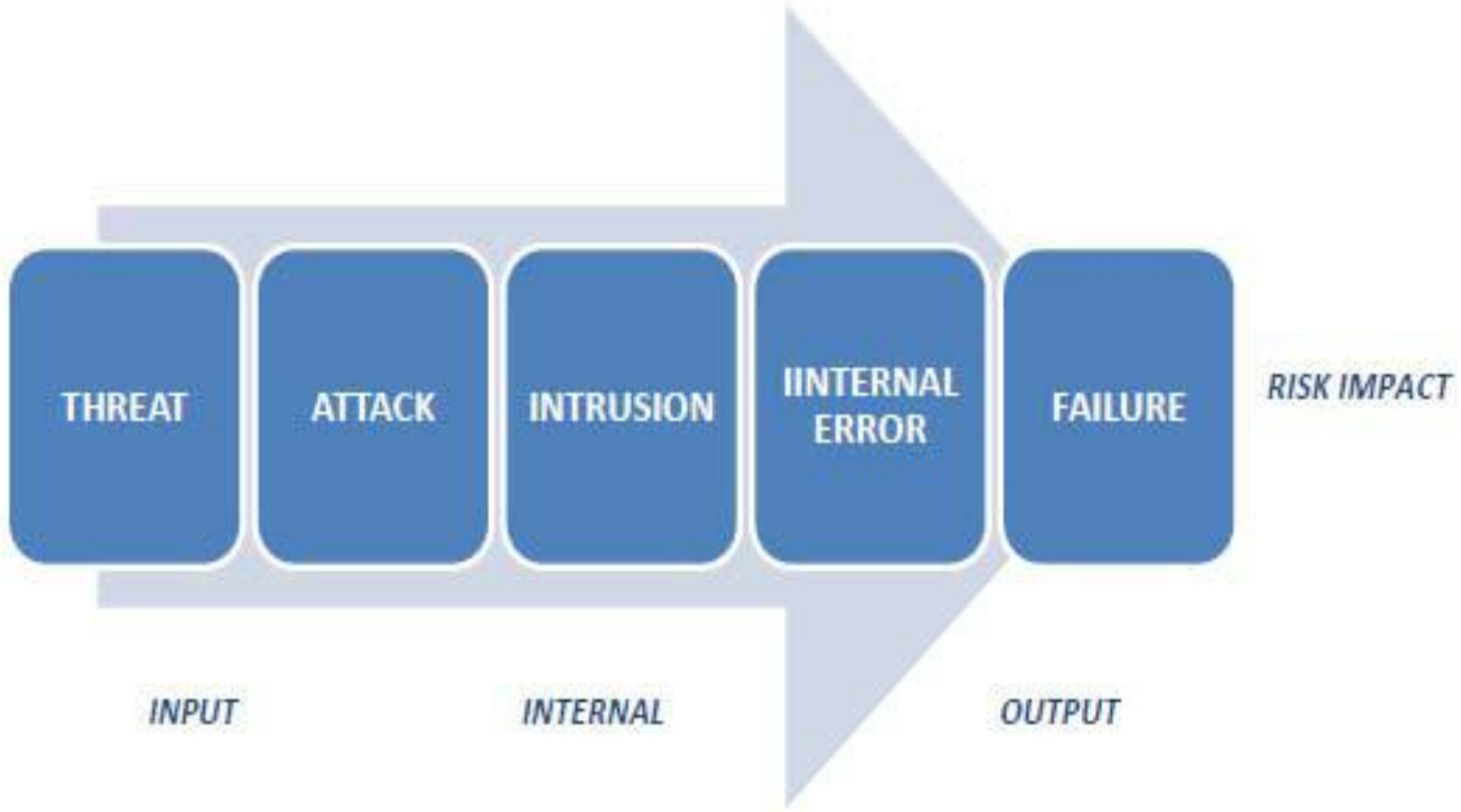
A Cause and Effect Approach Towards Risk Analysis

Laleh Pirzadeh and Erland Jonsson
Department of Computer Science and Engineering
Chalmers University of Technology
Göteborg, Sweden

The Causal Approach: Chain of Impairments



The main idea

- We suggest a Causal Approach towards risk analysis based on an existing security model.
- This approach takes system operation, causal relation between the impairments and latency into account.
- Thus, it exhibits the impact of the chain of impairments on system risk.
- It should lead to a more refined quantitative assessment of risk.

Current approaches

- Current approaches for risk analysis and quantification are in many cases based on a very simplistic assumption about the relation between risk event and risk impact.
- The probabilistic influence from the system operation, internal mechanisms and the impairments on system risk has been disregarded.
- Indeed, some authors have suggested more refined risk analysis methods. However, none of them has adopted the full input-output causality approach as the one presented in this paper.

Existing risk ”definition”

$$RISK = Event * Likelihood * Impact$$

- ***Event*** denotes some kind of initiating detrimental influence on the system, e.g. an attack, possibly leading to a system failure,
- **Likelihood** denotes the probability of the Event occurrence, and
- **Impact** indicates the resulting consequences caused by the Event
(including monetary, resource or other loss)

Extended risk ”definition”

- $RISK = Event * Probability\ of\ Occurence * \Sigma(Probability\ of\ Propagation * Loss)$

- **Event** denotes some kind of initiating detrimental influence on the system, e.g. an attack, possibly leading to a system failure,
- **Probability of Occurrence** (likelihood) is the probability that the Event occurs,
- **Probability of Propagation** is the probability that an Event leads to a specific failure. This failure is one of the possible failures that may result from a specific Event,
- **Loss** is the loss associated with each failure that the Event can lead to (e.g. in EUR), and
- **Sum** is the sum taken over all possible failures related to one specific Event with their related losses.

Conclusion

- We have suggested that risk should be calculated considering the probabilistic impact presented by system operation, impairment propagation and latency
- We claim that the suggested risk analysis method provides an improvement to current approaches and that it is more fine-grained and realistic than many other risk analysis methods.

Challenges and Future

- Probabilistic relations among different system's internal operations/mechanisms and their influence on the system failure call for further investigation.
- A need for more detailed information about system operation and their related risk: practicality?