

# Seguridad en el diseño: desde el principio

**Ricardo J. Rodríguez**

[rjrodriguez@unizar.es](mailto:rjrodriguez@unizar.es)

<http://www.ricardojrodriguez.es>



**Universidad**  
Zaragoza

16 de Septiembre, 2011

Este trabajo ha sido realizado en colaboración con **Simona Bernardi** (Centro Universitario de la Defensa) y **José Merseguer** (Universidad de Zaragoza)

**No cON Name 2011**

Barcelona, España

# Motivación (I)

## Fases del desarrollo de sistemas

- **Análisis**
- **Diseño**
- **Implementación**
- *Deployment* (y validación)

## Análisis

- **Captura de requisitos** (propiedades):
  - Funcionales: qué hace el sistema
    - Datos técnicos, procesamiento de la información. . .
  - No funcionales: cómo ha de comportarse el sistema
    - Cuántos clientes va a atender, cuál es la velocidad de transferencia. . .
- Figura de *ingeniero de requisitos*

# Motivación (II)

## Análisis de requisitos

- **Funcionales**: (más o menos) obvios
- **¿Y los no funcionales?**
  - Restricciones, usabilidad, rendimiento. . .
- Después: *ingeniero de sistemas + ingeniero de software*

## Seguridad: la olvidada (1)

- **Propiedad no funcional** del sistema
- **Falta de interés**
- Resultado: **“fix it later”**
  - Arreglar el problema cuando se tiene el problema. . .

# Motivación (III)

## Seguridad: la olvidada (2)

- Graves **consecuencias**
  - Alto coste de reimplementación/rediseño
  - Pérdidas financieras
  - Servicios caídos → pérdida de clientes
  - Revelación de datos confidenciales (e.g., Sony PSN)

## ¿Culpable?

- ¿Ingeniero de requisitos?
- ¿Ingeniero de sistemas?
- ¿Ingeniero de software?

# Motivación (III)

## Seguridad: la olvidada (2)

- Graves **consecuencias**
  - Alto coste de reimplementación/rediseño
  - Pérdidas financieras
  - Servicios caídos → pérdida de clientes
  - Revelación de datos confidenciales (e.g., Sony PSN)

## ¿Culpable?

- ¿Ingeniero de requisitos?
- ¿Ingeniero de sistemas?
- ¿Ingeniero de software?
- **¿ZP?**

# Motivación (III)

## Seguridad: la olvidada (2)

- Graves **consecuencias**
  - Alto coste de reimplementación/rediseño
  - Pérdidas financieras
  - Servicios caídos → pérdida de clientes
  - Revelación de datos confidenciales (e.g., Sony PSN)

## ¿Culpable?

- ¿Ingeniero de requisitos?
- ¿Ingeniero de sistemas?
- ¿Ingeniero de software?
- **¿ZP?**
- Todos (**no, ZP aquí no...**) y ninguno

# Motivación (IV)

Y, entonces, ¿qué?

- Mínimos conocimientos de seguridad
- Pensar en **seguridad en TODAS las fases del proyecto**
- **Cambio en la metodología** → *Secure Software Engineering*

# Motivación (IV)

Y, entonces, ¿qué?

- Mínimos conocimientos de seguridad
- Pensar en **seguridad en TODAS las fases del proyecto**
- **Cambio en la metodología** → *Secure Software Engineering*

**Seguridad:  
desde el principio hasta el final**

# Trabajos relacionados (I)

## Requisitos, arquitectura y aspectos. . .

- **Captura de requisitos**
  - Haley et al. (*SESS*, 2006)
  - Wolter et al. (*Requir. Eng.*, 2010)
- **Arquitectura**
  - Schmidt et al. (*SA*, 2006)
  - Yskout et al. (*ARES*, 2008)
  - Abi-Antoun et al. (*ASE*, 2010)
  - Heyman et al. (*ESSoS*, 2011)
- **Aspectos**
  - Braga et al. (*SoSym*, 2010)
  - Georg et al. (*TSE*, 2011)

# Trabajos relacionados (II)

## Metodologías, patrones, métodos formales...

- **Framework de diseño**
  - Mouratidis et al. (*CAiSE*, 2003)
  - Islan et al. (*SoSym*, 2010)
  - Khan, *Comp. F & S*, Aug 2011
- **Patrones de seguridad**
  - Fernández (*SERP*, 2004)
  - Halkidis et al. (*TDSC*, 2008)
- **Métodos formales** (autómatas o redes de Petri)
  - Schneider (*TISSEC*, 2000)
  - Horvath et al. (*SESS*, 2008)
  - Patzina et al. (*SD4RCES*, 2010)

# Trabajos relacionados (III)

## Métodos semi-formales. . .

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

# Trabajos relacionados (III)

## Métodos semi-formales. . .

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

## Propuesta basada en UML

- **Estándar *de facto***
- **Aspectos comportamentales y estructurales**
- Bien conocido → **¿facilita adición de seguridad?**

# Conocimientos previos (I)

## Perfiles UML: ¿qué es?

- Estándar OMG
- **Estereotipos y valores etiquetados**

# Conocimientos previos (I)

## Perfiles UML: ¿qué es?

- Estándar OMG
- **Estereotipos y valores etiquetados**
- **Anotar elementos UML**
  - **Expresar propiedades** no funcionales (NFP) en los diseños UML
  - **Extender semántica** del modelo

## Ejemplo OMG

- ***Modelling and Analysis of RT Embedded systems*** (MARTE)
  - Soporte para análisis de **rendimiento y schedulability**
  - Expresión de NFPs mediante sintaxis VSL (*Value Specification Language*)

---

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

# Conocimientos previos (II)

## Definición de seguridad

- **Confidencialidad**
- **Integridad**
- **Disponibilidad**

# Conocimientos previos (II)

## Definición de seguridad

- **Confidencialidad**
- **Integridad**
- **Disponibilidad**
- Estrecha relación con *dependability* (Avizienis)

## Perfil UML de *dependability*

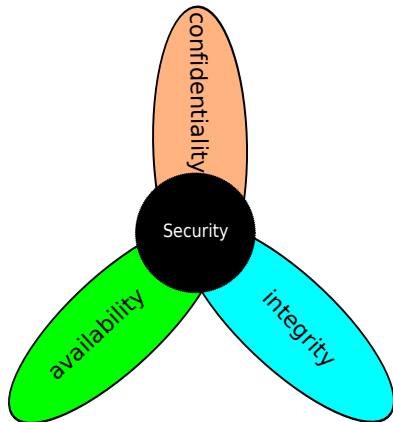
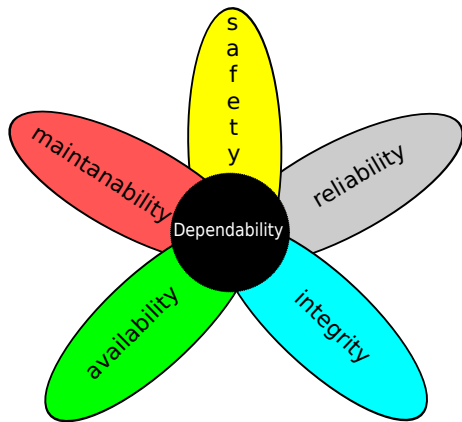
- **Dependability Analysis and Modelling (DAM)**
  - Especialización MARTE
  - Propiedades de **dependability**
- Mucha literatura con ejemplos de uso

---

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

# Conocimientos previos (III)



# Conocimientos previos (IV)

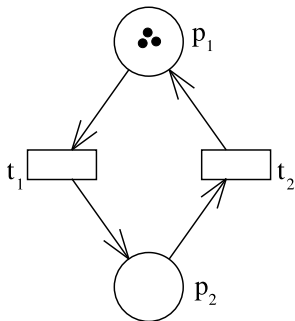
## Perfiles, ¿para qué?

- **Análisis cuantitativo**
  - Obtención de **modelos formales** (Redes de Petri, RdP)
  - **Explotación de características**

# Conocimientos previos (IV)

## Perfiles, ¿para qué?

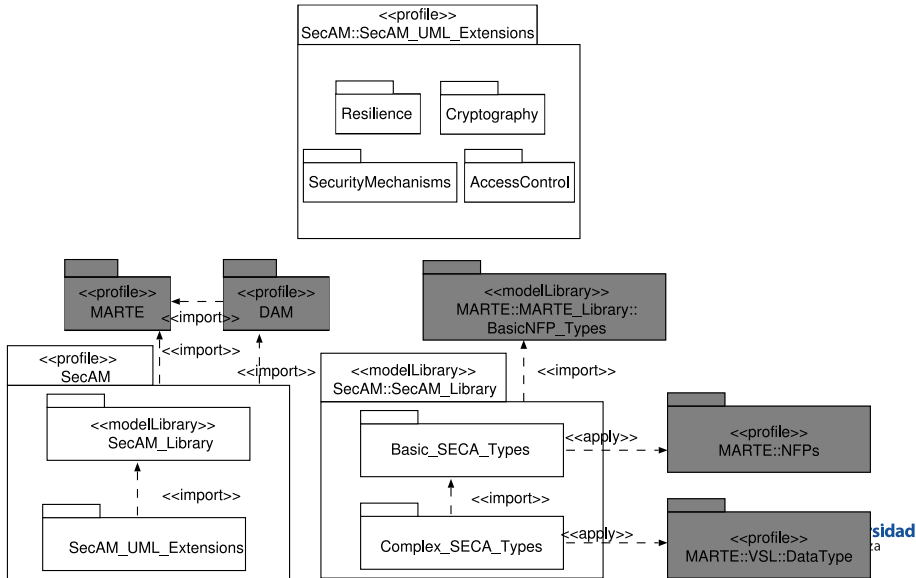
- **Análisis cuantitativo**
  - Obtención de **modelos formales** (Redes de Petri, RdP)
  - **Explotación de características**



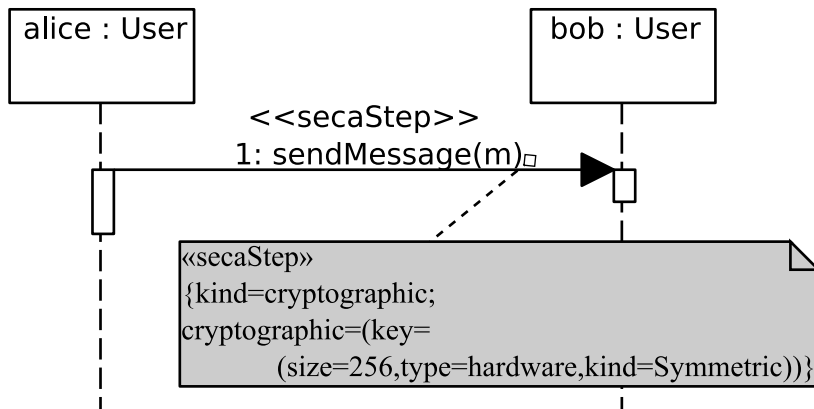
## Red de Petri

- **Modelo matemático**
- Lugares (círculos,  $p_X$ )
- Transiciones (rectángulos,  $t_X$ )
- Interpretación de transiciones
  - Inmediatas ( $t = 0$ )
  - Temporizadas (determinista o distribución probabilística)
- Marcas (puntos negros)

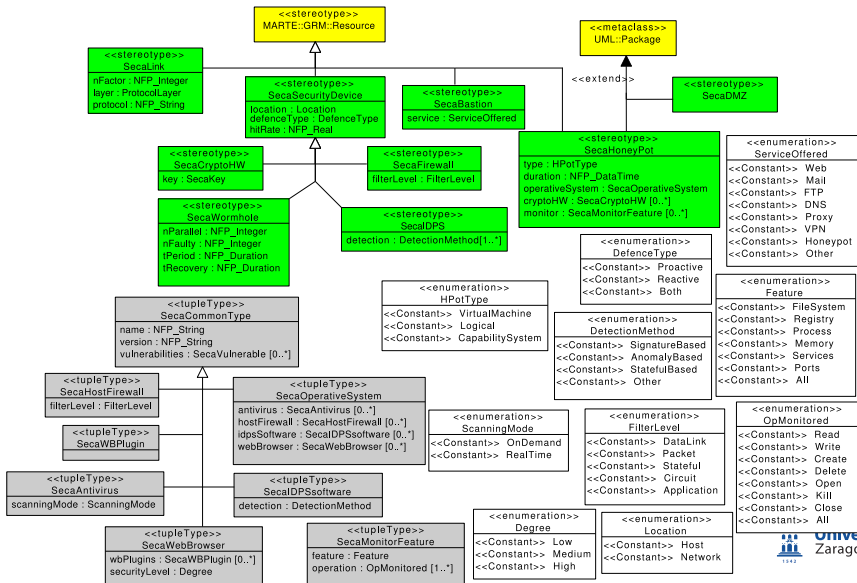
# Perfil UML SecAM (I): una visión general...



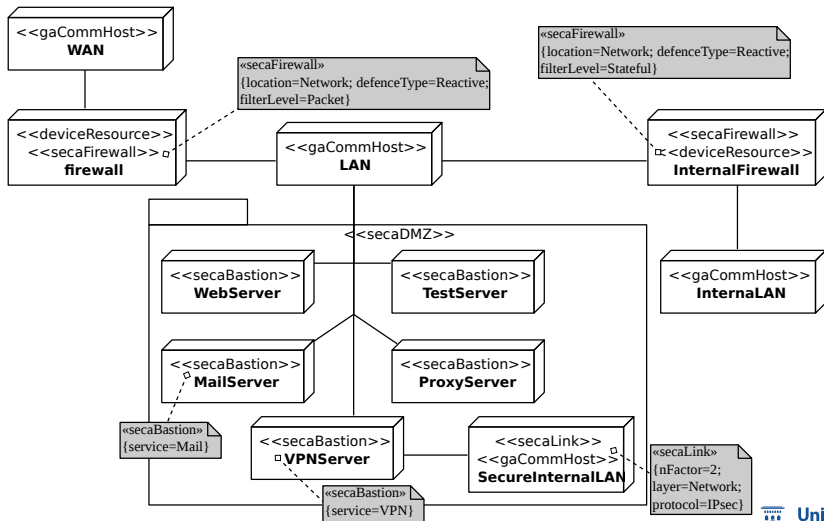


Perfil UML SecAM (II): paquete *Cryptography* (2)

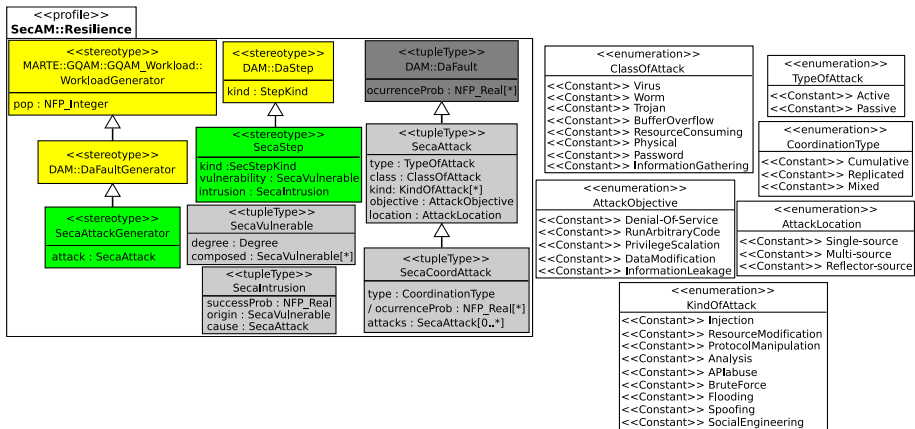
# Perfil UML SecAM (II): paquete SecurityMechanisms (1)



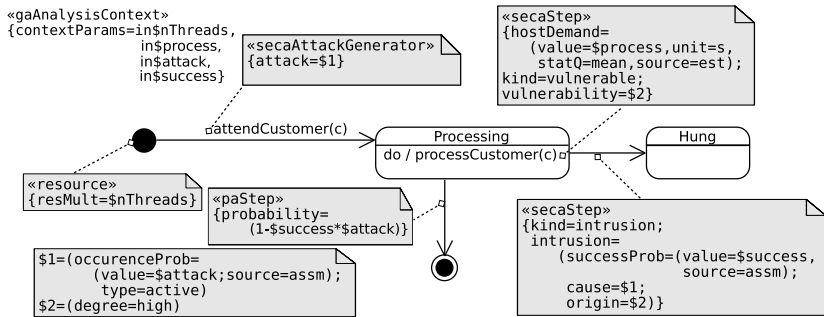
# Perfil UML SecAM (II): paquete *SecurityMechanisms* (2)



# Perfil UML SecAM (III): paquete Resilience (1)



# Perfil UML SecAM (III): paquete *Resilience* (2)



# Perfil UML SecAM (IV): paquete *AccessControl*

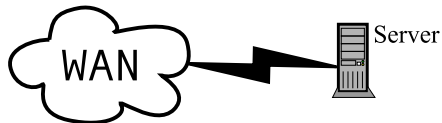
## Solución propuesta

- **Sujetos, operaciones y objetos**
- Operaciones: tipo de operación y permiso (booleano)
  - Lectura
  - Escritura
  - Acceso
  - Ejecución?
- Sujetos: auto-asociación
  - **Delegación de autorización**
  - **Separación de obligaciones**
- Idea: **especificación de políticas de acceso mediante OCL**  
(restricciones UML)

# Caso de uso (I): descripción del problema

## Problema

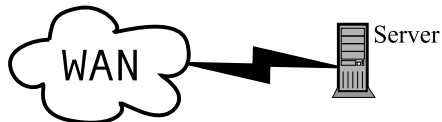
- Sistema de **servicios bajo demanda**
- 2 tipos de servicios
  - *Servicio 1*: 1s
  - *Servicio 2*: 2s
- **Máximo de peticiones simultáneas**: 100



# Caso de uso (I): descripción del problema

## Problema

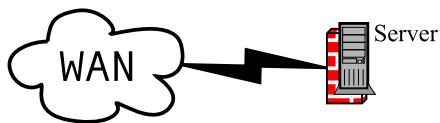
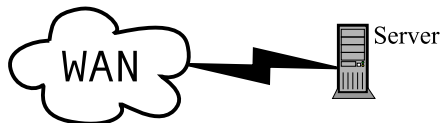
- Sistema de **servicios bajo demanda**
- 2 tipos de servicios
  - *Servicio 1*: 1s
  - *Servicio 2*: 2s
- **Máximo de peticiones simultáneas**: 100
- **Usuarios legítimos e ilegítimos**



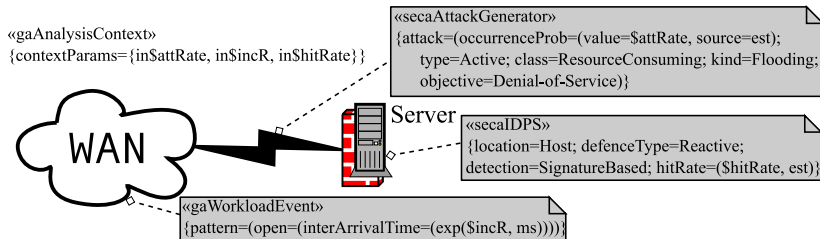
# Caso de uso (I): descripción del problema

## Problema

- Sistema de **servicios bajo demanda**
- 2 tipos de servicios
  - *Servicio 1*: 1s
  - *Servicio 2*: 2s
- **Máximo de peticiones simultáneas**: 100
- **Usuarios legítimos e ilegítimos**

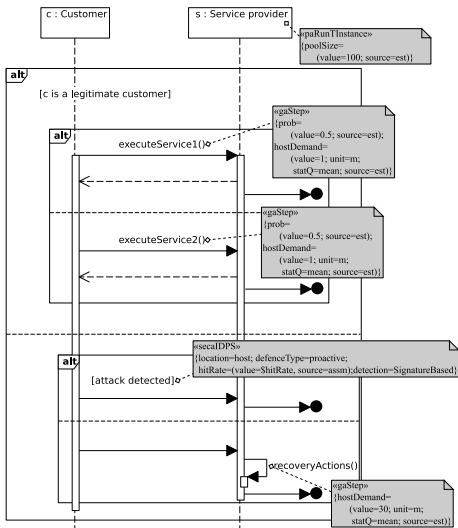


# Caso de uso (II): usando SecAM

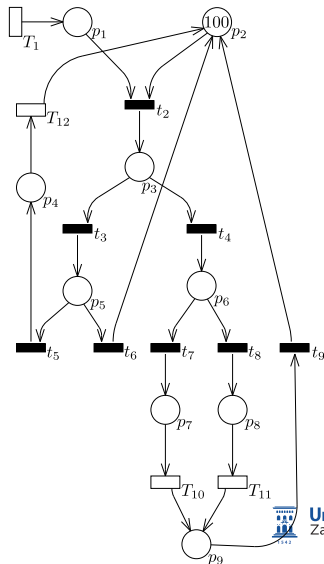
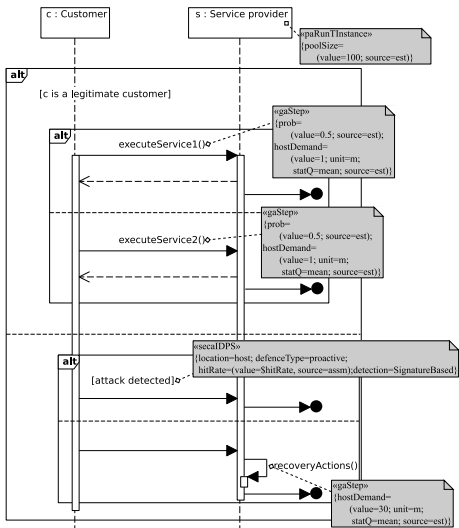


- 2 posibilidades:
  - IDPS1 (tasa de aciertos 80%)
  - IDPS2 (tasa de aciertos 95%)

# Caso de uso (III): más modelos. . .



# Caso de uso (III): más modelos...



# Caso de uso (IV): experimentos y resultados

## Parámetros de los experimentos

- **Entrada de clientes:** {5, 10, 20} clientes/s
- **Acierto** del *firewall*: 80%, 95%
- **Ataques:** [0.15% ... 37.5%]

# Caso de uso (IV): experimentos y resultados

## Parámetros de los experimentos

- **Entrada de clientes:** {5, 10, 20} clientes/s
- **Acierto del firewall:** 80%, 95%
- **Ataques:** [0.15% ... 37.5%]

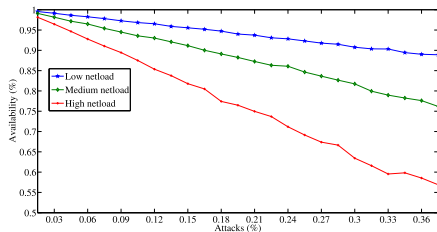


Figure: Detección 80%

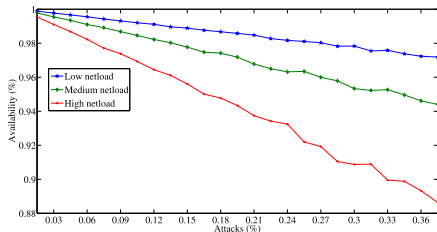


Figure: Detección 95%

# Conclusiones y trabajo futuro (I)

## Conclusiones

- Incorporación de **seguridad desde el principio**
- Uso de **perfiles UML**

# Conclusiones y trabajo futuro (I)

## Conclusiones

- Incorporación de **seguridad desde el principio**
- Uso de **perfiles UML**
- Facilidad de uso debido a **integración con UML**
- Facilidad de **implementación en *UML profile-case tools***

# Conclusiones y trabajo futuro (I)

## Conclusiones

- Incorporación de **seguridad desde el principio**
- Uso de **perfiles UML**
- Facilidad de uso debido a **integración con UML**
- Facilidad de **implementación en UML profile-case tools**
- **Integración con MARTE-DAM: performance + dependability**
- **Análisis cualitativo y cuantitativo**
- **Detectar problemas** de seguridad (o relacionados) en diseño
  - Ahorro en costes

# Conclusiones y trabajo futuro (II)

## Trabajo futuro

- Aspectos de seguridad no contemplados (*¿qué falta?*)
- **Refinar estado actual** de SecAM (*¿AccessControl?*)

# Conclusiones y trabajo futuro (II)

## Trabajo futuro

- Aspectos de seguridad no contemplados (*¿qué falta?*)
- **Refinar estado actual** de SecAM (*¿AccessControl?*)
- **¿Análisis cualitativo?**
- **¿Metodologías ágiles de desarrollo?**
- Soporte total mediante **herramienta**
  - Eclipse plug-in Papyrus
  - MARTE + DAM + (parte) SecAM ya implementado

# Contribuciones y agradecimientos (I)

## Publicaciones aceptadas

- R.J. Rodríguez, **On the Secure Software Development within UML Profiles**. In *Proceedings of 7<sup>th</sup> 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 1<sup>st</sup> 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 2<sup>nd</sup> International Workshop on Software Engineering for Resilient Systems*, 2010

# Contribuciones y agradecimientos (II)

## Publicaciones en progreso...

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

## Agradecimientos

- José Merseguer y Simona Bernardi
  - Grandes amigos, y mejor profesionales

# Contribuciones y agradecimientos (II)

## Publicaciones en progreso...

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

## Agradecimientos

- José Merseguer y Simona Bernardi
  - Grandes amigos, y mejor profesionales
- Asociación No CON Name

# Contribuciones y agradecimientos (II)

## Publicaciones en progreso...

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

## Agradecimientos

- José Merseguer y Simona Bernardi
  - Grandes amigos, y mejor profesionales
- Asociación No CON Name
- **A vosotros por aguantar este tostón...**

# Seguridad en el diseño: desde el principio

**Ricardo J. Rodríguez**

[rjrodriguez@unizar.es](mailto:rjrodriguez@unizar.es)

<http://www.ricardojrodriguez.es>



**Universidad**  
Zaragoza

16 de Septiembre, 2011

Este trabajo ha sido realizado en colaboración con **Simona Bernardi** (Centro Universitario de la Defensa) y **José Merseguer** (Universidad de Zaragoza)

**No cON Name 2011**

Barcelona, España