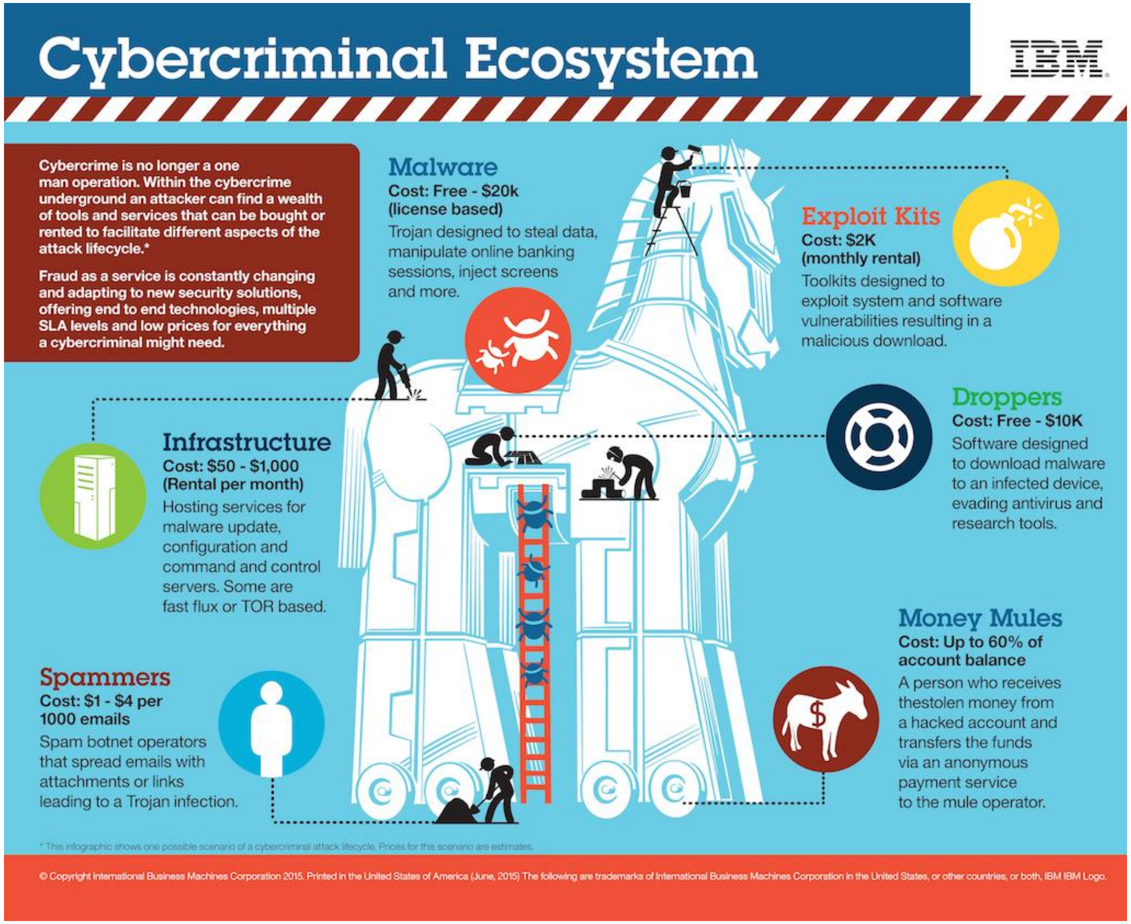
… like a disease

⇩

1. initial infection (phishing, dropper, social engineering,...) — infection
2. propagation (scanning ↻ penetration) — incubation
3. damage — outbreak

Cybercrime-as-a-Service

- Cyber-Crime-as-a-Service: A service (almost) as any other (…only illegal)
- …and quite affordable…



Source: https://securityintelligence.com/cybercrime-ecosystem-everything-is-for-sale/

IT-Security

The disease: APTs… (dark count?)

Source: https://www.itbusinessedge.com

The immune system

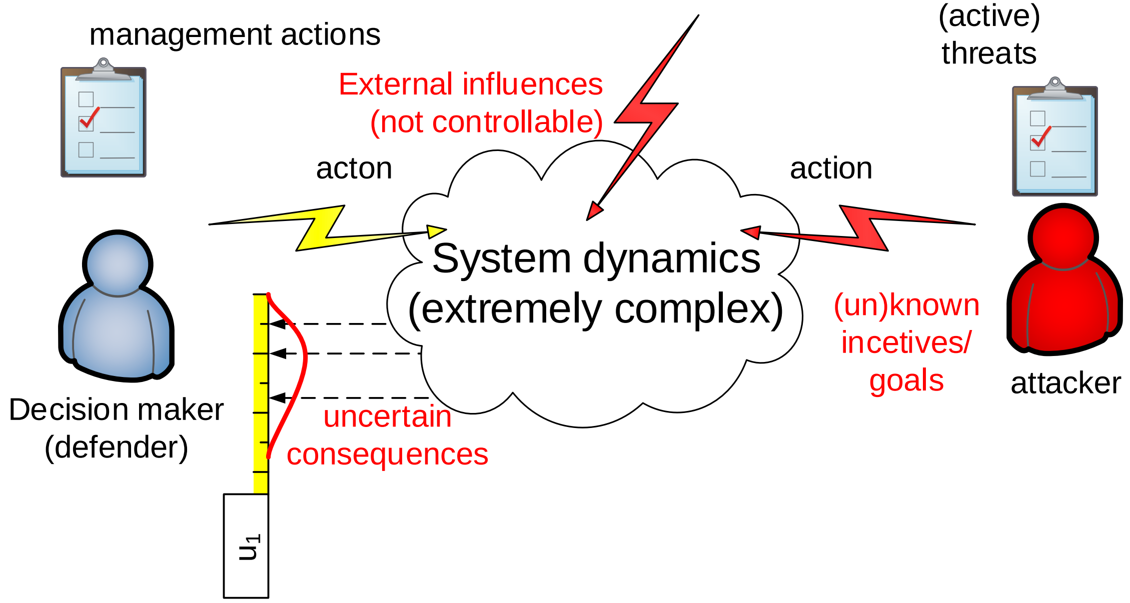
Source: http://www.techeconomy.it/

IT Security
IT Risk Management

… only why go to the doctor as long as you're healthy?

IT risk management as a game 1

- Player 1: Security Risk Manager Player 2: Attacker (partially unknown)
- Game: Risk minimization through "appropriate" management of the company



- Risk management = “best possible” controlling to minimize damage

⇨ game theory

Game theory – …by Example 1

- Example: Rock-Paper-Scissors
  - 2 players: player 1 chooses column, player 2 chooses row
  - 3 strategies per player
  - Outcome: +1 = player 1 wins, -1 = player 1 looses, 0 = draw

	Rock	Scissors	Paper
Rock	0	1	-1
Scissors	-1	0	1
Paper	1	-1	0

- Optimal strategy (for player 1)?

Game theory – ...by Example 2

- Example: Rock-Paper-Scissors
  - 2 players: player 1 chooses column, player 2 chooses row
  - 3 strategies per player
  - Outcome: +1 = player 1 wins, -1 = player 1 looses, 0 = draw

	Rock	Scissors	Paper
Rock	0	1	**-1** ☹
Scissors	-1	0	1
Paper	1	-1	0

- Optimal strategy (for player 1)? Always play „rock“? → player 2 always replies with „paper“ → player 1 loses constantly!

Game theory – ...by Example 2

- Example: Rock-Paper-Scissors
  - 2 players: player 1 chooses column, player 2 chooses row
  - 3 strategies per player
  - Outcome: +1 = player 1 wins, -1 = player 1 looses, 0 = draw

probability 1/3 (columns)

prob. 1/3 (rows)

	Rock	Scissors	Paper
Rock	0	1	-1
Scissors	-1	0	1
Paper	1	-1	0

- Optimal strategy (for player 1)? Take all three actions equiprobable (same for player 2) $\rightarrow$ Nash equilibrium (in mixed strategies = moving target defense)

Game theory – …by Example 3

- The „Battle-of-the-Sexes“
  - He: …wants to watch soccer
  - She: …wants to go to the opera
  - He: …rates soccer as +3, opera as +1
  - She: …rates soccer as +1, opera as +3

prob. Soccer: 25%, Opera: 75%

prob. Soc.: 75%
Opera: 25%

(↓ He, She →)	Soccer	Opera
Soccer	(3, 1)	(0, 0)
Opera	(0, 0)	(1, 3)

- Optimal behavior (= Nash equilibrium):
  Best possible/fair compromise for both sides

IT risk management as a game 2

- …quasi as „Rock-Paper-Scissors“: Defender vs. Attacker
- … only on the basis of damage scenarios & countermeasures

scenarios

counter-measures

	…	Threat	…
…			
Defense		Consequence	
…			

- Optimal security is "predictable" (Nash equilibrium), regardless of the actual behavior of the opponent

IT risk management as a game 3

- Restriction to:
  - Current defense policy (actual state)
  - Known/relevant threats

Identification of the "greatest" threat

	Threat X	Threat Y	Threat Z
...currently...		↑	
...			

- Solution of the game: ... delivers the greatest threat

IT risk management as a game 4

- Restriction to:
  - A fixed threat
  - Candidate countermeasures (target status) with permanent effect

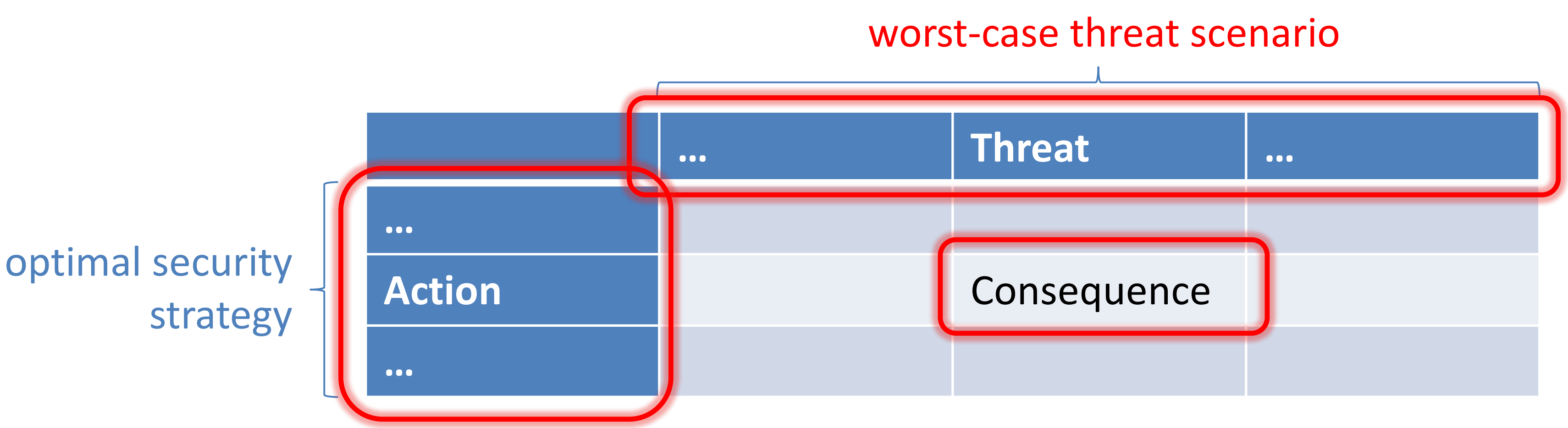
Determination of "best" security-action

	Threat X		
Action A			
Action B	←		
Action C			

- Solution of the game: ...provides the optimal countermeasure

IT risk management as a game 5

- Combination:
  - Multiple threats
  - Multiple countermeasures (without permanent effect → repetition required*)
    e.g., awareness training, …



- Solution of the game: optimal resource allocation for minimal risk under (all) worst-case scenarios

* „security is never done“

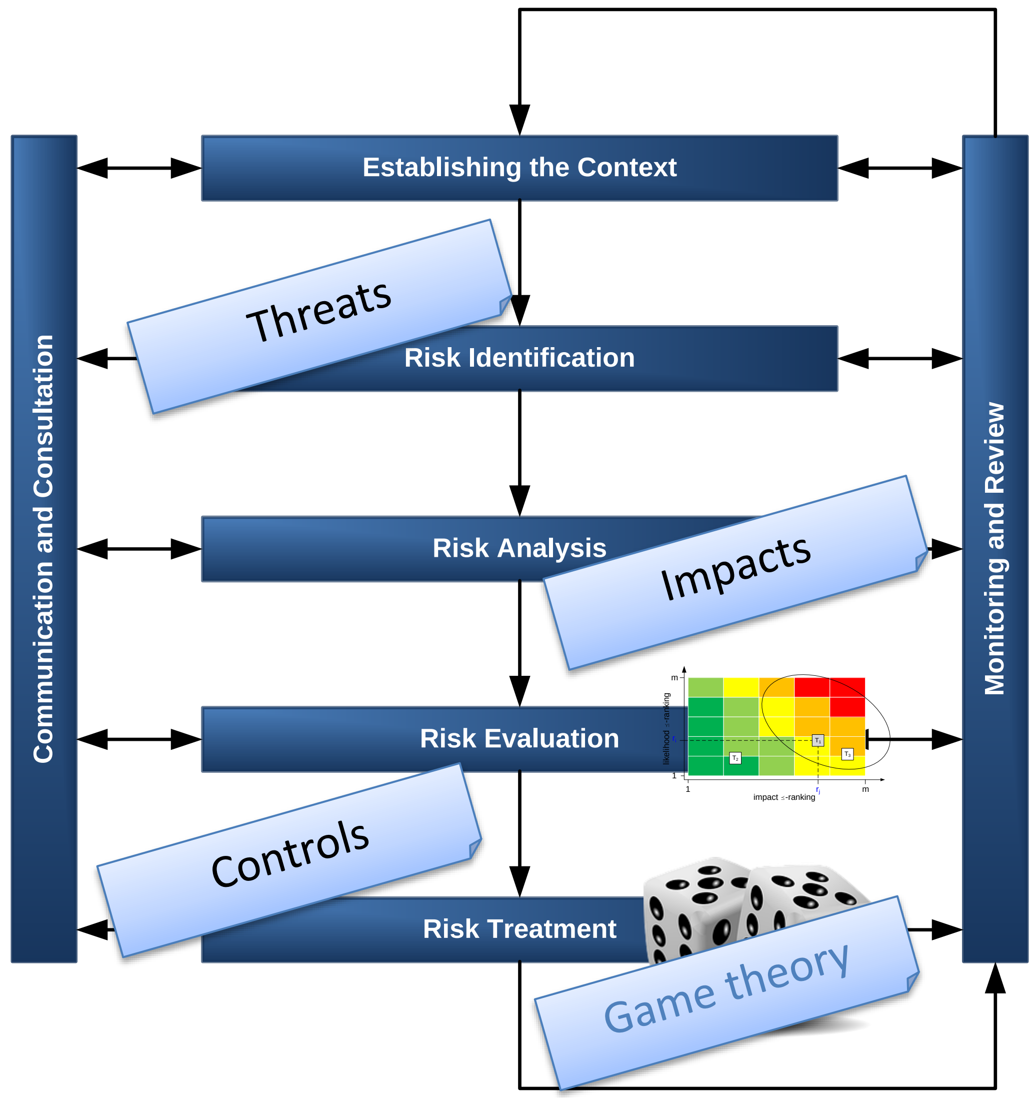
Positioning in the overall process

e.g., ISO 31000

- One of the best-known risk management models
- Best Practice

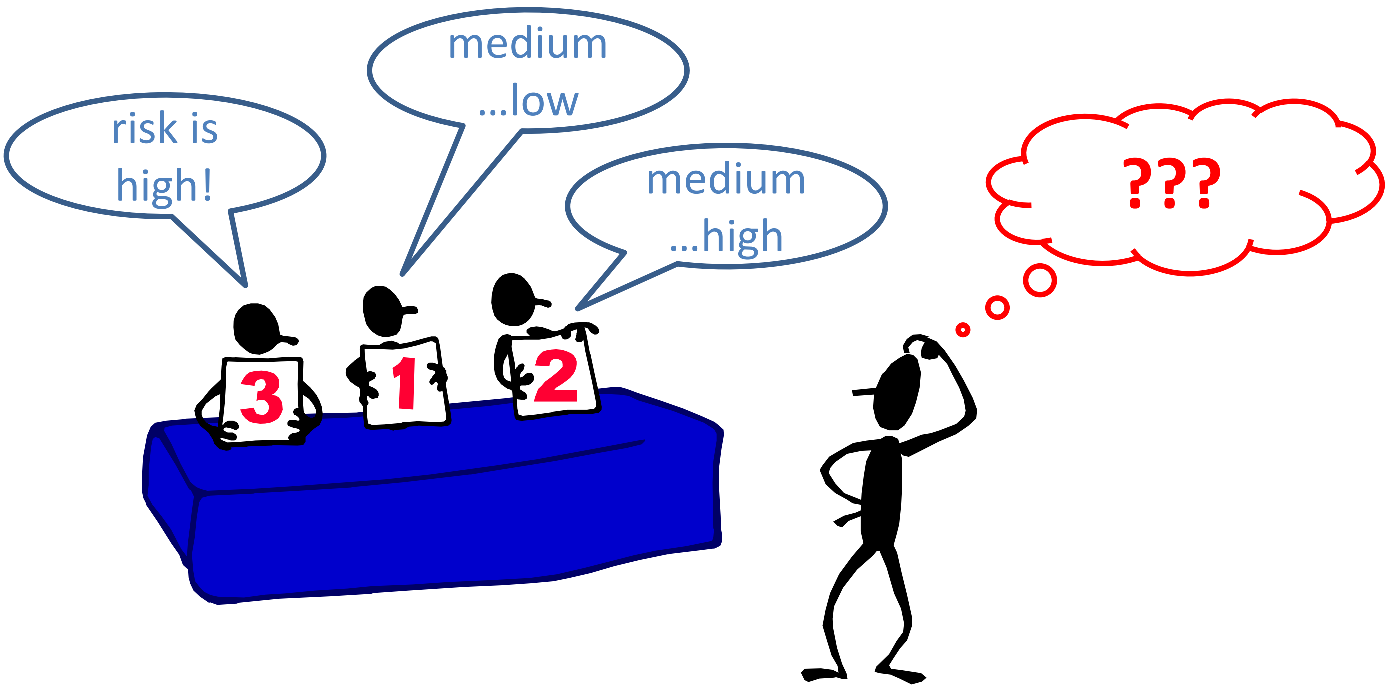
- Problems (in general)
  - awareness
  - divergences of opinion
  - consensus problems
  - evaluation problems
  - …

Research
(this talk)



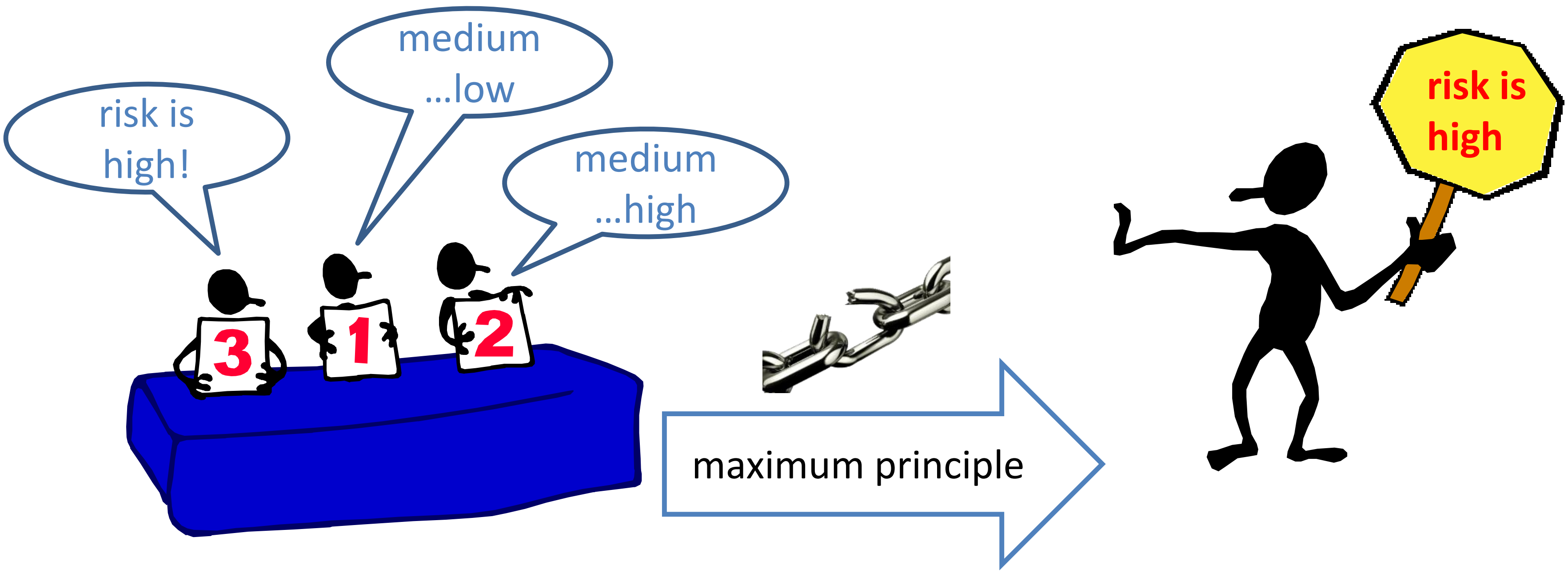
Risk Assessment

- "On risks and side effects, please ask...” → your experts
- A standard problem: you ask two people and get three opinions



Risk Assessment

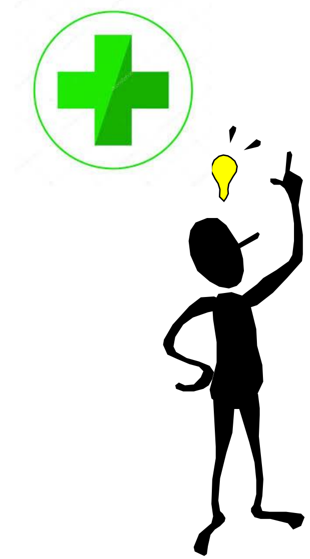
- "On risks and side effects, please ask...” → your experts
- A standard problem: you ask two people and get three opinions
- The standard solutions: Consensus, compromise, aggregation



...and for the aftermath?

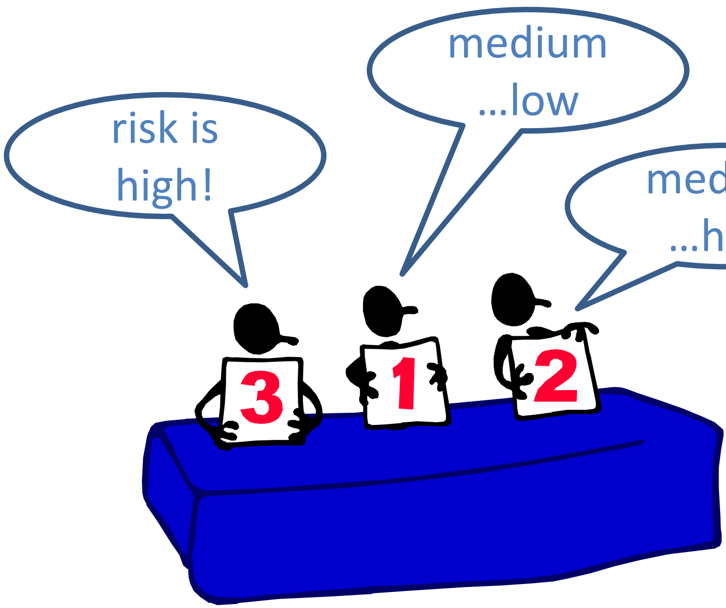
- If nevertheless (no) damage occurs:
  - ...were all ignored by the compromise → remission of guilt
  - ...some had pointed out possibly higher damages → "It is always easy to evaluate past events with the wisdom of hindsight.”
- → none of this is helpful to limit or repair the current damage...

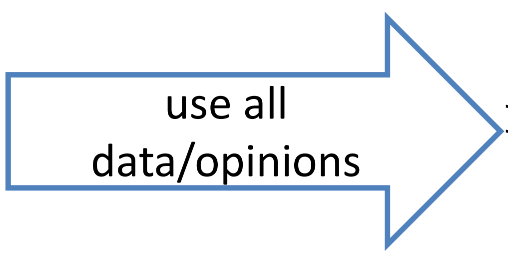
Risk Assessment “2.0”



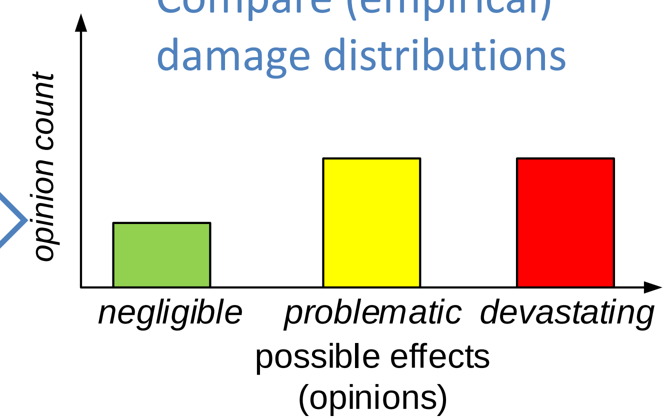
- "On risks and side effects, please ask...” → your experts
- A standard problem: you ask two people and get three opinions
- New research approach:

Avoid consensus troubles by “lossless” aggregation





Compare (empirical) damage distributions



Numbers vs. Distributions 1

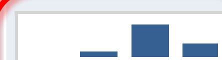
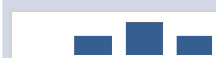
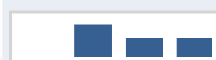
Example:

Component: database server, scenario: outage	Risk assessment (e.g., CVSS) by experts				
	#1	#2	#3	#4	…
Risk (actual state)	7.3	7.9	6.7	8.1	…
Countermeasure 1:	Other DBMS software				
Countermeasure 2:	Redundancy (mirroring)				
RaM* 1:	6.5	6.7	2.8	7.1	…
RaM 2:	6.3	6.9	3.2	7.0	…

* RaM: Risk after Mitigation

Numbers vs. Distributions 2

Example:

Component: database server, scenario: outage	Risk assessment	
	Max-principle (scalar)	Distribution
Risk (actual state)	8.1	
Countermeasure 1:	Other DBMS software	
Countermeasure 2:	Redundancy (mirroring)	
RaM* 1:	7.1	
RaM 2:	7.0	

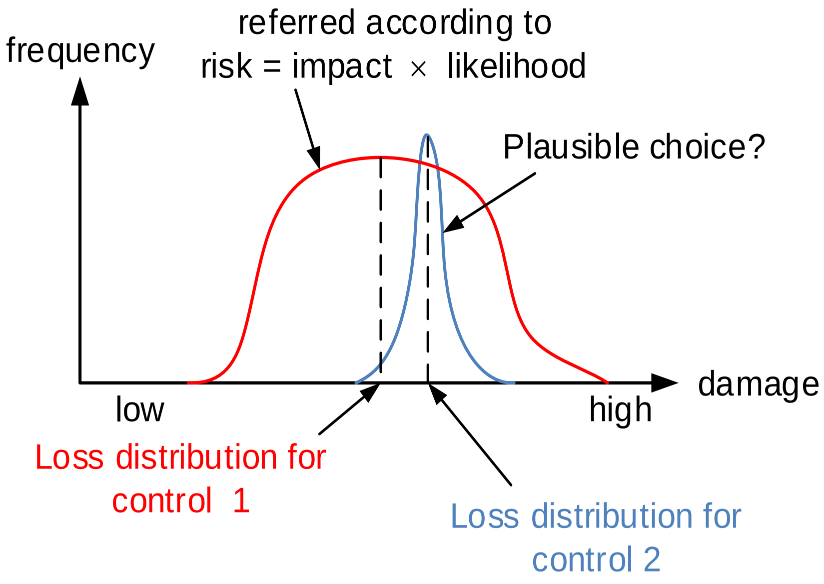
* RaM: Risk after Mitigation

best decision ???

best decision = minimal risk!

Comparison of Distributions 1

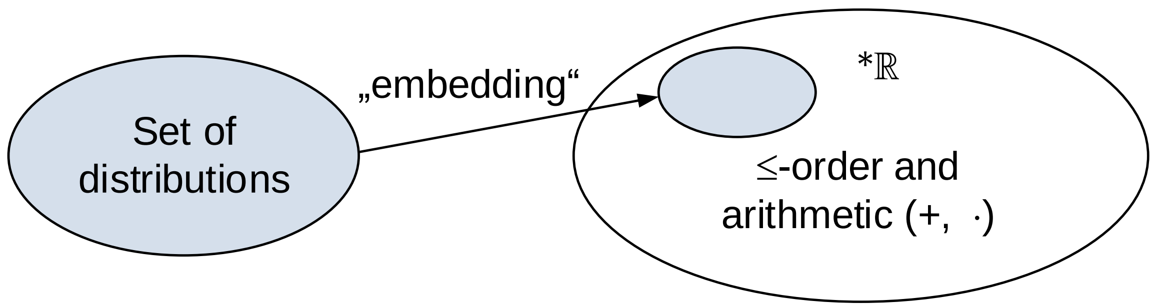
- The simplest method[1] „risk = impact × likelihood“ is not always best...
- Intuition:
  - small damages can be compensated by the "natural" resilience of the system (risk capital,...)
  - Improvements "on a small scale" generally do not require action
  - Potentially large (possible) damages are interesting (extreme value distributions,... tails of the distribution)
- Better selection criterion required



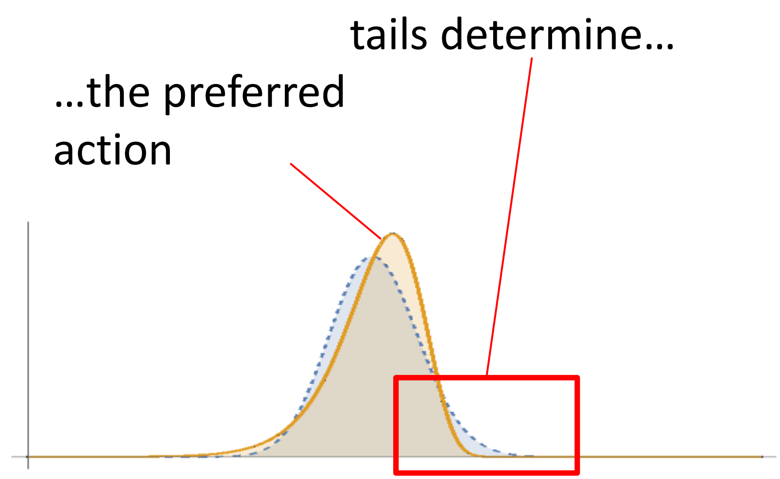
[1] Goodpasture, John C. (2004): *Quantitative methods in project management*. Boca Raton, Fla: J. Ross Pub.

Comparison of Distributions 2

- Idea (informal): Embed distributions in a (richer) structure[2]

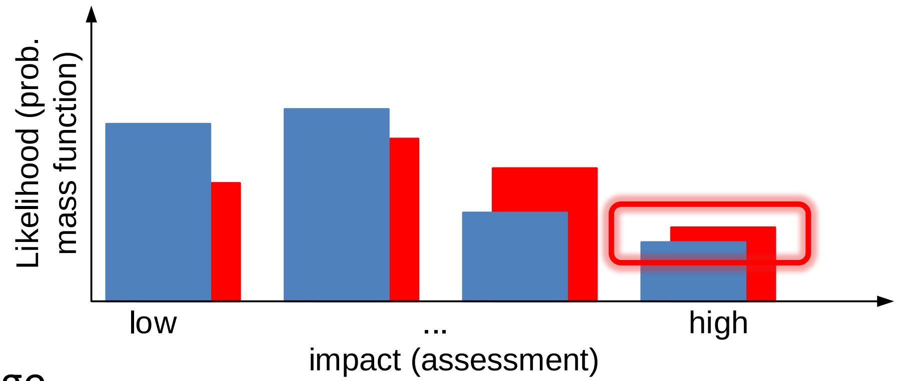


- Effects / Benefits:
  - Ranking of two actions determined by likelihood for extreme events ✓
  - Applicability of „more powerful“ mathematical methods (without additional efforts)

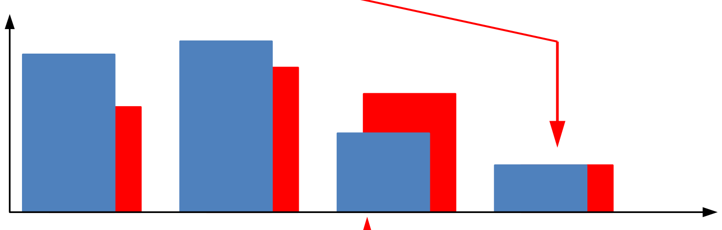


[2] S.Rass, S. König, S. Schauer: *Decisions with Uncertain Consequences – A Total Ordering on Loss-Distributions*, PLoS ONE, 2016 , 11 , e0168583

Comparison of Distributions 3



- Problem: Compare two categorical distributions describing the effectiveness of two measures (Control 1 vs. Control 2)
- Procedure:
  - Preference wherever larger damage is less likely.
  - On equal likelihood for the highest possible damage, the…



chance for the second-largest damage category tips the scale

  - …and so on…

...and for the aftermath?

If nevertheless (no) a damage occurs:

- ...all opinions were used for the evaluation equally → the whole team of experts bears the decision and the responsibility
- ...some had pointed out possibly higher damages → their statements might have been decisive for other (better?) measures.

Multiple Goals

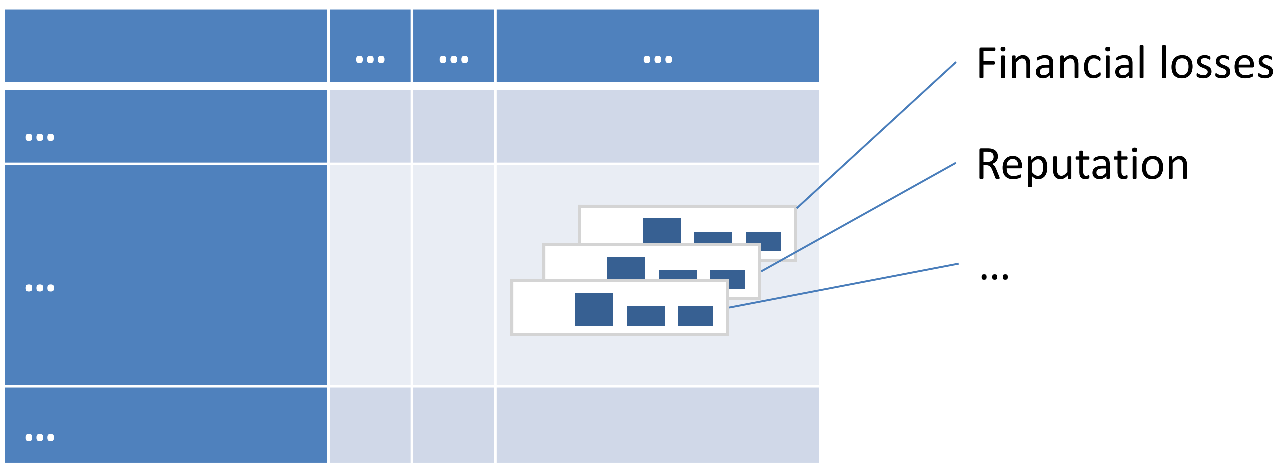
- Impact (damage) assessment: often categorical + multi-criteria
- Specific for individual contexts

Category	Financial loss	Image/Reputation[3]	…
Negligible			
Low	< 100.000€		
Medium			
High		Loss of > …% market share	
Very high			
Critical			

[3] Busby, J. S.; Onggo, B.S.S.; Liu, Y. (2016): *Agent-based computational modelling of social risk responses*. In: European Journal of Operational Research 251 (3), S. 1029–1042.

Multicriteria Optimization

- Models remain structurally unchanged…
- …and get only extended by an individual assessment per goal:



- Mathematical procedure analogous to the optimization of individual targets
- only transition to "weighted sum" of the individual target functions
- Result: Pareto optimality (depending on target priorities)

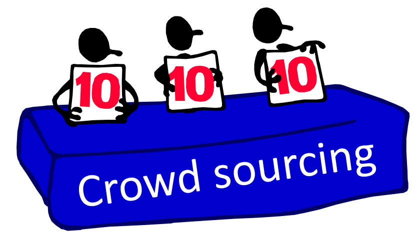
Practical implementation[4]: ISO 31000

Establishing the Context	External Context	Internal Context	Context of the RM Process	Criteria of the RM Process
Risk Identification	Asset Identification	Threat Identification	Vulnerability Identification	
Risk Analysis	Threat Scenario Definition	Consequence Analysis	Likelihood Analysis	
Risk Evaluation	Risk Selection	Risk Ranking	Risk Level Determination	
Risk Treatment	Attack Strategies	Defense Strategies	Mitigation Actions	Implementation Strategy

[4] S. Schauer: A Risk Management Approach for Highly Interconnected Networks
in: *Game Theory for Security and Risk Management*, Springer Birkhäuser, 2018 , pp. 285-311

Practical implementation[4]: ISO 31000

Establishing the Context	External Context	Internal Context	Context of the RM Process	Criteria of the RM Process
Risk Identification	Asset Identification	Threat Identification	Vulnerability Identification	
Risk Analysis	Threat Scenario Definition	Consequence Analysis	Likelihood Analysis	
Risk Evaluation	Risk Selection	Risk Ranking	Risk Level Determination	
Risk Treatment	Attack Strategies	Defense Strategies	Mitigation Actions	Implementation Strategy

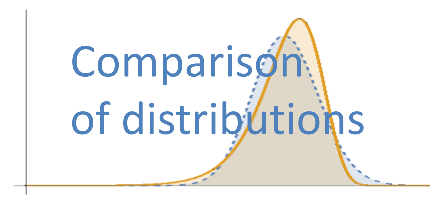


simulations

[4] S. Schauer: A Risk Management Approach for Highly Interconnected Networks in: *Game Theory for Security and Risk Management*, Springer Birkhäuser, 2018 , pp. 285-311

Practical implementation[4]: ISO 31000

Establishing the Context	External Context	Internal Context	Context of the RM Process	Criteria of the RM Process
Risk Identification	Asset Identification	Threat Identification	Vulnerability Identification	
Risk Analysis	Threat Scenario Definition	Consequence Analysis	Likelihood Analysis	
Risk Evaluation	Risk Selection	Risk Ranking	Risk Level Determination	
Risk Treatment	Attack Strategies	Defense Strategies	Mitigation Actions	Implementation Strategy



- No consensus-problems
- Natural treatment of vagueness and un-certainty

[4] S. Schauer: A Risk Management Approach for Highly Interconnected Networks in: *Game Theory for Security and Risk Management*, Springer Birkhäuser, 2018 , pp. 285-311

Practical implementation[4]: ISO 31000

Establishing the Context	External Context	Internal Context	Context of the RM Process	Criteria of the RM Process
Risk Identification	Asset Identification	Threat Identification	Vulnerability Identification	
Risk Analysis	Threat Scenario Definition	Consequence Analysis	Likelihood Analysis	
Risk Evaluation	Risk Selection	Risk Ranking	Risk Level Determination	
Risk Treatment	Attack Strategies	Defense Strategies	Mitigation Actions	Implementation Strategy

mathematically grounded optimal decisions

Game theory

[4] S. Schauer: A Risk Management Approach for Highly Interconnected Networks in: *Game Theory for Security and Risk Management*, Springer Birkhäuser, 2018 , pp. 285-311

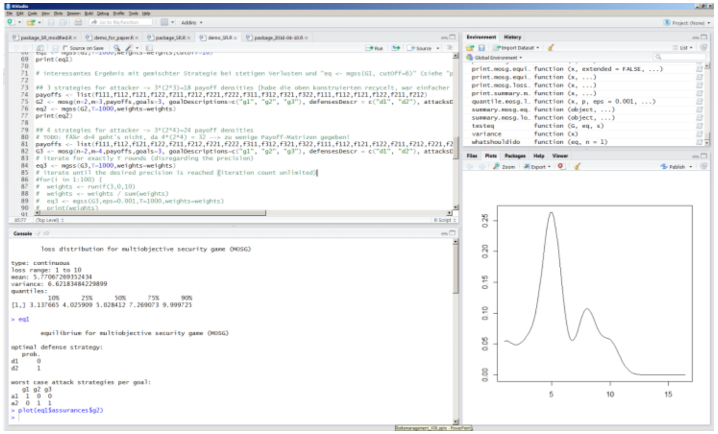
Research Project (finished in 10/2017)

- EU-Project „HyRiM“ – Hybrid Risk Management for Utility Networks (https://hyrim.net)

This project is supported by the European Commission
through the FP7-SEC-2013-1
Grant Agreement Number: 608090

Status of (our) Research

- Data collection: online portals (surveys, crowdsourcing …)
- The rest: implemented for the statistical software **R** (open source, GPL)
  - Construction of loss distributions from data
  - Comparison of distributions
  - Multi-criteria games and their solutions
- Package released under GPL @ https://hyrim.net/software
- Theory is freely available[5,6,7] (open access)



[5] Rass, S.; König, S.; Schauer, S. (2017): *Defending Against Advanced Persistent Threats Using Game-Theory*. In: PLoS ONE 12 (1), e0168675. DOI: 10.1371/journal.pone.0168675.

[6] Rass, S.; König, S.; Schauer, S. (2016): *Decisions with Uncertain Consequences-A Total Ordering on Loss-Distributions*. In: PLoS ONE 11 (12), e0168583. DOI: 10.1371/journal.pone.0168583.

[7] https://arxiv.org/abs/1506.07368 und https://arxiv.org/abs/1511.08591

Theory in a Book

- The following volume compiles most of the theory covered here, extended by
  - applications
  - selected further (alternative) game-theoretic models

- Published by Springer
  https://www.springer.com/us/book/9783319752679

- Available at Amazon and other retailers:

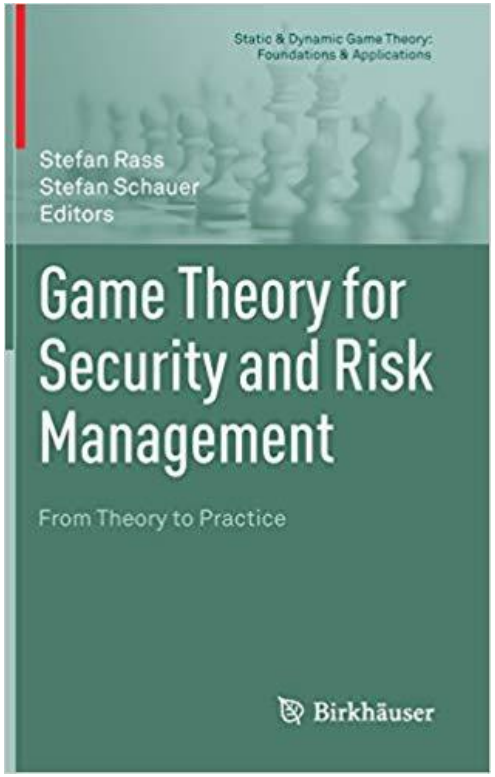
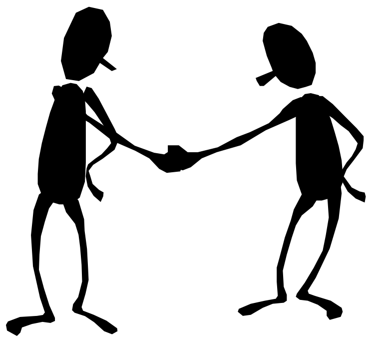


Image source: Amazon

Contemporary Security Games

- Game theory for Security → active area of research (www.gamesec-conf.org)
- Security by (game-theoretic) multipath transmission

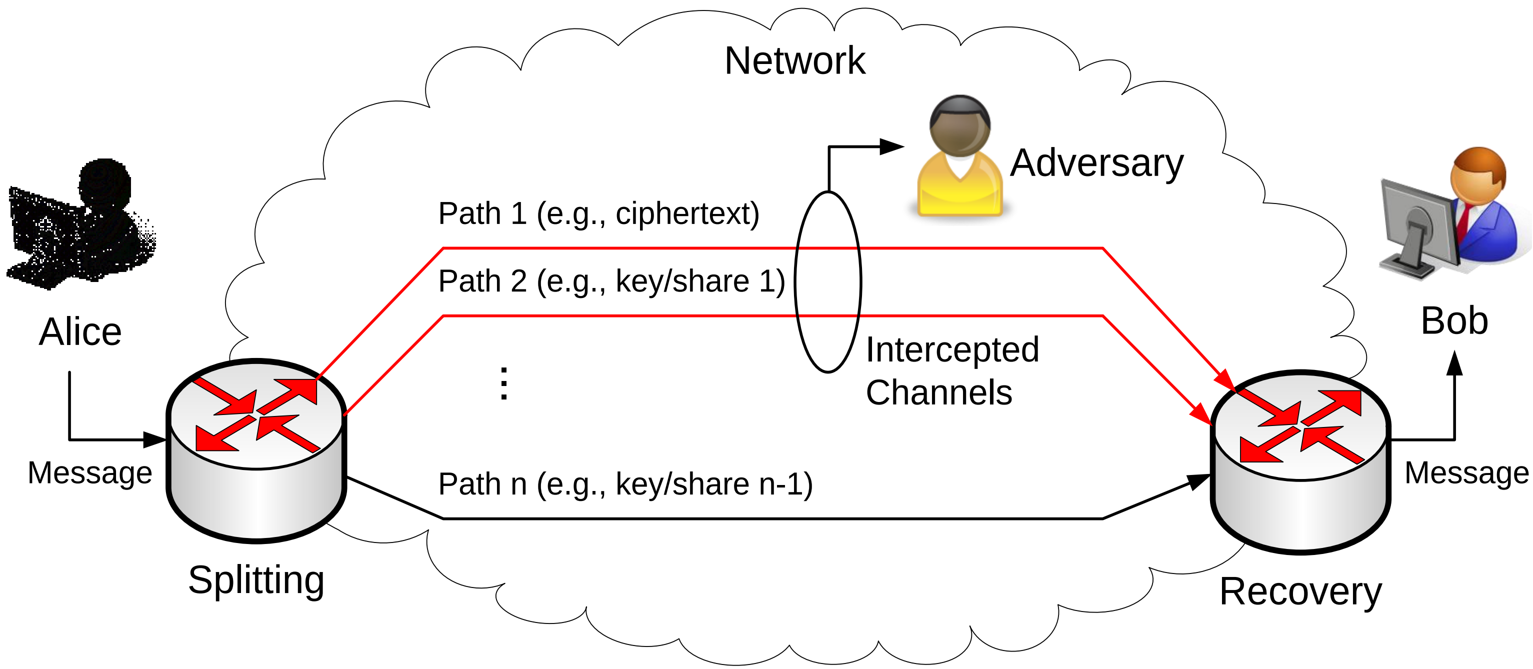
- End Users (a selection[8]):
  - US Air Force: recognition of malware
  - US Coast Guards: optimal patrolling in harbor areas
  - US Border Control: optimized border checks
  - Airline security: optimized passenger screenings
  - …
  - …maybe you?



[8] M. Tambe (2011): *Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned*, Cambridge University Press

Secure Multipath Routing[9] (SMR)

- Split the message into parts (e.g., via secret sharing)
- Deliver the parts over disjoint paths → enforce interception of several paths
- Implementable by segment or **preferred path routing**



Special case: 2-path transmission ≅ symmetric encryption

[9] S. Rass, B. Rainer, M. Vavti, J. Göllner, A. Peer, S. Schauer: *Secure Communication over Software-Defined Networks*, Springer J. on Mobile Networks and Applications, 2015 , 20 , pp. 105-110

SMR: Game-Theoretic Analysis

- Multipath transmission admits a simple game-theoretic formulation
- Risk ρ (saddle-point value of the game) upper-bounds the likelihood for a successful attack (analysis similar to stone-scissors-paper):

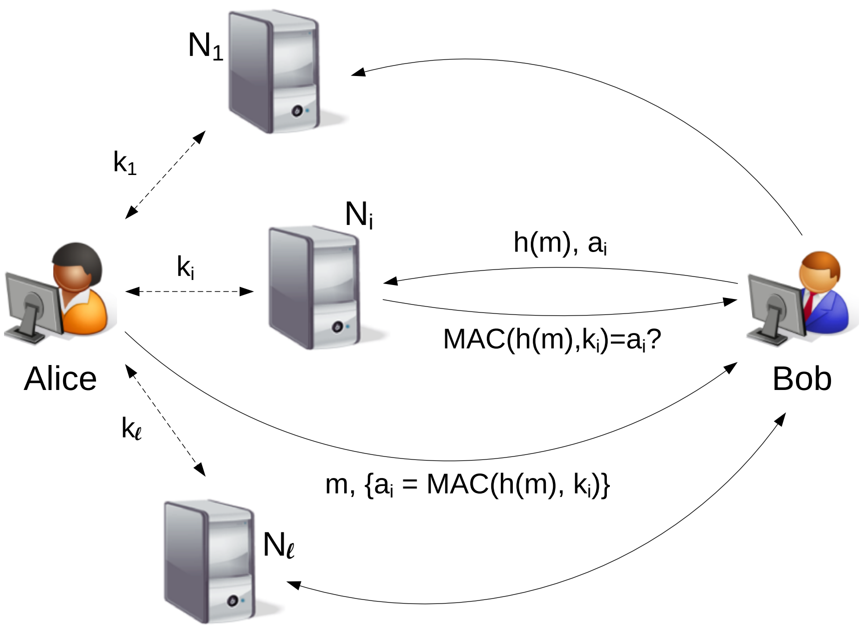
$$\Pr(\text{eavesdropping}) \leq \rho$$

- Theorem[10]: Let ρ be the game-theoretic risk. Then, every $\varepsilon > 0$ admits an efficient protocol (with polynomial overhead) such that the risk (likelihood) of eavesdropping is $\leq \varepsilon$, if and only if, $\rho < 1$.
- This even holds under the relaxed assumption that the attacker can fiddle with the routing (to a limited extent)
- Industrial research project „RSB“ by the Austrian Institute of Technology

[10] S. Rass, S. König: *Indirect Eavesdropping in Quantum Networks*, ICQNM 2011, XPS Publishing Services, p. 83-88, available @ ThinkMind (open access)

Multipath Authentication[10]

- Sender „signs“ a message using secrets shared with direct neighbours
- Receiver asks these neighbours to verify the message authentication code (MAC)
- Again: implementable by segment or **preferred path routing**



- Security analysis and –guarantees like for SMR (previous slide).
- Industrial research project „RSB“ by the Austrian Institute of Technology

[10] S. Rass, P. Schartner: *Multipath Authentication without shared Secrets and with Applications in Quantum Networks*, Proc. of the Int. Conf. on Security and Management (SAM), CSREA Press, 2010 , 1 , pp.111-115

Thanks for listening!

Questions?

IT security as a game

Decisions under uncertainty in risk management

Stefan Rass
Associate Professor @ Alpen-Adria Universität Klagenfurt
Institute of Applied Informatics – System Security
stefan.rass@aau.at