DOCTORAL CANDIDATE:	Gencer Erdogan
DEGREE:	Philosophiae Doctor
FACULTY:	Faculty of Mathematics and Natural Sciences
DEPARTMENT:	Department of Informatics
AREA OF EXPERTISE:	Security, Risk Analysis, Model-based Testing
SUPERVISORS:	Ketil Stølen, Professor, UiO (main supervisor)
	Lillian Røstad, Associate Professor II, NTNU
DATE OF DISPUTATION:	13th of January 2016
DISSERTATION TITLE:	*CORAL: A Model-Based Approach to Risk-Driven Security Testing*

The continuous increase of sophisticated cyber security risks exposed to the public, industry, and government through the web, mobile devices, social media, as well as targeted attacks via state-sponsored cyberespionage, clearly show the need for software security. Security testing is one of the most important practices to assure an acceptable level of security. However, security testers face the problem of determining the tests that are most likely to reveal severe security vulnerabilities. This is important in order to focus security testing on the most risky aspects of a system.

This thesis addresses the abovementioned problem and proposes an approach to support security testing with security risk assessment (risk-driven security testing). In particular, this thesis proposes a model-based approach to risk-driven security testing, named CORAL, which is specifically developed to help security testers select and design test cases based on the available risk picture. CORAL consists of seven steps supported by a risk analysis language. The risk analysis language is a modeling language based on UML interactions, and is formalized by an abstract syntax and a schematically defined natural-language semantics.

As part of the development and evaluation process of CORAL, we carried out three industrial case studies. In the first two case studies, we investigated how risk assessment may be used to identify security tests, as well as how security testing may be used to improve security risk analysis. The experiences we obtained from these two industrial case studies helped us to, among other things, shape the CORAL approach. In the third case study we carried out the CORAL approach in an industrial setting in order to evaluate its applicability. The results indicate that CORAL supports security testers in producing risk models that are valid and directly testable. By directly testable risk models we mean risk models that can be reused and specified as test cases based on the interactions in the risk models. This, in turn, helps testers to select and design test cases according to the most severe security risks posed on the system under test.