Security in model driven development – a survey

Jostein Jensen, Martin Gilje Jaatun

jostein.jensen@idi.ntnu.no, matin.g.jaatun@sintef.no

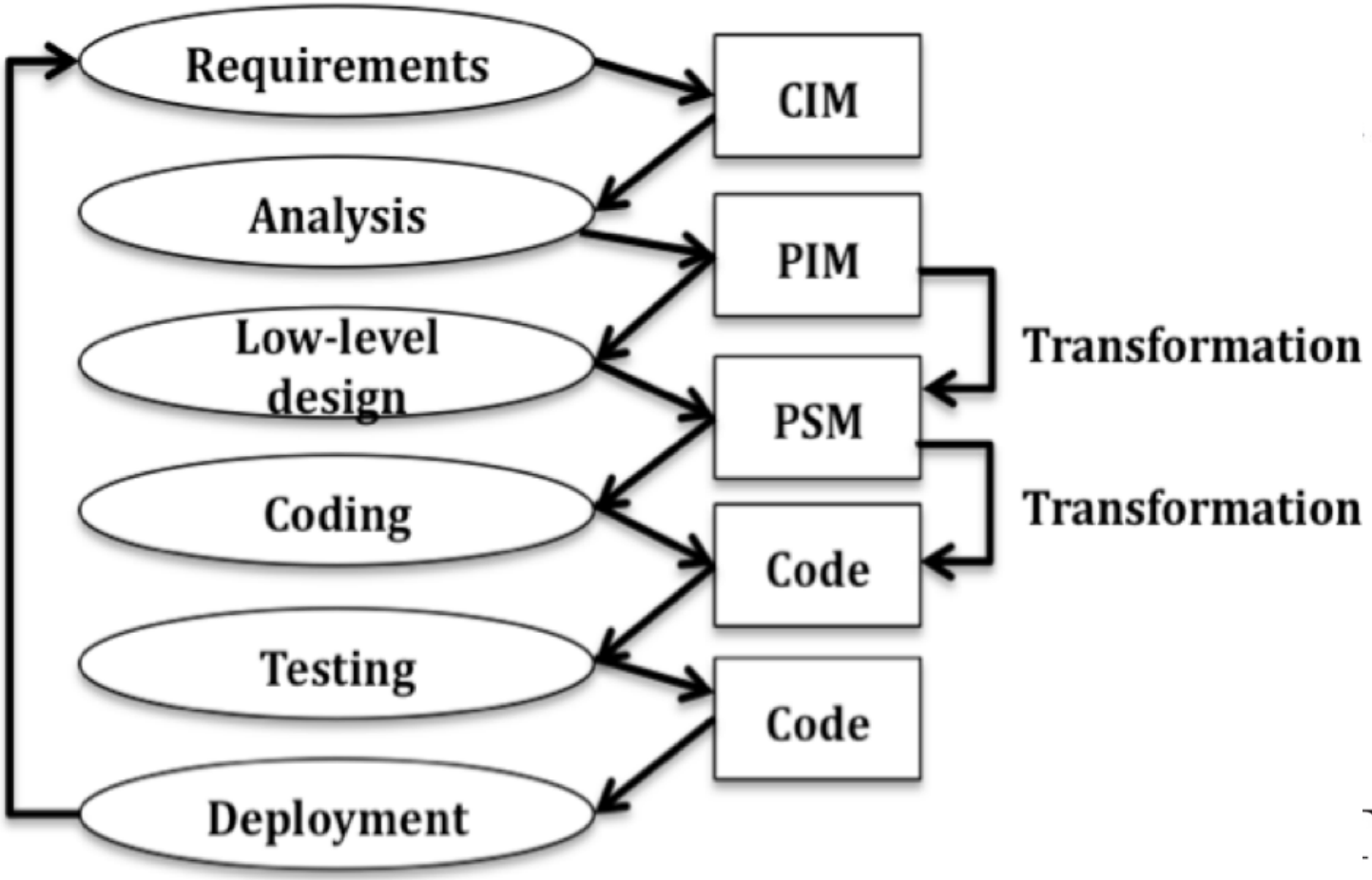
Agenda

- Introduction
- Research method
- Results
- Suggestions for further research

Introduction

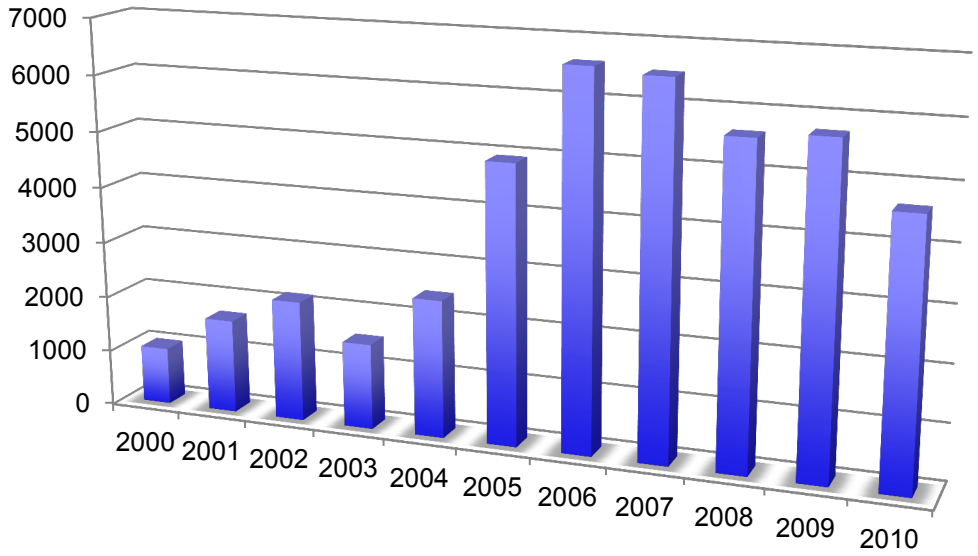
- MDD – promising approach to software development
- Aim to improve:
  - Portability
  - Platform independence
  - Cross-platform interoperability

The MDA Lifecycle



Why MDD and Security?

- Security often considered late (if at all)
- Early security focus will reduce cost
- Security + MDD = perfect for creating more secure applications?



Numbers from NIST NVD

NTNU
Norwegian University of Science and Technology

Research questions

RQ1	What are the **major scientific initiatives** describing automatic code generation from design models within the context of security in MDD?
RQ2	What **empirical studies** exist on the topic of security within MDD/MDA?
RQ3	What are the **strengths of the evidence** showing that security aspects successfully can be modelled as an inherent property and translated to more secure code?

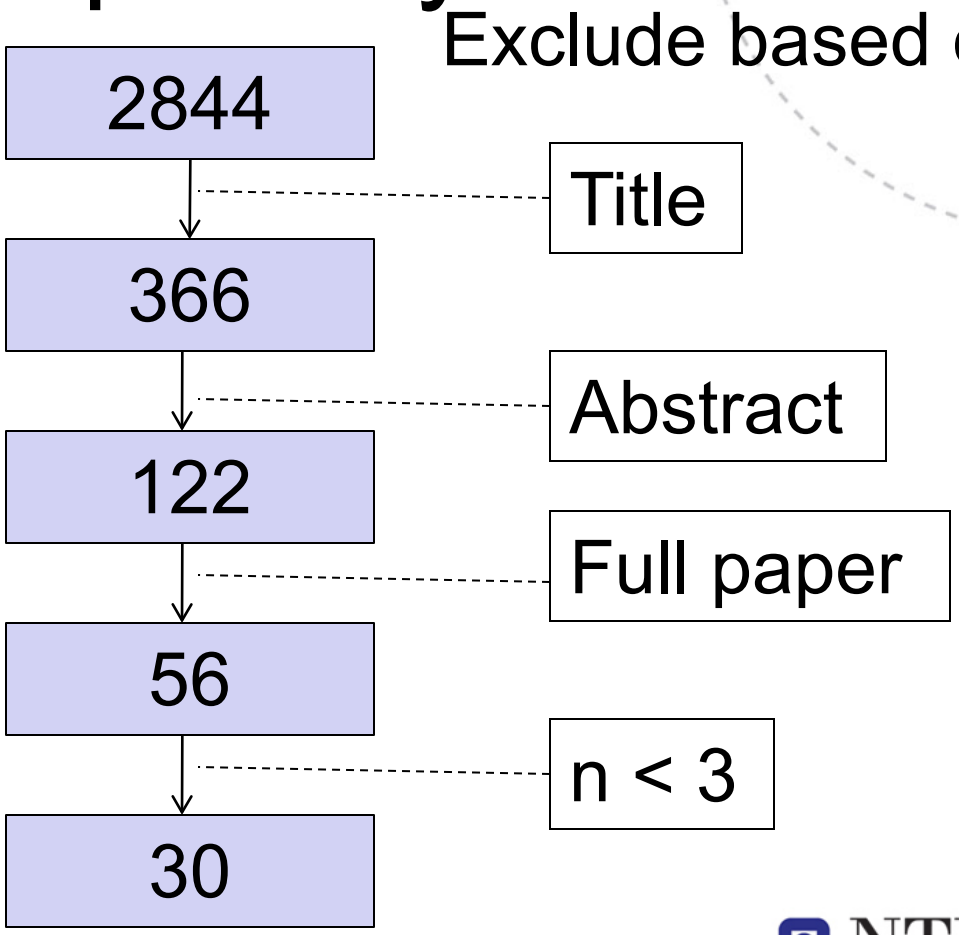
Identification of research

Approach: Systematic review

Sources: IEEE Xplore, ACM Digital Library, ISI Web of Knowledge, Compendex

Search phrase: ("model driven development" **OR** "model driven architecture" **OR** MDD **OR** MDA) **AND** Security

Selection of primary studies



NTNU
Norwegian University of Science and Technology

Major secure MDD initiatives (RQ1)

- Model driven security
- SECTET
- Secure development of data warehouses
- Security in business process models
- Secure smart card application development

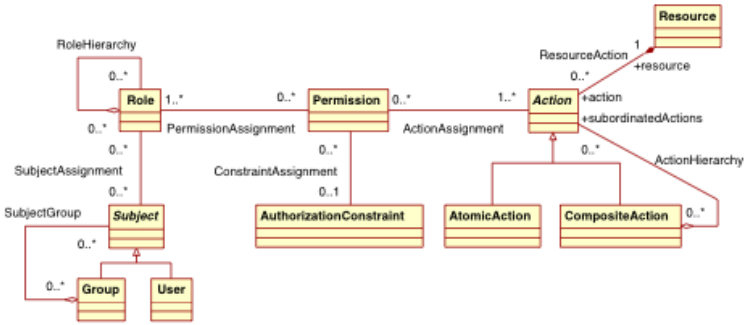


Figure 8: SecureUML metamodel

Figure copied from: D. Basin, J. Doser, and T. Lodderstedt, "Model Driven Security: From UML models to access control infrastructures," *Acm Transactions on Software Engineering and Methodology, vol. 15, pp. 39-91, Jan 2006.*

NTNU
Norwegian University of Science and Technology

Model Driven Security

- D. Basin, J. Doser, T. Lodderstedt
- Focus: Include RBAC in design models
  - Secure UML

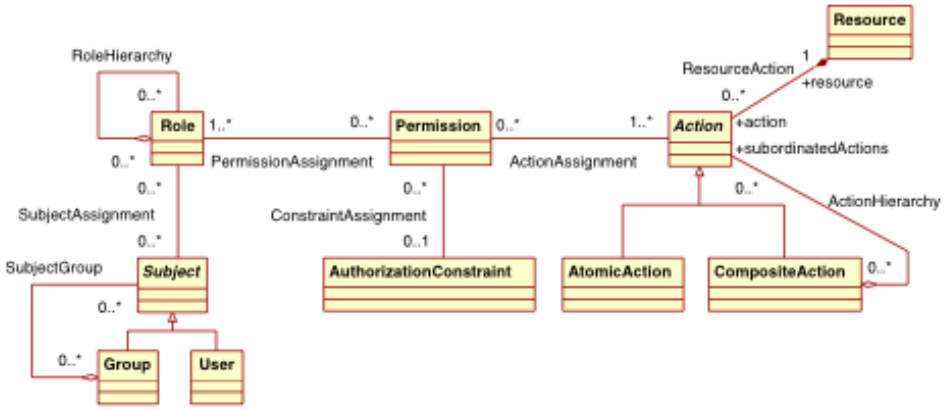


Figure 8: SecureUML metamodel

Figure copied from: D. Basin, J. Doser, and T. Lodderstedt, "Model Driven Security: From UML models to access control infrastructures," *Acm Transactions on Software Engineering and Methodology, vol. 15, pp. 39-91, Jan 2006.*

NTNU
Norwegian University of Science and Technology

SECTET

- M. Alam, R. Breu, M. Breu, M. Hafner, A. Nowak, J. Seifert, B. Weber, Z. Xinwen,

- Fokus: Integrate access control in interface models (SOA, web services)
  - SECTET-PL (OCL-based)

Secure Development of DW

- C. Blanco, E. Fernandez-Medina, I. de Guzman, A. Hernandez, J. Mazon, R. Perez-Castillo, M. Piattini, E. Soler, V. Stefanov, J. Trujillo

- Focus: Full life cycle support, from security in CIM to code
  - i★, UML profiles, OCL

Security in BPM

- A. Rodriguez, E. Fernandez-Medina, M. Piattini
- Focus: Model security aspects into business process models and convert to CIM

Secure Smart Card apps

- N. Moebius, K. Stenzel, H. Grandy, W. Reif
- Focus: define CIM and transform into card PSM, functional PSM and formal PSM.
  - The latter to be analysed to determine the correctness with respect to security of their applications.

Empirical studies (RQ2, RQ3)

- No indication that empirical studies exists
  - Impossible to answer RQ2 and RQ3

Discussion

- Lack of standardisation
  - Implications for the promises of MDD (interoperability, portability)
- Modelling of dynamic security aspects
- System hardening
- Complexity

Suggestions for further research

- Empirical research should be performed to determine whether security successfully can be included properly in MDD/MDA to build more secure systems.
- Modelling of security should be included as a standardisation activity in the MDD frameworks, such as MDA.
- Research should be performed to find an approach for modelling of input validation constraints.

Questions?