

# Model-based Security Engineering for Evolving Systems

Jan Jürjens

Open University (UK) and Microsoft Research (Cambridge)

[J.Jurjens@open.ac.uk](mailto:J.Jurjens@open.ac.uk)

**Abstract.** There is growing demand to evolve systems continuously to meet changing business needs, new regulations and policies, novel technologies and computing infrastructures. Unfortunately, the pace of required change affects developers' ability to establish and maintain desirable levels of quality of systems. Therefore, the aim of the Secure Change project is to develop techniques and tools that ensure "lifelong" compliance to security, privacy and dependability requirements of long-running evolving software systems. We present work towards addressing this challenge, namely an approach for modelbased security verification which supports change by providing a traceability link to the implementation. The approach uses a design model in the UML security extension UMLsec which can be formally verified against high-level security requirements such as secrecy and authenticity. An implementation of the specification can then be verified against the model through the traceability link. The approach supports software evolution in so far as the traceability mapping is updated when refactoring operations are regressively performed using our tool-supported refactoring technique. The proposed method has been applied to an implementation of the Internet security protocol SSL.