Popular science summary of the PhD thesis

PhD student	Sébastien Pierre Christophe Gondron
Title of the PhD thesis	Vertical Composition of Distributed Systems
PhD school/Department	DTU Compute

Science summary

* Please give a short popular summary in Danish or English (approximately half a page) suited for the publication of the title, main content, results and innovations of the PhD thesis also including prospective utilizations hereof. The summary should be written for the general public interested in science and technology:

Communicating on networks, like the Internet, requires to run a wide variety of security protocols. The specification and the analysis of their security properties is a fully-fledged research area. However, despite their actual deployment within real environment, security protocols have been mostly and comprehensively considered in isolation. Only little work has been undertaken about their compositions. Indeed, being proven secure in isolation is not a guarantee that their compositions are also secure.

In the literature, three families of compositions are classically identified: parallel, sequential and vertical. Previous results focus on parallel and sequential compositions. These compositionality results have a modular form: “given a suite of protocols that satisfy certain sufficient conditions and that are secure in isolation then their composition is a secure system as well”. These conditions are easy to check statically.

The main objective of this thesis is to formalize a paradigm for vertical composition of stateful protocols. We can notably model trace-based properties, such as confidentiality or authentication; we are however limited when it comes to equivalence-based properties, such as privacy-type properties, which are of uttermost importance on the Internet. This is the reason why we extended in this thesis (α, β)-privacy. This approach allows to express privacy goals as reachability properties and opens the way for vertical compositionality results that also encompass privacy-type properties.

Please email the summary to the PhD secretary at the department