Combinatorial Framework for Cybersecurity Incidents and Natural Disaster Risk Management

Dimitris E. Simos, Bernhard Garn, Klaus Kieseberg

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet
SBA Research
MATRIS

Overview

Question: Do certain sequences of events introduce failures into a system?

Objective: The goal of this serious game is to identify and locate potential problems in a system caused by a specific sequence of events through generating and testing multiple permutations of such sequences and analyzing their impact on the system. (Combinatorial Sequence Testing)

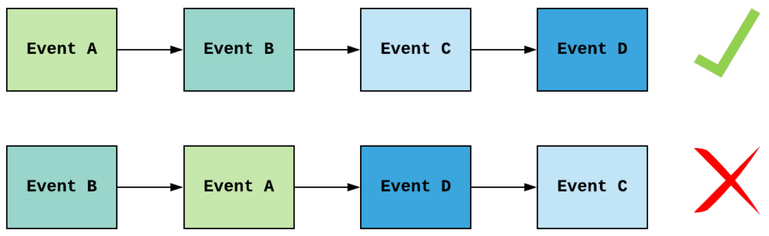

Figure 1: Sequences of events

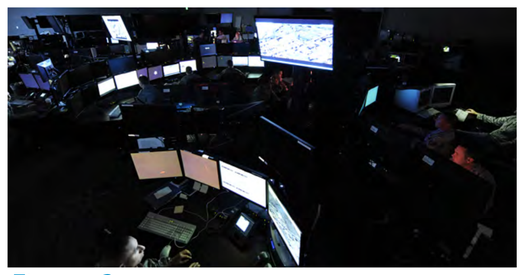

Figure 2: Serious game

Serious Games for Disasters (Planspiel)

- Multiple teams of participants from different backgrounds (e.g., security research, critical infrastructures, government).
- Multiple iterations of gameplay using different scenarios.
- Stakeholders choose corresponding crisis management responses.
- The decision making process is documented by observers.
- Results are used to evaluate the decisions taken by stakeholders and viability of the method.

Method

- Generate multiple permutations of a sequence of 5 to7 events using mathematical methods → **Scenarios**.
- Assign a weight $\omega(e)$ to each event e.
- Assess the impact of a sequence via its cumulative weight.

Using **Sequence Covering Arrays** helps minimizing the number of tests needed.

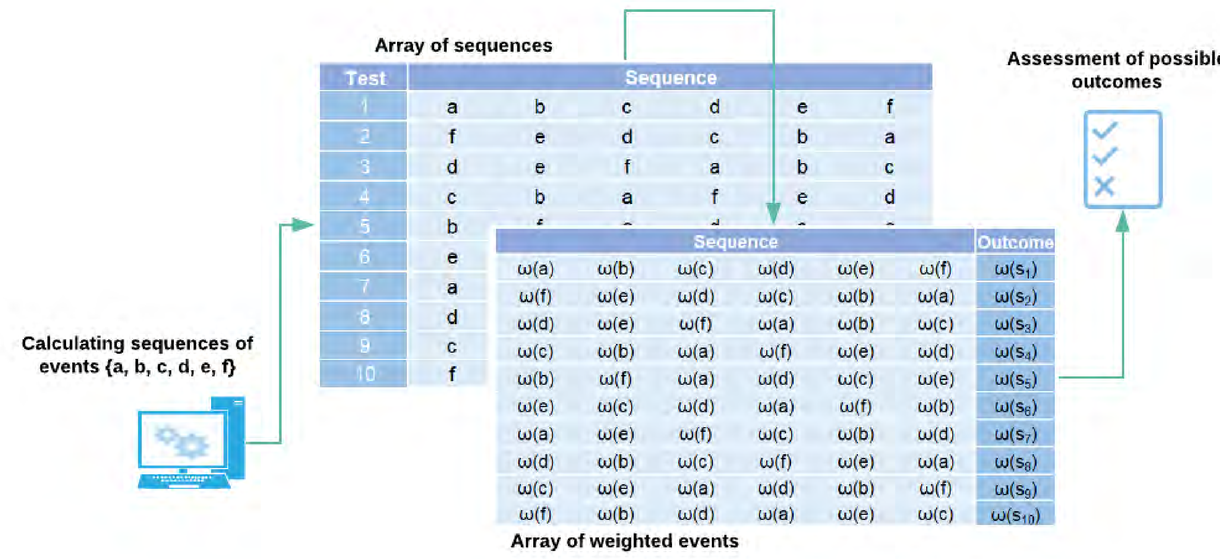

Figure 3: Analysis of the impact of sequences of events using Sequence Covering Arrays

What are Events?

Events could be:

- Deliberate actions of an acting party (harmless or malicious)
- Malfunctions of a device
- System changes
- Steps of a communication process
- Weather phenomena
- Natural disasters
- etc.

Applications

- Identifying risky sequences of events.
- Developing a framework for crisis prediction.
- Identifying the best response plan in case of critical situations.

Possible Future Work

- Applying this methodology to cyber-security and cyber-physical system security.
- Developing a framework for modeling natural disasters and recovery strategies.

Bundesministerium Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie
Bundesministerium Digitalisierung und Wirtschaftsstandort
FFG Forschung wirkt.
wirtschaftsagentur wien Ein Fonds der Stadt Wien
Europäische Kommission
FWF Der Wissenschaftsfonds.
netidee OPEN INNOVATIONS

SBA Research (SBA-K1) is a COMET Centre within the framework of COMET – Competence Centers for Excellent Technologies Programme and funded by BMK, BMDW, and the federal state of Vienna. The COMET Programme is managed by FFG.