

---

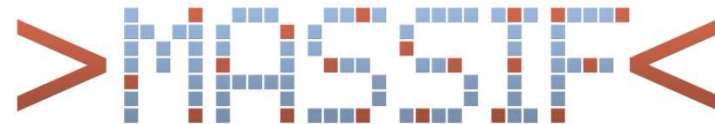
# A PROPERTY BASED SECURITY SIMULATION

A Property Based Security Risk Analysis Through Weighted Simulation

---

Timo Winkelvos, Fraunhofer SIT  
Darmstadt, Germany

ISSA Conference 2011



---

# A PROPERTY BASED SECURITY SIMULATION

---

1. Overview & Motivation
2. Components
3. Simulation
4. Conclusion & Challenges

# Agenda: Overview

1. Overview & Motivation
2. Components
3. Simulation
4. Conclusion & Challenges

# Overview & Motivation

Security Risk Analysis *means*

- probability
- system reaches state
- security properties are violated

How?

- probability
- system
- security properties



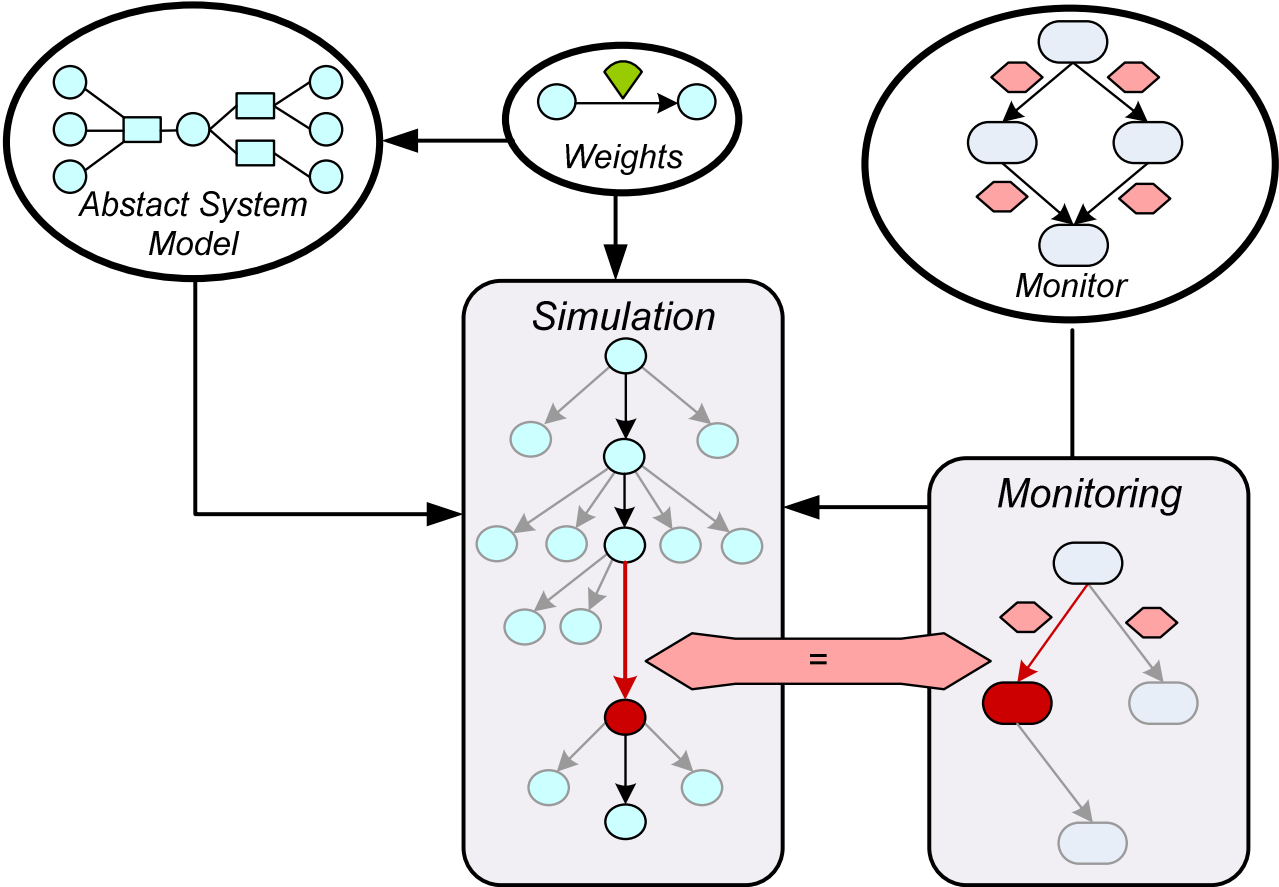
swayed random *Simulation*  
automata based *Model*  
*Monitor* automaton

# Overview & Motivation

## Security Risk Analysis *process*

- create a system model
- create the Monitor, representing (dynamic) security properties
- run the simulation
- concurrently validate the status using the monitor automaton
- collect behaviour of the Monitor
- analyse statistics thereof

# Overview



# Agenda: Components

1. Overview & Motivation
- 2. Components**
3. Simulation
4. Conclusion & Challenges

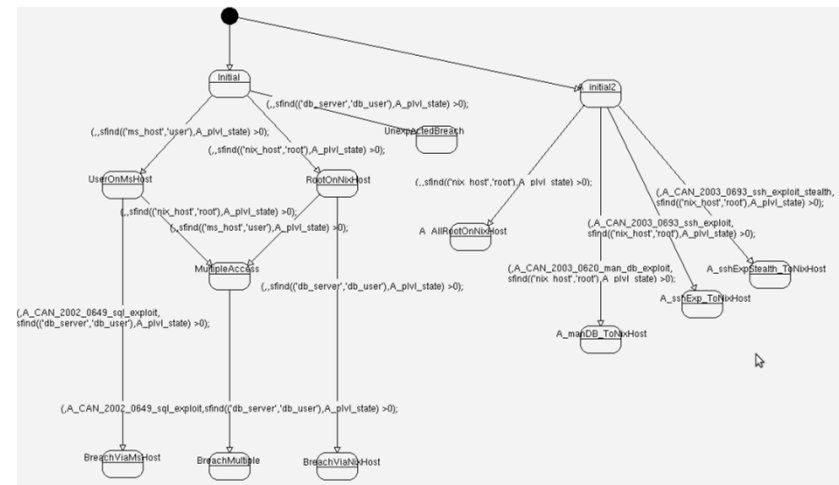
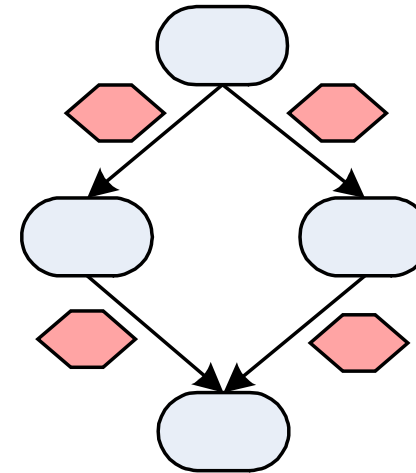


# Components

## The Monitor

### ■ Automaton

- named nodes
- edges
- represent logic predicates
- refer to present transition of the System Model
- pre- and post conditions of transition
- name of transition



# Components

## The Tool

- Tool: SHVT
  - Model Checker + abstraction tools
  - application: analyse network protocols, system specifications, etc
  - calculate reachability graph
    - graph algorithms
    - logic
    - further services

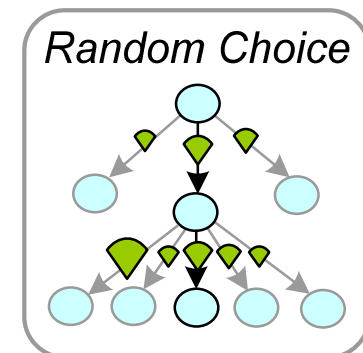
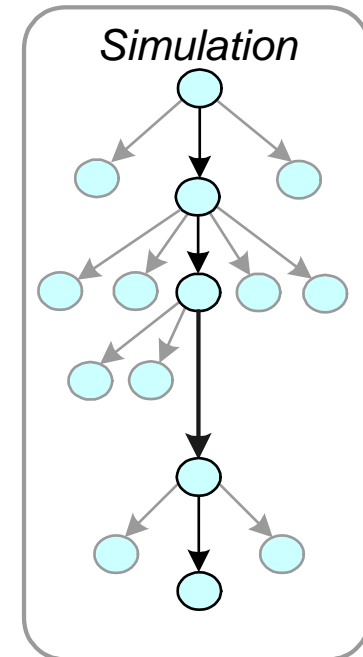
# Agenda: Simulation

1. Overview & Motivation
2. Components
- 3. Simulation**
4. Conclusion & Challenges

# Simulation

## Simulation Process

- for n cycles do:
  - start with  $s_0$
  - for any state do:
    - find alternatives  $t_i$
    - *randomly choose* next  $t_x$
    - apply it and *monitor*
  - until dead state or maximum depth
  - next cycle
- Cycle = random path through system



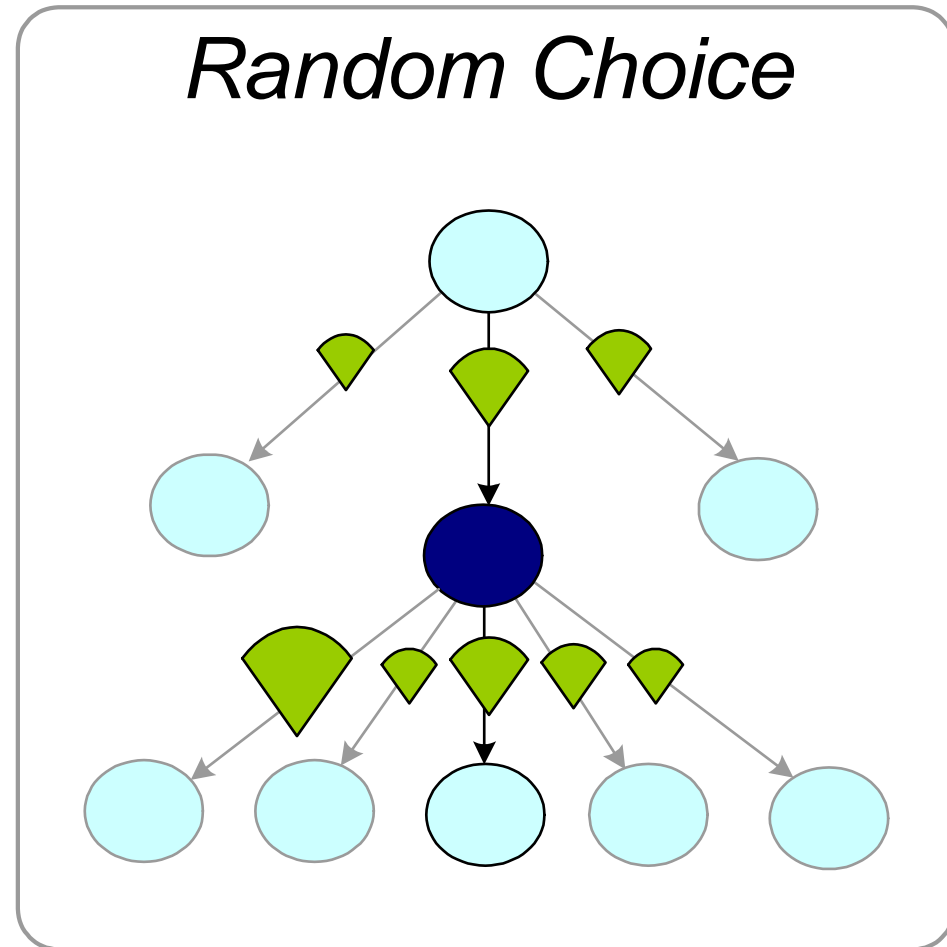
# Simulation

## Random Choice

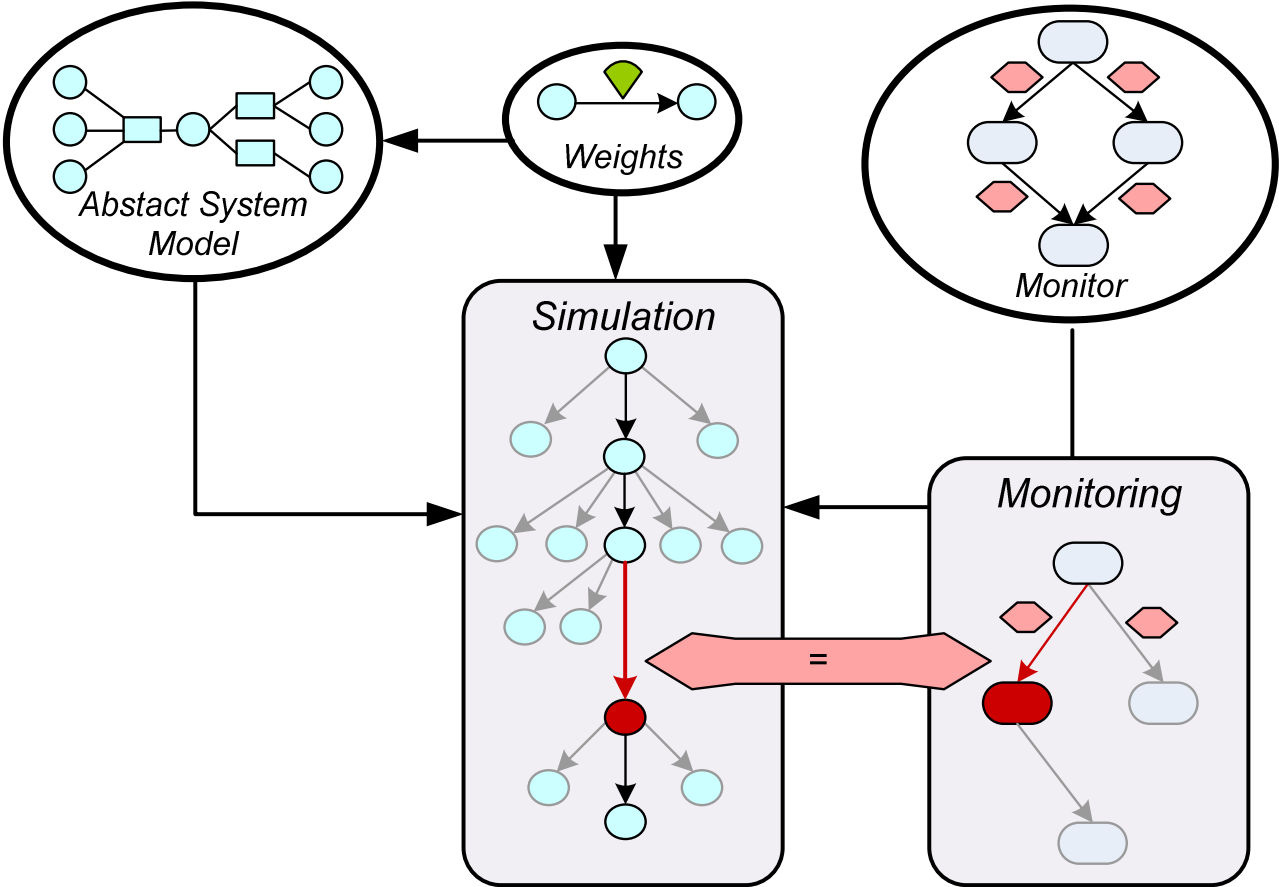
- Weights
  - relative classification of probability of probability

- choice of next transition  $t_x$

$$\mu_{s_x}(t_x) = \mu_{s_x}(g_x) = \frac{g_x}{\sum_j g_j}$$



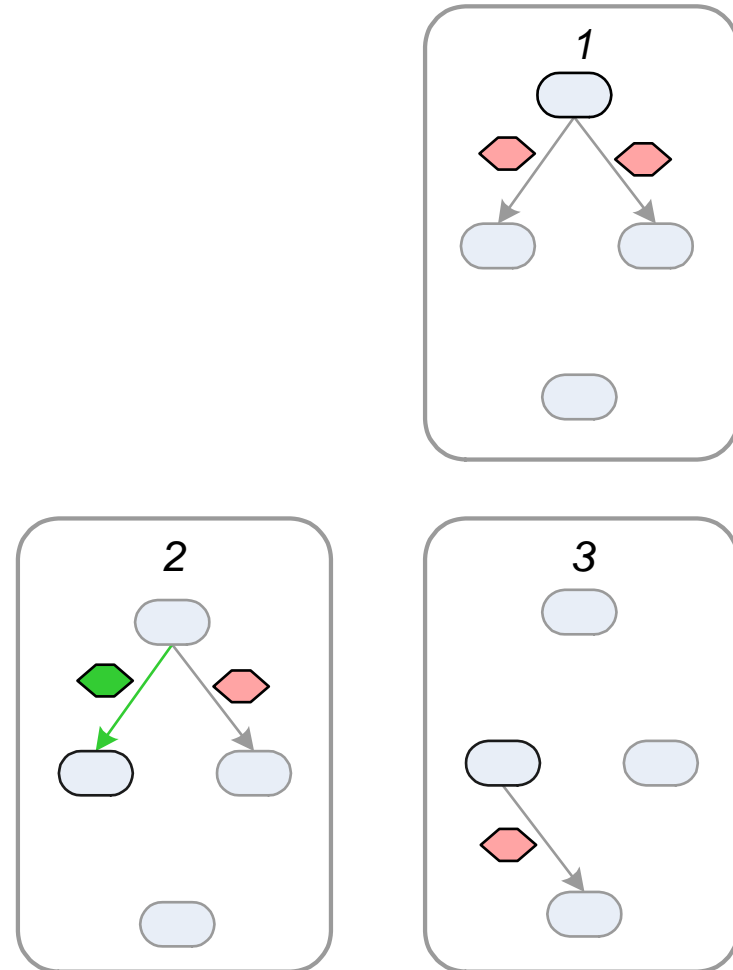
# Simulation



# Simulation

## Monitoring

- after any choice of transition
- all active predicates are validated
  - properties before, after and transition itself
  - $(pre, tn, suc) = true$
- any positive predicate triggers state change



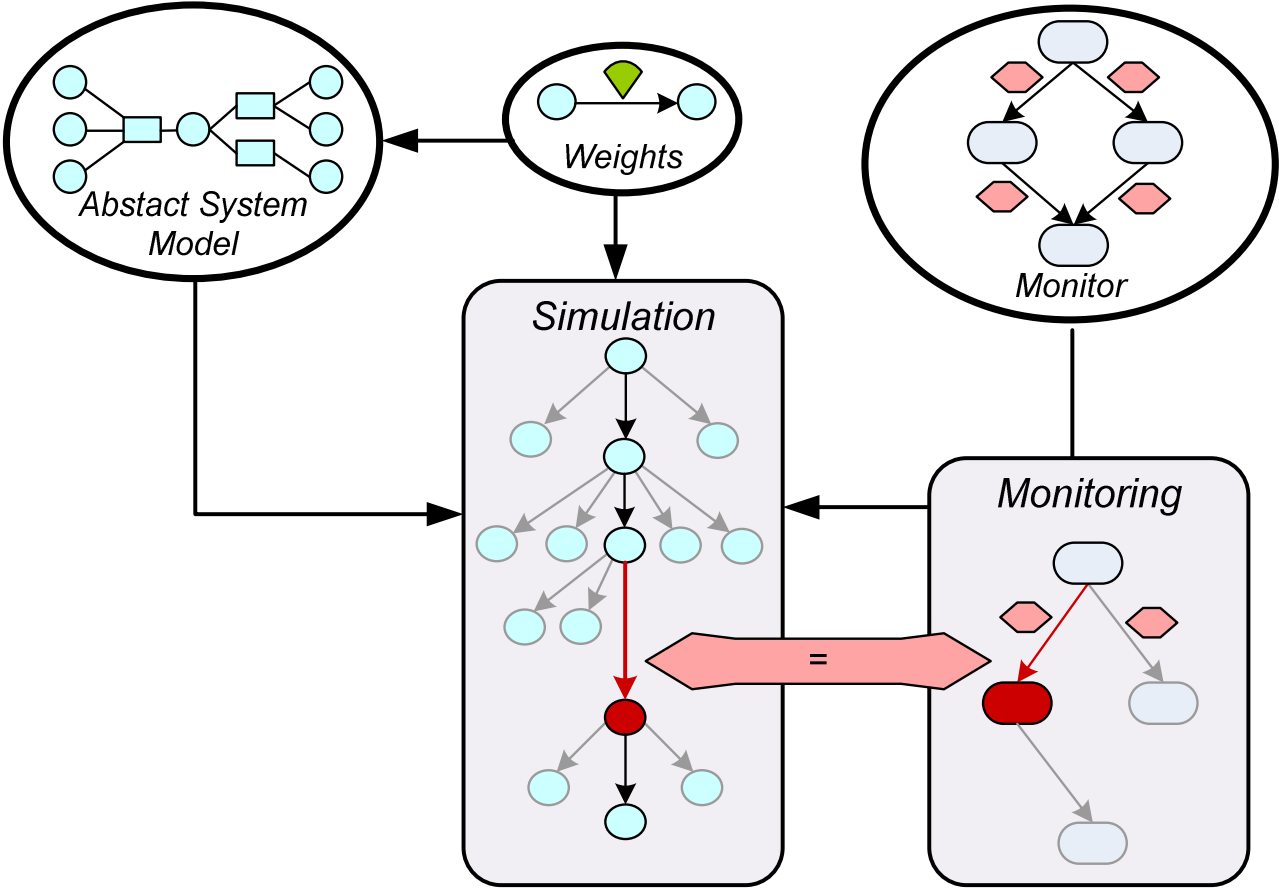
# Simulation

## Result

- collection of states and state changes of Monitor
- count how often does X happen?
- how many steps of simulation does the property hold?
- how does it come to that?
- *multiple active* states:
  - what other properties did hold at the same time?
- calculate *risk* in terms of ratio

Find root cause of security property violation!

# Simulation



# Agenda: Conclusion

1. Overview & Motivation
2. Components
3. Simulation
4. **Conclusion & Challenges**

# Conclusion & Challenges

## Simulation

- random choice of states with
  - unforeseeable transition alternatives
  - no quantification of all edges
  - future: risk analysis at runtime
- Weight factors
  - weight factors allow to sway/classify the choice
  - without knowledge of the respective state
  - interface with SIEM applications

# Conclusion & Challenges

## Risk Analysis

- dynamic security properties
  - Monitor: *process* of properties
  - *multiple active* states: situation of environment
- property oriented view
  - possibility to change *abstraction level*, still analyse same properties
  - includes *process* oriented properties

# Conclusion & Challenges

Outlook (as part of MASSIF project)

- risk forecast at runtime
  - continuous simulation
  - allow for changes while running sim
  - connect to SIEM via weights
  - via transitions
- analysis of complex system models including (business-, maintenance-, ...) processes
  - assumption: ambiguous alarms

# Conclusion & Challenges

## Outlook

- enhance statistic analysis
  - size of probes
  - variance of small probabilities
- enable simple creation of models (not lisp dialect)
- automatic generation of system model (MASSIF Partner SPIIRAS)

# Contact

Timo Winkelvos

Fraunhofer-Institute for Secure Information Technology  
Secure Engineering (formerly Security Modelling and Validation)

Rheinstraße 75  
D-64295 Darmstadt

Telefon: +49-6151-869-257

E-Mail: [timo.winkelvos@sit.fraunhofer.de](mailto:timo.winkelvos@sit.fraunhofer.de)

Internet: <http://www.sit.fraunhofer.de>

---

# A PROPERTY BASED SECURITY SIMULATION

A Property Based Security Risk Analysis Through Weighted Simulation

---

Thank You

