

Model-based Security Engineering with UML: The Last Decade and Towards the Future (Keynote)

Jan Jürjens

Software Engineering, TU Dortmund and Fraunhofer ISST
Dortmund, Germany, <http://jan.jurjens.de>

1. Model-based Security Engineering

The current state of the art in developing security-critical software and systems in practice is far from satisfactory: New security vulnerabilities are discovered on an almost daily basis. To address this problem, there has been a significant amount of work over the last 10 years on providing model-based development approaches based on the Unified Modeling Language which aim to raise the trustworthiness of security-critical systems (see Fig. 1 for a visualization of the main ideas and [6, 7, 2, 10, 8, 5, 1, 3, 4, 9] for some examples and overviews). Recently, model-based security has even managed to gain entry into Gartner's "hype cycle".

This keynote talk gives an overview over some developments in this field over the last 10 years, discusses the current state of affairs with respect to foundations, tool-support and industrial applications, and considers what might be particularly promising current and future developments.

One such current development is that of supporting evolution: Although approaches like those mentioned above do improve the trustworthiness of systems, they usually have a significant cost associated with their use. Also, most of these approaches focus on ensuring that security properties will be enforced during the initial development of the system. However, software systems are becoming increasingly long-living and undergo evolution throughout their lifetime. In order to enforce that the system remains secure despite its later evolution (which is bound to happen with most practical systems), one would usually have to apply the secure software development methodology from scratch. With ongoing evolution cycles, this will create costs that are in most cases unrealistic to meet. We therefore need a secure software development approach that supports maintaining the needed levels of security even through later software evolution. There exist some initiatives towards this goal (for example the EU project "Secure Change"), of which some results will be presented.

Acknowledgement: Partially supported by the EU project "Security Engineering for Lifelong Evolvable Systems (Secure Change)" (ICT-FET-231101).

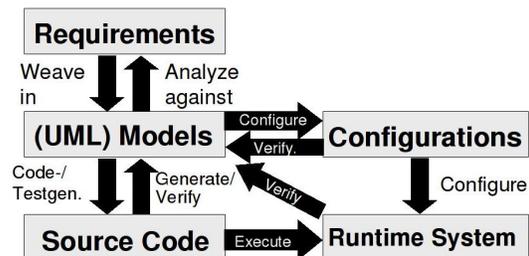


Figure 1. Model-based Security Engineering
References

- [1] D. Basin, J. Doser, and T. Lodderstedt. Model driven security: From UML models to access control infrastructures. *ACM Trans. Softw. Eng. Methodol.*, 15(1):39–91, 2006.
- [2] R. Breu, K. Burger, M. Hafner, J. Jürjens, G. Popp, G. Wimmel, and V. Lotz. Key issues of a formally based process model for security engineering. In *16th Int. Conf. Software & Systems Engineering & their Applications (ICSSEA)*, 2003.
- [3] F. den Braber, I. Hogganvik, M. Lund, K. Stolen, and F. Vraalsen. Model-based security analysis in seven steps – a guided tour to the CORAS method. *BT Technology Journal*, 25(1):101–117, 2007.
- [4] E. Fernández-Medina, J. Trujillo, R. Villarroel, and M. Piatini. Developing secure data warehouses with a UML extension. *Information Systems*, 32(6):826–856, 2007.
- [5] P. Giorgini, F. Massacci, and N. Zannone. Security and trust requirements engineering. In *FOSAD 2004/2005*, volume 3655 of *LNCS*, pages 237–272. Springer, 2005.
- [6] J. Jürjens. Towards development of secure systems using UMLsec. In *FASE'01*, volume 2029 of *LNCS*, pages 187–200. Springer, 2001.
- [7] J. Jürjens. *Principles for Secure Systems Design*. PhD thesis, Oxford University Computing Laboratory, 2002.
- [8] J. Jürjens. *Secure Systems Development with UML*. Springer, 2005.
- [9] J. Jürjens. Security and dependability engineering. In *Security and dependability for Ambient Intelligence*, number 3655 in *LNCS*, pages 21–36. Springer, 2009.
- [10] I. Ray, N. Li, R. France, and D.-K. Kim. Using UML to visualize Role-Based Access Control constraints. In *SACMAT 2004*, pages 115–124, 2004.