Doctoraat Vincent Naessens:

A Methodology for Anonymity Control in Electronic Services using Credentials

Vincent Naessens was born on March 23, 1977 in Kortrijk, Belgium. He received a Bachelor degree (Kandidaat Informatica) and a Master's degree (Licentiaat Informatica) in computer science from the Katholieke Universiteit Leuven. In 1999 he graduated at the K.U.Leuven with the thesis 'A Security Framework for Distributed Java Applications'. The same year, he started working as an assistant at the K.U.Leuven Campus Kortrijk and conducted research in the DistriNet (Distributed systems and computer Networks) research group at the Department of Computer Science at the K.U.Leuven. From October 2000 until September 2004, he worked on an IWT project on Anonymity and Privacy in Electronic Services. He received a PhD in Engineering in 2006. His promotor was Prof. Dr. ir. Bart De Decker.

The organization of all kinds of personal and business affairs is being digitized. At the same time, the Internet is gaining importance as a basic communication mechanism, which opens up a lot of these digitized processes to outsiders. The correct operation of these applications is fundamental and security/control is more than ever a crucial concern. Yet today, the identity and on-line behaviour of individuals is routinely recorded; users often have little knowledge of or control over such surveillance. A number of privacy-enhancing technologies have been developed in the last years in order to make systems that comply with the privacy requirements. Some of these technologies can be used as building blocks for secure systems. However, designing controlled anonymous applications is no sinecure.
His PhD work presents a methodology for designing controlled anonymous applications using the multi-paradigm modelling principles. Multi-paradigm modelling is introduced as a challenging approach for domain-specific modelling and has proven its feasibility in many fields. The advantage of using multiple formalisms in the design process of controlled anonymous applications is twofold. First, vertical multi-modelling allows to model at different levels of abstraction. Second, horizontal multi-modelling allows to derive models that are suitable for analysis and evaluation.

Analysis phase

control requirements:
- *(a) order/multiplicity constraints*
- *(b) access constraints*
- *(c) control measures*

performance requirements

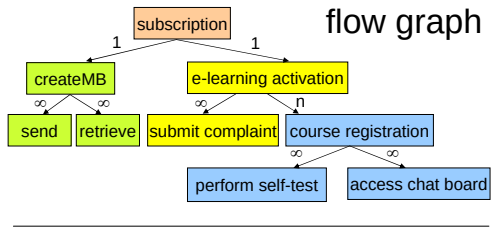
trust requirements

anonymity requirements

Conceptual design phase

order/multiplicity constraints →

flow graph



Types of service providers in an electronic student environment
- *Registrar*
- *Administrator mail servers*
- *Administrator e-learning environment*
- *Teacher*

unlinkability properties

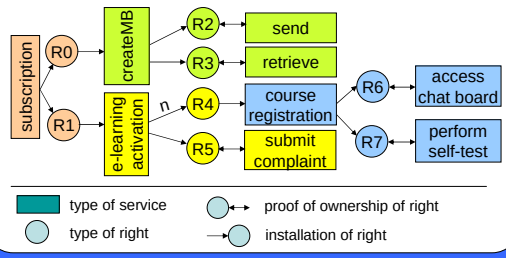
trust properties

control measures

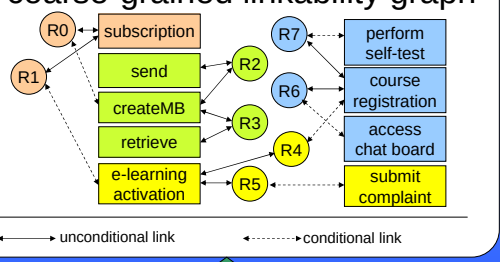
access constraints →

performance properties →

coloured Petri Net



coarse-grained linkability graph



Implementation phase

high-level credential primitives → fine-grained linkability graph

formalism
transformation
modelling constraints
generating properties
conflict detection
consistency check