On the Secure Software Development in Early Stages within UML Profiles

Ricardo J. Rodríguez
rjrodriguez@unizar.es
http://www.ricardojrodriguez.es

Universidad Zaragoza

19th September, 2011

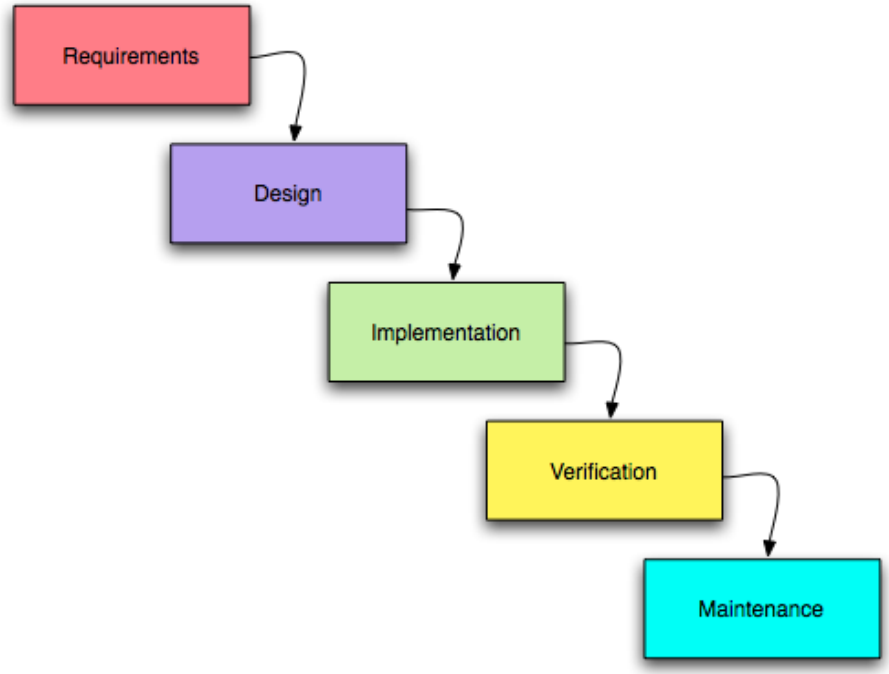
This work has been developed in collaboration with **Simona Bernardi** (Centro Universitario de la Defensa) and **José Merseguer** (Universidad de Zaragoza)

7th **Hack.LU**

Luxembourg, Luxembourg Grand-Duché

Motivation (I)

Development Cycle Phases



Analysis

- Requirements (properties):
  - Functional: what the system does
    - Technical data, data processing...
  - Non-functional: how the system does
    - No. of clients to attend, transfer speed...
- *Requirements engineer* role

Universidad Zaragoza 1542

Motivation (II)

Requirements analysis

- Functional: (more or less) obvious
- What about non-functional?
  - Constraints, usability, performance...
- After this: *systems engineer + software engineer*

Security: the Forgotten One (1)

- Non-functional property of the system
- Lack of interest
- Consequence: "fix it later"
  - Fix the problem when the problem raises...

Universidad Zaragoza 1542

Motivation (III)

Security: the Forgotten One (2)

- Severe consequences
  - High cost reimplementation/redesign
  - Financial looses
  - Down services $\rightarrow$ less customers
  - Disclosure of confidential data (e.g., Sony PSN)

Who pays?

- Requirements engineer?
- Systems engineer?
- Software engineer?

1542

Motivation (III)

Security: the Forgotten One (2)

- Severe consequences
  - High cost reimplementation/redesign
  - Financial looses
  - Down services $\rightarrow$ less customers
  - Disclosure of confidential data (e.g., Sony PSN)

Who pays?

- Requirements engineer?
- Systems engineer?
- Software engineer?
- Subprime lending?

1542

Motivation (III)

Security: the Forgotten One (2)

- Severe consequences
  - High cost reimplementation/redesign
  - Financial looses
  - Down services $\rightarrow$ less customers
  - Disclosure of confidential data (e.g., Sony PSN)

Who pays?

- Requirements engineer?
- Systems engineer?
- Software engineer?
- Subprime lending?
- All of'em (no, subprime crisis not here...) & nobody

1542

Motivation (IV)

So, then what?

- Minimum of security knowledge
- Think on security on ALL development phases
- Methodology change $\rightarrow$ *Secure Software Engineering*

Universidad Zaragoza 1542

Motivation (IV)

So, then what?

- Minimum of security knowledge
- Think on security on ALL development phases
- Methodology change $\rightarrow$ *Secure Software Engineering*

Security:
from the beginning to the end

Universidad Zaragoza
1542

Related work (I)

Requirements, architecture & aspects...

- Requirements analysis
  - Haley et al. (*SESS*, 2006)
  - Wolter et al. (*Requir. Eng.*, 2010)
- Architecture
  - Schmidt et al. (*SA*, 2006)
  - Yskout et al. (*ARES*, 2008)
  - Abi-Antoun et al. (*ASE*, 2010)
  - Heyman et al. (*ESSoS*, 2011)
- Aspect-oriented
  - Braga et al. (*SoSym*, 2010)
  - Georg et al. (*TSE*, 2011)

Universidad Zaragoza 1542

Related work (II)

Methodologies, patterns & formal methods...

- Design frameworks
  - Mouratidis et al. (*CAiSE*, 2003)
  - Islan et al. (*SoSym*, 2010)
  - Khan (*Comp. F & S, Aug 2011*)
  - SDL (Microsoft)
- Security patterns
  - Fernández (*SERP*, 2004)
  - Halkidis et al. (*TDSC*, 2008)
- Formal methods (automata or Petri nets)
  - Schneider (*TISSEC*, 2000)
  - Horvath et al. (*SESS*, 2008)
  - Patzina et al. (*SD4RCES*, 2010)

Universidad Zaragoza 1542

Related work (III)

Semi-formal methods...

- Using UML
  - Jürgens (UMLSec, *UML*, 2002)
  - Lodderstedt et al. (SecureUML, *UML*, 2002)
  - Goudalo et al. (*SECURWARE*, 2008)

Universidad Zaragoza 1542

Related work (III)

Semi-formal methods...

- Using UML
  - Jürgens (UMLSec, *UML*, 2002)
  - Lodderstedt et al. (SecureUML, *UML*, 2002)
  - Goudalo et al. (*SECURWARE*, 2008)

UML-based approach

- Standard *de facto*
- Structural and behavioural system aspects
- Well-known $\rightarrow$ does it make easier to add security?

Universidad Zaragoza 1542

Background (I)

UML profile: what?

- OMG standard
- Stereotypes and tagged values

Background (I)

UML profile: what?

- OMG standard
- Stereotypes and tagged values
- Annotate UML elements
  - Expressing Non-Functional Properties (NFP) on the UML designs
  - Extending model semantic

OMG example

- *Modelling and Analysis of RT Embedded systems* (MARTE)
  - Support for performance and schedulability analysis
  - NFPs expressed thru VSL (*Value Specification Language*) syntax

---

OMG. A UML profile for Modeling and Analysis of Real Time Embedded Systems (MARTE). *Document ptc/09-11-02*, 2009

Universidad Zaragoza 1542

Background (II)

Security definition (classic)

- Confidentiality
- Integrity
- Availability

Universidad Zaragoza
1542

Background (II)

Security definition (classic)

- Confidentiality
- Integrity
- Availability
- Tight relation with *dependability* (Avizienis)

Dependability UML profile

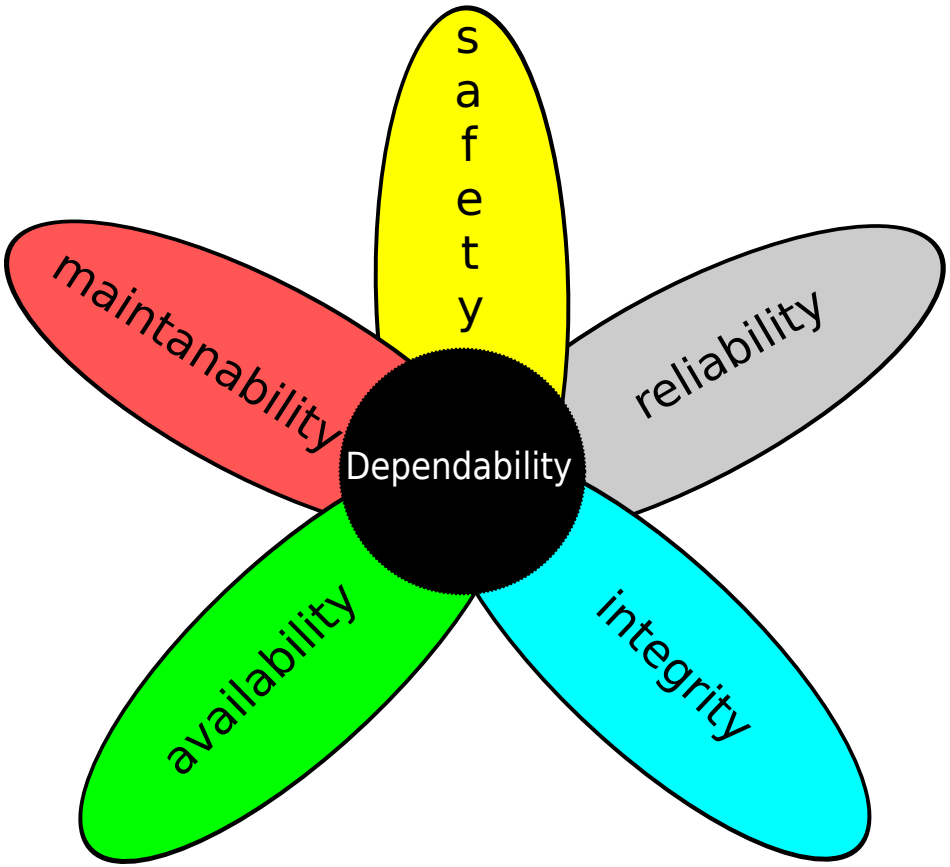
- Dependability Analysis and Modelling (DAM)
  - MARTE specialisation
  - Dependability properties into UML
- ++Literature (many use cases)

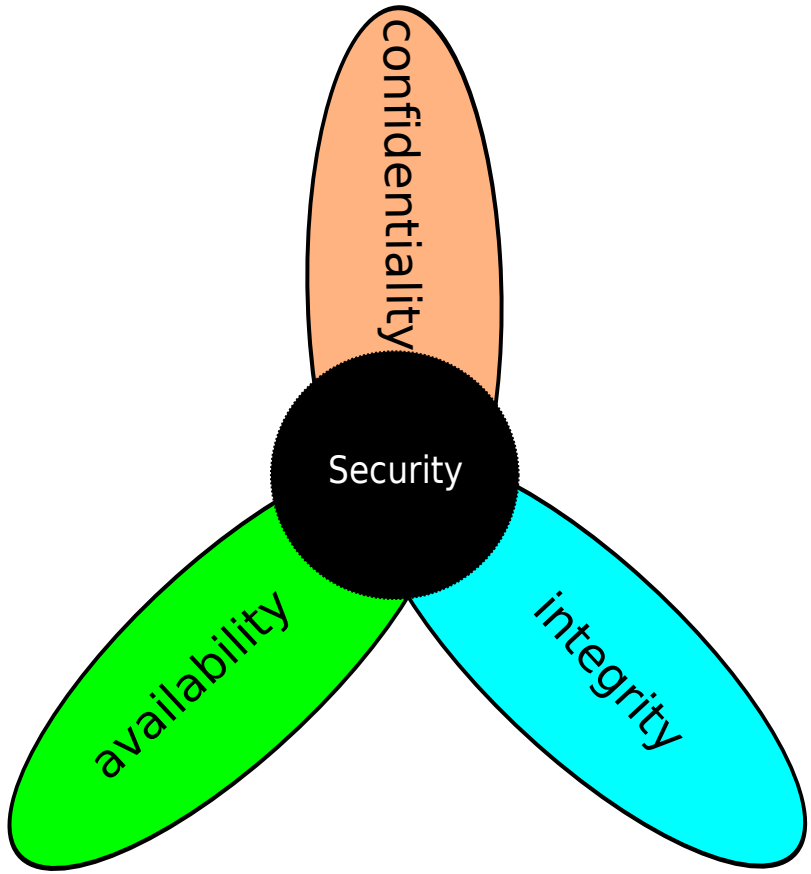
Avizienis, A. et al. Basic Concepts and Taxonomy of Dependable and Secure Computing. *TDSC*, 2004

Bernardi, S. et al. A Dependability Profile within MARTE. *Journal of Software and Systems Modelling*, 2009

Universidad Zaragoza 1542

Background (III)





Universidad Zaragoza
1542

Background (IV)

Ok mate, and all this, what for?

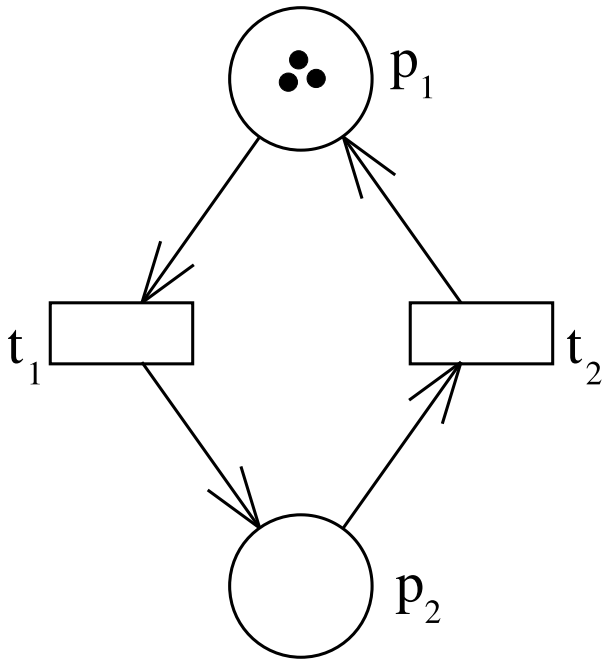
- Quantitative analysis
  - Conversion to formal models (Petri nets, PN)
  - Powerful analysis techniques

Universidad Zaragoza
1542

Background (IV)

Ok mate, and all this, what for?

- Quantitative analysis
  - Conversion to formal models (Petri nets, PN)
  - Powerful analysis techniques

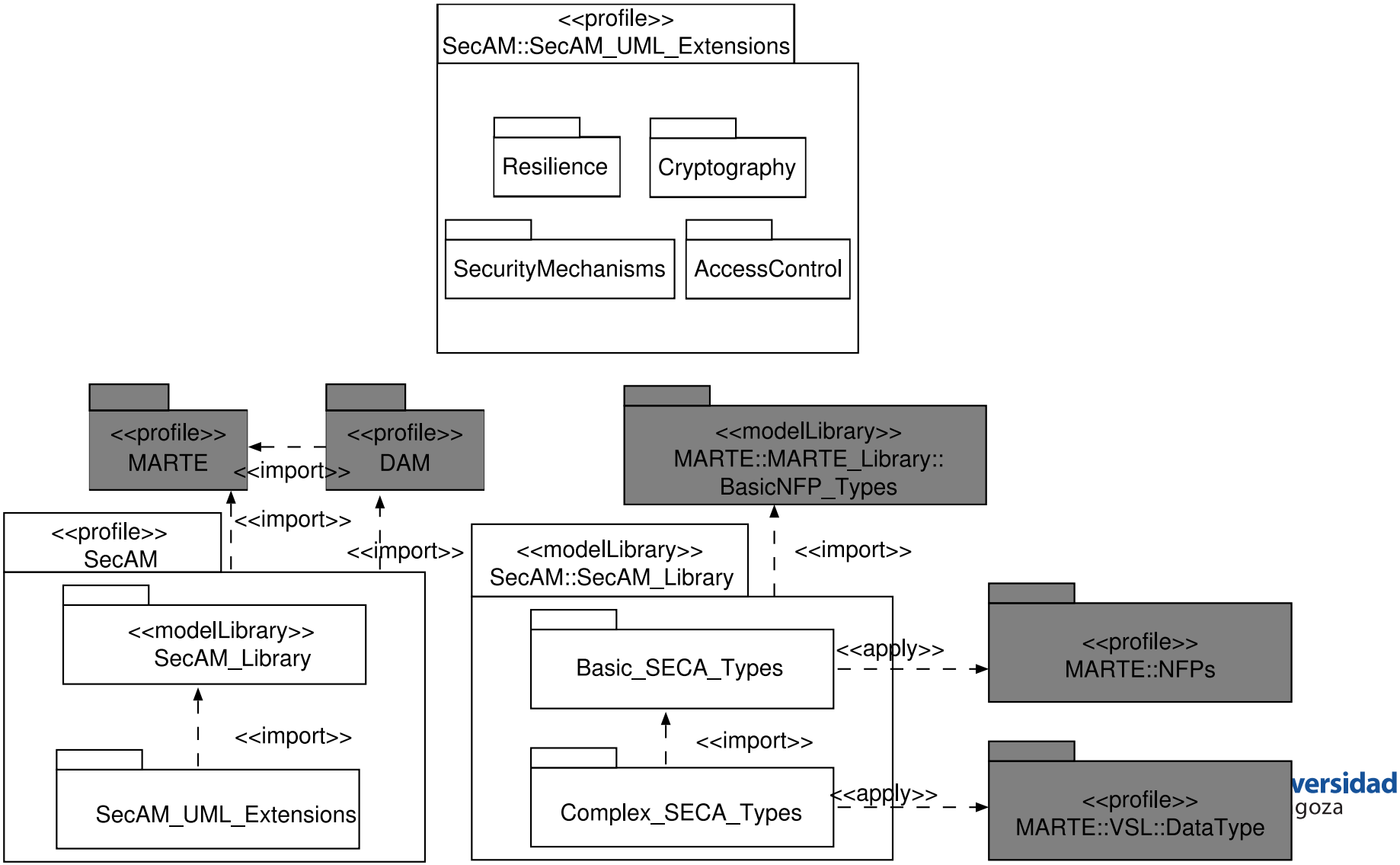


Petri net

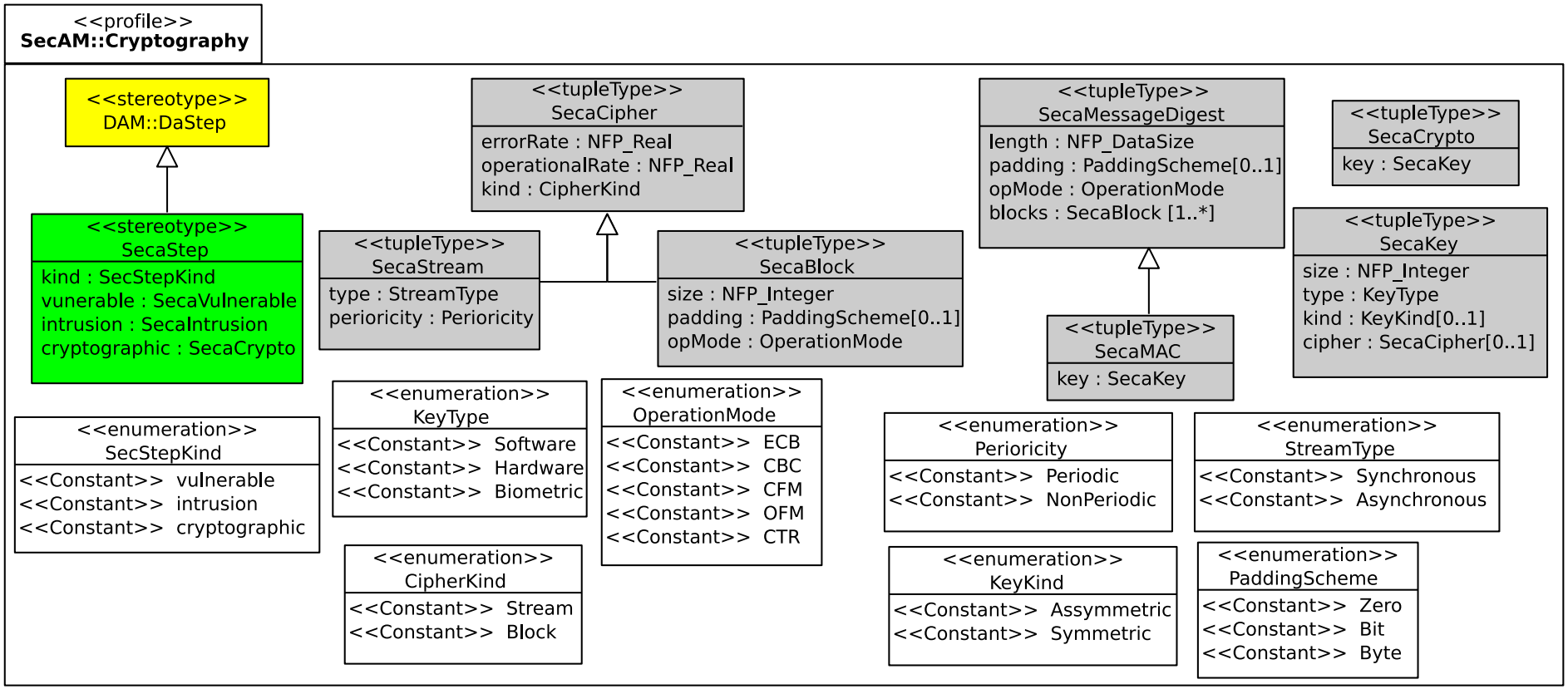
- Mathematical model
- Places (circles, p_X)
- Transitions (rectangles, t_X)
- Time transitions interpretation
  - Immediate ($t = 0$)
  - Timed (deterministic or probabilistic distribution)
- Tokens (black dots)

SecAM UML profile (I): a general overview...

Security Analysis and Modelling

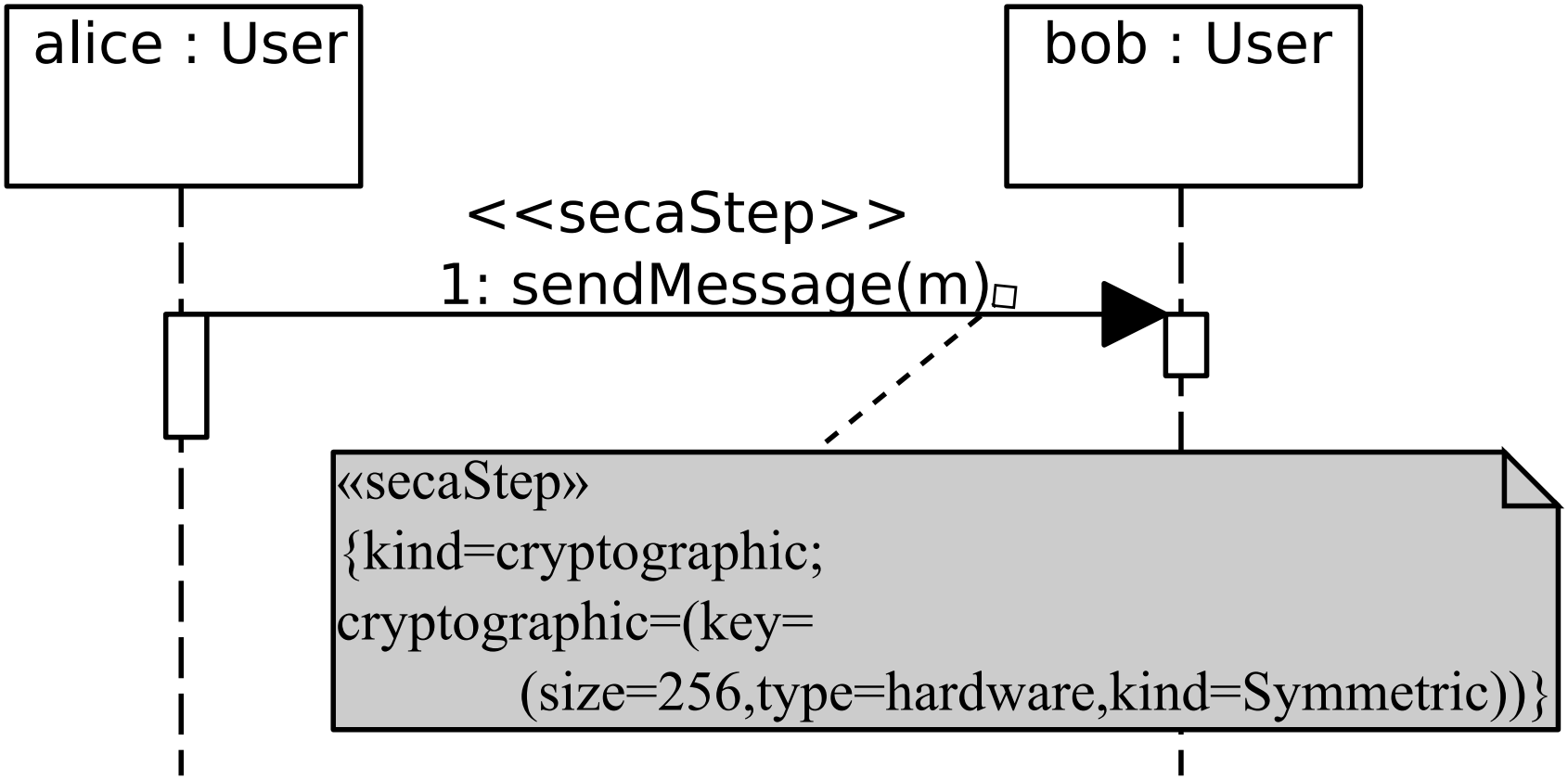


SecAM UML profile (II): *Cryptography* package (1)



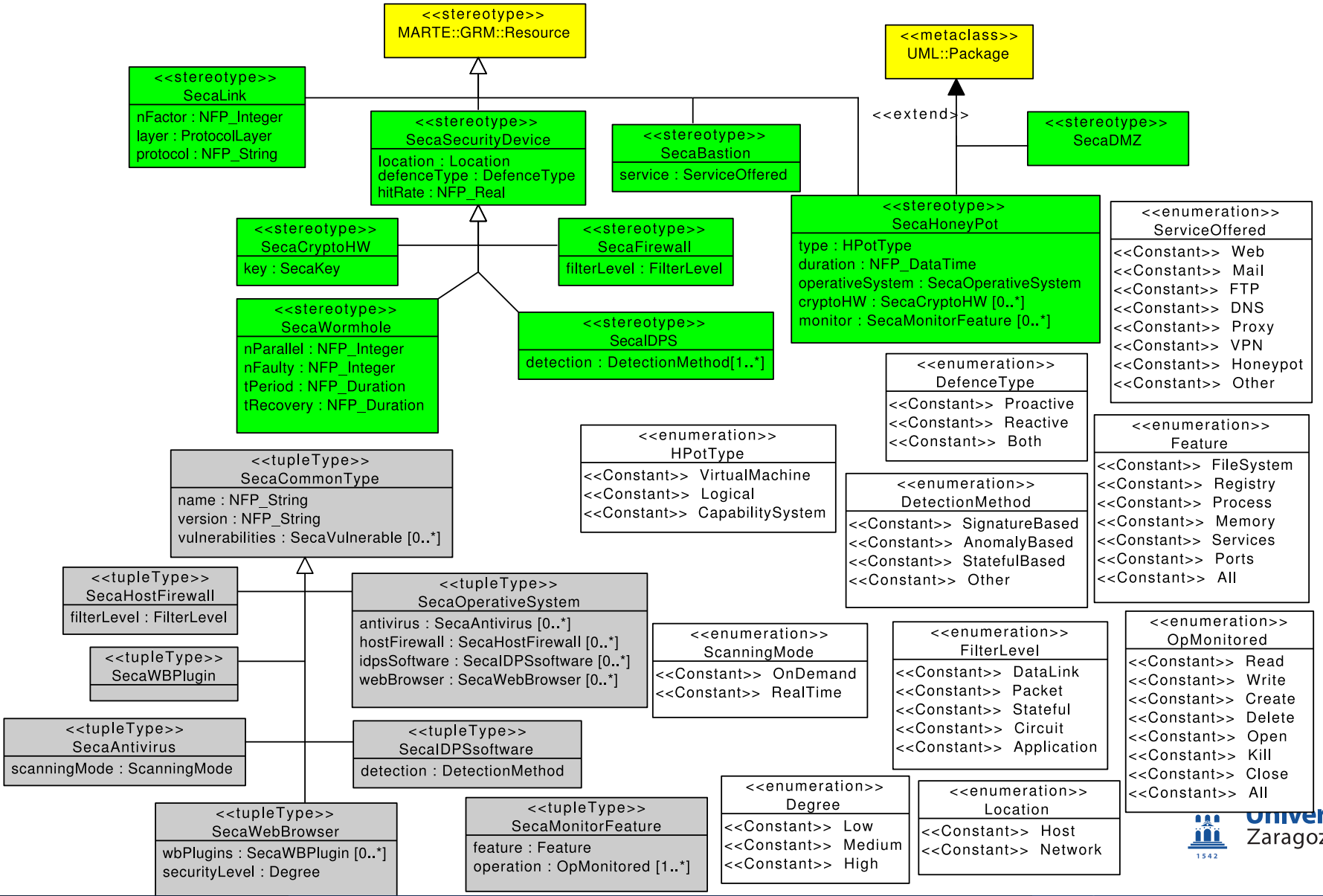
Universidad Zaragoza
1542

SecAM UML profile (II): *Cryptography* package (2)

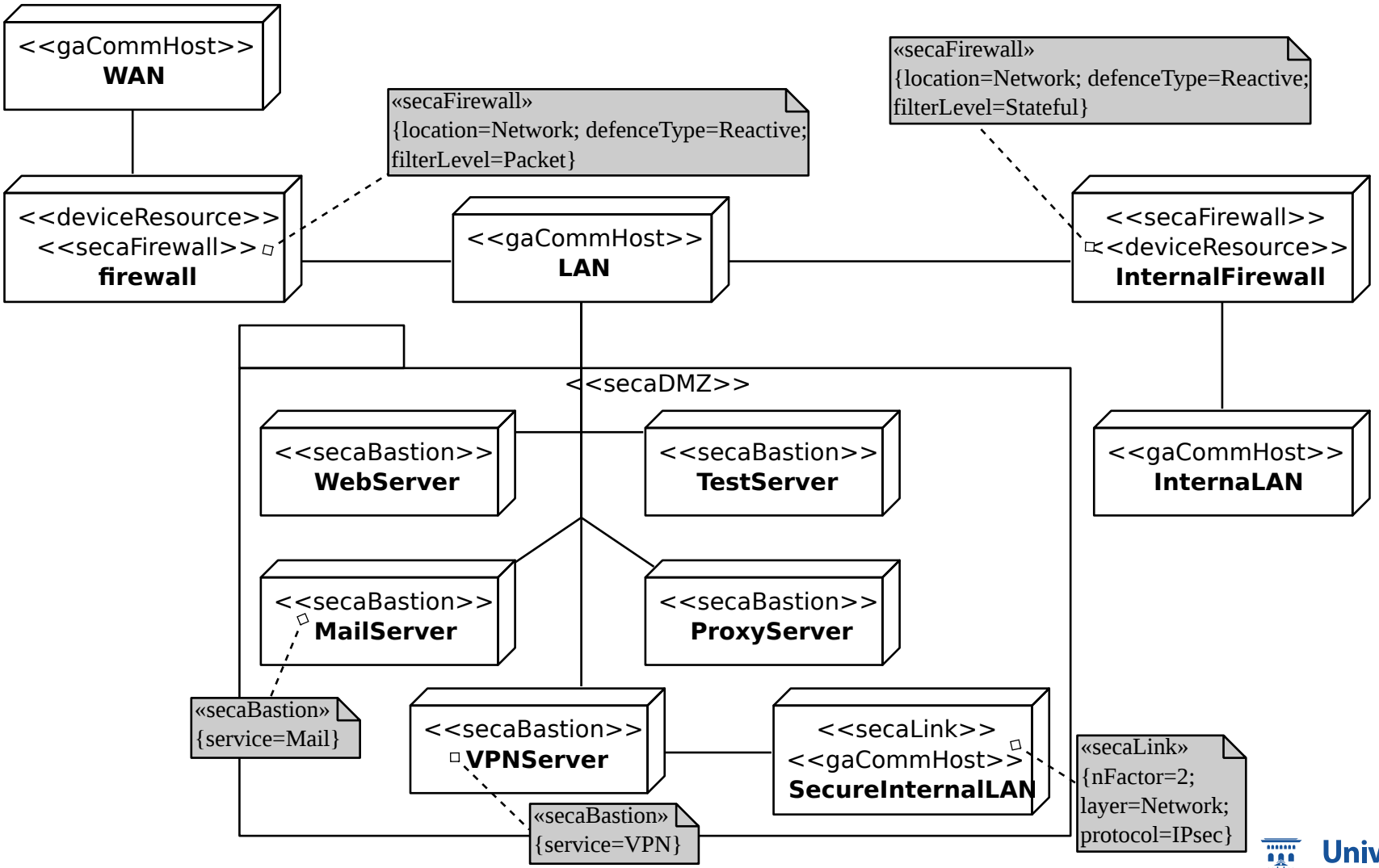


Universidad Zaragoza

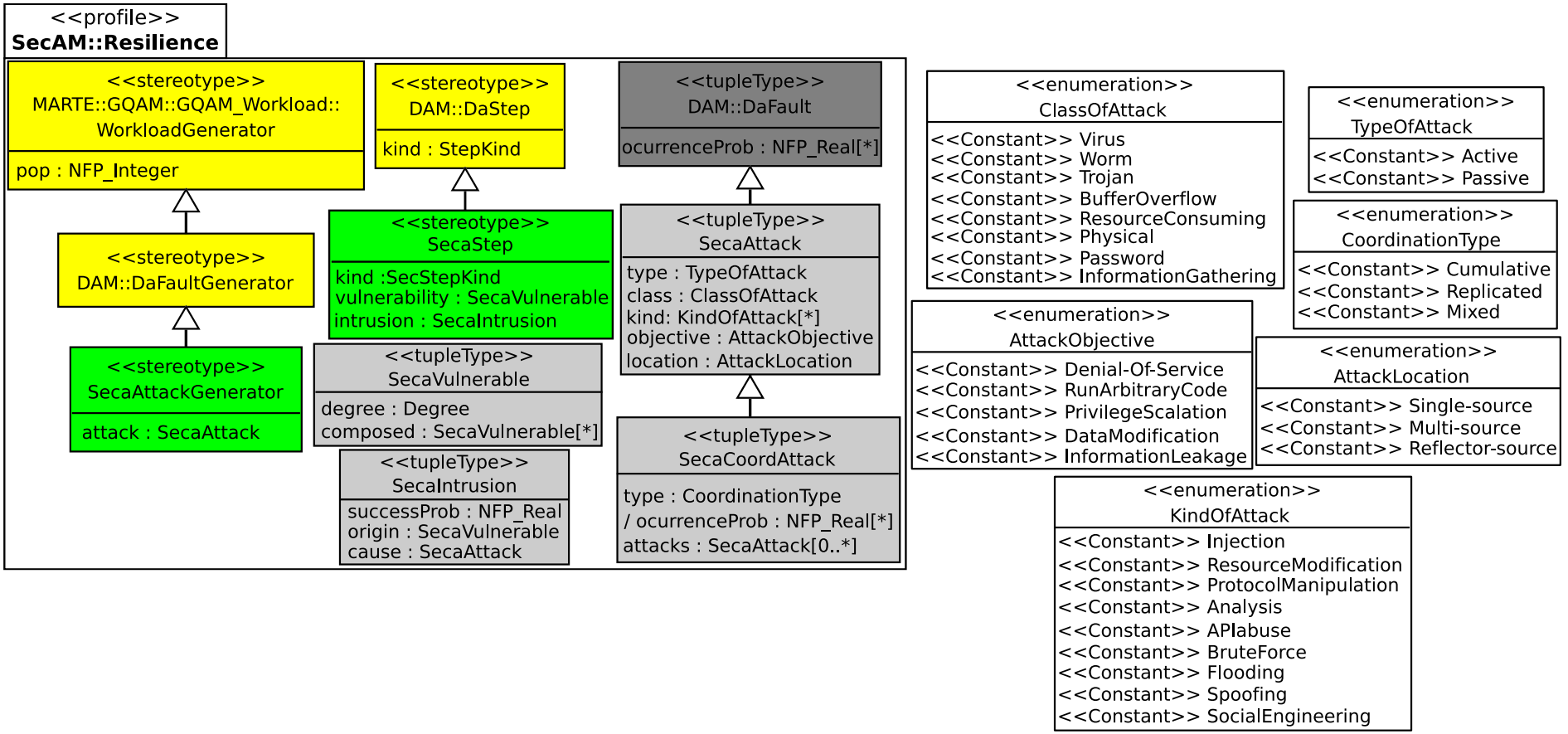
SecAM UML profile (II): *SecurityMechanisms* package (1)



SecAM UML profile (II): *SecurityMechanisms* package (2)

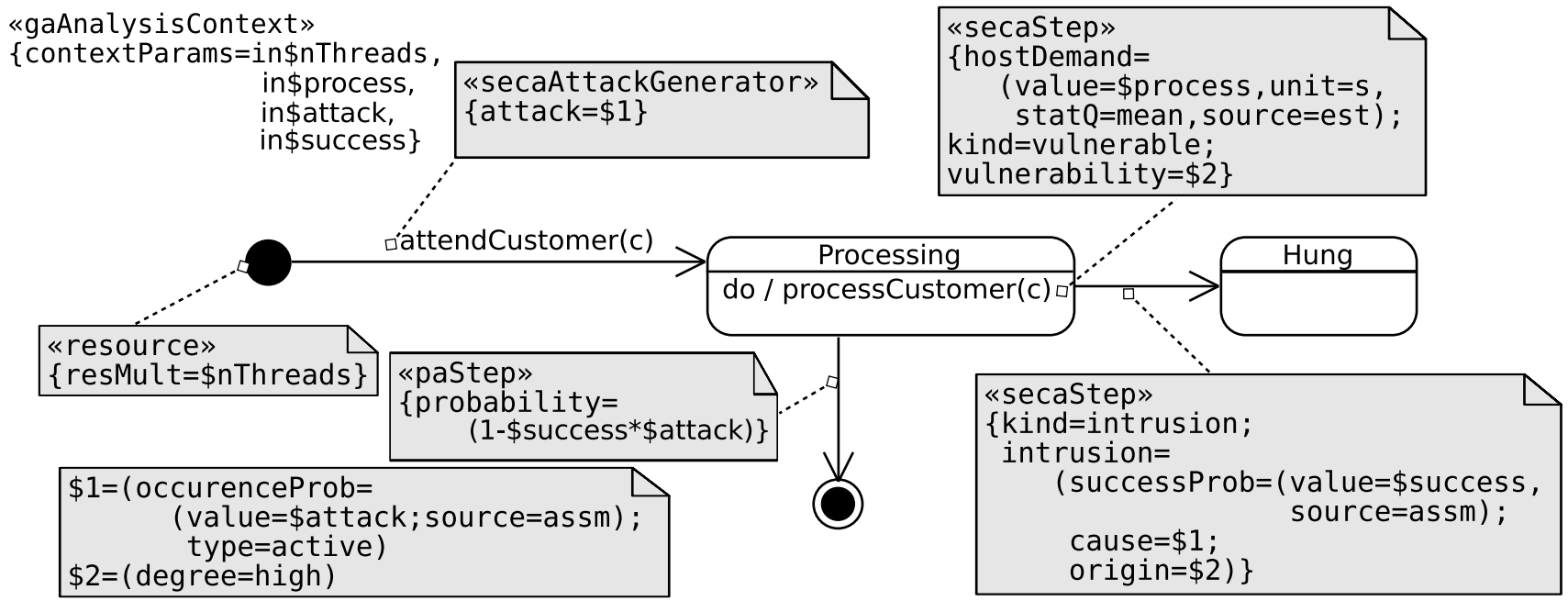


SecAM UML profile (III): *Resilience* package (1)



Universidad Zaragoza
1542

SecAM UML profile (III): *Resilience* package (2)



Universidad Zaragoza
1542

SecAM UML profile (IV): *AccessControl* package

Proposal (draft)

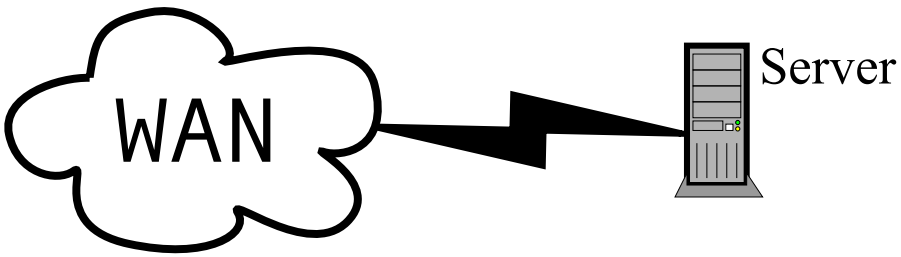
- Subjects, operations and objects
- Operations: kind and granted/not granted (boolean)
  - Read
  - Write
  - Access
  - Execution?
- Subjects: self-association
  - Delegation of authorisation
  - Separation of duties
- Idea: access control policies specified by OCL (UML constraints)

Universidad Zaragoza 1542

Use case (I): problem description

Problem

- Services on-demand system
- 2 kind of services
  - *Service 1*: 1s
  - *Service 2*: 2s
- Maximum of simultaneous requests: 100

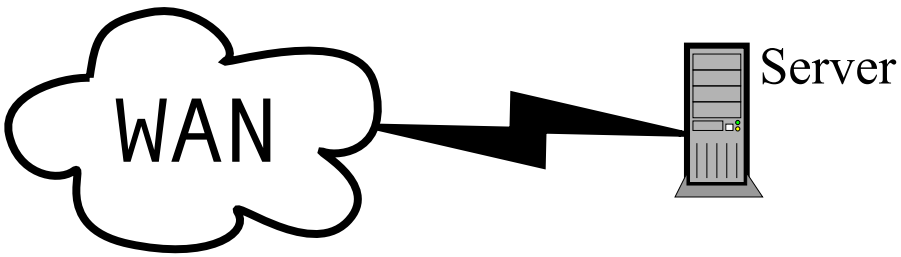


Universidad Zaragoza

Use case (I): problem description

Problem

- Services on-demand system
- 2 kind of services
  - *Service 1*: 1s
  - *Service 2*: 2s
- Maximum of simultaneous requests: 100
- Legitimate and illegitimate users

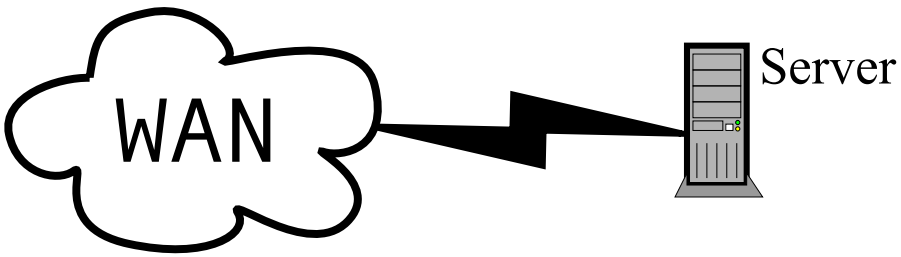


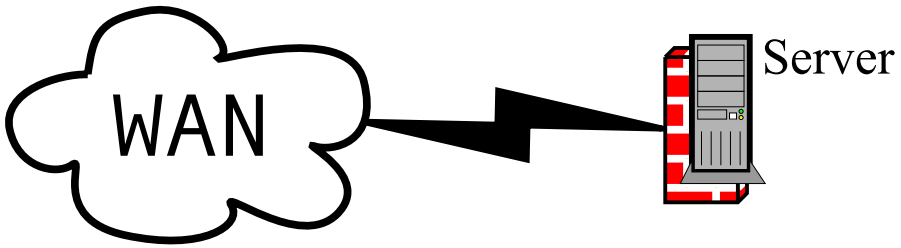
Universidad Zaragoza

Use case (I): problem description

Problem

- Services on-demand system
- 2 kind of services
  - *Service 1*: 1s
  - *Service 2*: 2s
- Maximum of simultaneous requests: 100
- Legitimate and illegitimate users

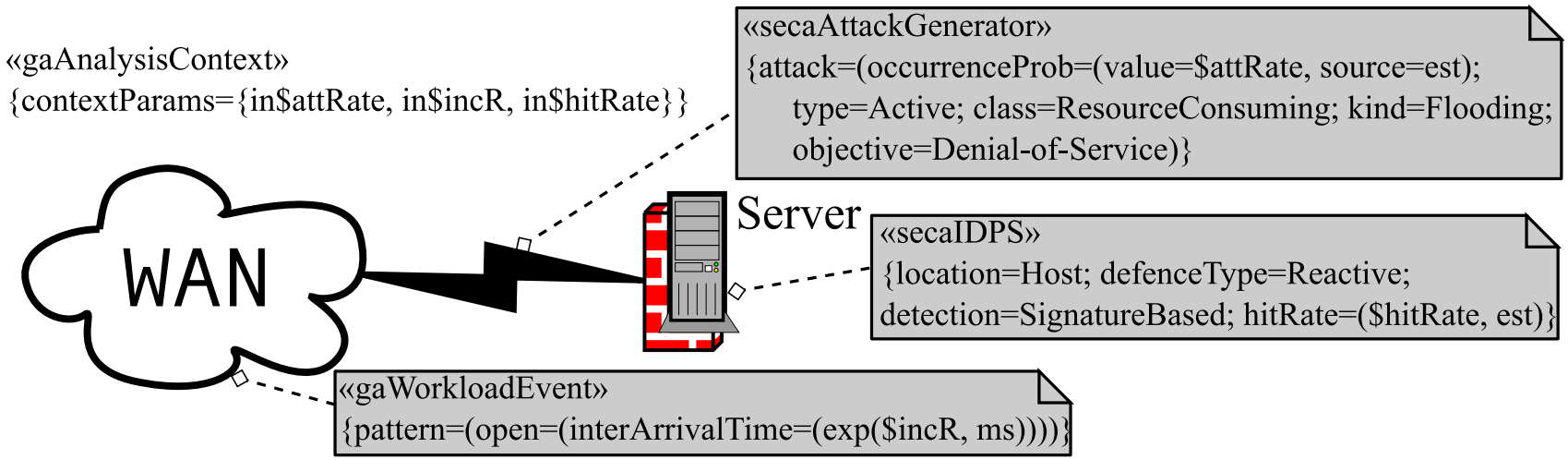




Universidad Zaragoza

Use case (II): using SecAM

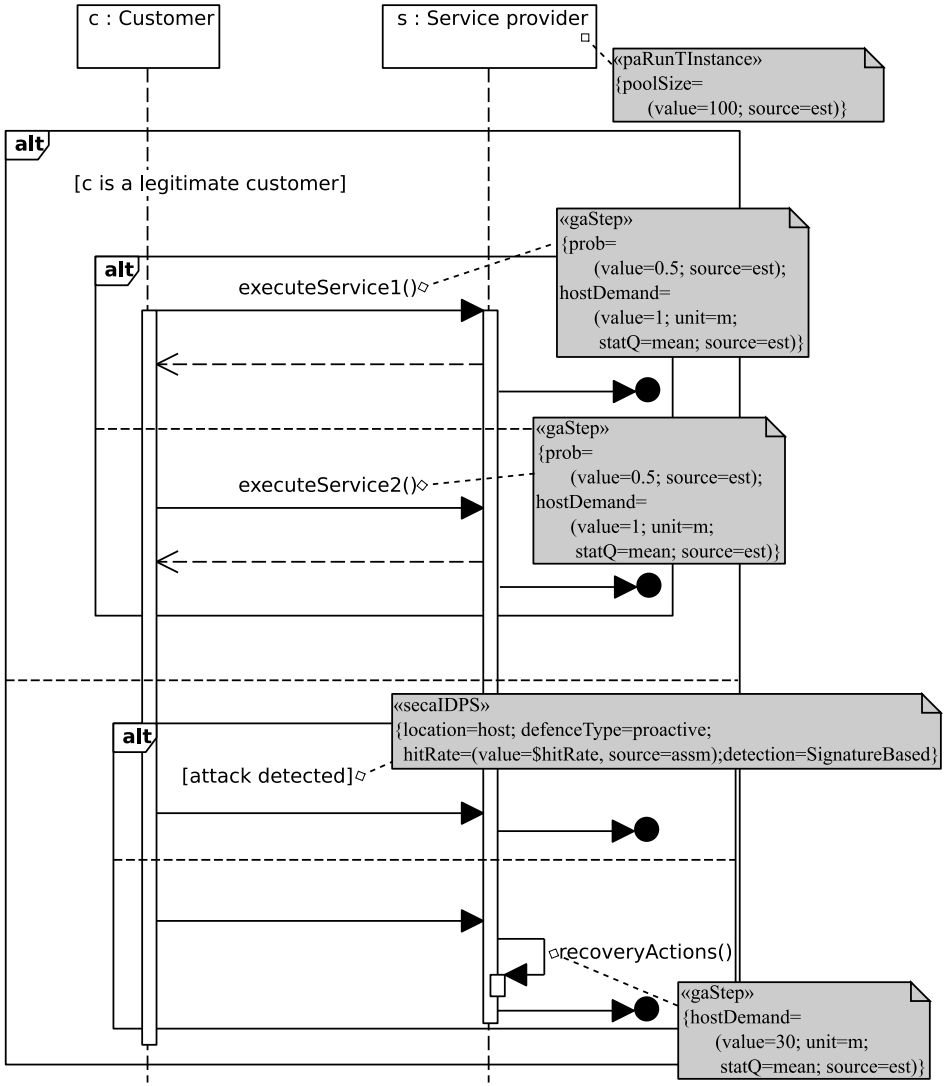
Adding a bit more information to the UML model



- 2 possibilities:
  - IDPS1 (hit rate 80%)
  - IDPS2 (hit rate 95%)

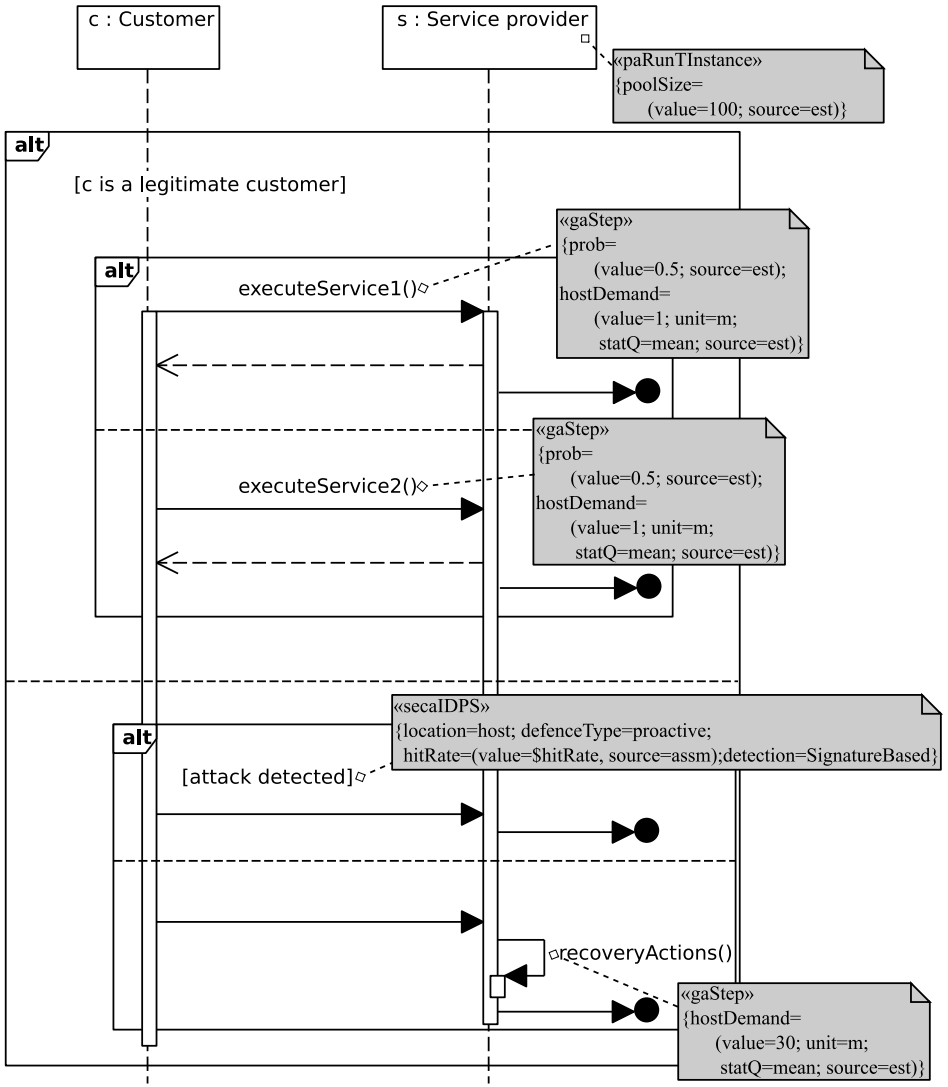
Universidad Zaragoza 1542

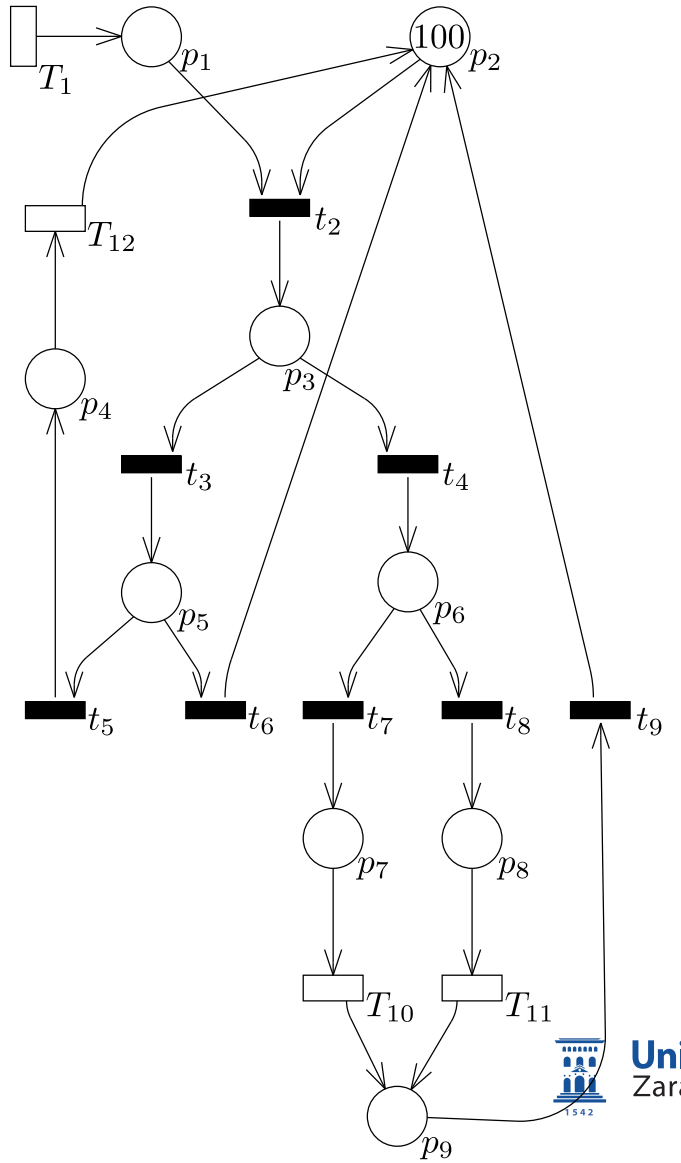
Use case (III): more models...



Universidad Zaragoza
1542

Use case (III): more models...





Universidad Zaragoza

Use case (IV): experiments and results

Experiments parameters

- Input customers ratio: $\{5, 10, 20\}$ customers/s
- Firewall hit rate: 80%, 95%
- Attacks rate: $[0.15\% \ldots 37.5\%]$

Universidad Zaragoza 1542

Use case (IV): experiments and results

Experiments parameters

- Input customers ratio: $\{5, 10, 20\}$ customers/s
- Firewall hit rate: 80%, 95%
- Attacks rate: $[0.15\% \ldots 37.5\%]$

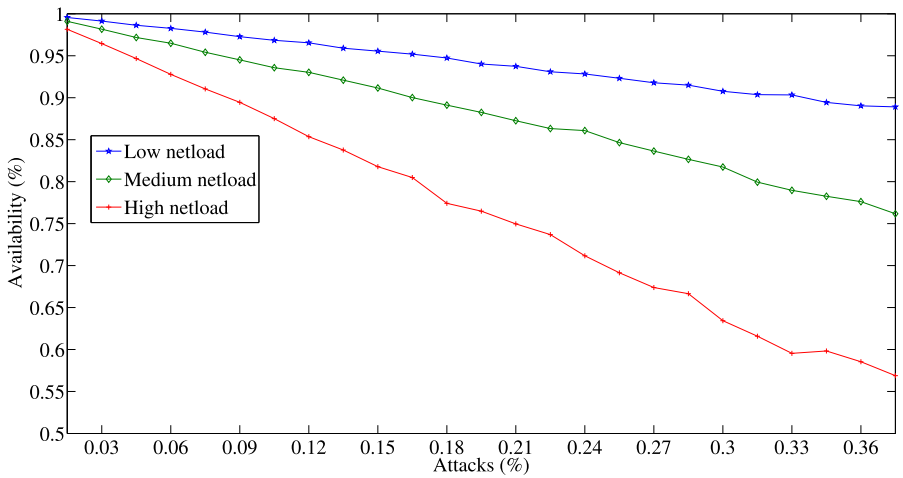


Figure: Detección 80%

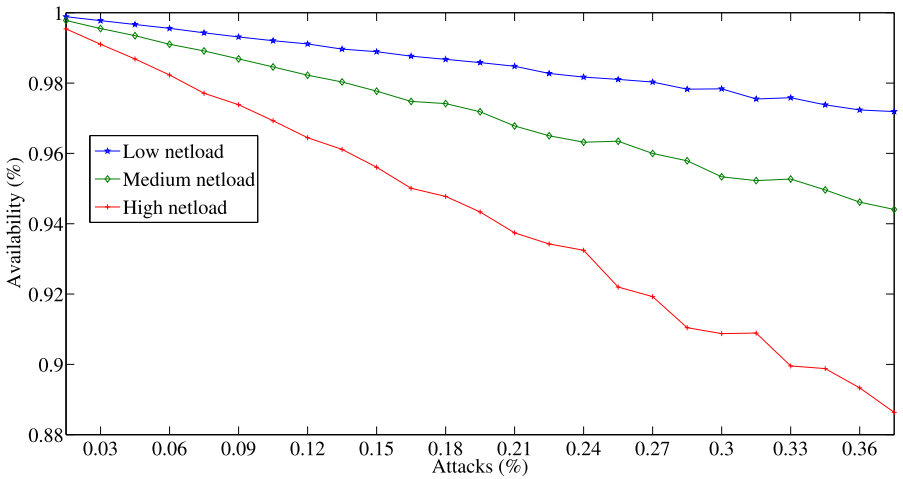


Figure: Detección 95%

Universidad Zaragoza

Conclusions and future work (I)

Conclusions

- Add security from the beginning
- Use of UML profiles

Universidad Zaragoza 1542

Conclusions and future work (I)

Conclusions

- Add security from the beginning
- Use of UML profiles
- Make easier its use due to UML compliant
- Make easier its addition into UML profile-case tools

Universidad Zaragoza 1542

Conclusions and future work (I)

Conclusions

- Add security from the beginning
- Use of UML profiles
- Make easier its use due to UML compliant
- Make easier its addition into UML profile-case tools
- SecAM-MARTE-DAM framework
  - Performance + dependability + security
- Quantitative and qualitative analysis
- Detect security problems (o related) in design phase
  - Save on costs! (and the cheerleader!)

Universidad Zaragoza 1542

Conclusions and future work (II)

Future work

- Security aspects not taken into account (what is missing?)
- Refine current status of `SecAM` (AccessControl?)

Universidad Zaragoza 1542

Conclusions and future work (II)

Future work

- Security aspects not taken into account (what is missing?)
- Refine current status of `SecAM` (AccessControl?)
- Qualitative analysis?
- Agile methods?
- Full support through tool
  - Eclipse plug-in Papyrus
  - MARTE + DAM + (part of) SecAM already added (but not in the last version :))

Universidad Zaragoza 1542

Contributions and acknowledges (I)

Accepted papers

- R.J. Rodríguez, On the Secure Software Development within UML Profiles. In *Proceedings of 7th Hack.LU Conference*, 2011
- R.J. Rodríguez and J. Merseguer, Integrating FT Techniques into the Design of Critical Systems. In *ISARCS'10: Proceedings of the 1st International Symposium on Architecting Critical Systems*, Lecture Notes on Computer Science, vol. 6150, pp. 33–51, Springer, 2010
- R.J. Rodríguez, J. Merseguer and S. Bernardi, Modelling and Analysing Security Aspects within UML. In *SERENE'10: Proceedings of the 2nd International Workshop on Software Engineering for Resilient Systems*, 2010

Universidad Zaragoza 1542

Contributions and acknowledges (II)

Work in progress...

- R.J. Rodríguez, J. Merseguer and S. Bernardi, Towards a Unified Profile for Security Modelling and Analysis (tentative title).
- R.J. Rodríguez, Y. Alosefer, J. Merseguer and O.F. Rana, Improving Security Capabilities into Systems by Honeypots Data Analysis (tentative title).
- SecAM + Business Process Modelling.

Acknowledges

- José Merseguer & Simona Bernardi
  - Good friends, and better professionals

Contributions and acknowledges (II)

Work in progress...

- R.J. Rodríguez, J. Merseguer and S. Bernardi, Towards a Unified Profile for Security Modelling and Analysis (tentative title).
- R.J. Rodríguez, Y. Alosefer, J. Merseguer and O.F. Rana, Improving Security Capabilities into Systems by Honeypots Data Analysis (tentative title).
- SecAM + Business Process Modelling.

Acknowledges

- José Merseguer & Simona Bernardi
  - Good friends, and better professionals
- Hack.LU conference committee

Contributions and acknowledges (II)

Work in progress...

- R.J. Rodríguez, J. Merseguer and S. Bernardi, Towards a Unified Profile for Security Modelling and Analysis (tentative title).
- R.J. Rodríguez, Y. Alosefer, J. Merseguer and O.F. Rana, Improving Security Capabilities into Systems by Honeypots Data Analysis (tentative title).
- SecAM + Business Process Modelling.

Acknowledges

- José Merseguer & Simona Bernardi
  - Good friends, and better professionals
- Hack.LU conference committee
- All of you by hearing my (quite) boring talk...

On the Secure Software Development in Early Stages within UML Profiles

Ricardo J. Rodríguez
rjrodriguez@unizar.es
http://www.ricardojrodriguez.es

Universidad Zaragoza

19th September, 2011

This work has been developed in collaboration with **Simona Bernardi** (Centro Universitario de la Defensa) and **José Merseguer** (Universidad de Zaragoza)

7th **Hack.LU**

Luxembourg, Luxembourg Grand-Duché