Partial state-of-the-art of model-driven security (MDS)

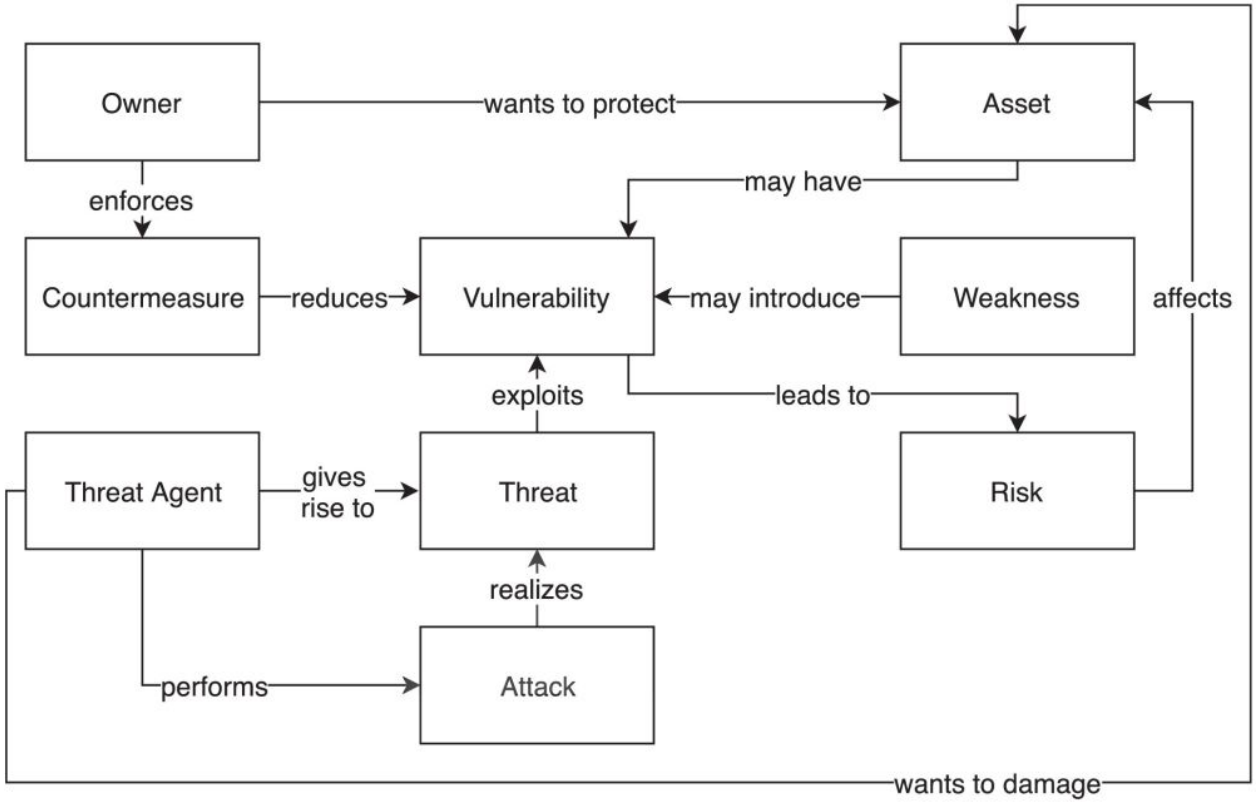
Nan MESSE
nan.messe@irit.fr

Institut de Recherche
en Informatique de Toulouse
CNRS - INP - UT3 - UT1 - UT2J

Keywords

- Model(-)based security
- Model(-)driven security
- Security/secure by design
- Threat modeling
- Risk analysis/assessment

Basic security-related concepts and their relations



Nan MESSE. Security by Design : An asset-based approach to bridge the gap between architects and security experts. 2021

Why MDS?

- Detect and prevent vulnerabilities early in the SDLC [1]
- Reduce maintenance cost [2,5]
- Better communication between security experts and domain experts [2,5]
- Design security at different levels of abstraction, while maintaining traceability between low-level and high-level concepts [2]
- Enable the application of formal methods [3,5]
- Bridge the gap between security requirement and design [5]

[1] GEISMANN, Johannes et BODDEN, Eric. A systematic literature review of model-driven security engineering for cyber–physical systems. *Journal of Systems and Software*, 2020, vol. 169, p. 110697.
[2] SHAKED, Avi et REICH, Yoram. Model-based Threat and Risk Assessment for Systems Design. In : *ICISSP*. 2021. p. 331-338.
[3] NGUYEN, Phu H., KLEIN, Jacques, LE TRAON, Yves, *et al.* A systematic review of model-driven security. In : *2013 20th Asia-Pacific Software Engineering Conference (APSEC)*. IEEE, 2013. p. 432-441.

Challenges

- Its adoption in practice is not yet widespread [2]
- The evolution of the system and the evolution of the threat [2]
- Legacy systems [1]
- Lack of formality, automation, process-integration and evaluation [3]
- Security properties have to be considered in a special way since they are non-functional properties [6]
- The security of platform layer is not often considered [7]

[2] VAN DEN BERGHE, Alexander, YSKOUT, Koen, SCANDARIATO, Riccardo, *et al.* A Lingua Franca for Security by Design. In : *2018 IEEE Cybersecurity Development (SecDev)*. IEEE, 2018. p. 69-76.
[5] Omar Masmali, Omar Badreddin. Model Driven Security: A Systematic Mapping Study. Software Engineering. Vol. 7, No. 2, 2019, pp. 30-38.
[6] NGUYEN, Phu H., KRAMER, Max, KLEIN, Jacques, *et al.* An extensive systematic review on the model-driven development of secure systems. *Information and Software Technology*, 2015, vol. 68, p. 62-81.

Dimensions

- Composant
  - Cyber level
  - Platform level
    - Runtime environment
    - Physical level

- Hierarchy / Relation
- Data
- Human
- Context

Fig. 1. Phases of the secure software development life cycle.

[7] GEISMANN, Johannes et BODDEN, Eric. A systematic literature review of model-driven security engineering for cyber–physical systems. *Journal of Systems and Software*, 2020, vol. 169, p. 110697.

Requirements

- Introduce the security aspect (control) since the requirement phase [2]
- Support for formal threat specification and formal security analysis [3,7]
- Support for automated transformation from models to implementation code [3]
- Increase the degree of automation of tracing and refining security requirements into implemented security solutions [7]
- Support different layers of the system [7]
- Allow compositional analyses (SoS) [7]
- Deal with both fully known parts and only partially known (or even unknown) parts of the system [7]
- The threat model should be extensible [7]
- The threat model should be strongly connected with system model [7]
- Deal with third-party code vulnerabilities [7]

[7] GEISMANN, Johannes et BODDEN, Eric. A systematic literature review of model-driven security engineering for cyber–physical systems. *Journal of Systems and Software*, 2020, vol. 169, p. 110697.

Standards

- MITRE
  - CAPEC
  - CWE
  - CVE
  - CPE
- Common Criteria
- OWASP
- SQUARE Process
- NIST SP 800-160

Methodologies discussed in [3]

- **SecureUML**
  - **Focus on access control constraints based on RBAC**
  - **Lack of support for formal analysis**
- **UMLSec**
  - **Address multiple security concerns (CIA)**
  - **Lack of automated transformation from models to implementation code**
- **SECTET**
  - **Secure web services by leveraging the OCL for specifying RBAC**
  - **Focus on generating security infrastructure (XACML), not all the source code**
- **SECUREMDD**
  - **specific for developing secure smart card application**
- **Secure data warehouses (DWs)**
  - **specific for developing secure DWs**

[3] NGUYEN, Phu H., KLEIN, Jacques, LE TRAON, Yves, *et al.* A systematic review of model-driven security. In : *2013 20th Asia-Pacific Software Engineering Conference (APSEC)*. IEEE, 2013. p. 432-441.

Other Methodologies

Platform specificity of the selected approaches.

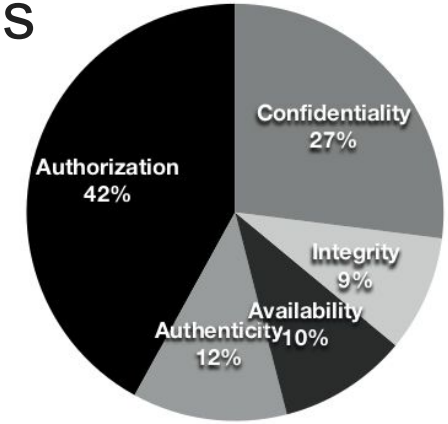
Approach	General	PS	CPS
SecureUML (Basin, 2006)	✓		
UMLsec (Jürjens, 2005)	✓		
SECTET (Hafner et al., 2006)	✓		
ModelSec (Sánchez et al., 2009)	✓		
Motii (2017)	✓		
Security4UML (Neri et al., 2013)	✓		
ISSEP (Ruiz et al., 2015)	✓		
SecureMDD (Moebius et al., 2009)		✓	
Security-enhanced SPACE (Gunawan et al., 2011)		✓	
Neureiter et al. (2016)		✓	
DREMS (Levendovszky et al., 2014)			✓
ProCom (Saadatmand and Leveque, 2012)			✓
Wasicek et al. (2014)			✓
Al Faruque et al. (2015)			✓
Eby et al. (2007)			✓
SysML-Sec (Li et al., 2018)			✓
SEED (Vasilevskaya, 2015)			✓

- **SoSSec [4]**
  - **Application domain: Systems-of-Systems (SoS)**
- **TRADES [2]**
  - **A domain specific language for security by design**

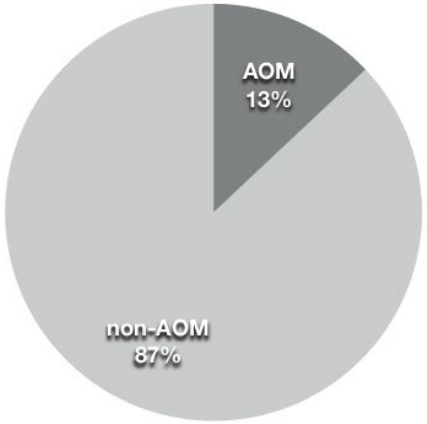
[2] SHAKED, Avi et REICH, Yoram. Model-based Threat and Risk Assessment for Systems Design. In : *ICISSP*. 2021. p. 331-338.
[4] EL HACHEM, Jamal, AL KHALIL, Tarek, CHIPRIANOV, Vanea, *et al.* A model driven method to design and analyze secure architectures of systems-of-systems. In : *2017 22nd International Conference on Engineering of Complex Computer Systems (ICECCS)*. IEEE, 2017. p. 166-169.
[7] GEISMANN, Johannes et BODDEN, Eric. A systematic literature review of model-driven security engineering for cyber–physical systems. *Journal of Systems and Software*, 2020, vol. 169, p. 110697.

Observations

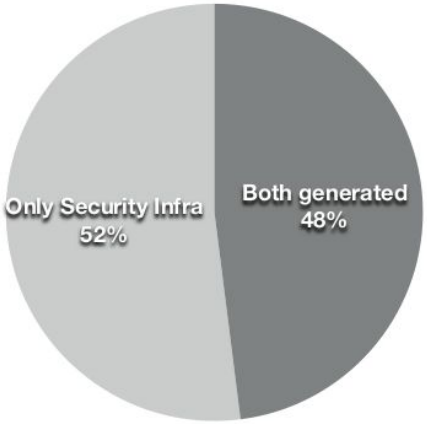
a) Security concerns addressed by MDS



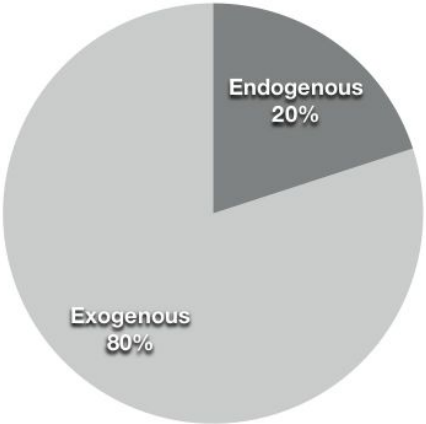
b) Aspect-Oriented Modeling vs. non-AOM



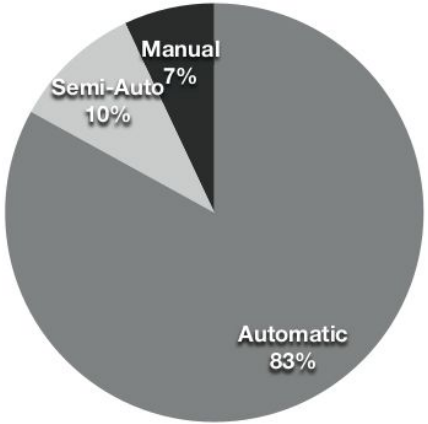
c) Code or Security Infrastructures generated?



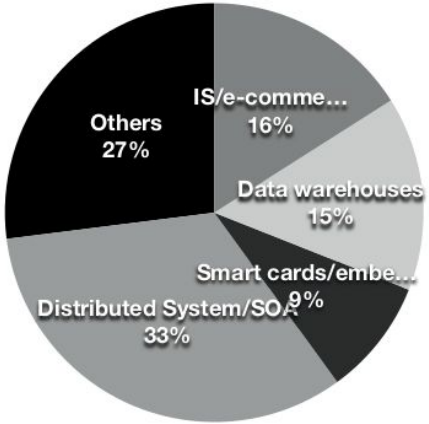
d) Transformations level



e) Transformations Automation



f) Application Domains of MDS



[3] NGUYEN, Phu H., KLEIN, Jacques, LE TRAON, Yves, *et al.* A systematic review of model-driven security. In : *2013 20th Asia-Pacific Software Engineering Conference (APSEC)*. IEEE, 2013. p. 432-441.

Observations

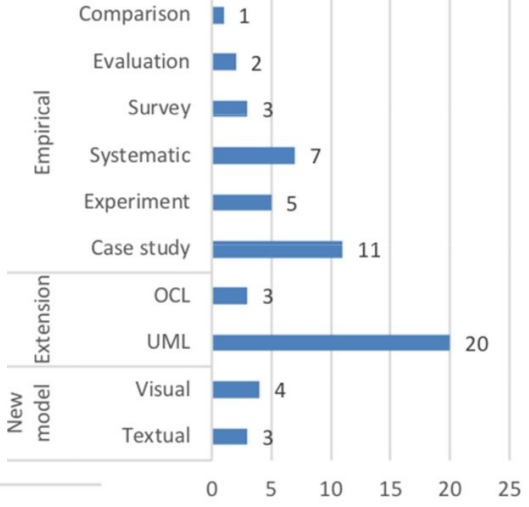


Figure 7. *Paper's main contribution.*

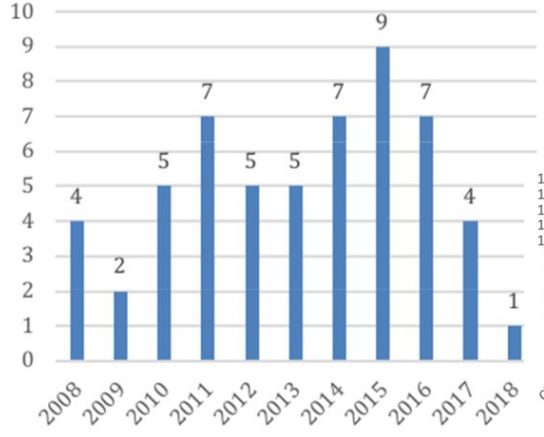


Figure 3. *Distribution of publication in ten years.*

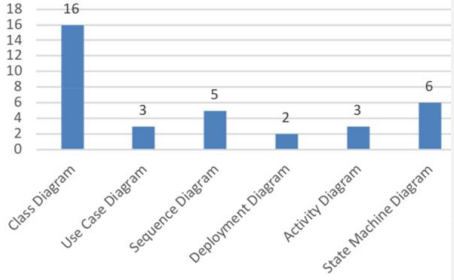


Figure 8. *UML Extensions distribution.*

Table 6. *This Authors geographic classification.*

Continent	Country	Authors		
		Primary	Others	Total
Europe	Germany	16	5	21
	France	11	2	13
	Luxembourg	2		2
	Norway	3		3
	Netherlands	1		1
	Austria	2		2
	Sweden		1	1
	UK	1	1	2
	Italy	1		1
	Hungary	1		1
	Belgium	1	1	2
North America	USA	1		1
	Canada	3	1	4
Africa	Morocco	1		1
	Tunisia		1	1
Asia	Malaysia	2		2
	Japan	2		2
	Bangladesh	1		1
	India	2		2
	Pakistan	1		1
	Iran	1		1
Australia	Australia	1		1
Total		56	14	70

[5] Omar Masmali, Omar Badreddin. Model Driven Security: A Systematic Mapping Study. Software Engineering. Vol. 7, No. 2, 2019, pp. 30-38.

Community

KU Leuven, BELGIUM

Koen Yskout
Riccardo Scandariato
Wouter Joosen

Germany

Jan Jürjens
Johannes Geismann
Eric Bodden

SnT, University of Luxembourg

Phu H. Nguyen
Jacques Klein
Yves Le Traon

Observations

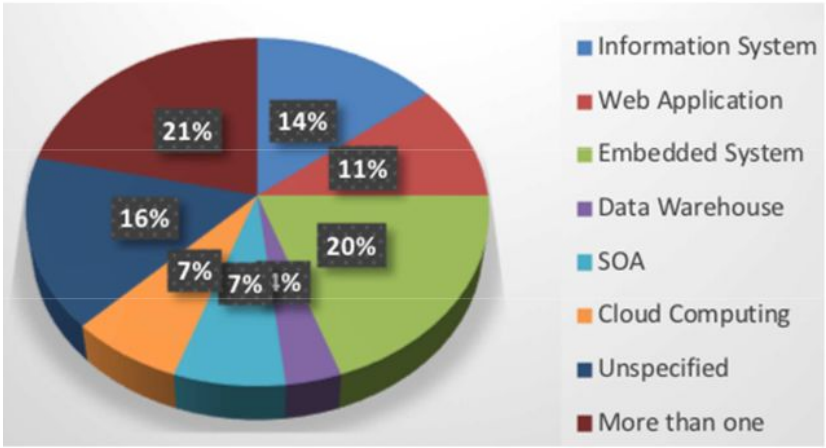


Figure 9. *Classification of the application domain.*

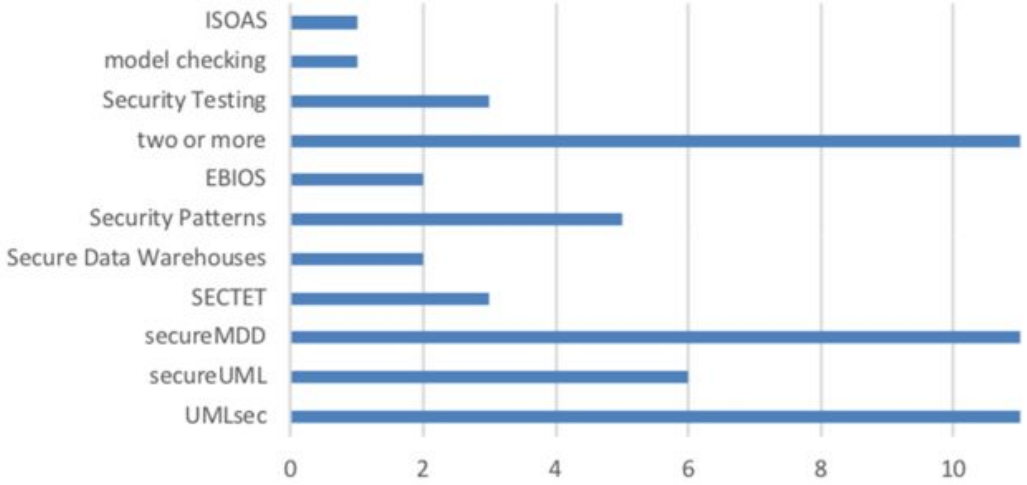


Figure 10. *MDS approaches.*

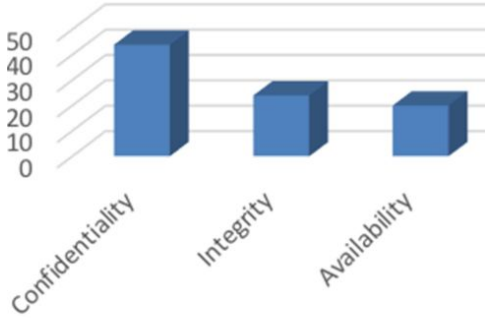


Figure 11. *Security concerns distribution.*

[5] Omar Masmali, Omar Badreddin. Model Driven Security: A Systematic Mapping Study. Software Engineering. Vol. 7, No. 2, 2019, pp. 30-38.

Potential research directions

- MDS approach (e.g. DSL) dealing with multiple security concerns [3]
- Evaluate MDS approaches with empirical studies or benchmarks [3]
- A common extensible threat model that is usable by all involved disciplines and stakeholders [7]
- Alignment of viewpoints from different system layers and the security layer
- The secure integration of third-party code into the system but also into the threat modeling approach [7]
- Common evaluation scenarios (EVITA project, CoCoMe, etc), with a list of weaknesses [7]
- Continuous integration of security requirement and security by design in DevSecOps

Conclusion

- MDS has resulted in a large number of publications, including general approaches and domain specific approaches.
- No systematic review on MDS after 2015 [6]
- More automated, formalized, towards DevSecOps !