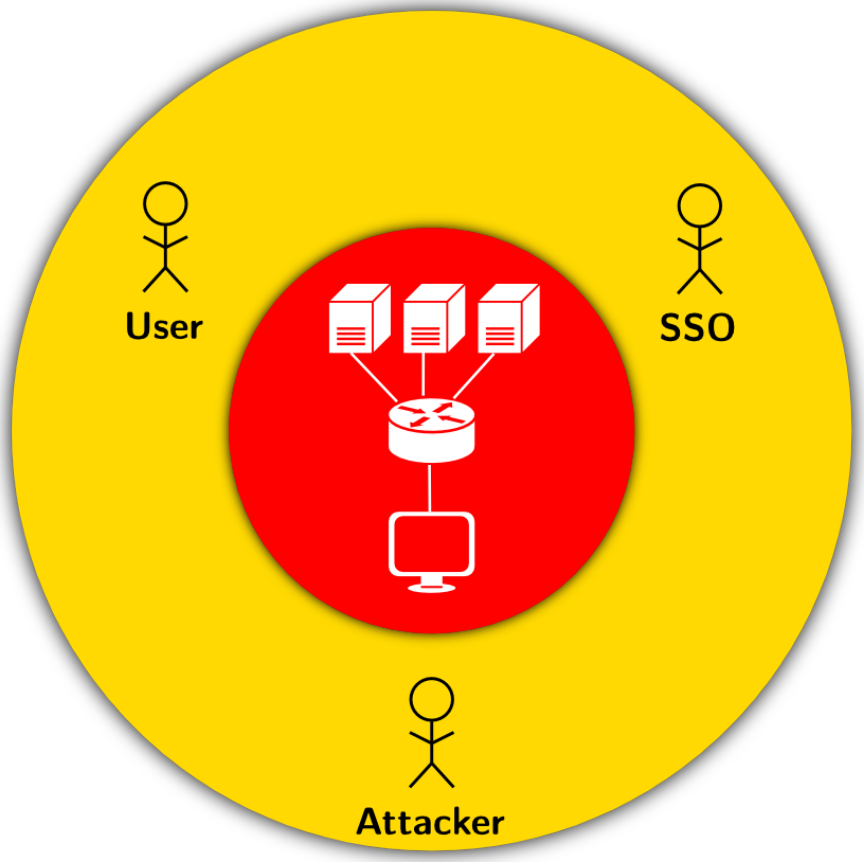
EDL als Ereigniskorrelationssprache in Multi-Sensor Intrusion Detection Systemen

Christoph Leuzinger

Informationssysteme und Sicherheit (ISSI)
Lehrstuhl VI
Fakultät für Informatik
TU Dortmund

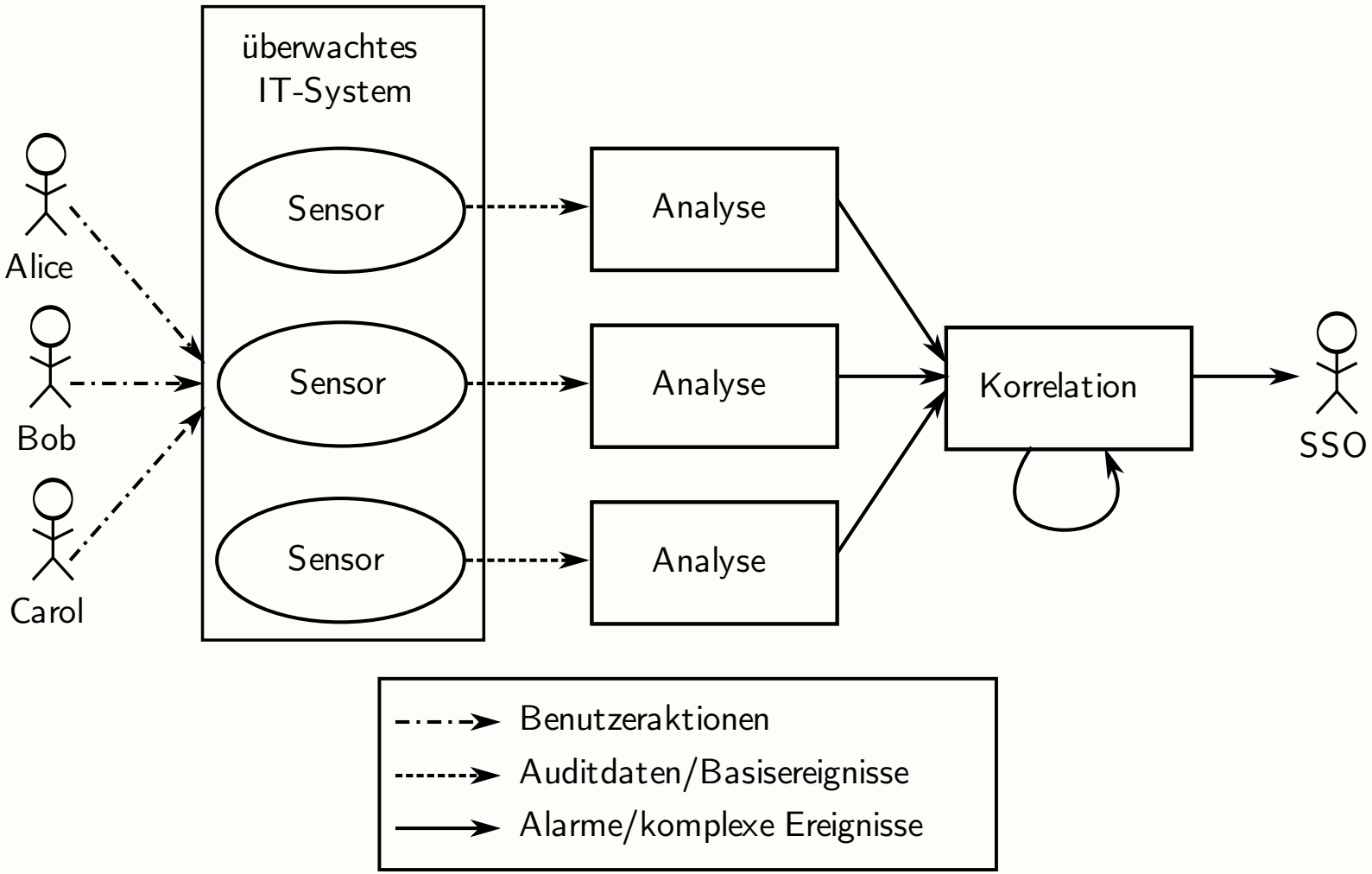
SPRING 4
14. September 2009

Szenario: Überwachung eines verteilten Systems



- Sicherung eines verteilten Systems durch reaktive Mechanismen
- Überwachung durch Erkennungssysteme an verschiedenen Knoten des Systems
- Korrelation der von den Erkennungssystemen emittierten Ereignisse

Modell eines Multi-Sensor IDS



Definition: Ereignis, Alarm, Meta-Alarm

- Ereignisse
  - repräsentieren Aktivitäten, die Änderungen des Zustands des überwachten Systems bewirken
  - besitzen Merkmale, die Information über die Aktivitäten enthalten
  - treiben den Korrelationsprozess an
- Alarme
  - sind von Analyseeinheiten emittierte Ereignisse
  - lenken die Aufmerksamkeit auf einen sicherheitsrelevanten Vorfall
- Meta-Alarme
  - sind vom Korrelationsprozess erzeugte Ereignisse
  - sind das Produkt von Korrelationsregeln

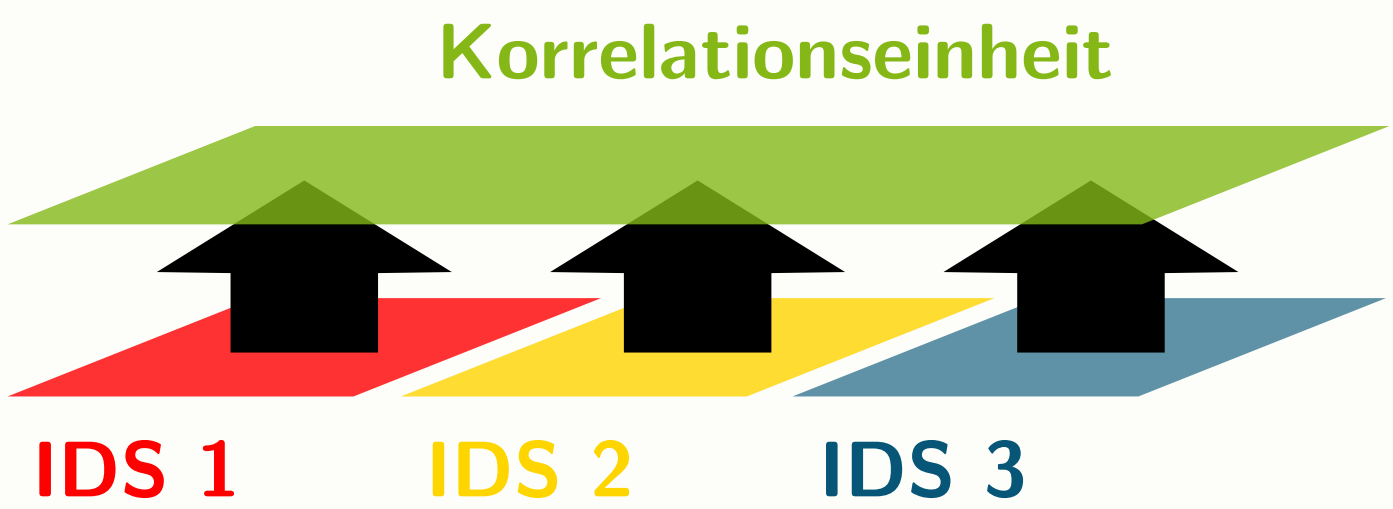
Ziele und Aufgaben der Ereigniskorrelation

Ⓐ Infrastruktur für MS-IDS
- Kollektion von Alarmereignissen
- Vorverarbeitung (Normalisierung und Vervollständigung)
- Verwerfen von Fehlalarmen (Verifikation)

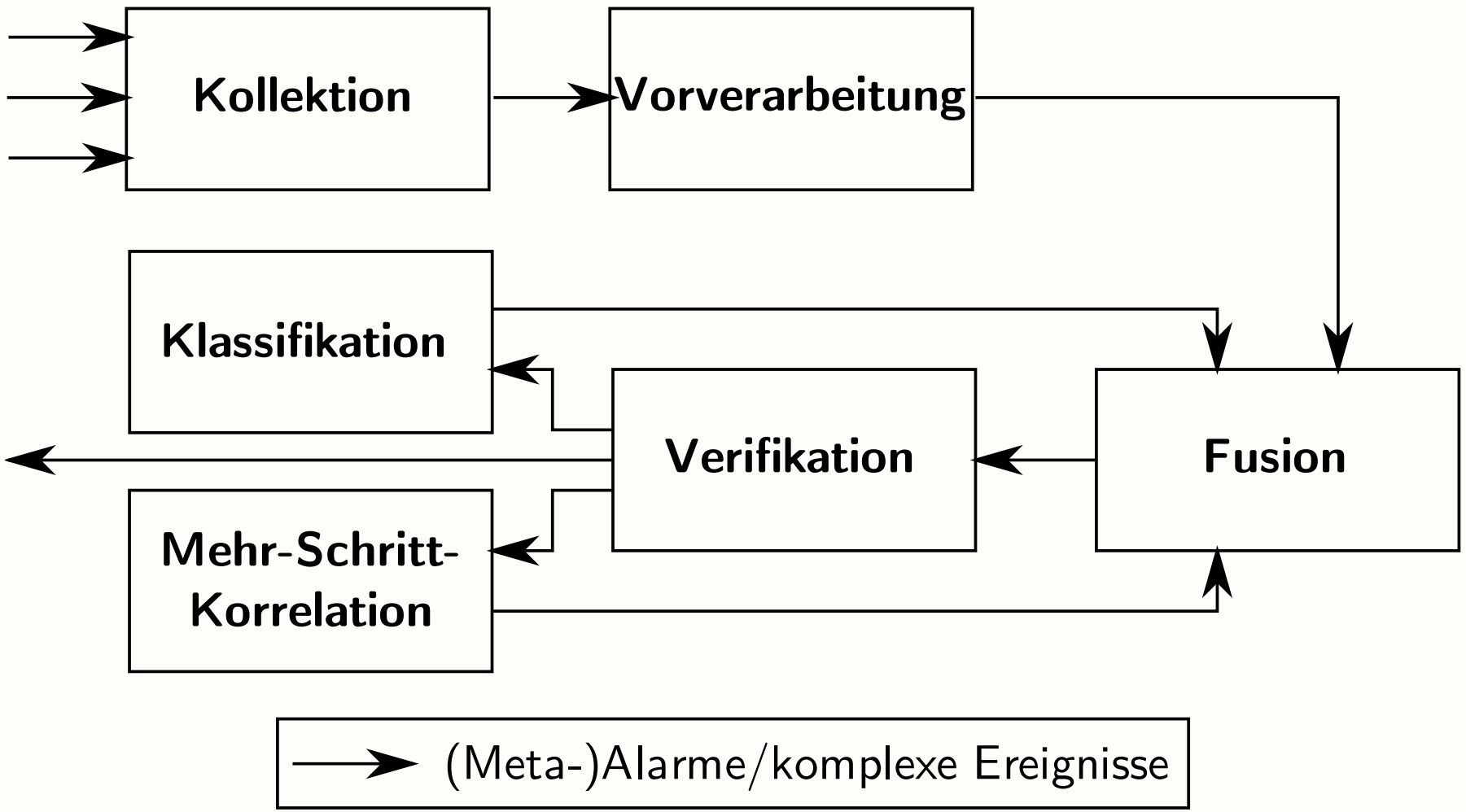
Ⓑ Darstellung von Zusammenhängen zwischen Alarmereignissen
- Behandlung von Duplikaten (Fusion)
- Übersetzung zwischen Abstraktionsebenen
  - Klassifikation
  - Mehr-Schritt-Muster

Abstraktion: System Views

- Sicht auf das Systemverhalten = Menge von Ereignissen
- Provided View
  - von den IDS emittierte Ereignisse
  - Sicht gegeben und beschränkt durch verfügbare Auditdaten, Möglichkeiten der Analyseeinheit und Datenschutzrichtlinien
- Expected View
  - von der Korrelationseinheit erwartete Ereignisse
  - Sicht gegeben durch reaktive Maßnahmen und forensische Interessen des SSO



Korrelationsprozess



Funktionalität

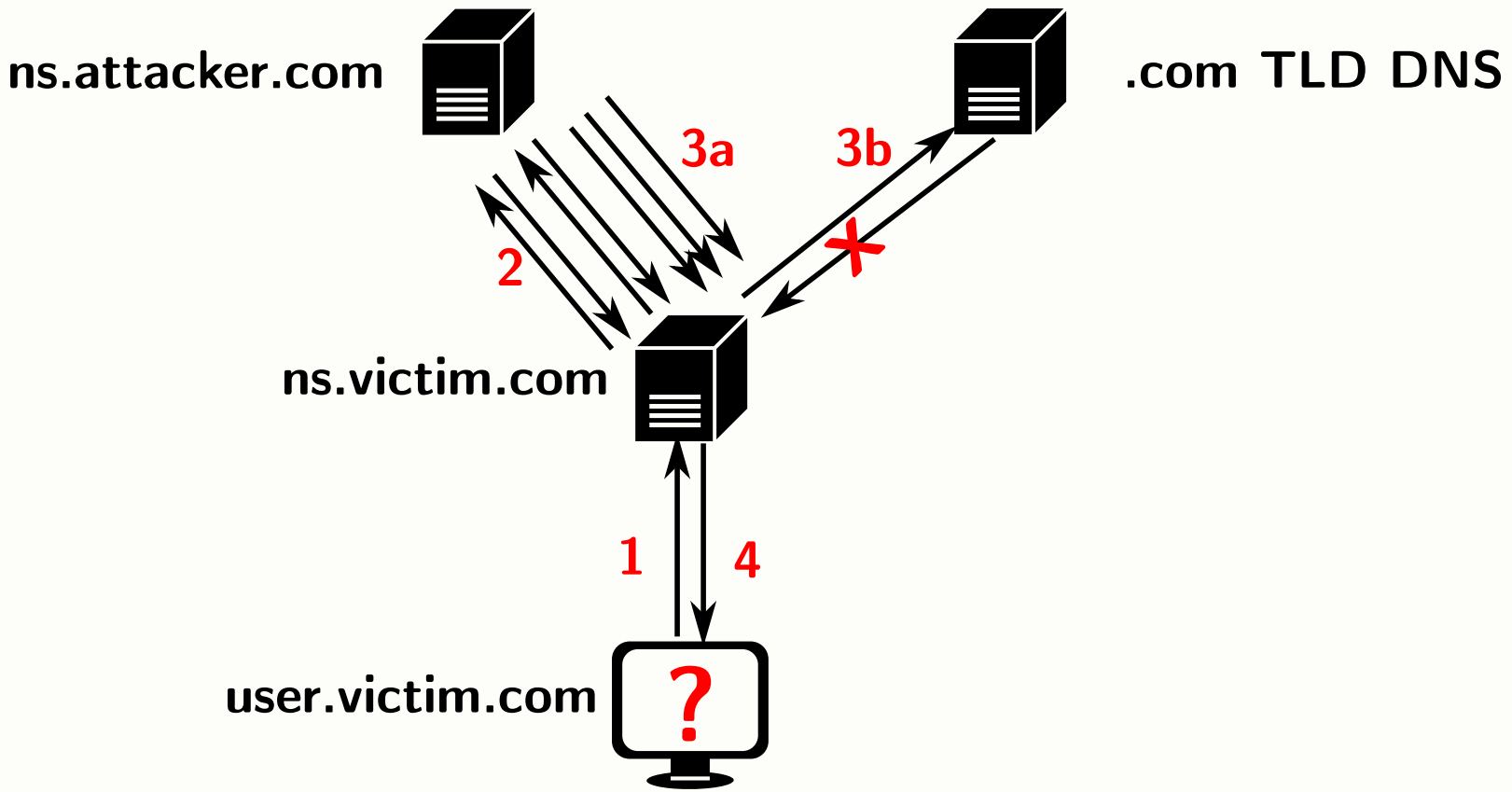
Korrelationstufe	Filter	Transformation	Aggregation	Komposition
Kollektion	•			
Vorverarbeitung		•		
Fusion			•	
Verifikation	•			
Klassifikation		•		
Mehr-Schritt-Korrelation			•	•

EDL als Ereigniskorrelationssprache

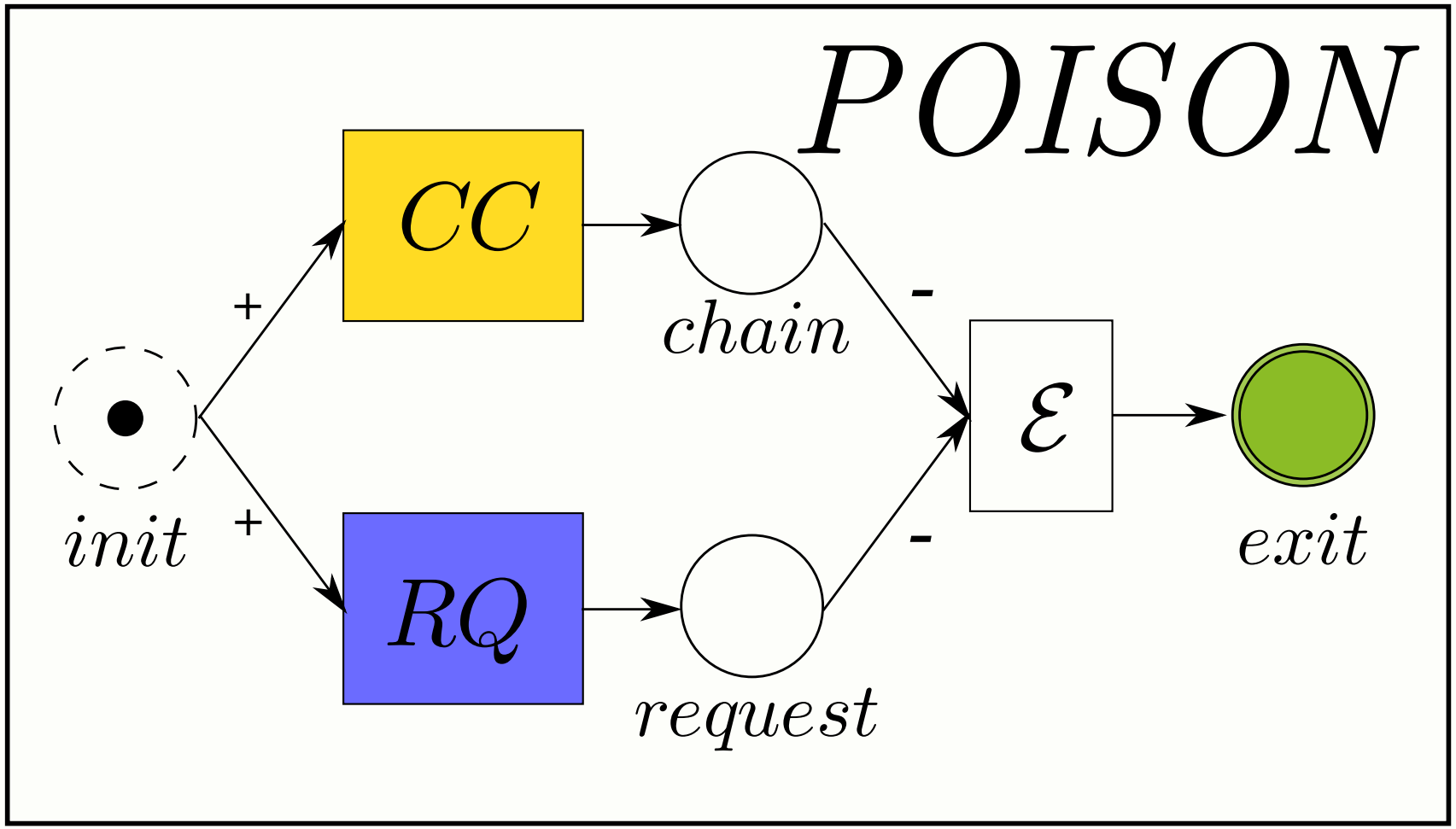
Funktionale Anforderungen

- Beschreibung von Korrelationsaufgaben
  - Korrelationsaufgaben bestehen aus Korrelationsregeln
  - Filter, Transformation, Aggregation und Komposition können als (mehrschrittige) Signaturen modelliert werden
  - EDL beschreibt komplexe, mehrschrittige Ereignisse
- Modellierung des Alarmkontexts
  - EDL erlaubt eine direkte Modellierung von Ereignisinstanzen als Token

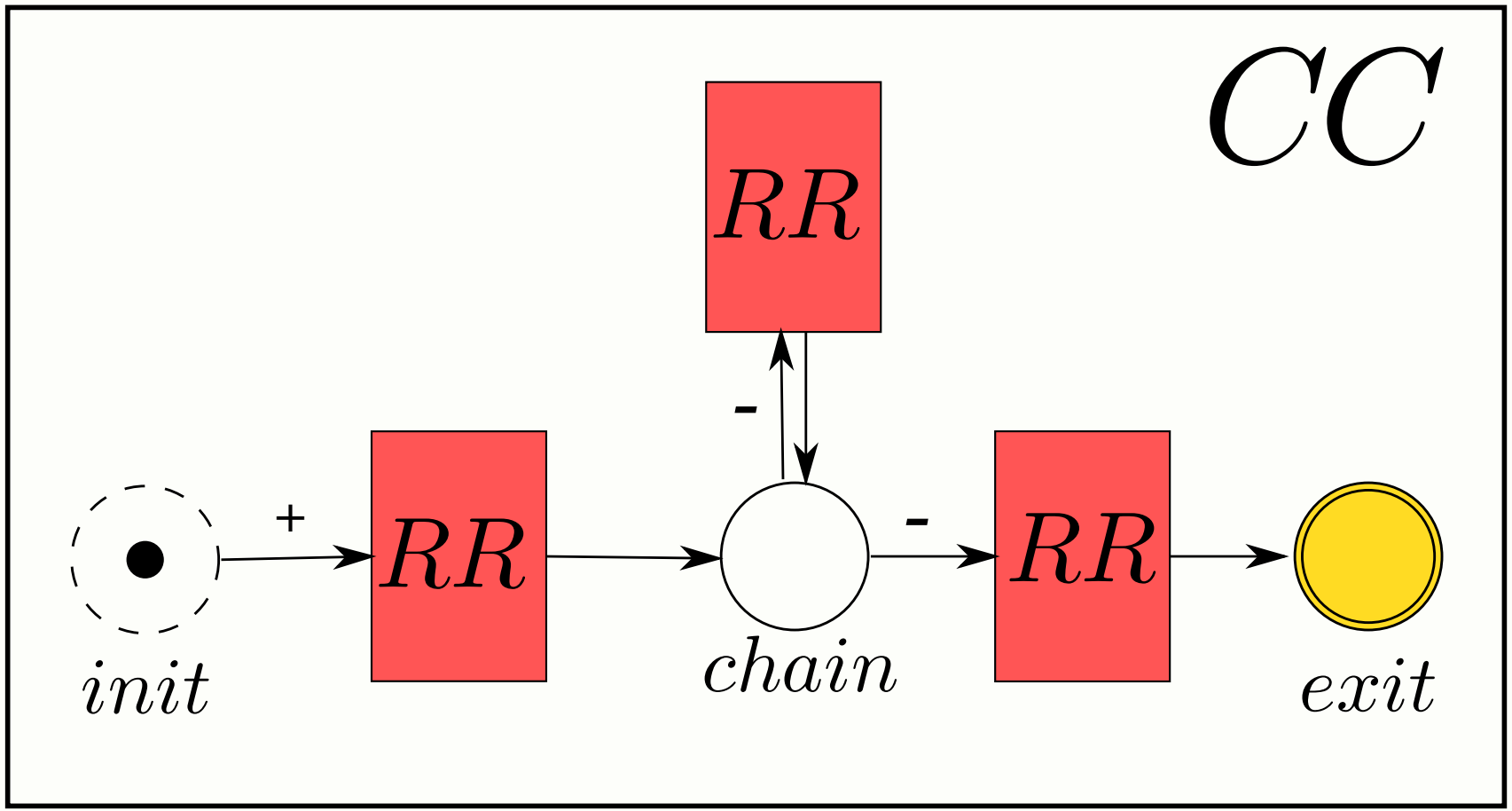
Beispiel: BIND 9 Cache Poisoning



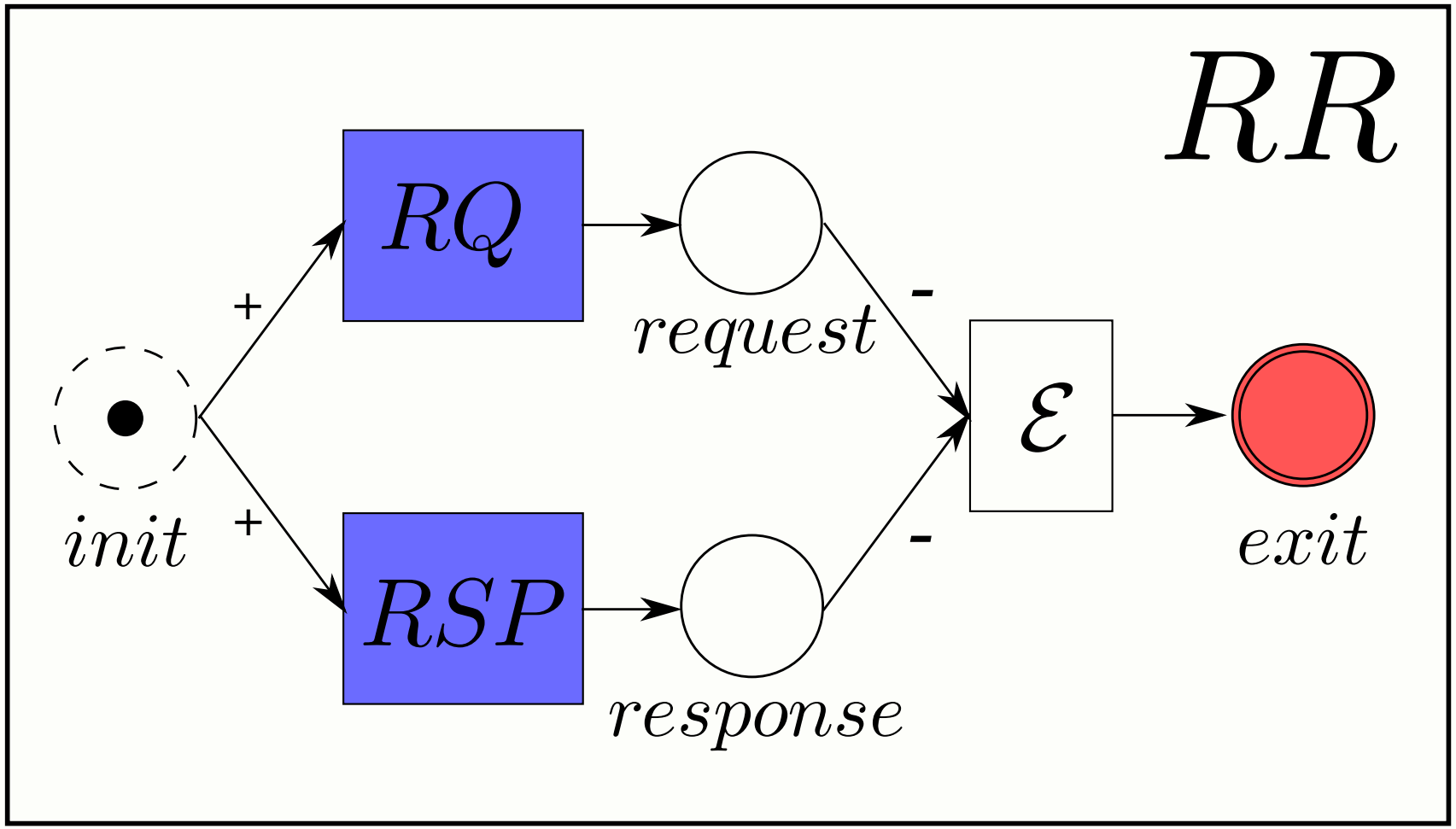
Beispiel: BIND 9 Cache Poisoning



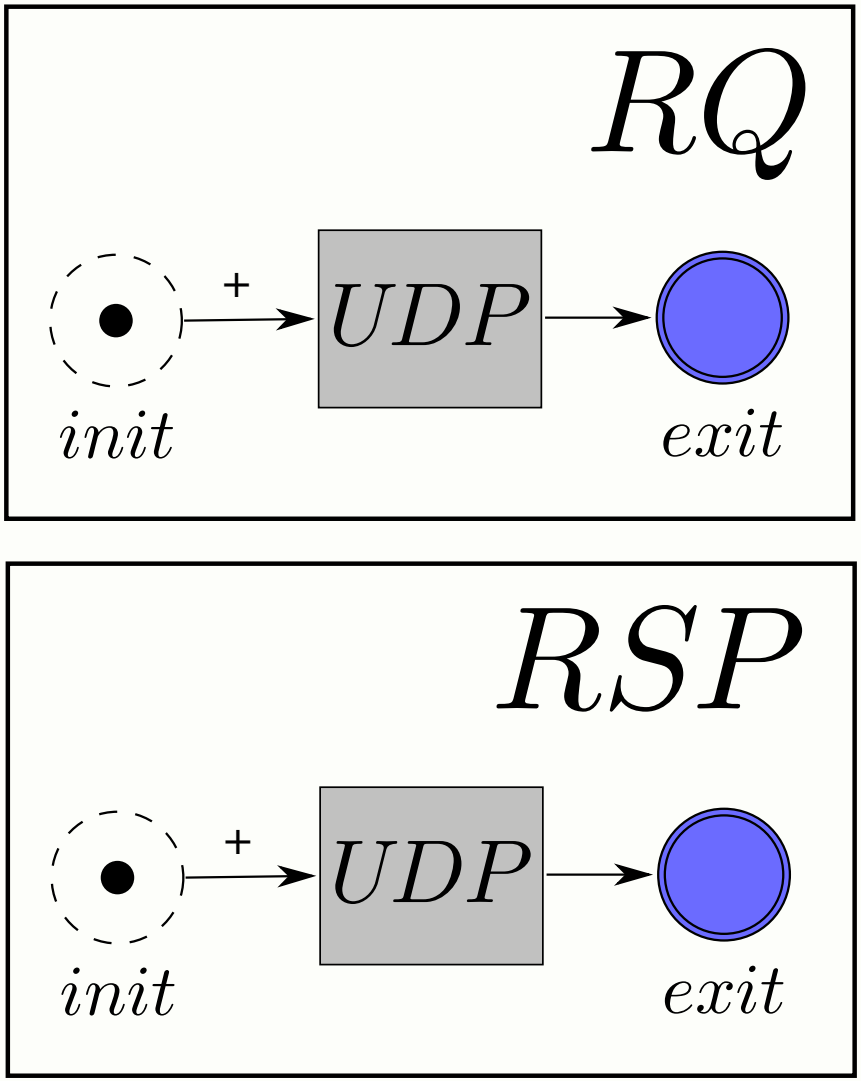
Beispiel: BIND 9 Cache Poisoning



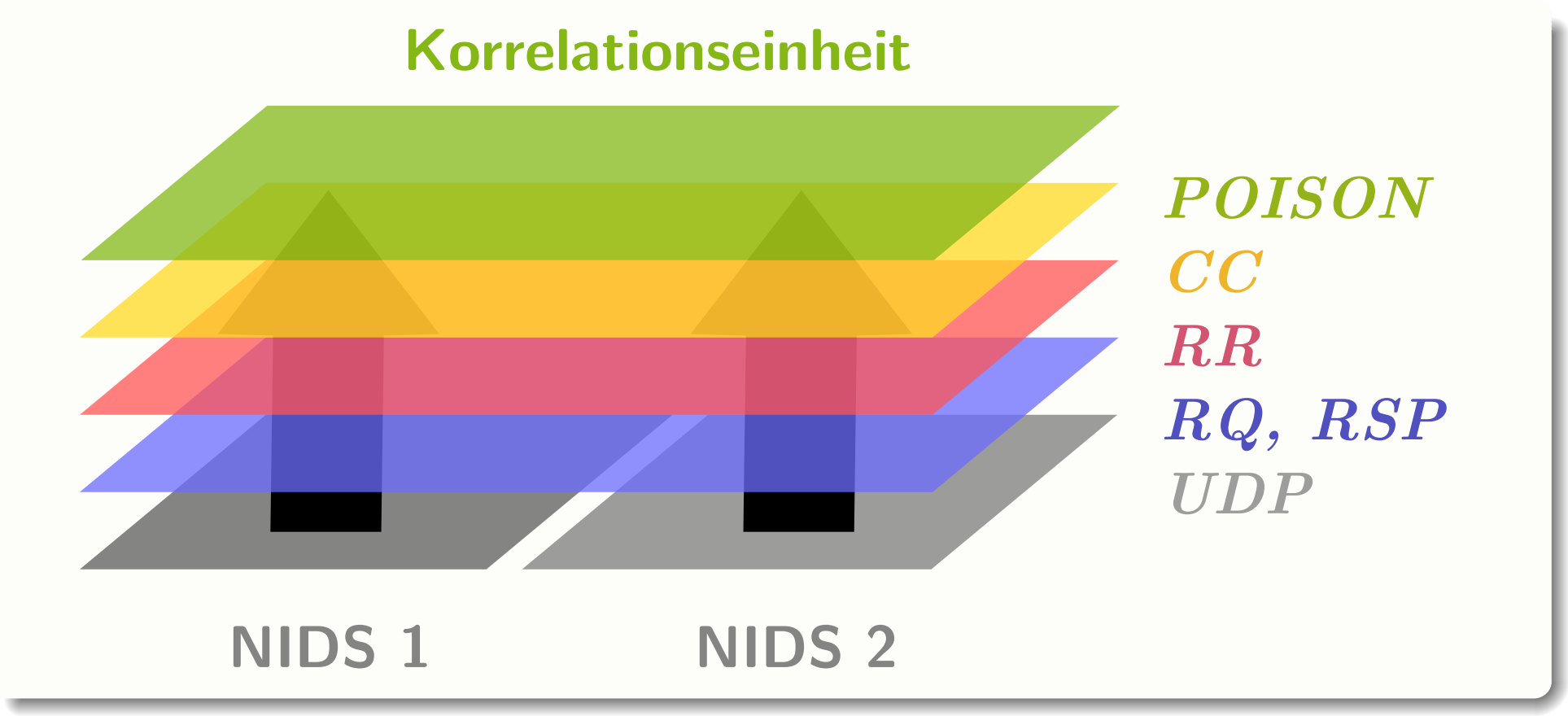
Beispiel: BIND 9 Cache Poisoning



Beispiel: BIND 9 Cache Poisoning

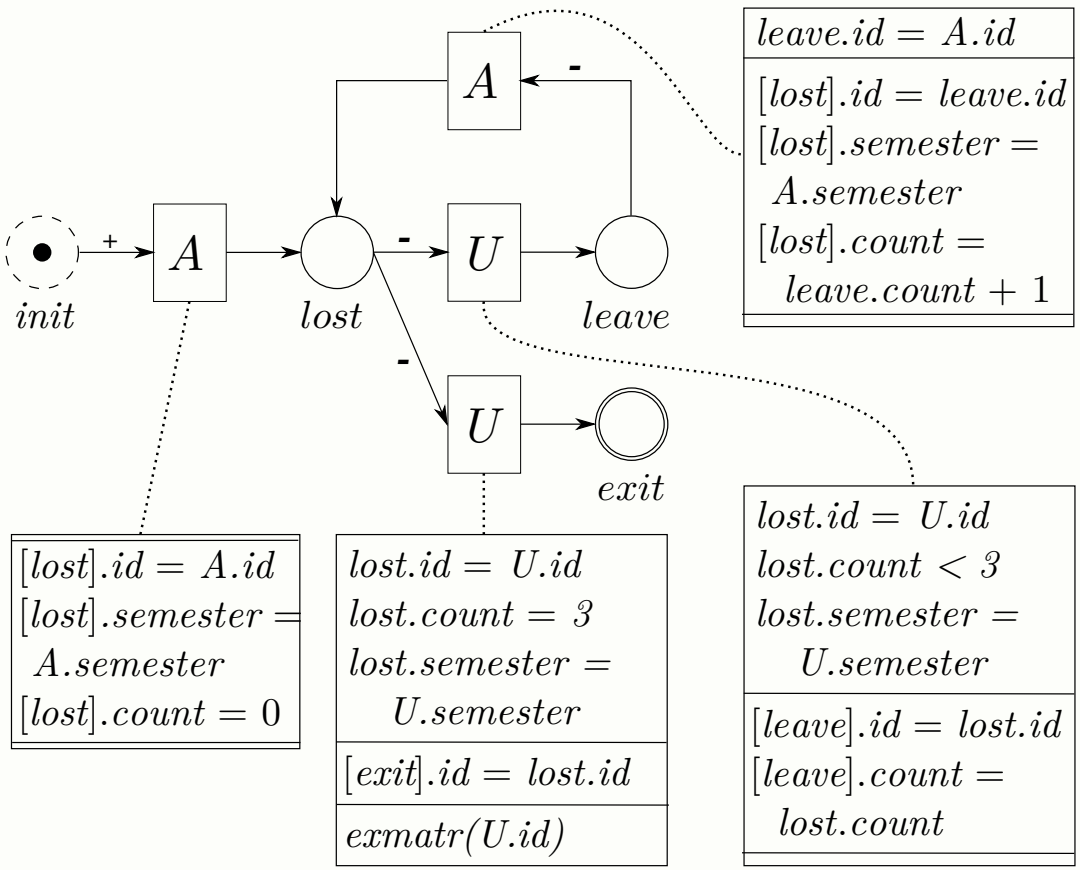


Beispiel: BIND 9 Cache Poisoning

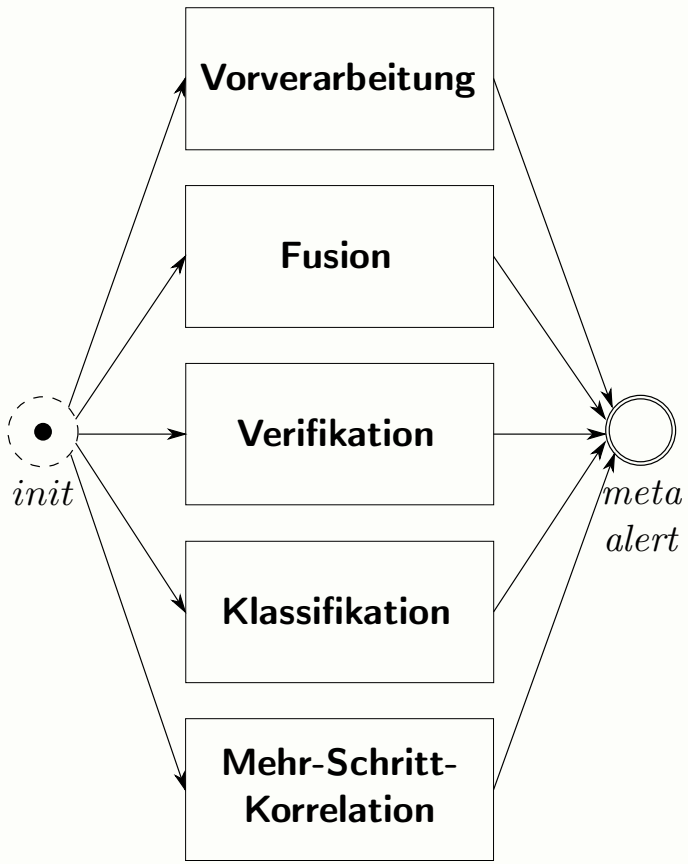


Beispiel: 15€ NRW-Ticket

- Alarm A: Student meldet Verlust des Studentenausweises
- Alarm U: Student meldet sich zum Urlaubssemester ab



Korrelationsprozess: Modellierung mit EDL-Signaturen



- Signatur beschreibt alle Stufen des Korrelationsprozesses für ein Alarmereignis
- Korrelationsstufen als EDL-Makros
- Ereignisinstanzen sind Resultate der Korrelationsstufen
- Merkmale kennzeichnen bereits durchlaufene Stufen (z. B. $fused$, $verified$)

Danke!

Vielen Dank für Eure Aufmerksamkeit.