A Methodology for Testing IPSec-based Systems

Uljana Boiko, Antonietta Lo Duca

ALaRI Institute,

University of Lugano

E-mail: {boiko, loduca}@a.alari.ch

Alberto Ferrante, Vincenzo Piuri

DTI,

University of Milan

E-mail: {ferrante, piuri}@dti.unimi.it

Presentation Outline

1. Introduction to IPSec;
2. Testing Methodology;
3. UML Specifications;
4. Conclusions and Future Work.

1/4. IPSec (1)

- Is a suite of protocols
  - adding security at IP (network) level;
- is very flexible;
- is very complex;
- we can have HW only, SW only, or mixed HW/SW implementations.

1/4. IPSec (2) - AH, ESP

- Is composed of two protocols:
  - Authentication Header (AH);
  - Encapsulating Security Payload (ESP);
- both protocols can be used in:
  - transport mode;
  - tunnel mode.

1/4. IPSec (3) - DBs

- IPSec uses two databases:
  - the Security Policy Database (SPD);
  - the Security Association Database (SAD):
    - the records are the Security Associations (SAs).

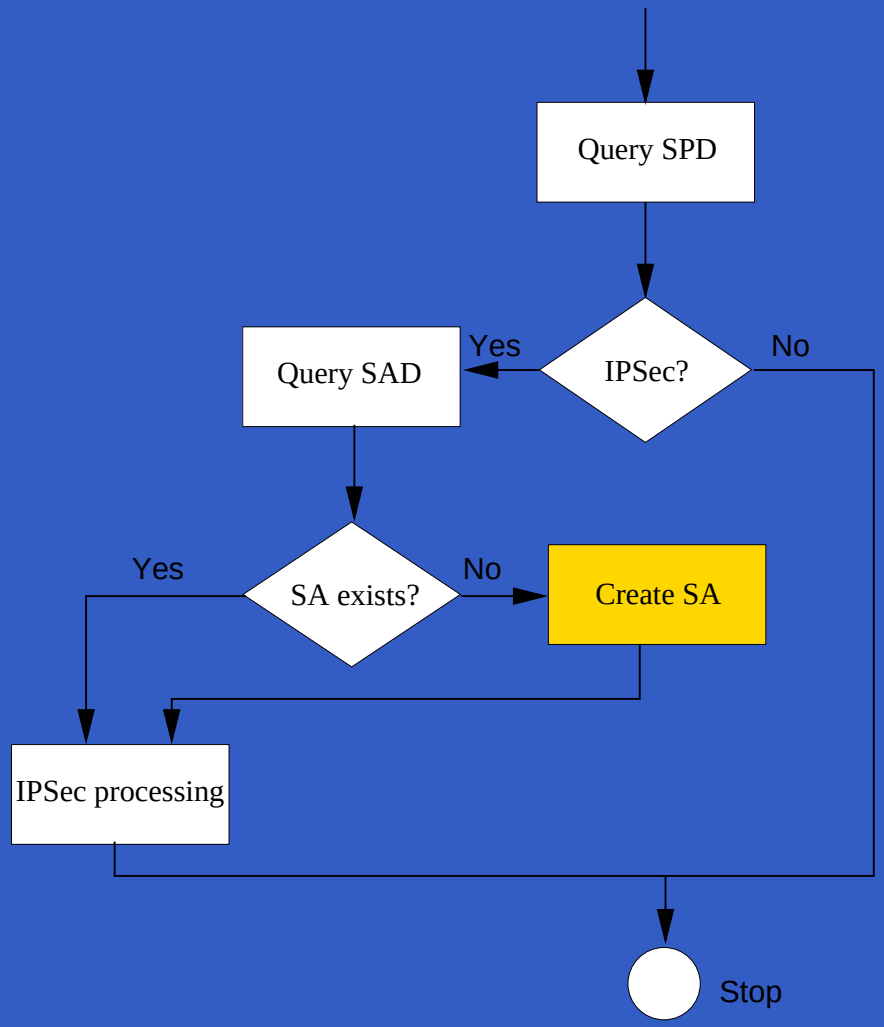
1/4. IPSec (4) - Security Associations

- Each SA contains:
  - protocol/algorithms settings;
  - keys for cryptographic algorithms;
- SAs are mono-directional:
  - two SAs need to be created for normal bidirectional communications.

1/4. IPSec (5) - IKE

- Internet Key Exchange (IKE) was taught to be used with IPSec to negotiate:
  - key exchange;
  - IPSec parameters;
- it creates the SAs;
- it allows many operational modes;
- IKEv2 is under development.

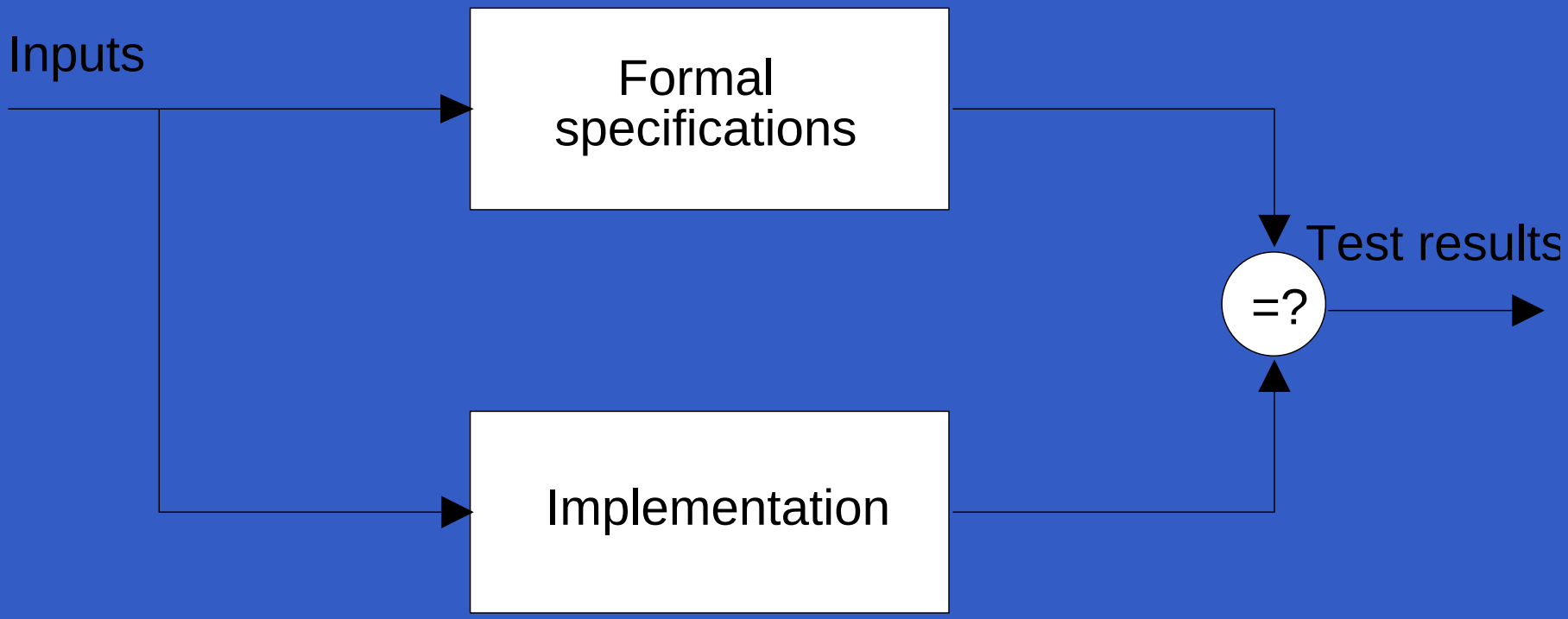
1/4. IPSec (6) – Packet Processing



2/4. Testing Methodology (1)

- We can perform:
  - functional testing;
  - interoperability testing;
- we are focusing on functional testing.

2/4. Testing Methodology (2)



University of Lugano
ALaRI
DTI

2/4. Testing Method. (3) - Model (1)

- Model is written in UML:
  - flexible and powerful;

- **class diagram**:
  - to describe the general structure of IPSec;
  - to describe the relations between different parts of IPSec.

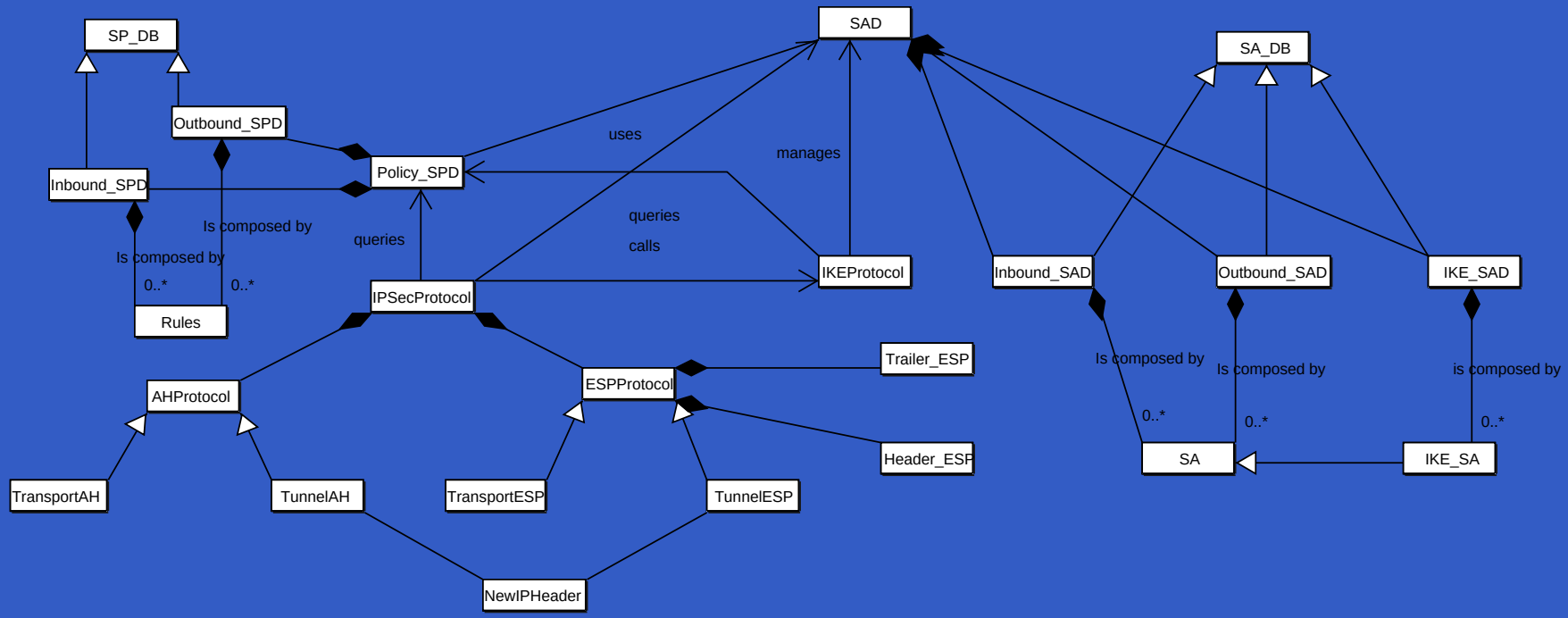
2/4. Testing Method. (4) - Model (2)

- **statecharts diagrams**:
  - used to describe the behavior;
  - formal language;
  - diagram nesting allows for a concise representation.

2/4. Testing Methodology (5)

- The UML model is also used to generate test patterns:
  - the *transition coverage* criterion has been used on statecharts;
- test patterns are composed of:
  - protocol settings;
  - inputs to be applied;
  - outputs.

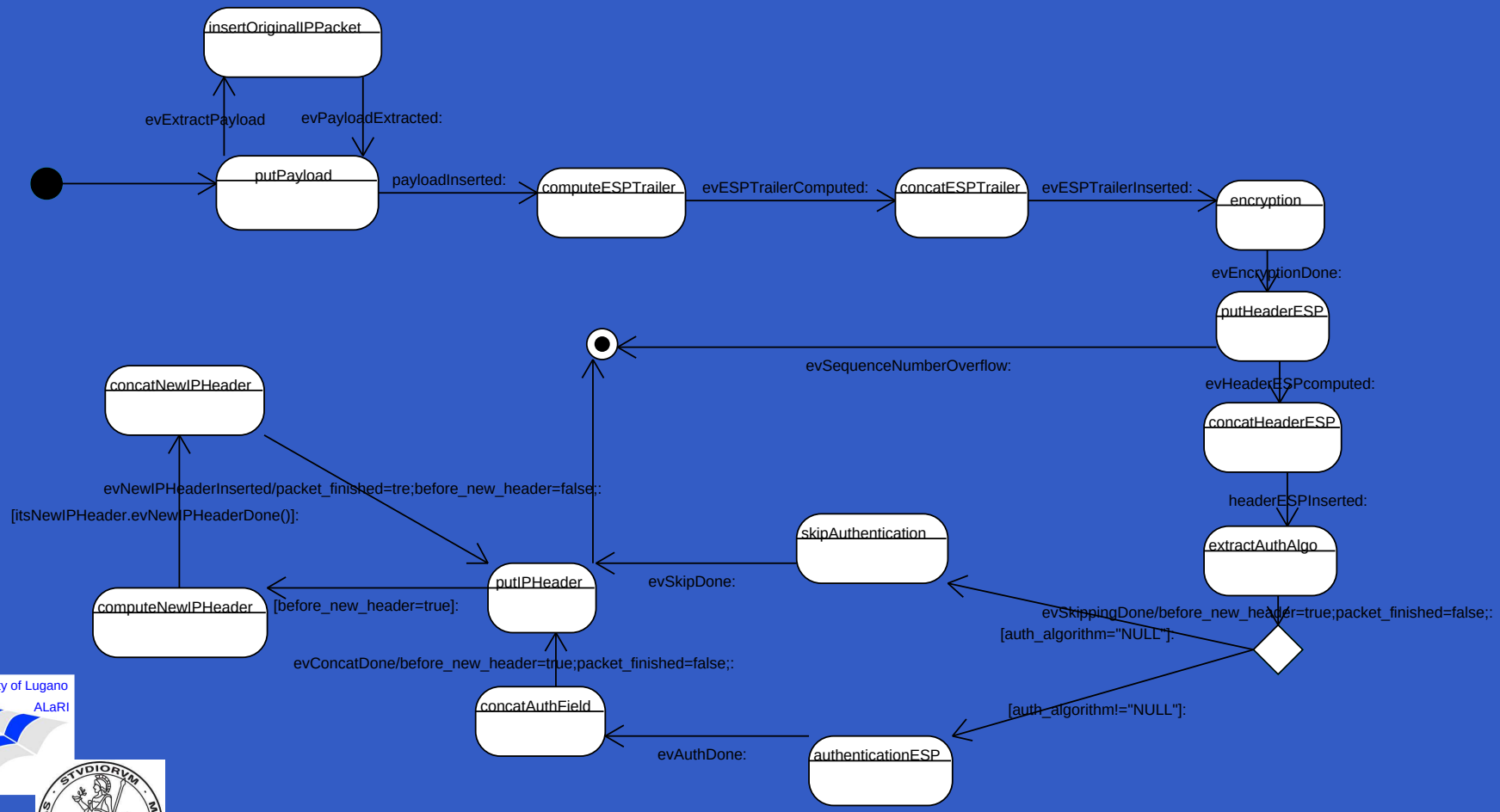
3/4. UML Model – Class Diagram



University of Lugano
ALaRI

DTI

3/4. UML – *TunnelESP* Statecharts



University of Lugano
ALaRI

DTI

4/4. Conclusions

- We have developed
  a testing methodology for IPSec;
- we have proved that
  the proposed solution is viable;
- we have developed
  an almost complete UML model of IPSec.

4/4. Future Work

- IPSec model will be completed and validated;
- different coverage criteria will be explored;
- connections between different settings (e.g., algorithms) will be explored to reduce the number of test cases.