

Serums Healthcare System: Completed and Secured

Eduard Baranov, Axel Legay

APPS 2022

University of St Andrews

zuyderland

accenture

IBM

sopra steria

scch { software competence center hagenberg }

University of Cyprus

UCLouvain

FUNDACIÓ CLÍNIC BARCELONA

University of Dundee

Introduction
Needs for Verification

- **Working with personal data**
  - Need for correctness and security
- **Is testing sufficient?**
  - No bugs found != system is correct
- **Formal methods**
  - Mathematical evidence for the result

Serums

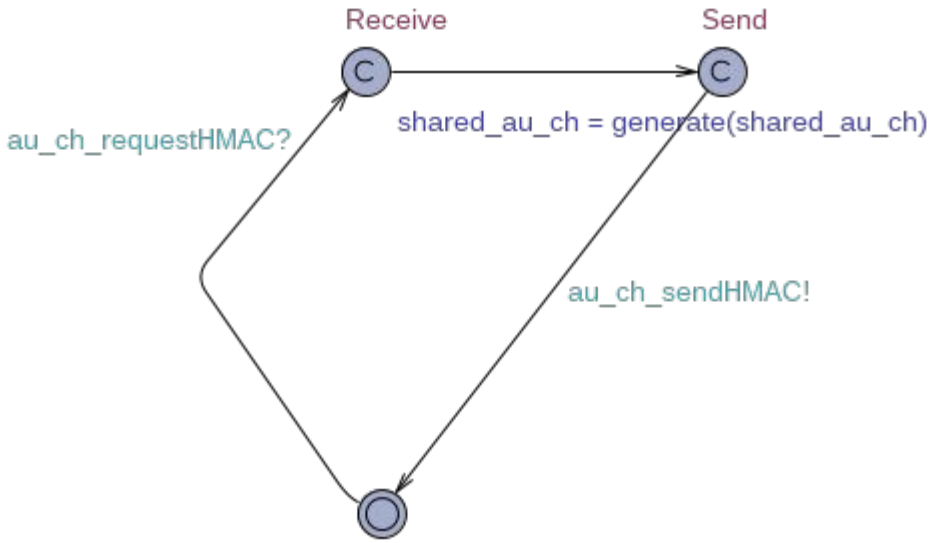
Introduction
Formal Methods - Model Checking

- **System model in formal language**
  - Based on Labelled Transition Systems
- **Set of properties**
  - Properties expressed in Temporal Logic
- **Verification tool**
  - We used Uppaal

Serums

Serums Model
Overview

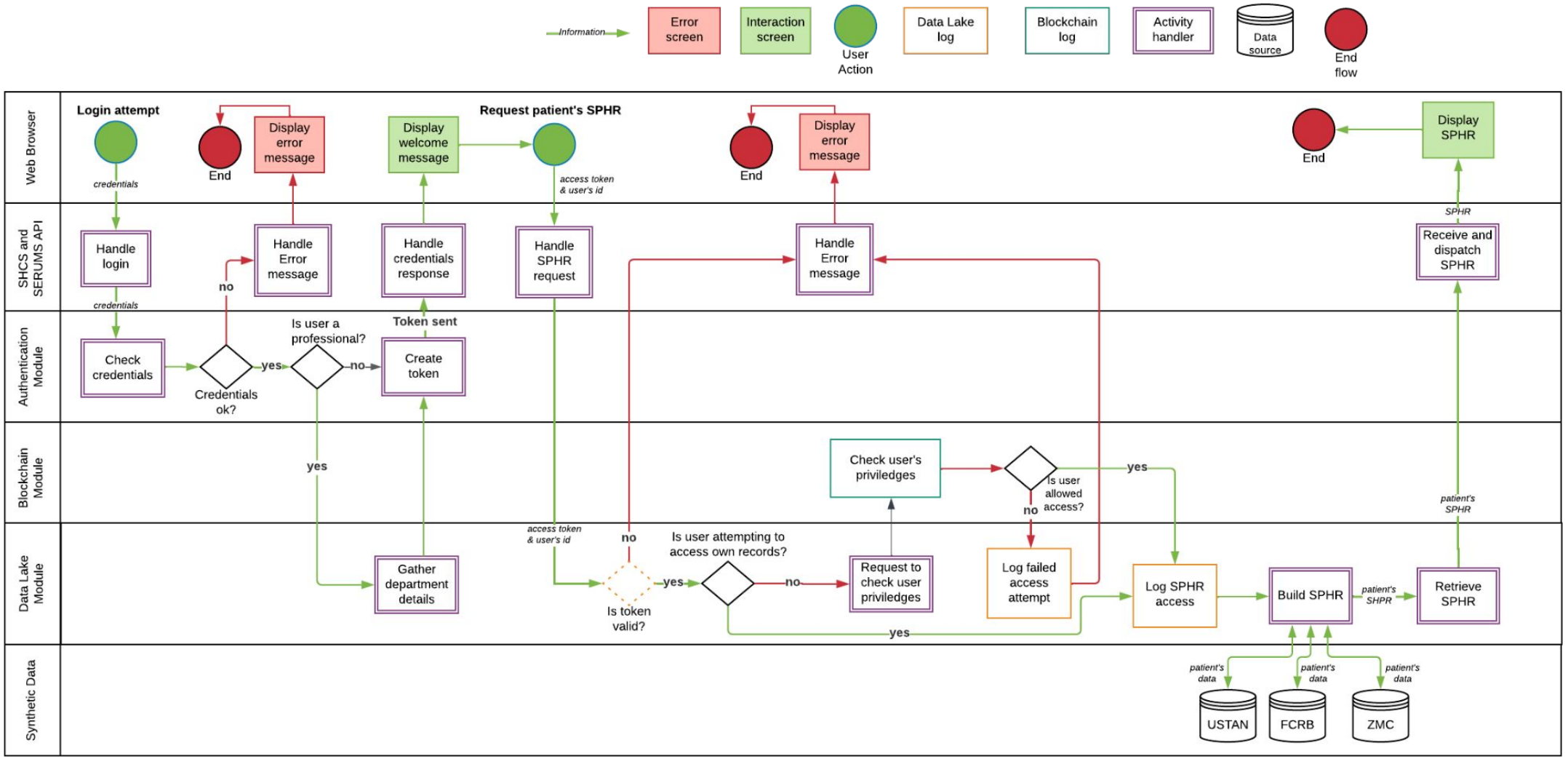
- **Network of timed automata**
- **Automata for**
  - Serums components
  - Users
- **Channels for synchronisation**
  - Interactions between components



Serums

Serums Model

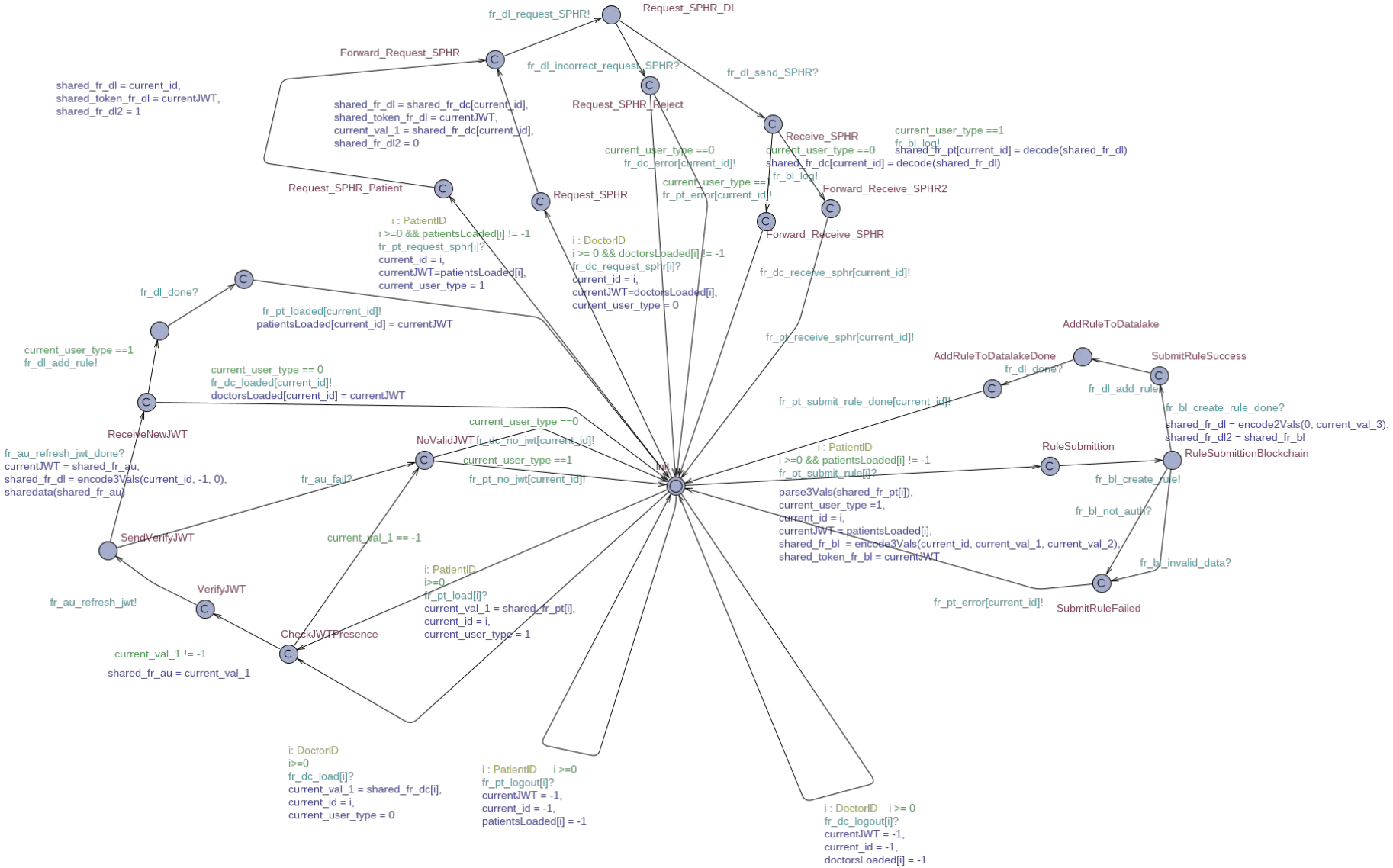
Serums Workflow



Note: Patient and doctor roles for same person, it is coded with different IDs in the system, so the functions available follow the current user type logged in the system.

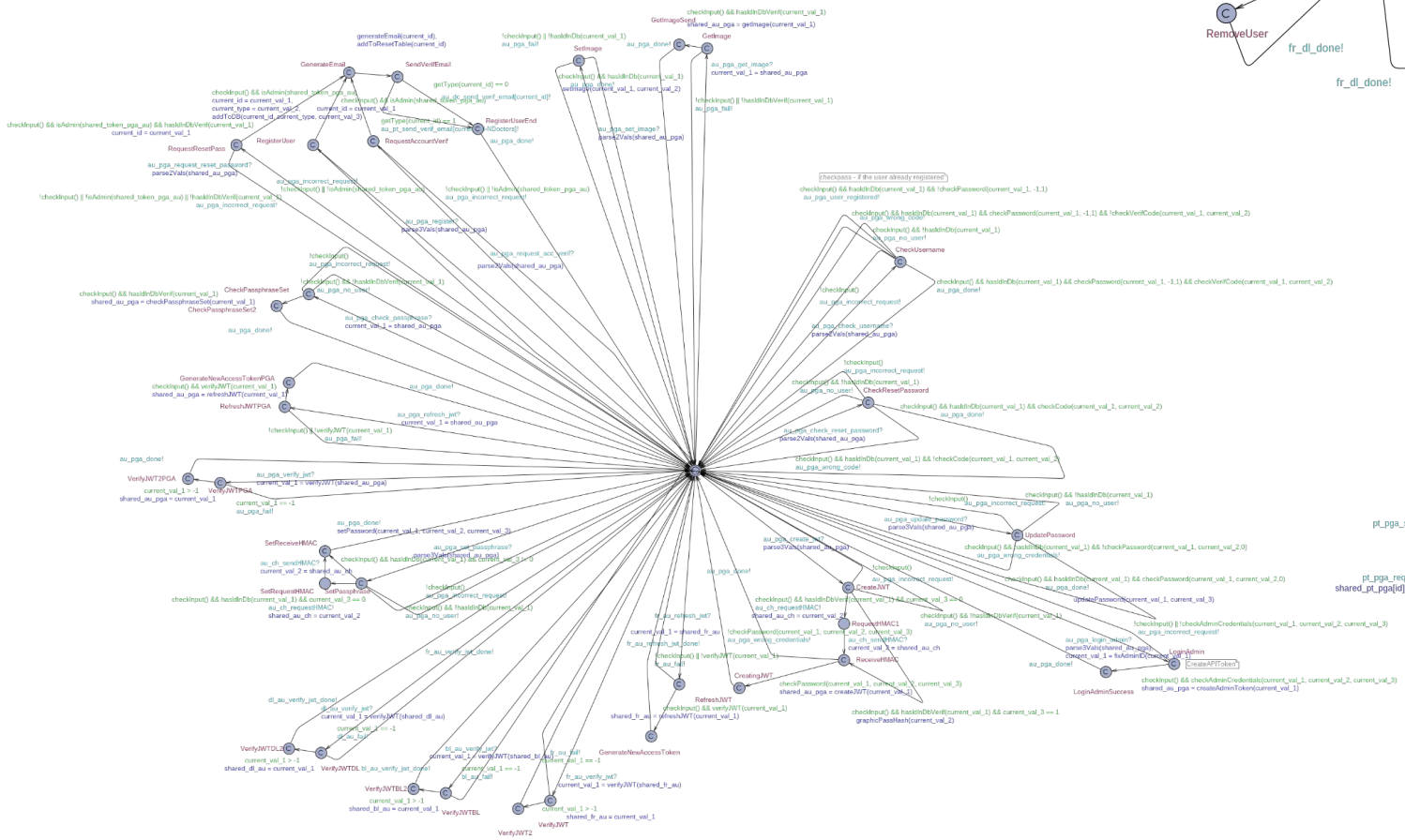
Serums

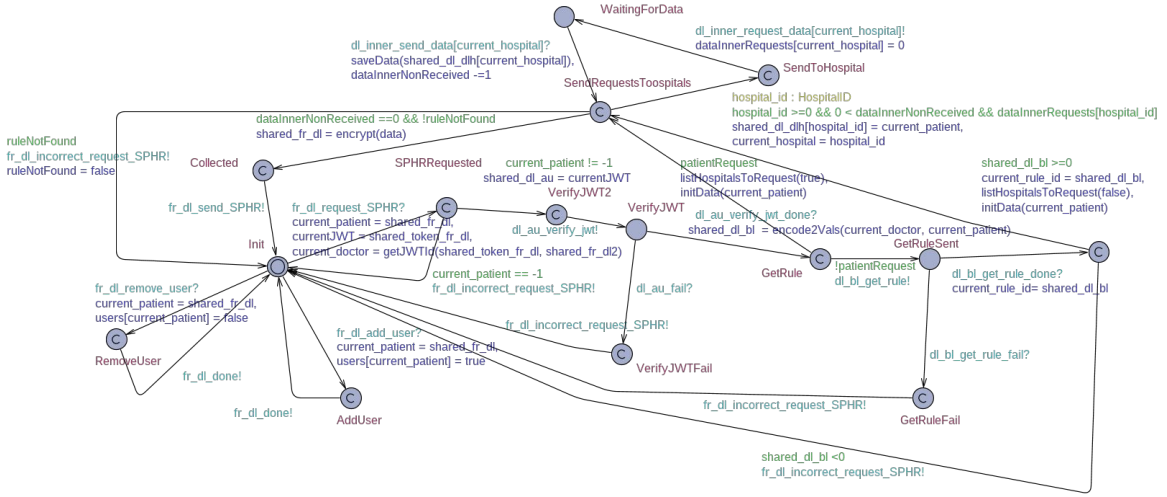
Serums Model
SHCS Component

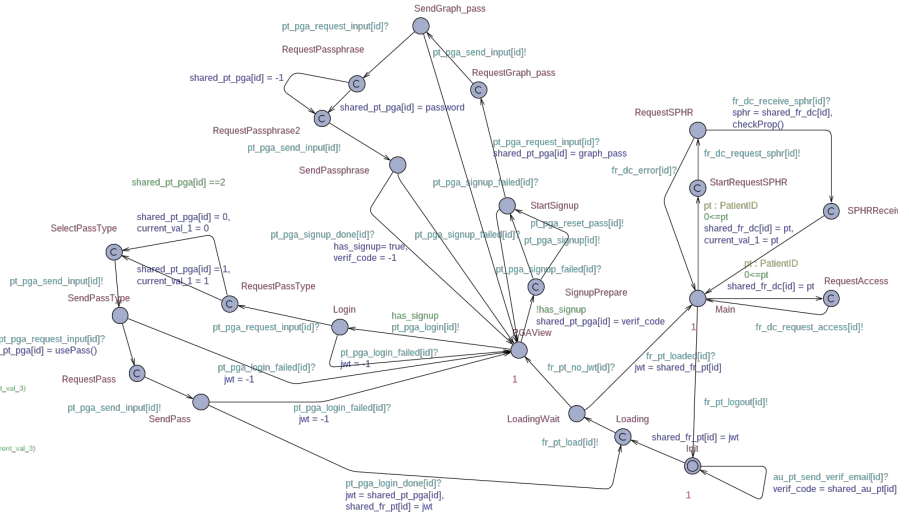


Serums

Serums Model
Automata Examples



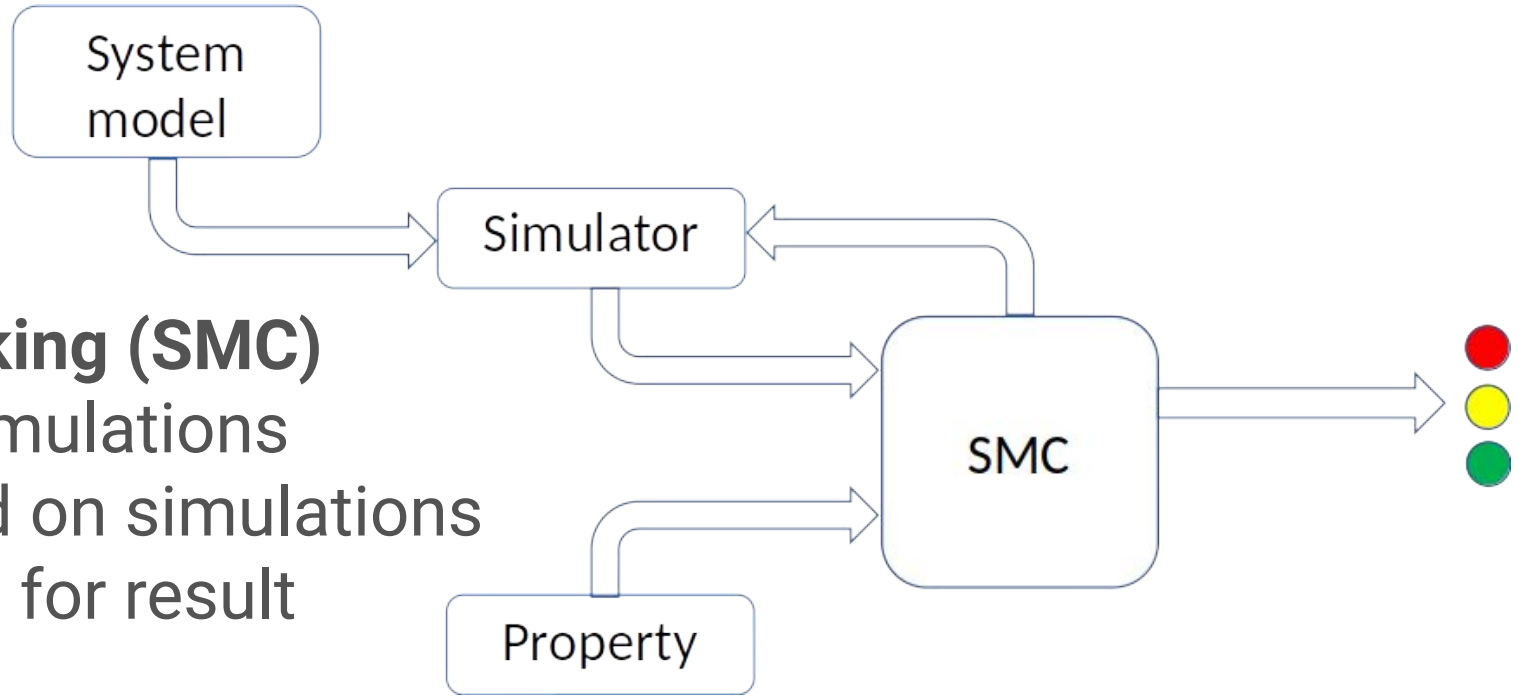




Serums

Verification
Statistical Model Checking

- **Temporal Logic**
  - MITL
  - Working on traces
- **Statistical Model Checking (SMC)**
  - Large number of simulations
  - Property is checked on simulations
  - Statistical methods for result



Serums

Verification
Uppaal SMC

- **Liveness**
  - Non-zero probability
  - E.g. “A user can login to the system”

- **Safety**
  - Probability close to 1
  - E.g. “A doctor can receive patient’s medical data only if the patient granted access”

- **<20 min for 0.9999 confidence**

Serums

Verification
Security Properties

- **Attacker does not follow “expected” behaviour**

- **Modify user’s automata to**
  - send different inputs
  - connect to different endpoints

What if a user sends wrong inputs?
What if a doctor requests data directly from Data Lake?

Serums

Conclusion

- **Formal methods can support design and development**
  - Important for systems requiring safety and security
- **Statistical Model Checking scales to real systems**
  - Several minutes on standard pc
- **Mathematical evidence for properties satisfaction**

Serums



THANK YOU!

University of St Andrews

zuyderland

accenture

IBM

sopra steria

scch { software competence center hagenberg }

University of Cyprus

UCLouvain

FUNDACIÓ CLÍNIC BARCELONA

University of Dundee