Sebastian Alexander Mödersheim - DTU Orbit (07/02/2019)

Mödersheim, Sebastian Alexander
samo@dtu.dk
Department of Applied Mathematics and Computer Science - Associate Professor
Formal Methods

Research outputs:

**Alpha-Beta Privacy**
Research output: Research - peer-review › Report – Annual report year: 2018

**A Typing Result for Stateful Protocols**
Research output: Research - peer-review › Article in proceedings – Annual report year: 2018

**A Typing Result for Stateful Protocols - Extended Version**
Research output: Research - peer-review › Report – Annual report year: 2018

**Stateful Protocol Composition**
Research output: Research - peer-review › Article in proceedings – Annual report year: 2018

**Stateful Protocol Composition - Extended Version**
Research output: Research - peer-review › Report – Annual report year: 2018

**The LIGHTest Foundation**
Research output: Research - peer-review › Report – Annual report year: 2018

**Formalizing and proving a typing result for security protocols in Isabelle/HOL**
Research output: Research - peer-review › Article in proceedings – Annual report year: 2017

**AIF-ω: Set-Based Protocol Abstraction with Countable Families**
Research output: Research - peer-review › Article in proceedings – Annual report year: 2016

**Security protocol specification and verification with AnBx**
Research output: Research - peer-review › Journal article – Annual report year: 2016

**Security Protocols: Specification, Verification, Implementation, and Composition**
Alice and Bob: Reconciling Formal Models and Implementation

Set-Pi: Set Membership pi-Calculus

Typing and compositionality for security protocols: A generalization to the geometric fragment

Typing and Compositionality for Security Protocols: A Generalization to the Geometric Fragment (Extended Version)

A Sound Abstraction of the Parsing Problem

A Sound Abstraction of the Parsing Problem (Extended Version)

Foundational aspects of security

Sufficient Conditions for Vertical Composition of Security Protocols (Extended Version)

Verification of Stateful Protocols - Set-Based Abstractions in the Applied Pi-Calculus

Defining Privacy Is Supposed to Be Easy

Detecting and Preventing Beacon Replay Attacks in Receiver-Initiated MAC Protocols for Energy Efficient WSNs
Verifying SeVeCom Using Set-based Abstraction
Research output: Research › Report – Annual report year: 2011

Verifying SeVeCom Using Set-based Abstraction
Research output: Research - peer-review › Article in proceedings – Annual report year: 2011

Vertical Protocol Composition
Research output: Research - peer-review › Article in proceedings – Annual report year: 2011

Abstraction by Set-Membership: Verifying Security Protocols and Web Services with Databases
Research output: Research - peer-review › Article in proceedings – Annual report year: 2010

A Formal Model of Identity Mixer
Research output: Research - peer-review › Article in proceedings – Annual report year: 2010

ASLan++ — A Formal Security Specification Language for Distributed Systems
Research output: Research - peer-review › Article in proceedings – Annual report year: 2011

Constraint Differentiation: Search-Space Reduction for the Constraint-Based Analysis of Security Protocols
Research output: Research - peer-review › Journal article – Annual report year: 2010

Verification Based on Set-Abstraction Using the AIF Framework
Research output: Research › Report – Annual report year: 2010

Projects:

Logical Foundations of AI Algorithms
Jensen, A. B., Villadsen, J. & Mödersheim, S. A.
01/02/2019 → 31/01/2022
Project: PhD

Vertical Composition of Distributed Systems
Gondron, S. P. C., Mödersheim, S. A. & Lluch Lafuente, A.
Grundforskningsfonden
01/07/2018 → 30/06/2021
Project: PhD
**Composec: Secure Composition of Distributed Systems**
Forskningsrådsfinansiering
01/10/2015 → 12/12/2018
Project: PhD

**Formalization of Algorithms and Logical inference Systems in Proof Assistants**
Institut stipendie (DTU)
15/09/2015 → 14/11/2018
Project: PhD

**Modeling and Verifying eID Protocols (Future ID)**
Anden EU-finansiering
15/12/2012 → 24/02/2016
Project: PhD

**Trusted Cryptography**
Kölbl, S., Rechberger, C., Knudsen, L. R., Mödersheim, S. A., Johansson, T., Rijmen, V., Johansson, T. & Rijmen, V.
Eksternt finansieret virksomhed
01/12/2013 → 12/12/2016
Project: PhD

**Attacker Models for Ubiquitous Computing**
Papini, D., Sharp, R., Jensen, C. D., Mödersheim, S. A. & Skou, A. J.
Institut stipendie (DTU)
01/10/2009 → 24/05/2013
Project: PhD

**Static Analysis for Model Checking**
Terepeta, M. T., Nielsen, H. R., Nielsen, F., Mödersheim, S. A., Cortesi, A. & Jensen, T.
1/3 FUU, 1/3 inst 1/3 Andet
01/08/2010 → 25/10/2013
Project: PhD