Content dependent information flow control
Information flow control extends access control by not only regulating who is allowed to access what data but also the subsequent use of the data. Applications within communications systems require such information flow control to be dependent on the actual contents of the data. We develop a combined Hoare logic and type system for enforcing content dependent information flow policies dealing with both integrity and confidentiality. We establish the soundness of the Hoare logic with respect to an instrumented operational semantics and illustrate the development on a running example. We also argue that a well-established approach to non-interference fails to distinguish between integrity and confidentiality. The development is performed for programs written in a concurrent language with synchronous communication and separate data domains.
A coordination language for databases

We present a coordination language for the modeling of distributed database applications. The language, baptized Klaim-DB, borrows the concepts of localities and nets of the coordination language Klaim but re-incarnates the tuple spaces of Klaim as databases. It provides high-level abstractions and primitives for the access and manipulation of structured data, with integrity and atomicity considerations. We present the formal semantics of Klaim-DB and develop a type system that avoids potential runtime errors such as certain evaluation errors and mismatches of data format in tables, which are monitored in the semantics. The use of the language is illustrated in a scenario where the sales from different branches of a chain of department stores are aggregated from their local databases. Raising the abstraction level and encapsulating integrity checks in the language primitives have benefited the modeling task considerably.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Formal Methods, University of Queensland
Authors: Li, X. (Intern), Wu, X. (Ekstern), Lluch Lafuente, A. (Intern), Nielson, F. (Intern), Nielson, H. R. (Intern)
Number of pages: 52
Publication date: 2017
Main Research Area: Technical/natural sciences

Publication information
Journal: Logical Methods in Computer Science
Volume: 13
Issue number: 1
ISSN (Print): 1860-5974
Ratings:
BFI (2018): BFI-level 2
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 2
Web of Science (2017): Indexed Yes
BFI (2016): BFI-level 2
Scopus rating (2016): CiteScore 1.02 SJR 0.493 SNIP 1.149
Web of Science (2016): Indexed yes
BFI (2015): BFI-level 2
Scopus rating (2015): SJR 0.579 SNIP 1.179 CiteScore 1.11
BFI (2014): BFI-level 2
Scopus rating (2014): SJR 0.55 SNIP 1.312 CiteScore 1.06
BFI (2013): BFI-level 2
Scopus rating (2013): SJR 0.63 SNIP 1.324 CiteScore 1.08
ISI indexed (2013): ISI indexed yes
Web of Science (2013): Indexed yes
BFI (2012): BFI-level 2
Scopus rating (2012): SJR 0.624 SNIP 1.042 CiteScore 0.85
ISI indexed (2012): ISI indexed yes
Web of Science (2012): Indexed yes
BFI (2011): BFI-level 2
Scopus rating (2011): SJR 0.656 SNIP 1.03 CiteScore 0.89
ISI indexed (2011): ISI indexed no
BFI (2010): BFI-level 2
Scopus rating (2010): SJR 0.668 SNIP 1.396
BFI (2009): BFI-level 2
Scopus rating (2009): SJR 0.881 SNIP 2.621
BFI (2008): BFI-level 2
Original language: English
Coordination Language, Database, Distribution
Asynchronous Distributed Execution of Fixpoint-Based Computational Fields

Coordination is essential for dynamic distributed systems whose components exhibit interactive and autonomous behaviors. Spatially distributed, locally interacting, propagating computational fields are particularly appealing for allowing components to join and leave with little or no overhead. Computational fields are a key ingredient of aggregate programming, a promising software engineering methodology particularly relevant for the Internet of Things. In our approach, space topology is represented by a fixed graph-shaped field, namely a network with attributes on both nodes and arcs, where arcs represent interaction capabilities between nodes. We propose a SMuC calculus where μ-calculus-like modal formulas represent how the values stored in neighbor nodes should be combined to update the present node. Fixpoint operations can be understood globally as recursive definitions, or locally as asynchronous converging propagation processes. We present a distributed implementation of our calculus. The translation is first done mapping SMuC programs into normal form, purely iterative programs and then into distributed programs. Some key results are presented that show convergence of fixpoint computations under fair asynchrony and under reinitialization of nodes. The first result allows nodes to proceed at different speeds, while the second one provides robustness against certain kinds of failure. We illustrate our approach with a case study based on a disaster recovery scenario, implemented in a prototype simulator that we use to evaluate the performance of a recovery strategy.
Atomistic Galois insertions for flow sensitive integrity

Several program verification techniques assist in showing that software adheres to the required security policies. Such policies may be sensitive to the flow of execution and the verification may be supported by combinations of type systems and Hoare logics. However, this requires user assistance and to obtain full automation we shall explore the over-approximating nature of static analysis. We demonstrate that the use of atomistic Galois insertions constitutes a stable framework in which to obtain sound and fully automatic enforcement of flow sensitive integrity. The framework is illustrated on a concurrent language with local storage and polyadic synchronous communication.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science , Formal Methods
Authors: Nielson, F. (Intern), Nielson, H. R. (Intern)
Pages: 82-107
Publication date: 2017
Main Research Area: Technical/natural sciences

Publication information
Journal: Computer Languages, Systems and Structures
Volume: 50
ISSN (Print): 1477-8424
Ratings:
BFI (2018): BFI-level 1
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 1
Web of Science (2017): Indexed Yes
BFI (2016): BFI-level 1
Scopus rating (2016): CiteScore 1.98 SJR 0.539 SNIP 1.272
BFI (2015): BFI-level 1
Scopus rating (2015): SJR 0.179 SNIP 0.883 CiteScore 0.72
BFI (2014): BFI-level 1
Scopus rating (2014): SJR 0.458 SNIP 1.109 CiteScore 0.89
BFI (2013): BFI-level 1
Scopus rating (2013): SJR 0.386 SNIP 0.996 CiteScore 1.12
ISI indexed (2013): ISI indexed yes
Web of Science (2013): Indexed yes
BFI (2012): BFI-level 1
Scopus rating (2012): SJR 0.242 SNIP 0.708 CiteScore 0.6
ISI indexed (2012): ISI indexed yes
BFI (2011): BFI-level 1
Scopus rating (2011): SJR 0.306 SNIP 0.701 CiteScore 0.91
ISI indexed (2011): ISI indexed yes
BFI (2010): BFI-level 1
Scopus rating (2010): SJR 0.341 SNIP 0.765
BFI (2009): BFI-level 1
Scopus rating (2009): SJR 0.599 SNIP 1.46
Web of Science (2009): Indexed yes
BFI (2008): BFI-level 1
Automated specification and verification of Web-based applications

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Formal Methods, Consiglio Nazionale delle Ricerche
Authors: ter Beek, M. H. (Ekstern), Lluch Lafuente, A. (Intern)
Pages: 51-51
Publication date: 2017
Main Research Area: Technical/natural sciences

Publication information
Journal: Journal of Logical and Algebraic Methods in Programming
Volume: 87
Ratings:
Web of Science (2018): Indexed yes
Web of Science (2017): Indexed Yes
Scopus rating (2016): CiteScore 0.88 SJR 0.394 SNIP 1.175
Scopus rating (2015): SJR 0.25 SNIP 1.166 CiteScore 0.55
Original language: English
DOIs:
10.1016/j.jlamp.2016.11.004
Publication: Research › Editorial – Annual report year: 2017

BProVe: A formal verification framework for business process models

Business Process Modelling has acquired increasing relevance in software development. Available notations, such as BPMN, permit to describe activities of complex organisations. On the one hand, this shortens the communication gap between domain experts and IT specialists. On the other hand, this permits to clarify the characteristics of software systems introduced to provide automatic support for such activities. Nevertheless, the lack of formal semantics hinders the automatic verification of relevant properties. This paper presents a novel verification framework for BPMN 2.0, called BProVe. It is based on an operational semantics, implemented using MAUDE, devised to make the verification general and effective. A complete tool chain, based on the Eclipse modelling environment, allows for rigorous modelling and analysis of Business Processes. The approach has been validated using more than one thousand models available on a publicly accessible repository. Besides showing the performance of BProVe, this validation demonstrates its practical benefits in identifying correctness issues in real models.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Formal Methods, University of Camerino
Authors: Corradini, F. (Ekstern), Fornari, F. (Ekstern), Polini, A. (Ekstern), Re, B. (Ekstern), Tiezzi, F. (Ekstern), Vandin, A. (Intern)
BProVe: Tool support for business process verification

This demo introduces BProVe, a tool supporting automated verification of Business Process models. BProVe analysis is based on a formal operational semantics defined for the BPMN 2.0 modelling language, and is provided as a freely accessible service that uses open standard formats as input data. Furthermore a plug-in for the Eclipse platform has been developed making available a tool chain supporting users in modelling and visualising, in a friendly manner, the results of the verification. Finally we have conducted a validation through more than one thousand models, showing the effectiveness of our verification tool in practice. (Demo video: https://youtu.be/iF5OM7vKtDA)

Choreographing Cyber-Physical Distributed Control Systems for the Energy Sector

Energy Systems are facing a significant change in the way their management and control is conceived. With the introduction of distributed and renewable energy based resources, a shift to a more distributed operation paradigm is emerging, overturning the conventional top-down design and operation principles. This shift creates a demand for distributed control systems (DCS) to facilitate a more adaptive and efficient operation of power networks. One key challenge here is to ensure the required reliability of distributed control systems. Whereas proven strategies exist for reliable control for coordination of physical actions, with increasing distribution of such control, the reliability and degradation properties in response to communications issues become more important. We build on the notion of Quality Choreographies, a formal model for the development of failure-aware distributed systems, and discuss how quality choreographies respond to the needs presented by DCS. We demonstrate
their applicability by modelling the Bully Algorithm, one of the de-facto election algorithms used in coordination of DCS.

**Effect-driven QuickChecking of compilers**

How does one test a language implementation with QuickCheck (aka. property-based testing)? One approach is to generate programs following the grammar of the language. But in a statically-typed language such as OCaml too many of these candidate programs will be rejected as ill-typed by the type checker. As a refinement Pałka et al. propose to generate programs in a goal-directed, bottom-up reading up of the typing relation. We have written such a generator. However many of the generated programs has output that depend on the evaluation order, which is commonly under-specified in languages such as OCaml, Scheme, C, C++, etc. In this paper we develop a type and effect system for conservatively detecting evaluation-order dependence and propose its goal-directed reading as a generator of programs that are independent of evaluation order. We illustrate the approach by generating programs to test OCaml's two compiler backends against each other and report on a number of bugs we have found doing so.

**Formal Analysis of Graphical Security Models**

The increasing usage of computer-based systems in almost every aspects of our daily life makes more and more dangerous the threat posed by potential attackers, and more and more rewarding a successful attack. Moreover, the complexity of these systems is also increasing, including physical devices, software components and human actors
interacting with each other to form so-called socio-technical systems. The importance of socio-technical systems to modern societies requires verifying their security properties formally, while their inherent complexity makes manual analyses impracticable.

Graphical models for security offer an unrivalled opportunity to describe socio-technical systems, for they allow to represent different aspects like human behaviour, computation and physical phenomena in an abstract yet uniform manner. Moreover, these models can be assigned a formal semantics, thereby allowing formal verification of their properties. Finally, their appealing graphical notations enable to communicate security concerns in an understandable way also to non-experts, often in charge of the decision making.

This dissertation argues that automated techniques can be developed on graphical security models to evaluate qualitative and quantitative security properties of socio-technical systems and to synthesise optimal attack and defence strategies.

In support to this claim we develop analysis techniques for widely-used graphical security models such as attack trees and attack-defence trees. Our analyses cope with the optimisation of multiple parameters of an attack and defence scenario. Improving on the literature, in case of conflicting parameters such as probability and cost we compute the set of optimal solutions in terms of Pareto efficiency. Moreover, we investigate the relation between attack and attack-defence trees and stochastic models in a verification-oriented setting, with the aim of leveraging the great many mature tools and analysis techniques developed for instance in the area of games.

**General information**
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Formal Methods
Authors: Aslanyan, Z. (Intern), Nielsen, F. (Intern), Probst, C. W. (Intern)
Number of pages: 208
Publication date: 2017

**Publication information**
Place of publication: Kgs. Lyngby
Publisher: Technical University of Denmark (DTU)
Original language: English

Series: DTU Compute PHD-2016
Number: 421
ISSN: 0909-3192
Main Research Area: Technical/natural sciences
Electronic versions:
phd421_Aslanyan_Z.pdf

**Relations**
Projects:
Formal Analysis of Graphical Security Models
Publication: Research › Ph.D. thesis – Annual report year: 2017

**Formalizing and proving a typing result for security protocols in Isabelle/HOL**
There are several works on the formalization of security protocols and proofs of their security in Isabelle/HOL; there have also been tools for automatically generating such proofs. This is attractive since a proof in Isabelle gives a higher assurance of the correctness than a pen-and-paper proof or the positive output of a verification tool. However several of these works have used a typed model, where the intruder is restricted to "well-typed" attacks. There also have been several works that show that this is actually not a restriction for a large class of protocols, but all these results so far are again pen-and-paper proofs. In this work we present a formalization of such a typing result in Isabelle/HOL. We formalize a constraint-based approach that is used in the proof argument of such typing results, and prove its soundness, completeness and termination. We then formalize and prove the typing result itself in Isabelle. Finally, to illustrate the real-world feasibility, we prove that the standard Transport Layer Security (TLS) handshake satisfies the main condition of the typing result.

**General information**
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Formal Methods
Authors: Hess, A. V. (Intern), Modersheim, S. (Intern)
Pages: 451-63
Publication date: 2017

**Host publication information**
Title of host publication: Proceedings of 2017 IEEE 30th Computer Security Foundations Symposium
Fraud Risk Modelling: Requirements Elicitation in the Case of Telecom Services

Telecom providers are losing tremendous amounts of money due to fraud risks posed to Telecom services and products. Currently, they are mainly focusing on fraud detection approaches to reduce the impact of fraud risks against their services. However, fraud prevention approaches should also be investigated in order to further reduce fraud risks and improve the revenue of Telecom providers. Fraud risk modelling is a fraud prevention approach aims at identifying the potential fraud risks, estimating the damage and setting up preventive mechanisms before the fraud risks lead to actual losses. In this paper, we highlight the important requirements for a usable and context-aware fraud risk modelling approach for Telecom services. To do so, we have conducted two workshops with experts from a Telecom provider and experts from multi-disciplinary areas. In order to show and document the requirements, we present two exemplary Telecom fraud scenarios, analyse and estimate the impacts of fraud risks qualitatively.

High Performance with Prescriptive Optimization and Debugging

Parallel programming is the dominant approach to achieve high performance in computing today. Correctly writing efficient and fast parallel programs is a big challenge mostly carried out by experts. We investigate optimization and debugging of parallel programs.

We argue that automatic parallelization and automatic vectorization is attractive as it transparently optimizes programs. The thesis contributes an improved dependence analysis for explicitly parallel programs. These improvements lead to more loops being vectorized, on average we achieve a speedup of 1.46 over the existing dependence analysis and vectorizer in GCC.

Automatic optimizations often fail for theoretical and practical reasons. When they fail we argue that a hybrid approach can be effective. Using compiler feedback, we propose to use the programmer’s intuition and insight to achieve high performance. Compiler feedback enlightens the programmer why a given optimization was not applied, and suggest how
to change the source code to make it more amenable to optimizations. We show how this can yield significant speedups and achieve 2.4 faster execution on a real industrial use case.

To aid in parallel debugging we propose the prescriptive debugging model, which is a user-guided model that allows the programmer to use his intuition to diagnose bugs in parallel programs. The model is scalable, yet capable enough, to be general-purpose. In our evaluation we demonstrate low run time overhead and logarithmic scalability. This enable the model to be used on extremely large parallel systems.

**General information**

State: Published
Organisations: Department of Applied Mathematics and Computer Science, Formal Methods, Embedded Systems Engineering
Authors: Jensen, N. B. (Intern), Probst, C. W. (Intern), Karlsson, S. (Intern)
Number of pages: 204
Publication date: 2017

**Publication information**

Place of publication: Kgs. Lyngby
Publisher: Technical University of Denmark (DTU)
Original language: English

Series: DTU Compute PHD-2016
Number: 437
ISSN: 0909-3192
Main Research Area: Technical/natural sciences
Electronic versions: phd437_Jensen_NB.pdf

**Relations**

Projects:
High Performance with Prescriptive Optimization and Debugging
Publication: Research › Ph.D. thesis – Annual report year: 2017

**Improving Loop Dependence Analysis**

Programmers can no longer depend on new processors to have significantly improved single-thread performance. Instead, gains have to come from other sources such as the compiler and its optimization passes. Advanced passes make use of information on the dependencies related to loops. We improve the quality of that information by reusing the information given by the programmer for parallelization. We have implemented a prototype based on GCC into which we also add a new optimization pass. Our approach improves the amount of correctly classified dependencies resulting in 46% average improvement in single-thread performance for kernel benchmarks compared to GCC 6.1.

**General information**

State: Published
Organisations: Formal Methods, Department of Applied Mathematics and Computer Science, Embedded Systems Engineering
Authors: Jensen, N. B. (Intern), Karlsson, S. (Intern)
Number of pages: 24
Pages: 1-24
Publication date: 2017
Main Research Area: Technical/natural sciences

**Publication information**

Journal: Acm Transactions on Architecture and Code Optimization
Volume: 14
Issue number: 3
ISSN (Print): 1544-3973
Ratings:
Web of Science (2018): Indexed yes
Web of Science (2017): Indexed yes
Scopus rating (2016): SJR 0.315 SNIP 1.068 CiteScore 1.61
Scopus rating (2015): SJR 0.366 SNIP 1.198 CiteScore 1.42
Scopus rating (2014): SJR 0.343 SNIP 1.235 CiteScore 1.35
Scopus rating (2013): SJR 0.326 SNIP 1.147 CiteScore 1.45
Information Flow for Timed Automata

One of the key demands of cyberphysical systems is that they meet their safety goals. Timed Automata has established itself as a formalism for modelling and analysing the real-time safety aspects of cyberphysical systems. Increasingly it is also demanded that cyberphysical systems meet a number of security goals for confidentiality and integrity. Information Flow Control is an approach to ensuring that there are no flows of information that violate the stated security policy.

Many-to-Many Information Flow Policies

Information flow techniques typically classify information according to suitable security levels and enforce policies that are based on binary relations between individual levels, e.g., stating that information is allowed to flow from one level to another. We argue that some information flow properties of interest naturally require coordination patterns that involve sets of security levels rather than individual levels: some secret information could be safely disclosed to a set of confidential channels of incomparable security levels, with individual leaks considered instead illegal; a group of competing agencies might agree to disclose their secrets, with individual disclosures being undesired, etc. Motivated by this we propose a simple language for expressing information flow policies where the usual admitted flow relation between individual security levels is replaced by a relation between sets of security levels, thus allowing to capture coordinated flows of information. The flow of information is expressed in terms of causal dependencies and the satisfaction of a policy is defined with respect to an event structure that is assumed to capture the causal structure of system computations. We suggest applications to secret exchange protocols, program security and security architectures, and discuss the relation to classic notions of information flow control.
Microservices: Yesterday, Today, and Tomorrow

Microservices is an architectural style inspired by service-oriented computing that has recently started gaining popularity. Before presenting the current state of the art in the field, this chapter reviews the history of software architecture, the reasons that led to the diffusion of objects and services first, and microservices later. Finally, open problems and future challenges are introduced. This survey primarily addresses newcomers to the discipline, while offering an academic viewpoint on the topic. In addition, we investigate some practical issues and point out a few potential solutions.

Model checking exact cost for attack scenarios

Attack trees constitute a powerful tool for modelling security threats. Many security analyses of attack trees can be seamlessly expressed as model checking of Markov Decision Processes obtained from the attack trees, thus reaping the benefits of a coherent framework and a mature tool support. However, current model checking does not encompass the exact cost analysis of an attack, which is standard for attack trees. Our first contribution is the logic erPCTL with cost-related operators. The extended logic allows to analyse the probability of an event satisfying given cost bounds and to compute the exact cost of an event. Our second contribution is the model checking algorithm for erPCTL. Finally, we apply our framework to the analysis of attack trees.
QuickChecking static analysis properties

A static analysis can check programs for potential errors. A natural question that arises is therefore: who checks the checker? Researchers have given this question varying attention, ranging from basic testing techniques, informal monotonicity arguments, thorough pen-and-paper soundness proofs, to verified fixed point checking. In this paper, we demonstrate how quickchecking can be useful to test a range of static analysis properties with limited effort. We show how to check a range of algebraic lattice properties, to help ensure that an implementation follows the formal specification of a lattice. Moreover, we offer a number of generic, type-safe combinators to check transfer functions and operators on lattices, to help ensure that these are, eg, monotone, strict, or invariant. We substantiate our claims by quickchecking a type analysis for the Lua programming language.
Time dependent policy-based access control

Access control policies are essential to determine who is allowed to access data in a system without compromising the data's security. However, applications inside a distributed environment may require those policies to be dependent on the actual content of the data, the flow of information, while also on other attributes of the environment such as the time. In this paper, we use systems of Timed Automata to model distributed systems and we present a logic in which one can express time-dependent policies for access control. We show how a fragment of our logic can be reduced to a logic that current model checkers for Timed Automata such as UPPAAL can handle and we present a translator that performs this reduction. We then use our translator and UPPAAL to enforce time-dependent policy-based access control on an example application from the aerospace industry.
An Adaptive Middleware for Improved Computational Performance

The performance improvements in computer systems over the past 60 years have been fueled by an exponential increase in energy efficiency. In recent years, the phenomenon known as the end of Dennard’s scaling has slowed energy efficiency improvements — but improving computer energy efficiency is more important now than ever. Traditionally, most improvements in computer energy efficiency have come from improvements in lithography — the ability to produce smaller transistors — and computer architecture - the ability to apply those transistors efficiently. Since the end of scaling, we have seen diminishing returns from developments in lithography and modern computer architectures are so complicated requiring significant programming effort to exploit efficiently —software developers undertaking such a task will need all the help they can get, in order to keep the programming effort down.

In this thesis we champion using software to improve energy efficiency — in particular we develop guidelines for reasoning and evaluating software performance on modern computers, and a middleware that has been designed for modern computers, improving computational performance both in terms of energy and execution time. Our middleware consists of a new power manager, synchronization libraries using hardware transactional memory (for locks, barriers, and task synchronization), and two concurrent map data structures, which can be deployed in computer systems with little to no effort. At a fundamental level, we are improving computational performance by exploiting modern hardware features, such as dynamic voltage-frequency scaling and transactional memory. Adapting software is an iterative process, requiring that we continually revisit it to meet new requirements or realities; a time consuming process which we hope to simplify by analyzing the realities of modern computers, and providing guidelines explaining how to get the most performance out of them.
Analysis of Security Protocols in Embedded Systems

Embedded real-time systems have been adopted in a wide range of safety-critical applications—including automotive, avionics, and train control systems—where the focus has long been on safety (i.e., protecting the external world from the potential damage caused by the system) rather than security (i.e., protecting the system from the external world). With increased connectivity of these systems to external networks the attack surface has grown, and consequently there is a need for securing the system from external attacks. Introducing security protocols in safety critical systems requires careful considerations on the available resources, especially in meeting real-time and resource constraints, as well as cost and reliability requirements. For this reason many proposed security protocols in this domain have peculiar features, not present in traditional security literature.

In this thesis we tackle the problem of analysing security protocols in safety critical embedded systems from multiple perspectives, extending current state-of-the-art analysis techniques where the combination of safety and security hinders our efforts. Examples of protocols in automotive control systems will follow throughout the thesis. We initially take a combined perspective of the safety and security features, by giving a security analysis and a schedulability analysis of the embedded protocols, with intertwined considerations. Then we approach the problem of the expressiveness of the tools used in the analysis, extending saturation-based techniques for formal protocol verification in the symbolic model. Such techniques gain much of their efficiency by coalescing all reachable states into a single set of facts. However, distinguishing different states is a requirement for modelling the protocols that we consider. Our effort in this direction is to extend saturation-based techniques so that enough state information can be modelled and analysed. Finally, we present a methodology for proving the same security properties in the computational model, by means of typing protocol implementations.

A Parametric Abstract Domain for Lattice-Valued Regular Expressions

We present a lattice-valued generalization of regular expressions as an abstract domain for static analysis. The parametric abstract domain rests on a generalization of Brzozowski derivatives and works for both finite and infinite lattices. We develop both a co-inductive, simulation algorithm for deciding ordering between two domain elements and a widening operator for the domain. Finally we illustrate the domain with a static analysis that analyses a communicating process.
against a lattice-valued regular expression expressing the environment’s network communication.

**General information**

State: Published
Organisations: Department of Applied Mathematics and Computer Science, Formal Methods
Authors: Midtgaard, J. (Intern), Nielson, F. (Intern), Nielson, H. R. (Intern)
Pages: 338-360
Publication date: 2016

**Host publication information**

Title of host publication: Proceedings of the 23rd International Symposium on Static Analysis (SAS 2016)
Publisher: Springer
ISBN (Print): 978-3-662-53412-0
ISBN (Electronic): 978-3-662-53413-7

**A Process Framework for Designing Software Reference Architectures for Providing Tools as a Service**

Software Reference Architecture (SRA), which is a generic architecture solution for a specific type of software systems, provides foundation for the design of concrete architectures in terms of architecture design guidelines and architecture elements. The complexity and size of certain types of software systems need customized and systematic SRA design and evaluation methods. In this paper, we present a software Reference Architecture Design process Framework (RADeF) that can be used for analysis, design and evaluation of the SRA for provisioning of Tools as a Service as part of a cloud-enabled workSPACE (TSPACE). The framework is based on the state of the art results from literature and our experiences with designing software architectures for cloud-based systems. We have applied RADeF SRA design two types of TSPACE: software architecting TSPACE and software implementation TSPACE. The presented framework emphasizes on keeping the conceptual meta-model of the domain under investigation at the core of SRA design strategy and use it as a guiding tool for design, evaluation, implementation and evolution of the SRA. The framework also emphasizes to consider the nature of the tools to be provisioned and underlying cloud platforms to be used while designing SRA. The framework recommends adoption of the multi-faceted approach for evaluation of SRA and quantifiable measurement scheme to evaluate quality of the SRA. We foresee that RADeF can facilitate software architects and researchers during design, application and evaluation of a SRA and its instantiations into concrete software systems.

**General information**

State: Published
Organisations: Department of Applied Mathematics and Computer Science, Formal Methods, IT University of Copenhagen
Authors: Chauhan, M. A. (Intern), Babar, M. A. (Ekstern), Probst, C. W. (Intern)
Pages: 111-126
Publication date: 2016

**Host publication information**

Title of host publication: Proceedings of the 17th International Conference on Product-Focused Software Process Improvement (PROFES 2016)
Publisher: Springer
ISBN (Print): 978-3-319-49093-9
ISBN (Electronic): 978-3-319-49094-6

**A Process Framework for Designing Software Reference Architectures for Providing Tools as a Service**

Software Reference Architecture (SRA), which is a generic architecture solution for a specific type of software systems, provides foundation for the design of concrete architectures in terms of architecture design guidelines and architecture elements. The complexity and size of certain types of software systems need customized and systematic SRA design and evaluation methods. In this paper, we present a software Reference Architecture Design process Framework (RADeF) that can be used for analysis, design and evaluation of the SRA for provisioning of Tools as a Service as part of a cloud-enabled workSPACE (TSPACE). The framework is based on the state of the art results from literature and our experiences with designing software architectures for cloud-based systems. We have applied RADeF SRA design two types of TSPACE: software architecting TSPACE and software implementation TSPACE. The presented framework emphasizes on keeping the conceptual meta-model of the domain under investigation at the core of SRA design strategy and use it as a guiding tool for design, evaluation, implementation and evolution of the SRA. The framework also emphasizes to consider the nature of the tools to be provisioned and underlying cloud platforms to be used while designing SRA. The framework recommends adoption of the multi-faceted approach for evaluation of SRA and quantifiable measurement scheme to evaluate quality of the SRA. We foresee that RADeF can facilitate software architects and researchers during design, application and evaluation of a SRA and its instantiations into concrete software systems.
Attack tree analysis for insider threats on the IoT using isabelle

The Internet-of-Things (IoT) aims at integrating small devices around humans. The threat from human insiders in "regular" organisations is real; in a fully-connected world of the IoT, organisations face a substantially more severe security challenge due to unexpected access possibilities and information flow. In this paper, we seek to illustrate and classify insider threats in relation to the IoT (by 'smart insiders'), exhibiting attack vectors for their characterisation. To model the attacks we apply a method of formal modelling of Insider Threats in the interactive theorem prover Isabelle. On the classified IoT attack examples, we show how this logical approach can be used to make the models more precise and to analyse the previously identified Insider IoT attacks using Isabelle attack trees.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Formal Methods, Middlesex University, University of Oxford
Authors: Kammüller, F. (Ekstern), Nurse, J. R. C. (Ekstern), Probst, C. W. (Intern)
Number of pages: 13
Pages: 234-246
Publication date: 2016

Host publication information
Volume: 9750
Publisher: Springer
Editor: Tryfonas, T.
ISBN (Print): 978-3-319-39380-3
ISBN (Electronic): 978-3-319-39381-0
Series: Lecture Notes in Computer Science
ISSN: 0302-9743
BFI conference series: Human-Computer Interaction (5000411)
Main Research Area: Technical/natural sciences
DOIs: 10.1007/978-3-319-39381-0_21
Source: FindIt
Source-ID: 2307015849
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

Enforcing Availability in Failure-Aware Communicating Systems
Choreographic programming is a programming-language design approach that drives error-safe protocol development in distributed systems. Motivated by challenging scenarios in Cyber-Physical Systems (CPS), we study how choreographic programming can cater for dynamic infrastructures where the availability of components may change at runtime. We introduce the Global Quality Calculus (GCq), a process calculus featuring novel operators for multiparty, partial and collective communications; we provide a type discipline that controls how partial communications refer only to available components; and we show that well-typed choreographies enjoy progress.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Formal Methods
Authors: López-Acosta, H. (Intern), Nielson, F. (Intern), Nielson, H. R. (Intern)
Pages: 195-211
Publication date: 2016
Fine-grained Information Flow for Concurrent Computation

It is essential to protect IT systems against security threats. An example would be the control of aircraft, which uses an internal network that passengers can access. It is important to ensure that malicious code on passenger equipment cannot endanger flight safety.

Information flow control is an important approach to the protection of systems against such threats. Notable examples include tainting analyses in languages such as Javascript, and program transformations on cryptographic algorithms to avoid information leakage through running time. A wide variety of techniques, including type systems and reference monitors, have been proposed in the context of programming languages and process calculi, to enforce such properties. The most widely used definitions of information flow security are noninterference-like properties.

For concurrent systems where processes communicate with each other to accomplish computational tasks, fine-grained security policies can be formulated by distinguishing between whether communication can happen, and what is communicated. As the first contribution of this PhD thesis, we formulate a noninterference-like property that takes all combinations of sensitivity levels for “whether” and “what” into consideration, emphasizing the importance of the integrity case where the former is more sensitive than the latter. This case captures the effect of Message Authentication Codes (MAC) and the consequence of Denial of Service (DoS) attacks. It is also proved that the property degenerates to a classical one when the two dimensions are intentionally blurred.

As the second contribution, we focus on the “what” dimension and further allow the flow policy to vary under different contents stored and communicated. This is the area of content-dependent (or conditional) information flow, which has recently been studied for sequential programs. We generalize the use and enforcement of content-dependent flow policies to concurrent, communicating processes. A security type system is developed, incorporating a Hoare logic component that provides approximations of the memory contents at different program points. Most proofs for the theoretical results on content-dependency are performed in the Coq proof assistant.

The third contribution of this thesis is the obtainment of compositionality results that support modular security analyses of computer systems.

A multiplexer pattern that separates sensitive and non-sensitive network traffic is used as a running example. Whether communications can happen is easily influenced by an attacker — attacking one of the incoming channels would suffice. In any case, the two data paths are still differentiable by the sensitivity levels of what is communicated. In case the destinations of messages are determined by their tagging, content-dependent policies are able to convey the correlation between the sensitivity level of a message and its tagging, and our Hoare-logic equipped type system allows a modular analysis of the overall system.
Formal modelling and analysis of socio-technical systems

Attacks on systems and organisations increasingly exploit human actors, for example through social engineering. This non-technical aspect of attacks complicates their formal treatment and automatic identification. Formalisation of human behaviour is difficult at best, and attacks on socio-technical systems are still mostly identified through brainstorming of experts. In this work we discuss several approaches to formalising socio-technical systems and their analysis. Starting from a flow logic-based analysis of the insider threat, we discuss how to include the socio aspects explicitly, and show a formalisation that proves properties of this formalisation. On the formal side, our work closes the gap between formal and informal approaches to socio-technical systems. On the informal side, we show how to steal a birthday cake from a bakery by social engineering.

Future-dependent Flow Policies with Prophetic Variables

Content-dependency often plays an important role in the information flow security of real world IT systems. Content dependency gives rise to informative policies and permissive static enforcement, and sometimes avoids the need for downgrading. We develop a static type system to soundly enforce future-dependent flow policies - policies that can depend on not only the current values of variables, but also their final values. The final values are referred to using what we call prophetic variables, just as the initial values can be referenced using logical variables in Hoare logic. We develop and enforce a notion of future-dependent security for open systems, in the spirit of "non-deducibility on strategies". We also illustrate our approach in scenarios where future-dependency has advantages over present-dependency and avoids mixtures of upgradings and downgradings.
Guaranteeing Privacy-Observing Data Exchange

Privacy is a major concern in large parts of the world when exchanging information. Ideally, we would like to be able to have fine-grained control about how information that we deem sensitive can be propagated and used. While privacy policy languages exist, it is not possible to control whether the entity that receives data is living up to its own policy specification. In this work we present our initial work on an approach that empowers data owners to specify their privacy preferences, and data consumers to specify their data needs. Using a static analysis of the two specifications, our approach then finds a communication scheme that complies with these preferences and needs. While applicable to online transactions, the same techniques can be used in development of IT systems dealing with sensitive data. To the best of our knowledge, no existing privacy policy languages supports negotiation of policies, but only yes/no answers. We also discuss how the same approach can be used to identify a qualitative level of sharing, where data may be shared according to, e.g., the level of trust to another entity.

Iterated Process Analysis over Lattice-Valued Regular Expressions

We present an iterated approach to statically analyze programs of two processes communicating by message passing. Our analysis operates over a domain of lattice-valued regular expressions, and computes increasingly better approximations of each process's communication behavior. Overall the work extends traditional semantics-based program
analysis techniques to automatically reason about message passing in a manner that can simultaneously analyze both values of variables as well as message order, message content, and their interdependencies.

Model Based Analysis of Insider Threats
In order to detect malicious insider attacks it is important to model and analyse infrastructures and policies of organisations and the insiders acting within them. We extend formal approaches that allow modelling such scenarios by quantitative aspects to enable a precise analysis of security designs. Our framework enables evaluating the risks of an insider attack to happen quantitatively. The framework first identifies an insider's intention to perform an inside attack, using Bayesian networks, and in a second phase computes the probability of success for an inside attack by this actor, using probabilistic model checking. We provide prototype tool support using Matlab for Bayesian networks and PRISM for the analysis of Markov decision processes, and validate the framework with case studies.

Modelling and Verifying Communication Failure of Hybrid Systems in HCSP
Hybrid systems are dynamic systems with interacting discrete computation and continuous physical processes. They have become ubiquitous in our daily life, e.g. automotive, aerospace and medical systems, and in particular, many of them are safety-critical. For a safety-critical hybrid system, the physical process evolves continuously with respect to time, and the discrete controller monitors and controls the physical process in a correct way such that the whole system satisfies the given safety requirements. The safety of hybrid systems depends heavily on the control from the controllers. However, in the presence of communication failure, the expected control from the controller will get lost and as a consequence the physical process cannot behave as expected. In this paper, we mainly consider the communication failure caused by the non-engagement of one party in communication action, i.e. the communication itself fails to occur. To address this issue,
this paper proposes a formal framework by extending HCSP, a formal modeling language for hybrid systems, for modeling and verifying hybrid systems in the absence of receiving messages due to communication failure. We present two inference systems for verifying the models in the framework by leveraging the expressivity of the assertion languages and the efficiency of proofs, and correspondingly implement two theorem provers in Isabelle/HOL. To illustrate our approach, we consider a case study on train on-board control system originating from Chinese Train Control System, for which the two provers are applied separately and the proof results are compared.

**General information**

State: Published
Organisations: Department of Applied Mathematics and Computer Science, Formal Methods, Chinese Academy of Sciences
Authors: Wang, S. (Ekstern), Nielson, F. (Intern), Nielson, H. R. (Intern), Zhan, N. (Ekstern)
Pages: 1111-1130
Publication date: 2016
Main Research Area: Technical/natural sciences

**Publication information**

Journal: Computer Journal
Volume: 60
Issue number: 8
ISSN (Print): 0010-4620
Ratings:
- BFI (2018): BFI-level 2
- Web of Science (2018): Indexed yes
- BFI (2017): BFI-level 2
- Web of Science (2017): Indexed Yes
- BFI (2016): BFI-level 2
- Scopus rating (2016): CiteScore 0.84 SJR 0.285 SNIP 0.664
- BFI (2015): BFI-level 2
- Scopus rating (2015): SJR 0.32 SNIP 0.683 CiteScore 0.79
- BFI (2014): BFI-level 2
- Scopus rating (2014): SJR 0.401 SNIP 1.202 CiteScore 1.14
- BFI (2013): BFI-level 2
- Scopus rating (2013): SJR 0.467 SNIP 1.342 CiteScore 1.42
- ISI indexed (2013): ISI indexed yes
- BFI (2012): BFI-level 2
- Scopus rating (2012): SJR 0.409 SNIP 1.269 CiteScore 1.39
- ISI indexed (2012): ISI indexed yes
- BFI (2011): BFI-level 2
- Scopus rating (2011): SJR 0.564 SNIP 1.4 CiteScore 1.35
- ISI indexed (2011): ISI indexed yes
- BFI (2010): BFI-level 2
- Scopus rating (2010): SJR 0.604 SNIP 1.238
- Web of Science (2010): Indexed yes
- BFI (2009): BFI-level 2
- Scopus rating (2009): SJR 0.717 SNIP 1.402
- BFI (2008): BFI-level 2
- Scopus rating (2008): SJR 0.63 SNIP 1.339
- Scopus rating (2007): SJR 0.77 SNIP 1.742
- Scopus rating (2006): SJR 0.572 SNIP 1.191
- Scopus rating (2005): SJR 0.495 SNIP 1.504
- Scopus rating (2004): SJR 0.548 SNIP 1.163
- Scopus rating (2003): SJR 0.433 SNIP 1.023
- Scopus rating (2002): SJR 0.566 SNIP 0.91
- Scopus rating (2001): SJR 0.416 SNIP 0.859
- Scopus rating (2000): SJR 0.267 SNIP 0.724
- Scopus rating (1999): SJR 0.212 SNIP 0.677
Quantitative Verification and Synthesis of Attack-Defence Scenarios

Attack-defence trees are a powerful technique for formally evaluating attack-defence scenarios. They represent in an intuitive, graphical way the interaction between an attacker and a defender who compete in order to achieve conflicting objectives. We propose a novel framework for the formal analysis of quantitative properties of complex attack-defence scenarios, using an extension of attack-defence trees which models temporal ordering of actions and allows explicit dependencies in the strategies adopted by attackers and defenders. We adopt a game-theoretic approach, translating attack-defence trees to two-player stochastic games, and then employ probabilistic model checking techniques to formally analyse these models. This provides a means to both verify formally specified security properties of the attack-defence scenarios and, dually, to synthesise strategies for attackers or defenders which guarantee or optimise some quantitative property, such as the probability of a successful attack, the expected cost incurred, or some multi-objective trade-off between the two. We implement our approach, building upon the PRISM-games model checker, and apply it to a case study of an RFID goods management system.

Security protocol specification and verification with AnBx

Designing distributed protocols is complex and requires actions at very different levels: from the design of an interaction flow supporting the desired application-specific guarantees to the selection of the most appropriate network-level protection mechanisms. To tame this complexity, we propose AnBx, a formal protocol specification language based on the popular Alice & Bob notation. AnBx offers channels as the main abstraction for communication, providing different authenticity and/or confidentiality guarantees for message transmission. AnBx extends existing proposals in the literature with a novel notion of forwarding channels, enforcing specific security guarantees from the message originator to the final
recipient along a number of intermediate forwarding agents. We give a formal semantics of AnBx in terms of a state transition system expressed in the AVISPA Intermediate Format. We devise an ideal channel model and a possible cryptographic implementation, and we show that, under mild restrictions, the two representations coincide, thus making AnBx amenable to automated verification with different tools. We demonstrate the benefits of the declarative specification style distinctive of AnBx by revisiting the design of two existing e-payment protocols: iKP and SET.

**General information**

State: Published  
Organisations: Department of Applied Mathematics and Computer Science, Formal Methods, Università Ca' Foscari Venezia, Newcastle University  
Authors: Bugliesi, M. (Ekstern), Calzavara, S. (Ekstern), Mödersheim, S. A. (Intern), Modesti, P. (Ekstern)

**Publication information**

Journal: Journal of Information Security and Applications  
Volume: 30  
ISSN (Print): 2214-2126  
Ratings:  
BFI (2018): BFI-level 1  
Web of Science (2018): Indexed yes  
BFI (2017): BFI-level 1  
BFI (2016): BFI-level 1  
Scopus rating (2016): SJR 0.377 SNIP 1.186 CiteScore 1.65  
BFI (2015): BFI-level 1  
Scopus rating (2015): SJR 0.268 SNIP 0.565  
BFI (2014): BFI-level 1  
Scopus rating (2014): SJR 0.184 SNIP 0.555  
BFI (2013): BFI-level 1  
Scopus rating (2013): SJR 0.152 SNIP 0.678  
ISI indexed (2013): ISI indexed no  
BFI (2012): BFI-level 1  
Scopus rating (2012): SJR 0.172 SNIP 0.481  
ISI indexed (2012): ISI indexed no  
BFI (2011): BFI-level 1  
Scopus rating (2011): SJR 0.191 SNIP 0.416  
ISI indexed (2011): ISI indexed no  
BFI (2010): BFI-level 1  
Scopus rating (2010): SJR 0.252 SNIP 0.828  
BFI (2009): BFI-level 1  
Scopus rating (2009): SJR 0.119 SNIP 0.422  
BFI (2008): BFI-level 1  
Scopus rating (2008): SJR 0.154 SNIP 0.295  
Scopus rating (2007): SJR 0.125 SNIP 0.082  
Scopus rating (2006): SJR 0.142 SNIP 0.28  
Scopus rating (2005): SJR 0.159 SNIP 0.549  
Scopus rating (2004): SJR 0.117 SNIP 0.113  
Scopus rating (2003): SJR 0.113 SNIP 0.182  
Scopus rating (2002): SJR 0.112 SNIP 0.409  
Scopus rating (2001): SJR 0.12 SNIP 0.189  
Scopus rating (2000): SJR 0.101 SNIP 0.035  
Scopus rating (1999): SJR 0.1 SNIP 0.2  
Original language: English  
Protocol specification, Protocol verification, Model-checking, e-payment  
DOIs:  
10.1016/j.jisa.2016.05.004  
Source: FindIt
Security Protocols: Specification, Verification, Implementation, and Composition

An important aspect of Internet security is the security of cryptographic protocols that it deploys. We need to make sure that such protocols achieve their goals, whether in isolation or in composition, i.e., security protocols must not suffer from any aw that enables hostile intruders to break their security. Among others, tools like OFMC [MV09b] and Proverif [Bla01] are quite efficient for the automatic formal verification of a large class of protocols. These tools use different approaches such as symbolic model checking or static analysis. Either approach has its own pros and cons, and therefore, we need to combine their strengths. Moreover, we need to ensure that the protocol implementation coincides with the formal model that we verify using such tools.

This thesis shows that we can simplify the formal verification of protocols in several ways. First, we introduce an Alice and Bob style language called SPS (Security Protocol Specification) language, that enables users, without requiring deep expertise in formal models from them, to specify a wide range of real-world protocols in a simple and intuitive way. Thus, SPS allows users to verify their protocols using different tools, and generate robust implementations in different languages. Moreover, SPS has the "ultimate" formal semantics for Alice and Bob notation in the presence of an arbitrary set of cryptographic operators and their algebraic theory. Despite its generality, this semantics is mathematically simpler than any previous attempt.

Second, we introduce two types of relative soundness results that reduce complex verification problems into simpler ones. The first kind is typing results showing that if a security protocol, that fulfills a number of sufficient conditions, has an attack then it has a well-typed attack. The second kind considers the parallel composition of protocols, showing that if the parallel composition of two protocols, that fulfill a number of sufficient conditions, allows for an attack then one of the protocols, at least, has an attack in isolation. In fact, we unify and generalize over prior relative soundness results. The most important generalization is the support for all security properties of the geometric fragment proposed by [Gut14].

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology
Authors: Almousa, O. (Intern), Mödersheim, S. A. (Intern), Nielson, H. R. (Intern)
Number of pages: 164
Publication date: 2016

Publication Information
Place of publication: Kgs. Lyngby
Publisher: Technical University of Denmark (DTU)
Original language: English

Series: DTU Compute PHD-2015
Number: 391
ISSN: 0909-3192
Main Research Area: Technical/natural sciences
Electronic versions: phd391_Almousa_O.pdf
Publication: Research › Ph.D. thesis – Annual report year: 2016

Statistical Model Checking for Product Lines
We report on the suitability of statistical model checking for the analysis of quantitative properties of product line models by an extended treatment of earlier work by the authors. The type of analysis that can be performed includes the likelihood of specific product behaviour, the expected average cost of products (in terms of the attributes of the products’ features) and the probability of features to be (un)installed at runtime. The product lines must be modelled in QFLan, which extends the probabilistic feature-oriented language PFLan with novel quantitative constraints among features and on behaviour and with advanced feature installation options. QFLan is a rich process-algebraic specification language whose operational behaviour interacts with a store of constraints, neatly separating product configuration from product behaviour. The resulting probabilistic configurations and probabilistic behaviour converge in a discrete-time Markov chain semantics, enabling the analysis of quantitative properties. Technically, a Maude implementation of QFLan, integrated with Microsoft’s SMT constraint solver Z3, is combined with the distributed statistical model checker MultiVeStA, developed by one of the authors. We illustrate the feasibility of our framework by applying it to a case study of a product line of bikes.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Formal Methods, National Research Council of Italy, French National Institute for Computer Science and Applied Mathematics, IMT Institute for Advanced Studies Lucca
The need to assess security and take protection decisions is at least as old as our civilisation. However, the complexity and development speed of our interconnected technical systems have surpassed our capacity to imagine and evaluate risk scenarios. This holds in particular for risks that are caused by the strategic behaviour of adversaries. Therefore, technology-supported methods are needed to help us identify and manage these risks. In this paper, we describe the attack navigator: a graph-based approach to security risk assessment inspired by navigation systems. Based on maps of a socio-technical system, the attack navigator identifies routes to an attacker goal. Specific attacker properties such as skill or resources can be included through attacker profiles. This enables defenders to explore attack scenarios and the effectiveness of defense alternatives under different threat conditions.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Formal Methods, Cybernetica AS, Delft University of Technology
Authors: Probst, C. W. (Intern), Willemsen, J. (Ekstern), Pieters, W. (Ekstern)
Number of pages: 17
Publication date: 2016

Host publication information
Title of host publication: Revised Selected Papers from the 2nd International Workshop on Graphical Models for Security (GrAlSec 2015)
Publisher: Springer
ISBN (Print): 978-3-319-29967-9
ISBN (Electronic): 978-3-319-29968-6
Series: Lecture Notes in Computer Science
Volume: 9390
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
Electronic versions:
paper.pdf. Embargo ended: 07/02/2017
DOIs:
10.1007/978-3-319-29968-6_1
Source: FindIt
Source-ID: 277319873
The Navigation Metaphor in Security Economics

The navigation metaphor for cybersecurity merges security architecture models and security economics. By identifying the most efficient routes for gaining access to assets from an attacker's viewpoint, an organization can optimize its defenses along these routes. The well-understood concept of navigation makes it easier to motivate and explain security investment to a wide audience, encouraging strategic security decisions.

General information

State: Published
Organisations: Department of Applied Mathematics and Computer Science, Formal Methods, Delft University of Technology, LUST, Consult Hyperion, University of London, KPMG Netherlands
Number of pages: 8
Pages: 14-21
Publication date: 2016
Main Research Area: Technical/natural sciences

Publication information

Volume: 14
Issue number: 3
ISSN (Print): 1540-7993
Ratings:
  BFI (2018): BFI-level 1
  Web of Science (2018): Indexed yes
  BFI (2017): BFI-level 1
  Web of Science (2017): Indexed Yes
  BFI (2016): BFI-level 1
  Scopus rating (2016): SJR 0.355 SNIP 1.243 CiteScore 1.39
  Web of Science (2016): Indexed yes
  BFI (2015): BFI-level 1
  Scopus rating (2015): SJR 0.561 SNIP 1.408 CiteScore 1.14
  BFI (2014): BFI-level 1
  Scopus rating (2014): SJR 0.369 SNIP 1.448 CiteScore 1.06
  BFI (2013): BFI-level 1
  Scopus rating (2013): SJR 0.458 SNIP 1.827 CiteScore 1.58
  ISI indexed (2013): ISI indexed yes
  BFI (2012): BFI-level 1
  Scopus rating (2012): SJR 0.488 SNIP 1.953 CiteScore 1.84
  ISI indexed (2012): ISI indexed yes
  BFI (2011): BFI-level 1
  Scopus rating (2011): SJR 0.458 SNIP 2.203 CiteScore 1.69
  ISI indexed (2011): ISI indexed yes
  BFI (2010): BFI-level 1
  Scopus rating (2010): SJR 0.471 SNIP 1.581
  BFI (2009): BFI-level 1
  Scopus rating (2009): SJR 0.469 SNIP 1.41
  BFI (2008): BFI-level 1
  Scopus rating (2008): SJR 0.614 SNIP 1.477
  Scopus rating (2007): SJR 1.025 SNIP 2.538
  Scopus rating (2006): SJR 0.967 SNIP 2.651
  Scopus rating (2005): SJR 0.662 SNIP 2.603
  Scopus rating (2004): SJR 0.765 SNIP 2.654
  Web of Science (2003): Indexed yes
Original language: English

Electrical and Electronic Engineering, Computer Networks and Communications, Law, attack navigators, attacker profiles, cyberattacks, e-commerce, hackers, Internet/Web technologies, navigation, security, security economics, security models
Towards Static Analysis of Policy-Based Self-adaptive Computing Systems
For supporting the design of self-adaptive computing systems, the PSCEL language offers a principled approach that relies on declarative definitions of adaptation and authorisation policies enforced at runtime. Policies permit managing system components by regulating their interactions and by dynamically introducing new actions to accomplish task-oriented goals. However, the runtime evaluation of policies and their effects on system components make the prediction of system behaviour challenging. In this paper, we introduce the construction of a flow graph that statically points out the policy evaluations that can take place at runtime and exploit it to analyse the effects of policy evaluations on the progress of system components.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Formal Methods, Università degli Studi di Firenze
Authors: Margheri, A. (Ekstern), Nielson, H. R. (Intern), Nielson, F. (Intern), Pugliese, R. (Ekstern)
Number of pages: 16
Pages: 554-569
Publication date: 2016

Host publication information
Title of host publication: Leveraging Applications of Formal Methods, Verification and Validation. Foundational Techniques: Proceedings. Part 1
Publisher: Springer
ISBN (Print): 978-3-319-47165-5
ISBN (Electronic): 978-3-319-47166-2
Series: Lecture Notes in Computer Science
Volume: 9952
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
Conference: 7th International Symposium On Leveraging Applications Of Formal Methods, Verification And Validation, Corfu, Greece, 10/10/2016 - 10/10/2016
Policy languages, Self-adaptive systems, Static analysis
DOIs: 10.1007/978-3-319-47166-2_39
Source: FindIt
Source-ID: 2348793072
Publication: Research - peer-review › Article in proceedings – Annual report year: 2017

Towards Unifying OpenMP Under the Task-Parallel Paradigm Implementation and Performance of the taskloop Construct
OpenMP 4.5 introduced a task-parallel version of the classical thread-parallel for-loop construct: the taskloop construct. With this new construct, programmers are given the opportunity to choose between the two parallel paradigms to parallelize their for loops. However, it is unclear where and when the two approaches should be used when writing efficient parallel applications. In this paper, we explore the taskloop construct. We study performance differences between traditional thread-parallel for loops and the new taskloop directive. We introduce an efficient implementation and compare our implementation to other taskloop implementations using micro-and kernel-benchmarks, as well as an application. We show that our taskloop implementation on average results in a 3.2% increase in peak performance when compared against corresponding parallel-for loops.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering, Formal Methods
Transforming Graphical System Models to Graphical Attack Models

Manually identifying possible attacks on an organisation is a complex undertaking; many different factors must be considered, and the resulting attack scenarios can be complex and hard to maintain as the organisation changes. System models provide a systematic representation of organisations that helps in structuring attack identification and can integrate physical, virtual, and social components. These models form a solid basis for guiding the manual identification of attack scenarios. Their main benefit, however, is in the analytic generation of attacks. In this work we present a systematic approach to transforming graphical system models to graphical attack models in the form of attack trees. Based on an asset in the model, our transformations result in an attack tree that represents attacks by all possible actors in the model, after which the actor in question has obtained the asset.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Formal Methods, Aalborg University, Middlesex University
Authors: Ivanova, M. G. (Intern), Probst, C. W. (Intern), Hansen, R. R. (Ekstern), Kammüller, F. (Ekstern)
Pages: 82-96
Publication date: 2016

Understanding How Components of Organisations Contribute to Attacks

Attacks on organisations today explore many different layers, including buildings infrastructure, IT infrastructure, and human factor – the physical, virtual, and social layer. Identifying possible attacks, understanding their impact, and attributing their origin and contributing factors is difficult. Recently, system models have been used for automatically identifying possible attacks on the modelled organisation. The generated attacks consider all three layers, making the contribution of building infrastructure, computer infrastructure, and humans (insiders and outsiders) explicit. However, this
contribution is only visible in the attack trees as part of the performed steps; it cannot be mapped back to the model directly since the actions usually involve several elements (attacker and targeted actor or asset). Especially for large attack trees, understanding the relations between several model components quickly results in a large quantity of interrelations, which are hard to grasp. In this work we present several approaches for visualising attributes of attacks such as likelihood of success, impact, and required time or skill level. The resulting visualisations provide a link between attacks on an organisations and the contribution of parts of an organisation to the attack and its impact.

**A calculus for attribute-based communication**

The notion of attribute-based communication seems promising to model and analyse systems with huge numbers of interacting components that dynamically adjust and combine their behaviour to achieve specific goals. A basic process calculus, named AbC, is introduced that has as primitive construct exactly attribute-based communication and its impact on the above mentioned kind of systems is considered. An AbC system consists of a set of parallel components each of which is equipped with a set of attributes. Communication takes place in a broadcast fashion and communication links among components are dynamically established by taking into account interdependences determined by predicates over attributes. First, the syntax and the reduction semantics of AbC are presented, then its expressiveness and effectiveness is demonstrated by modelling two scenarios from the realm of TV streaming channels. An example of how well-established process calculi could be encoded into AbC is given by considering the translation into AbC of a proto-typical π-calculus process.
A calculus of quality for robustness against unreliable communication

A main challenge in the development of distributed systems is to ensure that the components continue to behave in a reasonable manner even when communication becomes unreliable. We propose a process calculus, the Quality Calculus, for programming software components where it becomes natural to plan for default behaviour in case the ideal behaviour fails due to unreliable communication and thereby to increase the quality of service offered by the system. The development is facilitated by a SAT-based robustness analysis to determine whether or not the code is vulnerable to unreliable communication. The framework is illustrated on the design of a fragment of a wireless sensor network, and is substantiated by formal proofs of correctness of the analysis, which relate the original reduction semantics of the calculus to a new semantics with explicit substitutions.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology
Authors: Nielsen, H. R. (Intern), Nielsen, F. (Intern), Vigo, R. (Intern)
Pages: 611-639
Publication date: 2015
Main Research Area: Technical/natural sciences

Publication information
Journal: The Journal of Logic and Algebraic Programming
Volume: 84
Issue number: 5
ISSN (Print): 1567-8326
Ratings:
BFI (2018): BFI-level 2
BFI (2017): BFI-level 2
BFI (2016): BFI-level 2
Scopus rating (2016): SJR 0.437 SNIP 1.333
BFI (2015): BFI-level 2
Scopus rating (2015): SJR 0.663 SNIP 3.127 CiteScore 1.55
Web of Science (2015): Indexed yes
BFI (2014): BFI-level 2
Scopus rating (2014): SJR 0.523 SNIP 1.773 CiteScore 1.31
BFI (2013): BFI-level 2
Scopus rating (2013): SJR 0.512 SNIP 1.272 CiteScore 1.08
ISI indexed (2013): ISI indexed yes
BFI (2012): BFI-level 2
Scopus rating (2012): SJR 0.622 SNIP 1.434 CiteScore 1.37
ISI indexed (2012): ISI indexed yes
Web of Science (2012): Indexed yes
BFI (2011): BFI-level 2
Scopus rating (2011): SJR 0.594 SNIP 1.223 CiteScore 1.11
ISI indexed (2011): ISI indexed yes
BFI (2010): BFI-level 2
Scopus rating (2010): SJR 0.569 SNIP 1.105
ISI indexed (2010): ISI indexed yes
BFI (2009): BFI-level 2
Scopus rating (2009): SJR 0.718 SNIP 1.949
Web of Science (2009): Indexed yes
BFI (2008): BFI-level 2
Scopus rating (2008): SJR 0.778 SNIP 1.771
Web of Science (2008): Indexed yes
Scopus rating (2007): SJR 1.827 SNIP 2.219
Scopus rating (2006): SJR 1.092 SNIP 1.519
A Fixpoint-Based Calculus for Graph-Shaped Computational Fields

Coordination is essential for dynamic distributed systems exhibiting autonomous behaviors. Spatially distributed, locally interacting, propagating computational fields are particularly appealing for allowing components to join and leave with little or no overhead. In our approach, the space topology is represented by a graph-shaped field, namely a network with attributes on both nodes and arcs, where arcs represent interaction capabilities between nodes. We propose a calculus where computation is strictly synchronous and corresponds to sequential computations of fixpoints in the graph-shaped field. Under some conditions, those fixpoints can be computed by synchronised iterations, where in each iteration the attributes of a node is updated based on the attributes of the neighbours in the previous iteration. Basic constructs are reminiscent of the semiring μ-calculus, a semiring-valued generalisation of the modal μ-calculus, which provides a flexible mechanism to specify the neighbourhood range (according to path formulae) and the way attributes should be combined (through semiring operators). Additional control-How constructs allow one to conveniently structure the fixpoint computations. We illustrate our approach with a case study based on a disaster recovery scenario, implemented in a prototype simulator that we use to evaluate the performance of a disaster recovery strategy.
SPS and an automatic translation to robust real-world implementations and corresponding formal models, and we prove this translation correct with respect to the semantics.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, King’s College London
Authors: Almousa, O. (Intern), Mödersheim, S. A. (Intern), Viganò, L. (Ekstern)
Pages: 66-85
Publication date: 2015

Host publication information
Title of host publication: Programming Languages with Applications to Biology and Security: Essays Dedicated to Pierpaolo Degano on the Occasion of His 65th Birthday
Publisher: Springer
ISBN (Print): 978-3-319-25526-2
ISBN (Electronic): 978-3-319-25527-9

A Probabilistic Analysis Framework for Malicious Insider Threats
Malicious insider threats are difficult to detect and to mitigate. Many approaches for explaining behaviour exist, but there is little work to relate them to formal approaches to insider threat detection. In this work we present a general formal framework to perform analysis for malicious insider threats, based on probabilistic modelling, verification, and synthesis techniques. The framework first identifies insiders’ intention to perform an inside attack, using Bayesian networks, and in a second phase computes the probability of success for an inside attack by this actor, using probabilistic model checking.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, Technical University of Denmark, Middlesex University
Authors: Chen, T. (Ekstern), Kammueller, F. (Ekstern), Nemli, I. (Ekstern), Probst, C. W. (Intern)
Pages: 178-189
Publication date: 2015

Host publication information
Publisher: Springer
Editors: Tryfonas, T., Askoxylakis, I.
ISBN (Print): 978-3-319-20375-1
ISBN (Electronic): 978-3-319-20376-8

Electronic versions:
20150409_Chen_Kammueller_Nemli_Probst_ProbabilisticAnalysisFramework.pdf
DOIs:
10.1007/978-3-319-20376-8_16
Source: PublicationPreSubmission
Source-ID: 116483718
A SAT-Based Analysis of a Calculus for Wireless Sensor Networks

In viewing the common unreliability problem in wireless communications, the CWQ calculus (a Calculus for Wireless sensor networks from Quality perspective) was recently proposed for modeling and reasoning about WSNs (Wireless Sensor Networks) and their applications from a quality perspective. The CWQ calculus ensures that sensor nodes, even though in an unreliable communication network, can behave in a reasonable manner. Nevertheless, in CWQ calculus, the topological structure is considered at the network level and it is tightly coupled with the processes and other configurations, this may limit its flexibility. In this paper, to make the CWQ calculus more flexible to be able to model and reason about networks of different topological structures, we extend it to be a parametric framework. In the parametric framework, we extract the topological structure of a network and make it to be a configuration such that all topological structure-changes can be captured by this framework. Moreover, in this paper we also develop a SAT-based analysis of the extended calculus to avoid reaching error configurations due to unreliable communications in WSNs and use the SAT-solver Z3 to check the vulnerability of the whole network. Finally, we give a real-world case study with the scenario of refueling a car to demonstrate the applicability of the extended calculus and the SAT-based analysis.

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling, Department of Applied Mathematics and Computer Science, Language-Based Technology, East China Normal University
Authors: Wu, X. (Ekstern), Nielson, H. R. (Intern), Zhu, H. (Ekstern)
Pages: 23-30
Publication date: 2015

Host publication information
Title of host publication: Proceedings of the 2015 International Symposium on Theoretical Aspects of Software Engineering (TASE 2015)
Publisher: IEEE
ISBN (Print): 978-1-4673-7612-9
BFI conference series: International Symposium on Theoretical Aspects of Software Engineering (5000148)
Main Research Area: Technical/natural sciences
Conference: 9th International Symposium on Theoretical Aspects of Software Engineering (TASE 2015), Nanjing, China, 12/09/2015 - 12/09/2015
DOIs: 10.1109/TASE.2015.23
Source: FindIt
Source-ID: 276550381
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

A Scalable Prescriptive Parallel Debugging Model

Debugging is a critical step in the development of any parallel program. However, the traditional interactive debugging model, where users manually step through code and inspect their application, does not scale well even for current supercomputers due its centralized nature. While lightweight debugging models, which have been proposed as an alternative, scale well, they can currently only debug a subset of bug classes. We therefore propose a new model, which we call prescriptive debugging, to fill this gap between these two approaches. This user-guided model allows programmers to express and test their debugging intuition in a way that helps to reduce the error space. Based on this debugging model we introduce a prototype implementation embodying this model, the DySectAPI, allowing programmers to construct probe trees for automatic, event-driven debugging at scale. In this paper we introduce the concepts behind DySectAPI and, using both experimental results and analytical modelling, we show that the DySectAPI implementation can run with a low overhead on current systems. We achieve a logarithmic scaling of the prototype and show predictions that even for a large system the overhead of the prescriptive debugging model will be small.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, Embedded Systems Engineering, Lawrence Livermore National Laboratory, Technical University of Denmark
Authors: Jensen, N. B. (Intern), Quarfot Nielsen, N. (Ekstern), Lee, G. L. (Ekstern), Karlsson, S. (Intern), Legendre, M. (Ekstern), Schulz, M. (Ekstern), Ahn, D. H. (Ekstern)
Pages: 473-483
Publication date: 2015

Host publication information
Title of host publication: Proceedings of the 29th IEEE International Parallel and Distributed Processing Symposium (IPDPS 2015)
Publisher: IEEE
Attack Tree Generation by Policy Invalidation

Attacks on systems and organisations increasingly exploit human actors, for example through social engineering, complicating their formal treatment and automatic identification. Formalisation of human behaviour is difficult at best, and attacks on socio-technical systems are still mostly identified through brainstorming of experts. In this work we formalize attack tree generation including human factors; based on recent advances in system models we develop a technique to identify possible attacks analytically, including technical and human factors. Our systematic attack generation is based on invalidating policies in the system model by identifying possible sequences of actions that lead to an attack. The generated attacks are precise enough to illustrate the threat, and they are general enough to hide the details of individual steps.
The ultimate aim of the framework is to foster the development of systems resilient to DoS by means of a principled design process, in which formal models allow, and verification tools enforce, the production of such robust code.

**General information**

State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology
Authors: Vigo, R. (Intern), Nielson, H. R. (Intern), Nielson, F. (Intern)
Number of pages: 190
Publication date: 2015

**Publication information**
Place of publication: Kgs. Lyngby
Publisher: Technical University of Denmark (DTU)
Original language: English
Series: DTU Compute PHD-2014
Number: 353
ISSN: 0909-3192
Main Research Area: Technical/natural sciences
Electronic versions: phd353_Vigo_R.pdf
Publication: Research Ph.D. thesis – Annual report year: 2015

**AVOCLOUDY: a simulator of volunteer clouds**

The increasing demand of computational and storage resources is shifting users toward the adoption of cloud technologies. Cloud computing is based on the vision of computing as utility, where users no more need to buy machines but simply access remote resources made available on-demand by cloud providers. The relationship between users and providers is defined by a service-level agreement, where the non-fulfillment of its terms is regulated by the associated penalty fees. Therefore, it is important that the providers adopt proper monitoring and managing strategies. Despite their reduced application, intelligent agents constitute a feasible technology to add autonomic features to cloud operations. Furthermore, the volunteer computing paradigm—one of the Information and Communications Technology (ICT) trends of the last decade—can be pulled alongside traditional cloud approaches, with the purpose to ‘green’ them. Indeed, the combination of data center and volunteer resources, managed by agents, allows one to obtain a more robust and scalable cloud computing platform. The increased challenges in designing such a complex system can benefit from a simulation-based approach, to test autonomic management solutions before their deployment in the production environment. However, currently available simulators of cloud platforms are not suitable to model and analyze such heterogeneous, large-scale, and highly dynamic systems. We propose the AVOCLOUDY simulator to fill this gap. This paper presents the internal architecture of the simulator, provides implementation details, summarizes several notable applications, and provides experimental results that measure the simulator performance and its accuracy. The latter experiments are based on real-world worldwide distributed computations on top of the PlanetLab platform.

**General information**
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, University of Parma, IMT Institute for Advanced Studies Lucca
Authors: Sebastio, S. (Ekstern), Amoretti, M. (Ekstern), Lluch Lafuente, A. (Intern)
Pages: 3-30
Publication date: 2015
Main Research Area: Technical/natural sciences

**Publication information**
Journal: Software: Practice & Experience
Volume: 46
Issue number: 1
ISSN (Print): 0038-0644
Ratings:
BFI (2018): BFI-level 2
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 2
Web of Science (2017): Indexed Yes
BFI (2016): BFI-level 2
Scopus rating (2016): SJR 0.409 SNIP 1.298 CiteScore 1.61
BFI (2015): BFI-level 2
Awareness and Control in Adaptable Transition Systems

**General information**

State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, University of Pisa, University of Southampton
Authors: Bruni, R. (Ekstern), Corradini, A. (Ekstern), Gadducci, F. (Ekstern), Lluch Lafuente, A. (Intern), Vandin, A. (Intern)
Pages: 19-21
Publication date: 2015

**Host publication information**

Title of host publication: Proceedings of the International Workshop on Petri Nets and Software Engineering (PNSE’15)
Editors: Moldt, D., Rölke, H., Störrle, H.

Series: CEUR Workshop Proceedings
Volume: 1372
ISSN: 1613-0073
Main Research Area: Technical/natural sciences
A white box perspective on behavioural adaptation
We present a white-box conceptual framework for adaptation developed in the context of the EU Project ASCENS coordinated by Martin Wirsing. We called it CoDA, for Control Data Adaptation, since it is based on the notion of control data. CoDA promotes a neat separation between application and adaptation logic through a clear identification of the set of data that is relevant for the latter. The framework provides an original perspective from which we survey a representative set of approaches to adaptation, ranging from programming languages and paradigms to computational models and architectural solutions.

Declarative interpretations of session-based concurrency
Session-based concurrency is a type-based approach to the analysis of communication-intensive systems. Correct behavior in these systems may be specified in an operational or declarative style: the former defines how interactions are structured; the latter defines governing conditions. In this paper, we investigate the relationship between operational and declarative models of session-based concurrency. We propose two interpretations of session π-calculus processes as declarative processes in linear concurrent constraint programming (lcc). They offer a basis on which both operational and declarative requirements can be specified and reasoned about. By coupling our interpretations with a type system for lcc, we obtain robust declarative encodings of π-calculus mobility.
Developing merged CDIO based curricula for diploma (B.Eng.) IT study programs at DTU

Starting 2007, the Danish government drew up a new map of universities through a process of mergers of a number of universities and research institutions (UFM 2007), as part of the national innovation strategy. In the beginning of 2013, the Engineering College Copenhagen (IHK, now DTU Ballerup) merged with the Technical University of Denmark (DTU Lyngby). The goal of the merger was to educate ever more innovative diploma engineers to fulfill the needs by Danish industry through combining a practice-oriented development environment and a research-oriented environment.

Merging a university with an engineering college implies merging two different cultures: established teaching staff, different study lines; a difficult undertaking at best. Existing study lines must be merged, overlaps and differences identified and handled, and in general a common understanding and language must be established.

The two institutions represented before the merger well 3500 B.Eng. students. The goal of the merger was to combine the best of the existing educations rooted in a practice-oriented development environment and a research-oriented environment. At the same time, the merger was supposed to contribute to the national innovation strategy.

In this paper we describe the process of developing new, merged B.Eng curricula in the IT field (Diploma IT), as part of the merger between DTU Lyngby and IHK. Particular attention will be given to the following subjects:

• The design process used to develop the new merged study programs;
• Involvement of stakeholders in designing the new curricula;
• Introduction of a common interdisciplinary innovation course in the programs; and
• Education of teaching staff: Integration into one organization.
**Discretionary Information Flow Control for Interaction-Oriented Specifications**

This paper presents an approach to specify and check discretionary information flow properties of concurrent systems. The approach is inspired by the success of the interaction-oriented paradigm to concurrent systems (cf. choreographies, behavioural types, protocols,...) in providing behavioural guarantees of global properties such as deadlock-absence. We show how some information flow properties are easier to formalise and check on a global interaction-oriented description of a concurrent system rather than on a local process-oriented description of the components of the system. We use a simple choreography description language adapted from the literature of choreographies and session types. We provide a generic method to instrument the semantics with information flow annotations. Policies are used to specify the admissible flows of information. The main contribution of the paper is a sound type system for statically checking if a system specification ensures an information flow policy. The approach is illustrated with two archetypal examples of distributed and parallel computing systems: a protocol for an identity-secured data providing service and a parallel MapReduce computation.

**General information**

State: Published  
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology  
Authors: Lluch Lafuente, A. (Intern), Nielsen, F. (Intern), Nielsen, H. R. (Intern)  
Pages: 427-450  
Publication date: 2015

**Host publication information**

Title of host publication: Logic, Rewriting, and Concurrency: Essays Dedicated to José Meseguer on the Occasion of His 65th Birthday  
Publisher: Springer  
ISBN (Print): 978-3-319-23164-8  
ISBN (Electronic): 978-3-319-23165-5

Series: Lecture Notes in Computer Science  
Volume: 9200  
ISSN: 0302-9743  
Main Research Area: Technical/natural sciences

Information flow control, Discretionary access control, Choreographies, Communication protocols, Interaction-oriented computing, Parallel computing, Service-oriented computing, Highperformance computing

Electronic versions:  
Discretionary_Information_Flow_Control_for_Interaction_Oriented_Specifications.pdf  
DOIs:  
10.1007/978-3-319-23165-5_20

Source: PublicationPreSubmission  
Source-ID: 118084583  
Publication: Research - peer-review Book chapter – Annual report year: 2015

**Experiences with Compiler Support for Processors with Exposed Pipelines**

Field programmable gate arrays, FPGAs, have become an attractive implementation technology for a broad range of computing systems. We recently proposed a processor architecture, Tinuso, which achieves high performance by moving complexity from hardware to the compiler tool chain. This means that the compiler tool chain must handle the increased complexity. However, it is not clear if current production compilers can successfully meet the strict constraints on instruction order and generate efficient object code. In this paper, we present our experiences developing a compiler backend using the GNU Compiler Collection, GCC. For a set of C benchmarks, we show that a Tinuso implementation with our GCC backend reaches a relative speedup of up to 1.73 over a similar Xilinx Micro Blaze configuration while using 30% fewer hardware resources. While our experiences are generally positive, we expose some limitations in GCC that need to be addressed to achieve the full performance potential of Tinuso.

**General information**

State: Published  
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, Embedded Systems Engineering  
Authors: Jensen, N. B. (Intern), Schleuniger, P. (Intern), Hindborg, A. E. (Intern), Walter, M. (Intern), Karlsson, S. (Intern)  
Pages: 137-143  
Publication date: 2015

**Host publication information**

Title of host publication: Proceedings of the 29th International Parallel and Distributed Processing Symposium Workshops (IPDPSW 2015)
Factorization of Behavioral Integrity
We develop a bisimulation-based noninterference property that describes the allowed dependencies between communication behaviors of different integrity levels. The property is able to capture all possible combinations of integrity levels for the “presence” and “content” of actual communications. Channels of low presence integrity and high content integrity can be used to model the effect of Message Authentication Codes or the consequence of Denial of Service Attacks. In case the distinction between “presence” and “content” is deliberately blurred, the noninterference property specialises to a classical process-algebraic property (called SBNDC). A compositionality result is given to facilitate a structural approach to the analysis of concurrent systems.

Hardware Transactional Memory Optimization Guidelines, Applied to Ordered Maps
Synchronization of concurrent data structures is difficult to get right. Fine-grained synchronization locks small data chunks, but requires too high an overhead per chunk, traditional coarse-grained synchronization locks big data chunks, and thereby makes them unavailable to other threads. Neither synchronization method scales well. Recently, hardware transactional memory was introduced, which allows threads to use transactions instead of locks. So far, applying hardware transactional memory has shown mixed results. We believe this is because transactions are different from locks, and using them efficiently requires reasoning about those differences. In this paper we present 5 guidelines for applying hardware transactional memory efficiently, and apply the guidelines to BT-trees, a concurrent ordered map. Evaluating BT-trees on standard benchmarks shows that they are up to 5.3 times faster than traditional maps using hardware transactional memory, and up to 3.9 times faster than state of the art concurrent ordered maps.
Hoare Logic for Disjunctive Information Flow

Information flow control extends access control by not only regulating who is allowed to access what data but also the subsequent use of the data accessed. Applications within communication networks require such information flow control to depend on the actual data. For a concurrent language with synchronous communication and separate data domains we develop a Hoare logic for enforcing disjunctive information flow policies. We establish the soundness of the Hoare logic with respect to an operational semantics and illustrate the development on a running example.

How to Trust the Re-use of Data

Research in natural sciences and life sciences involve carrying out experiments to collect data as well as carrying out analysis to interpret the data. Increasingly data is being made available to other scientists in big databases. The scientific process builds on the idea that research results can be independently validated by other researchers. However, the concern about the correct re-use of data is also increasing. As illustrated by a currently evolving case of alleged scientific mispractice there is a need to support a reliable re-use of data. To solve this challenge we introduce an enriched coordination language based on Klaim, that can model the coordination of the re-use of data in the research community. We define the formal semantics of our language and develop a static analysis that can be used to check whether we have a trustworthy re-use of data.
Improving Energy Saving Techniques by Ambient Intelligence Scheduling

Energy saving is one of the most challenging aspects of modern ambient intelligence technologies, for both domestic and business usages. In this paper we show how to combine Ambient Intelligence and Artificial Intelligence techniques to solve the problem of scheduling a set of devices under a given set of constraints, like limits to the maximal energy usage (Energy Span) and maximal energy absorption (Energy Peak). We provide a method that can be used to schedule the usage of devices in a given environment in a way that respects the input constraints. We adapt an existent approach to scheduling for Ambient Intelligence to a specific framework and exhibit a sample usage for a real life system, Elettra, that is in use in an industrial context.

Klaim-DB: A Modeling Language for Distributed Database Applications

We present the modelling language, Klaim-DB, for distributed database applications. Klaim-DB borrows the distributed nets of the coordination language Klaim but essentially re-incarnates the tuple spaces of Klaim as databases, and provides high-level language abstractions for the access and manipulation of structured data, with integrity and atomicity considerations. We present the formal semantics of KlaimDB and illustrate the use of the language in a scenario where the sales from different branches of a chain of department stores are aggregated from their local databases. It can be
seen that raising the abstraction level and encapsulating integrity checks (concerning the schema of tables, etc.) in the language primitives for database operations benefit the modelling task considerably.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, East China Normal University
Authors: Wu, X. (Ekstern), Li, X. (Intern), Lluch Lafuente, A. (Intern), Nielson, F. (Intern), Nielson, H. R. (Intern)
Pages: 197-212
Publication date: 2015

Host publication information
Title of host publication: Coordination Models and Languages: Proceedings of the 17th IFIP WG 6.1 International Conference (COORDINATION 2015)
Publisher: Springer
ISBN (Print): 978-3-319-19281-9
ISBN (Electronic): 978-3-319-19282-6

Series: Lecture Notes in Computer Science
Volume: 9037
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
Conference: 17th IFIP WG 6.1 International Conference, COORDINATION 2015, Grenoble, France, 02/06/2015 - 02/06/2015

Electronic versions:
klaim_db.pdf
DOIs:
10.1007/978-3-319-19282-6_13
Source: FindIt
Source-ID: 274873271
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

Meta-Logical Reasoning in Higher-Order Logic
The semantics of first-order logic (FOL) can be described in the meta-language of higher-order logic (HOL). Using HOL one can prove key properties of FOL such as soundness and completeness. Furthermore, one can prove sentences in FOL valid using the formalized FOL semantics. To aid in the construction of the proof an interactive proof assistant like Isabelle can be used. The proof assistant can even automate simple proofs using the formalized FOL semantics.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Algorithms and Logic, Language-Based Technology
Authors: Villadsen, J. (Intern), Schlichtkrull, A. (Intern), Hess, A. V. (Intern)
Number of pages: 1
Publication date: 2015
Main Research Area: Technical/natural sciences

Electronic versions:
logica_poster.pdf
Source: PublicationPreSubmission
Source-ID: 118753616
Publication: Research - peer-review › Poster – Annual report year: 2015

Modelling and Analysing Access Control Policies in XACML 3.0
XACML (eXtensible Access Control Markup Language) is a prominent access control language that is widely adopted both in industry and academia. XACML is an international standard in the field of information security. The problem with XACML is that its specification is described in natural language (c.f. GM03,Mos05,Ris13) and manual analysis of the overall effect and consequences of a large XACML policy set is a very daunting and time-consuming task.

In this thesis we address the problem of understanding the semantics of access control policy language XACML, in particular XACML version 3.0. The main focus of this thesis is modelling and analysing access control policies in XACML 3.0.
There are two main contributions in this thesis. First, we study and formalise XACML 3.0, in particular the Policy Decision Point (PDP). The concrete syntax of XACML is based on the XML format, while its standard semantics is described normatively using natural language. The use of English text in standardisation leads to the risk of misinterpretation and ambiguity. In order to avoid this drawback, we define an abstract syntax of XACML 3.0 and a formal XACML semantics. Second, we propose a logic-based XACML analysis framework using Answer Set Programming (ASP). With ASP we model an XACML PDP that loads XACML policies and evaluates XACML requests against these policies. The expressivity of ASP and the existence of efficient implementations of the answer set semantics provide the means for declarative specification and verification of properties of XACML policies.

Overall, we focus into two different area. The first part focuses on the access control language. More specifically our focus is on the understanding XACML 3.0. The second part focuses on how we use Logic Programming (LP) to model access control policies. We show that there is a relation between XACML and LP through their semantics. We close the thesis by presenting applications in analysing access control properties and a case study. These applications show that these two approaches (AC paradigm and LP paradigm) can be combined together.

We close the thesis by presenting applications in analysing access control properties and a case study. We present access control security policies in a Smart Grid from Smart Meter perspective.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology
Authors: Ramli, C. D. P. K. (Intern), Nielson, H. R. (Intern), Nielson, F. (Intern)
Number of pages: 217
Publication date: 2015

Publication information
Place of publication: Kgs. Lyngby
Publisher: Technical University of Denmark (DTU)
Original language: English
Series: DTU Compute PHD-2015
Number: 364
ISSN: 0909-3192
Main Research Area: Technical/natural sciences
Access Control Policies, IT Security, Control Systems, XACML, Composition Policies, Logic Programming, Answer Set Programming, Smart Grid, Smart Meter
Electronic versions:
phd364_Ramli_CDPK.pdf
Publication: Research › Ph.D. thesis – Annual report year: 2015

Modelling and Analysing Socio-Technical Systems
Modern organisations are complex, socio-technical systems consisting of a mixture of physical infrastructure, human actors, policies and processes. An increasing number of attacks on these organisations exploits vulnerabilities on all different levels, for example combining a malware attack with social engineering. Due to this combination of attack steps on technical and social levels, risk assessment in socio-technical systems is complex. Therefore, established risk assessment methods often abstract away the internal structure of an organisation and ignore human factors when modelling and assessing attacks. In our work we model all relevant levels of socio-technical systems, and propose evaluation techniques for analysing the security properties of the model. Our approach simplifies the identification of possible attacks and provides qualified assessment and ranking of attacks based on the expected impact.

We demonstrate our approach on a home-payment system. The system is specifically designed to help elderly or disabled people, who may have difficulties leaving their home, to pay for some services, e.g., care-taking or rent. The payment is performed using the remote control of a television box with a contactless payment card (see Figure 1). When a transfer is initiated, a password is needed in order to authenticate the owner of the card.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology
Authors: Aslanyan, Z. (Intern), Ivanova, M. G. (Intern), Nielson, F. (Intern), Probst, C. W. (Intern)
Pages: 121-124
Publication date: 2015

Host publication information
Title of host publication: Proceedings of the 1st International Workshop on Socio-Technical Perspective in IS Development (STPIS’15)
Editors: Kowalski, S., Bednar, P., Bider, I.
Modelling Social-Technical Attacks with Timed Automata

Attacks on a system often exploit vulnerabilities that arise from human behaviour or other human activity. Attacks of this type, so-called socio-technical attacks, cover everything from social engineering to insider attacks, and they can have a devastating impact on an unprepared organisation. In this paper we develop an approach towards modelling socio-technical systems in general and socio-technical attacks in particular, using timed automata and illustrate its application by a complex case study. Thanks to automated model checking and automata theory, we can automatically generate possible attacks in our model and perform analysis and simulation of both model and attack, revealing details about the specific interaction between attacker and victim. Using timed automata also allows for intuitive modelling of systems, in which quantities like time and cost can be easily added and analysed.

Pareto Efficient Solutions of Attack-Defence Trees

Attack-defence trees are a promising approach for representing threat scenarios and possible countermeasures in a concise and intuitive manner. An attack-defence tree describes the interaction between an attacker and a defender, and is evaluated by assigning parameters to the nodes, such as probability or cost of attacks and defences. In case of multiple parameters most analytical methods optimise one parameter at a time, e.g., minimise cost or maximise probability of an attack. Such methods may lead to sub-optimal solutions when optimising conflicting parameters, e.g., minimising cost while maximising probability.

In order to tackle this challenge, we devise automated techniques that optimise all parameters at once. Moreover, in the case of conflicting parameters our techniques compute the set of all optimal solutions, defined in terms of Pareto efficiency. The developments are carried out on a new and general formalism for attack-defence trees.
Proceedings 11th International Workshop on Automated Specification and Verification of Web Systems

These proceedings contain the papers presented at the 11th International Workshop on Automated Specification and Verification of Web Systems (WWV 2015), which was held on 23 June 2015 in Oslo, Norway, as a satellite workshop of the 20th International Symposium on Formal Methods (FM 2015). WWV is a yearly interdisciplinary forum for researchers originating from the following areas: declarative, rule-based programming, formal methods, software engineering and web-based systems. The workshop fosters the cross-fertilisation and advancement of hybrid methods from such areas.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science , Language-Based Technology, Consiglio Nazionale delle Ricerche
Authors: ter Beek, M. H. (ed.) (Ekstern), Lluch Lafuente, A. (ed.) (Intern)
Publication date: 2015

Publication information
Original language: English
Series: Electronic Proceedings in Theoretical Computer Science
ISSN: 2075-2180
Main Research Area: Technical/natural sciences
DOIs:
10.4204/EPTCS.188
Publication: Research - peer-review › Book – Annual report year: 2015

Proceedings 8th Interaction and Concurrency Experience

This volume contains the proceedings of ICE 2015, the 8th Interaction and Concurrency Experience, which was held in Grenoble, France on the 4th and 5th of June 2015 as a satellite event of DisCoTec 2015. The ICE procedure for paper selection allows PC members to interact, anonymously, with authors. During the review phase, each submitted paper is published on a discussion forum with access restricted to the authors and to all the PC members not declaring a conflict of interest. The PC members post comments and questions to which the authors reply. Each paper was reviewed by three PC members, and altogether 9 papers, including 1 short paper, were accepted for publication (the workshop also featured 4 brief announcements which are not part of this volume). We were proud to host three invited talks, by Leslie Lamport (shared with the FRIDA workshop), Joseph Sifakis and Steve Ross-Talbot. The abstracts of the last two talks are included in this volume together with the regular papers.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science , Language-Based Technology, Universite de Lorraine, IMT Institute for Advanced Studies Lucca, Università di Bologna
Publication date: 2015

Publication information
Original language: English
Series: Electronic Proceedings in Theoretical Computer Science
ISSN: 2075-2180
Main Research Area: Technical/natural sciences
DOIs:
10.4204/EPTCS.189
Publication: Research - peer-review › Book – Annual report year: 2015

Protocol-Based Verification of Message-Passing Parallel Programs

We present ParTypes, a type-based methodology for the verification of Message Passing Interface (MPI) programs written in the C programming language. The aim is to statically verify programs against protocol specifications, enforcing properties such as fidelity and absence of deadlocks. We develop a protocol language based on a dependent type system for message-passing parallel programs, which includes various communication operators, such as point-to-point messages, broadcast, reduce, array scatter and gather. For the verification of a program against a given protocol, the protocol is first translated into a representation read by VCC, a software verifier for C. We successfully verified several MPI programs in a running time that is independent of the number of processes or other input parameters. This contrasts with alternative techniques, notably model checking and runtime verification, that suffer from the state-explosion problem or that otherwise depend on parameters to the program itself. We experimentally evaluated our approach against state-of-the-art tools for MPI to conclude that our approach offers a scalable solution.
Quantitative Analysis of Probabilistic Models of Software Product Lines with Statistical Model Checking

We investigate the suitability of statistical model checking techniques for analysing quantitative properties of software product line models with probabilistic aspects. For this purpose, we enrich the feature-oriented language FLAN with action rates, which specify the likelihood of exhibiting particular behaviour or of installing features at a specific moment or in a specific order. The enriched language (called PFLAN) allows us to specify models of software product lines with probabilistic configurations and behaviour, e.g. by considering a PFLAN semantics based on discrete-time Markov chains.

The Maude implementation of PFLAN is combined with the distributed statistical model checker MultiVeStA to perform quantitative analyses of a simple product line case study. The presented analyses include the likelihood of certain behaviour of interest (e.g. product malfunctioning) and the expected average cost of products.
Reconciling White-Box and Black-Box Perspectives on Behavioral Self-adaptation

This paper proposes to reconcile two perspectives on behavioral adaptation commonly taken at different stages of the engineering of autonomic computing systems. Requirements engineering activities often take a black-box perspective: A system is considered to be adaptive with respect to an environment whenever the system is able to satisfy its goals irrespectively of the environment perturbations. Modeling and programming engineering activities often take a white-box perspective: A system is equipped with suitable adaptation mechanisms and its behavior is classified as adaptive depending on whether the adaptation mechanisms are enacted or not. The proposed approach reconciles black- and white-box perspectives by proposing several notions of coherence between the adaptivity as observed by the two perspectives: These notions provide useful criteria for the system developer to assess and possibly modify the adaptation requirements, models and programs of an autonomic system.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, University of Pisa, Ludwig-Maximilians-Universität, University of Southampton
Authors: Bruni, R. (Ekstern), Corradini, A. (Ekstern), Gadducci, F. (Ekstern), Hölzl, M. (Ekstern), Lluch Lafuente, A. (Intern), Vandin, A. (Intern), Wirsing, M. (Ekstern)
Pages: 163-184
Publication date: 2015

Replica-Based High-Performance Tuple Space Computing

We present the tuple-based coordination language RepliKlaim, which enriches Klaim with primitives for replica-aware coordination. Our overall goal is to offer suitable solutions to the challenging problems of data distribution and locality in large-scale high performance computing. In particular, RepliKlaim allows the programmer to specify and coordinate the replication of shared data items and the desired consistency properties. The programmer can hence exploit such flexible mechanisms to adapt data distribution and locality to the needs of the application, so to improve performance in terms of concurrency and data access. We investigate issues related to replica consistency, provide an operational semantics that guides the implementation of the language, and discuss the main synchronization mechanisms of our prototypical run-time framework. Finally, we provide a performance analysis, which includes scenarios where replica-based specifications and relaxed consistency provide significant performance gains.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, IMT Institute for Advanced Studies Lucca
Authors: Andric, M. (Ekstern), De Nicola, R. (Ekstern), Lluch Lafuente, A. (Intern)
Pages: 3-18
Publication date: 2015
Replicating Data for Better Performances in X10

Linguistic primitives for replica-aware coordination offer suitable solutions to the challenging problems of data distribution and locality in large-scale high-performance computing. The data replication mechanisms that had previously been designed to extend Klaim with replicated tuples are now used to experiment with X10, a parallel programming language primarily targeting clusters of multi-core processors linked in a large-scale system via high-performance networks. Our approach aims at allowing the programmer to specify and coordinate the replication of shared data items by taking into account the desired consistency properties. The programmer can hence exploit such flexible mechanisms to adapt data distribution and locality to the needs of the application, in order to improve performance in terms of concurrency and data access. We investigate issues related to replica consistency and provide a performance analysis, which includes scenarios where replica based specifications and relaxed consistency provide significant performance gains.

General information
State: Published
Organisations: Language-Based Technology, Department of Applied Mathematics and Computer Science, IMT Institute for Advanced Studies Lucca
Authors: Andrić, M. (Ekstern), De Nicola, R. (Ekstern), Lluch Lafuente, A. (Intern)
Pages: 236-251
Publication date: 2015

Host publication information
Title of host publication: Semantics, Logics, and Calculi: Essays Dedicated to Hanne Riis Nielson and Flemming Nielson on the Occasion of Their 60th Birthdays
Publisher: Springer
Editors: Probst, C. W., Hansen, R. R., Hankin, C.
ISBN (Print): 978-3-319-27809-4
ISBN (Electronic): 978-3-319-27810-0

Series: Lecture Notes in Computer Science
Volume: 9560
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
DOIs:
10.1007/978-3-319-27810-0_12
Source: FindIt
Source-ID: 2291785454
Publication: Research - peer-review › Book chapter – Annual report year: 2016

Set-Pi: Set Membership pi-Calculus

Communication protocols often rely on stateful mechanisms to ensure certain security properties. For example, counters and timestamps can be used to ensure authentication, or the security of communication can depend on whether a particular key is registered to a server or it has been revoked. ProVerif, like other state of the art tools for protocol analysis, achieves good performance by converting a formal protocol specification into a set of Horn clauses, that represent a monotonically growing set of facts that a Dolev-Yao attacker can derive from the system. Since this set of facts is not state-dependent, the category of protocols of our interest cannot be precisely analysed by such tools, as they would report false attacks due to the over-approximation.
In this paper we present Set-π, an extension of the Applied π-calculus that includes primitives for handling databases of objects, and propose a translation from Set-π into Horn clauses that employs the set-membership abstraction to capture the non-monotonicity of the state. Furthermore, we give a characterisation of authentication properties in terms of the set properties in the language, and prove the correctness of our approach. Finally we showcase our method with three examples, a simple authentication protocol based on counters, a key registration protocol, and a model of the Yubikey security device.

Statistical analysis of probabilistic models of software product lines with quantitative constraints

We investigate the suitability of statistical model checking for the analysis of probabilistic models of software product lines with complex quantitative constraints and advanced feature installation options. Such models are specified in the feature-oriented language QF Lan, a rich process algebra whose operational behaviour interacts with a store of constraints, neatly separating product configuration from product behaviour. The resulting probabilistic configurations and behaviour converge seamlessly in a semantics based on DTMCs, thus enabling quantitative analyses ranging from the likelihood of certain behaviour to the expected average cost of products. This is supported by a Maude implementation of QF Lan, integrated with the SMT solver Z3 and the distributed statistical model checker MultiVeStA. Our approach is illustrated with a bikes product line case study.
Stochastic Model Checking of the Stochastic Quality Calculus

The Quality Calculus uses quality binders for input to express strategies for continuing the computation even when the desired input has not been received. The Stochastic Quality Calculus adds generally distributed delays for output actions and real-time constraints on the quality binders for input. This gives rise to Generalised Semi-Markov Decision Processes for which few analytical techniques are available.

We restrict delays on output actions to be exponentially distributed while still admitting real-time constraints on the quality binders. This facilitates developing analytical techniques based on stochastic model checking and we compute closed form solutions for a number of interesting scenarios. The analyses are applied to the design of an intelligent smart electrical meter of the kind to be installed in European households by 2020.

Systematic derivation of correct variability-aware program analyses

A recent line of work lifts particular verification and analysis methods to Software Product Lines (SPL). In an effort to generalize such case-by-case approaches, we develop a systematic methodology for lifting single-program analyses to SPLs using abstract interpretation. Abstract interpretation is a classical framework for deriving static analyses in a compositional, step-by-step manner. We show how to take an analysis expressed as an abstract interpretation and lift each of the abstract interpretation steps to a family of programs (SPL). This includes schemes for lifting domain types, and combinators for lifting analyses and Galois connections. We prove that for analyses developed using our method, the soundness of lifting follows by construction. The resulting variational abstract interpretation is a conceptual framework for understanding, deriving, and validating static analyses for SPLs. Then we show how to derive the corresponding variational dataflow equations for an example static analysis, a constant propagation analysis. We also describe how to approximate variability by applying variability-aware abstractions to SPL analysis. Finally, we discuss how to efficiently implement our method and present some evaluation results.
The SCEL Language: Design, Implementation, Verification

SCEL (Service Component Ensemble Language) is a new language specifically designed to rigorously model and program autonomic components and their interaction, while supporting formal reasoning on their behaviors. SCEL brings together various programming abstractions that allow one to directly represent aggregations, behaviors and knowledge according to specific policies. It also naturally supports programming interaction, self-awareness, context-awareness, and
adaptation. The solid semantic grounds of the language is exploited for developing logics, tools and methodologies for formal reasoning on system behavior to establish qualitative and quantitative properties of both the individual components and the overall systems.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, IMT Institute for Advanced Studies Lucca, Consiglio Nazionale delle Ricerche, Università degli Studi di Firenze, University of Southampton
Authors: Rocco De Nicola, R. X. (Ekstern), Latella, D. (Ekstern), Lluch Lafuente, A. (Intern), Loreti, M. (Ekstern), Margheri, A. M. (Ekstern), Massink, M. (Ekstern), Morichetta, A. (Ekstern), Pugliese, R. (Ekstern), Tiezzi, F. (Ekstern), Vandin, A. (Intern)
Pages: 3-71
Publication date: 2015

Host publication information
Title of host publication: Software Engineering for Collective Autonomic Systems: The ASCENS Approach
Publisher: Springer
ISBN (Print): 978-3-319-16309-3
ISBN (Electronic): 978-3-319-16310-9
Series: Lecture Notes in Computer Science
Volume: 8998
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
Electronic versions: The_SCEL_Language.pdf
DOIs: 10.1007/978-3-319-16310-9_1
Source: PublicationPreSubmission
Source-ID: 118084655
Publication: Research - peer-review › Book chapter – Annual report year: 2015

Tool-based Risk Assessment of Cloud Infrastructures as Socio-Technical Systems
Assessing risk in cloud infrastructures is difficult. Typical cloud infrastructures contain potentially thousands of nodes that are highly interconnected and dynamic. Another important component is the set of human actors who get access to data and computing infrastructure. The cloud infrastructure therefore constitutes a socio-technical system. Attacks on socio-technical systems are still mostly identified through expert brainstorming. However, formal risk assessment for systems including human actors requires modeling human behavior, which is difficult at best. In this chapter, we present a modeling exercise for cloud infrastructures using the socio-technical model developed in the TRESPASS project; after showing how to model typical components of a cloud infrastructure, we show how attacks are identified on this model and discuss their connection to risk assessment. The technical part of the model is extracted automatically from the configuration of the cloud infrastructure, which is especially important for systems so dynamic and complex.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, IBM Research
Authors: Nidd, M. (Ekstern), Ivanova, M. G. (Intern), Probst, C. W. (Intern), Tanner, A. (Ekstern)
Pages: 495-517
Publication date: 2015

Host publication information
Title of host publication: The Cloud Security Ecosystem: Technical, Legal, Business and Management Issues
Publisher: Elsevier Science
ISBN (Print): 978-0-12-801595-7
Chapter: 22
Main Research Area: Technical/natural sciences
Electronic versions: 2015_NiddIvanovaProbstTanner_100.pdf
DOIs: 10.1016/B978-0-12-801595-7.00022-7
Source: PublicationPreSubmission
Source-ID: 116483939
Publication: Research - peer-review › Book chapter – Annual report year: 2015
Typing and compositionality for security protocols: A generalization to the geometric fragment
We integrate, and improve upon, prior relative soundness results of two kinds. The first kind are typing results showing that any security protocol that fulfils a number of sufficient conditions has an attack if it has a well-typed attack. The second kind considers the parallel composition of protocols, showing that when running two protocols in parallel allows for an attack, then at least one of the protocols has an attack in isolation. The most important generalization over previous work is the support for all security properties of the geometric fragment.

General information
State: Published
Organisations: Language-Based Technology, Department of Applied Mathematics and Computer Science, Newcastle University, King's College London
Authors: Almousa, O. (Intern), Mödersheim, S. A. (Intern), Modesti, P. (Ekstern), Viganò, L. (Ekstern)
Pages: 209-229
Publication date: 2015

Host publication information
Title of host publication: Proceedings of the 20th European Symposium on Research in Computer Security (ESORICS 2015): Part II
Publisher: Springer
Editors: Pernul, G., Ryan, P. Y. A., Weippl, E.
ISBN (Print): 978-3-319-24176-0
ISBN (Electronic): 978-3-319-24177-7

Series: Lecture Notes in Computer Science
Volume: 9327
ISSN: 0302-9743
BFI conference series: European Symposium on Research in Computer Security (5010386)
Main Research Area: Technical/natural sciences
Electronic versions:
Almousa_Typing_and_compositionality.pdf
DOIs: 10.1007/978-3-319-24177-7_11
Source: FindIt
Source-ID: 2290355758
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

Typing and Compositionality for Security Protocols: A Generalization to the Geometric Fragment (Extended Version)
We integrate, and improve upon, prior relative soundness results of two kinds. The first kind are typing results showing that if any security protocol that fulfils a number of sufficient conditions has an attack then it has a well-typed attack. The second kind considers the parallel composition of protocols, showing that when running two protocols in parallel allows for an attack, then at least one of the protocols has an attack in isolation. The most important generalization over previous work is the support for all security properties of the geometric fragment.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Newcastle University, King's College London
Authors: Almousa, O. (Intern), Mödersheim, S. A. (Intern), Modesti, P. (Ekstern), Viganò, L. (Ekstern)
Number of pages: 26
Publication date: 2015

Publication information
Place of publication: Kgs. Lyngby
Publisher: Technical University of Denmark (DTU)
Original language: English
Number: 3
ISSN: 1601-2321
Main Research Area: Technical/natural sciences
Electronic versions:
A Sound Abstraction of the Parsing Problem

In formal verification, cryptographic messages are often represented by algebraic terms. This abstracts not only from the intricate details of the real cryptography, but also from the details of the non-cryptographic aspects: the actual formatting and structuring of messages. We introduce a new algebraic model to include these details and define a small, simple language to precisely describe message formats. We support fixed-length fields, variable-length fields with offsets, tags, and encodings into smaller alphabets like Base64, thereby covering both classical formats as in TLS and modern XML-based formats. We define two reasonable properties for a set of formats used in a protocol suite. First, each format should be un-ambiguous: any string can be parsed in at most one way. Second, the formats should be pairwise disjoint: a string can be parsed as at most one of the formats. We show how to easily establish these properties for many practical formats. By replacing the formats with free function symbols we obtain an abstract model that is compatible with all existing verification tools. We prove that the abstraction is sound for un-ambiguous, disjoint formats: there is an attack in the concrete message model if there is one in the abstract message model. Finally we present highlights of a practical case study on TLS.

General Information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, Technical University of Denmark
Authors: Mödersheim, S. A. (Intern), Katsoris, G. (Ekstern)
Number of pages: 16
Publication date: 2014

A Sound Abstraction of the Parsing Problem (Extended Version)

In formal verification, cryptographic messages are often represented by algebraic terms. This abstracts not only from the intricate details of the real cryptography, but also from the details of the non-cryptographic aspects: the actual formatting and structuring of messages. We introduce a new algebraic model to include these details and define a small, simple language to precisely describe message formats. We support fixed-length fields, variable-length fields with offsets, tags, and encodings into smaller alphabets like Base64, thereby covering both classical formats as in TLS and modern XML-based formats. We define two reasonable properties for a set of formats used in a protocol suite. First, each format should be un-ambiguous: any string can be parsed in at most one way. Second, the formats should be pairwise disjoint: a string can be parsed as at most one of the formats. We show how to easily establish these properties for many practical formats. By replacing the formats with free function symbols we obtain an abstract model that is compatible with all existing verification tools. We prove that the abstraction is sound for unambiguous, disjoint formats: there is an attack in the concrete message model if there is one in the abstract message model. Finally we present highlights of a practical case study on TLS.

General Information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, Technical University of Denmark
Authors: Mödersheim, S. A. (Intern), Katsoris, G. (Ekstern)
Number of pages: 16
Publication date: 2014
Automated Generation of Attack Trees

Attack trees are widely used to represent threat scenarios in a succinct and intuitive manner, suitable for conveying security information to non-experts. The manual construction of such objects relies on the creativity and experience of specialists, and therefore it is error-prone and impracticable for large systems. Nonetheless, the automated generation of attack trees has only been explored in connection to computer networks and leveraging rich models, whose analysis typically leads to an exponential blow-up of the state space. We propose a static analysis approach where attack trees are automatically inferred from a process algebraic specification in a syntax-directed fashion, encompassing a great many application domains and avoiding incurring systematically an exponential explosion. Moreover, we show how the standard propositional denotation of an attack tree can be used to phrase interesting quantitative problems, that can be solved through an encoding into Satisfiability Modulo Theories. The flexibility and effectiveness of the approach is demonstrated on the study of a national-scale authentication system, whose attack tree is computed thanks to a Java implementation of the framework.

Automatic generation of application specific FPGA multicore accelerators

High performance computing systems make increasing use of hardware accelerators to improve performance and power properties. For large high-performance FPGAs to be successfully integrated in such computing systems, methods to raise the abstraction level of FPGA programming are required. In this paper we propose a tool flow, which automatically generates highly optimized hardware multicore systems based on parameters. Profiling feedback is used to adjust these parameters to improve performance and lower the power consumption. For an image processing application we show that our tools are able to identify optimal performance energy trade-offs points for a multicore based FPGA accelerator.
Can We Efficiently Check Concurrent Programs Under Relaxed Memory Models in Maude?

Relaxed memory models offer suitable abstractions of the actual optimizations offered by multi-core architectures and by compilers of concurrent programming languages. Using such abstractions for verification purposes is challenging in part due to their inherent non-determinism which contributes to the state space explosion. Several techniques have been proposed to mitigate those problems so to make verification under relaxed memory models feasible. We discuss how to adopt some of those techniques in a Maude-based approach to language prototyping, and suggest the use of other techniques that have been shown successful for similar verification purposes.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, IMT Institute for Advanced Studies Lucca
Authors: Arrahman, Y. A. (Ekstern), Andric, M. (Ekstern), Beggiato, A. (Ekstern), Lluch Lafuente, A. (Intern)
Pages: 21-41
Publication date: 2014
Code Commentary and Automatic Refactorings using Feedback from Multiple Compilers
Optimizing compilers are essential to the performance of parallel programs on multi-core systems. It is attractive to expose parallelism to the compiler letting it do the heavy lifting. Unfortunately, it is hard to write code that compilers are able to optimize aggressively and therefore tools exist that can guide programmers with refactorings allowing the compilers to optimize more aggressively. We target the problem with many false positives that these tools often generate, where the amount of feedback can be overwhelming for the programmer. Our approach is to use a filtering scheme based on feedback from multiple compilers and show how we are able to filter out 87.6% of the comments by only showing the most promising comments.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, Embedded Systems Engineering
Authors: Jensen, N. B. (Intern), Probst, C. W. (Intern), Karlsson, S. (Intern)
Number of pages: 4
Publication date: 2014

Host publication information
Title of host publication: Proceedings of the 7th Swedish Workshop on Multicore Computing (MCC’14)
Main Research Area: Technical/natural sciences
Electronic versions:
mcc14_NicklasBoJensen.pdf
Source: PublicationPreSubmission
Source-ID: 104282777
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

Collaborative Compiler Vectorization

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, Embedded Systems Engineering
Authors: Jensen, N. B. (Intern), Probst, C. W. (Intern), Karlsson, S. (Intern)
Number of pages: 1
Publication date: 2014
Event: Poster session presented at 9th International Conference on High-Performance and Embedded Architectures and Compilers, Vienna, Austria.
Main Research Area: Technical/natural sciences
Electronic versions:
poster_hipeac_2014_valid.pdf

Bibliographical note
Poster at the HiPEAC’14 Poster Session
Source: PublicationPreSubmission
Source-ID: 102241744
Publication: Research › Poster – Annual report year: 2014
Combining Generated Data Models with Formal Invalidation for Insider Threat Analysis
In this paper we revisit the advances made on invalidation policies to explore attack possibilities in organizational models. One aspect that has so far eloped systematic analysis of insider threat is the integration of data into attack scenarios and its exploitation for analyzing the models. We draw from recent insights into generation of insider data to complement a logic based mechanical approach. We show how insider analysis can be traced back to the early days of security verification and the Lowe-attack on NSPK. The invalidation of policies allows model checking organizational structures to detect insider attacks. Integration of higher order logic specification techniques allows the use of data refinement to explore attack possibilities beyond the initial system specification. We illustrate this combined invalidation technique on the classical example of the naughty lottery fairy. Data generation techniques support the automatic generation of insider attack data for research. The data generation is however always based on human generated insider attack scenarios that have to be designed based on domain knowledge of counter-intelligence experts. Introducing data refinement and invalidation techniques here allows the systematic exploration of such scenarios and exploit data centric views into insider threat analysis.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, Middlesex University
Authors: Kammuller, F. (Ekstern), Probst, C. W. (Intern)
Pages: 229-235
Publication date: 2014

Host publication information
Title of host publication: 2014 IEEE Security and Privacy Workshops (SPW)
Publisher: IEEE
Main Research Area: Technical/natural sciences
Conference: 2014 IEEE Security and Privacy Workshops (SPW), San Jose, California, United States, 17/05/2014 - 17/05/2014
Insider threats, policies, formal methods
Electronic versions:
KammullerProbst_MIST14_CombiningGeneratedDataModelsWithFormalInvalidationForInsiderThreatAnalysis.pdf
DOIs: 10.1109/SPW.2014.45
Links:

Bibliographical note
Source: PublicationPreSubmission
Source-ID: 100963147
Publication: Research - peer-review ▶ Article in proceedings – Annual report year: 2014

Compiler Feedback using Continuous Dynamic Compilation during Development
Optimizing compilers are vital for performance. However, compilers ability to optimize aggressively is limited in some cases. To address this limitation, we have developed a compiler guiding the programmer in making small source code changes, potentially making the source code more amenable to optimization. This tool can help programmers understand what the optimizing compiler has done and suggest automatic source code changes in cases where the compiler refrains from optimizing. We have integrated our tool into an integrated development environment, interactively giving feedback as part of the programmers development flow. We have evaluated our preliminary implementation and show it can guide to a 12% improvement in performance. Furthermore the tool can be used as an interactive optimization adviser improving the performance of the code generated by a production compiler. Here it can lead to a 153% improvement in performance, indicating the feasibility of the tool as a performance adviser for a production compiler.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, Embedded Systems Engineering
Authors: Jensen, N. B. (Intern), Karlsson, S. (Intern), Probst, C. W. (Intern)
Number of pages: 12
Publication date: 2014

Host publication information

Recently, cyber security has become an important topic on the agenda of many organisations. It is already widely acknowledged that attacks do happen, and decision makers face the problem of how to respond. As it is almost impossible to secure a complex system completely, it is important to have an adequate estimate of the effectiveness of security measures when making investment decisions. Risk concepts are known in principle, but estimating the effectiveness of countermeasure proves to be difficult and cannot be achieved by qualitative approaches only. In this chapter, the authors consider the question of how to guarantee cost-effectiveness of security measures. They investigate the possibility of using existing frameworks and tools, the challenges in a security context as opposed to a safety context, and directions for future research.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, Delft University of Technology, University of Twente
Authors: Pieters, W. (Ekstern), Probst, C. W. (Intern), Lukszo, Z. (Ekstern), Montoya, L. (Ekstern)
Pages: 139-156
Publication date: 2014

Host publication information
Title of host publication: Approaches and Processes for Managing the Economics of Information Systems
Publisher: IGI global
Editors: Tsiakis, T., Kargidis, T., Katsaros, P.
ISBN (Print): 978-1-4666-4983-5
Chapter: 9
Main Research Area: Technical/natural sciences
DOI: 10.4018/978-1-4666-4983-5.ch009
Source: PublicationPreSubmission
Source-ID: 101754591
Publication: Research - peer-review › Report chapter – Annual report year: 2014

Denial-of-Service Security Attack in the Continuous-Time World

Hybrid systems are integrations of discrete computation and continuous physical evolution. The physical components of such systems introduce safety requirements, the achievement of which asks for the correct monitoring and control from the discrete controllers. However, due to denial-of-service security attack, the expected information from the controllers is not received and as a consequence the physical systems may fail to behave as expected. This paper proposes a formal framework for expressing denial-of-service security attack in hybrid systems. As a virtue, a physical system is able to plan for reasonable behavior in case the ideal control fails due to unreliable communication, in such a way that the safety of the system upon denial-of-service is still guaranteed. In the context of the modeling language, we develop an inference system for verifying safety of hybrid systems, without putting any assumptions on how the environments behave. Based on the inference system, we implement an interactive theorem prover and have applied it to check an example taken from train control system.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, Chinese Academy of Sciences
Authors: Wang, S. (Ekstern), Nielson, F. (Intern), Nielson, H. R. (Intern)
Pages: 149-165
Publication date: 2014

Host publication information
Title of host publication: Formal Techniques for Distributed Objects, Components, and Systems. Proceedings
Publisher: Springer
DySectAPI: Scalable Prescriptive Debugging

We present the DySectAPI, a tool that allow users to construct probe trees for automatic, event-driven debugging at scale. The traditional, interactive debugging model, whereby users manually step through and inspect their application, does not scale well even for current supercomputers. While lightweight debugging models scale well, they can currently only debug a subset of bug classes. DySectAPI fills the gap between these two approaches with a novel user-guided approach. Using both experimental results and analytical modeling we show how DySectAPI scales and can run with a low overhead on current systems.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, Embedded Systems Engineering, Lawrence Livermore National Laboratory, Mesosphere Inc
Authors: Jensen, N. B. (Intern), Karlsson, S. (Intern), Quarfot Nielsen, N. (Ekstern), Lee, G. L. (Ekstern), Ahn, D. H. (Ekstern), Legendre, M. (Ekstern), Schulz, M. (Ekstern)
Number of pages: 1
Publication date: 2014
Event: Poster session presented at International Conference for High Performance Computing, Networking, Storage and Analysis, SC14, New Orleans, United States.
Main Research Area: Technical/natural sciences
Electronic versions:
post237s2_file2.pdf
Links:
Publication: Research - peer-review › Poster – Annual report year: 2014
ELB-trees - Efficient Lock-free B+trees

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, Embedded Systems Engineering
Authors: Bonnichsen, L. F. (Intern), Karlsson, S. (Intern), Probst, C. W. (Intern)
Number of pages: 1
Publication date: 2014
Event: Poster session presented at 9th International Conference on High-Performance and Embedded Architectures and Compilers, Vienna, Austria.
Main Research Area: Technical/natural sciences
Electronic versions: actualPoster.pdf

Bibliographical note
Poster at the HiPEAC'14 Poster Session
Source: PublicationPreSubmission
Source-ID: 102243655
Publication: Research › Poster – Annual report year: 2014

ELB-trees - Efficient Lock-free B+trees
As computer systems scale in the number of processors, data structures with good parallel performance become increasingly important. Lock-free data structures promise improved parallel performance at the expense of higher complexity and sequential execution time. We present ELBtrees, a new lock-free dictionary with simple synchronization in the common case, making it almost 30 times faster than sequential library implementations at 24 threads.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, Embedded Systems Engineering
Authors: Bonnichsen, L. F. (Intern), Karlsson, S. (Intern), Probst, C. W. (Intern)
Number of pages: 4
Publication date: 2014

Host publication information
Main Research Area: Technical/natural sciences
Electronic versions: abstract_ELB_trees.pdf
Source: PublicationPreSubmission
Source-ID: 102243974
Publication: Research › peer-review › Conference abstract in proceedings – Annual report year: 2014

Exploring adaptive program behavior

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology
Authors: Bonnichsen, L. F. (Intern), Probst, C. W. (Intern)
Number of pages: 1
Publication date: 2014
Main Research Area: Technical/natural sciences
Electronic versions: poster3.pdf
Exploring Adaptive Program Behavior
Modern computer systems are increasingly complex, with ever changing bottlenecks. This makes it difficult to ensure consistent performance when porting software, or even running it. Adaptivity, ie, switching between program variations, and dynamic recompilation have been suggested as solutions. Both solutions come at a cost; adaptivity issues a runtime overhead and requires more design effort, while dynamic recompilation takes time to perform. In this project, we plan to investigate the possibilities, limitations, and benefits of these techniques. This abstract covers our thoughts on how adaptivity and dynamic recompilation can be integrated and evaluated.

Formal Security Analysis of the MaCAN Protocol.
Embedded real-time network protocols such as the CAN bus cannot rely on off-the-shelf schemes for authentication, because of the bandwidth limitations imposed by the network. As a result, both academia and industry have proposed custom protocols that meet such constraints, with solutions that may be deemed insecure if considered out of context. MaCAN is one such compatible authentication protocol, proposed by Volkswagen Research and a strong candidate for being adopted by the automotive industry.

In this work we formally analyse MaCAN with ProVerif, an automated protocol verifier. Our formal analysis identifies two flaws in the original protocol: one creates unavailability concerns during key establishment, and the other allows re-using authenticated signals for different purposes. We propose and analyse a modification that improves its behaviour while fitting the constraints of CAN bus. Although the revised scheme improves the situation, it is still not completely secure. We argue that the modified protocol makes a good compromise between the desire to secure automotive systems and the limitations of CAN networks.
Foundational aspects of security
This Special Issue of the Journal of Computer Security focuses on foundational aspects of security, which in recent years have helped change much of the way we think about and approach system security.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, Centre National de la Recherche Scientifique, Ecole Polytechnique, University of Luxembourg
Authors: Chatzikokolakis, K. (Ekstern), Mödersheim, S. A. (Intern), Palamidessi, C. (Ekstern), Pang, J. (Ekstern)
Pages: 201-202
Publication date: 2014
Main Research Area: Technical/natural sciences
Publication information
Journal: Journal of Computer Security
Volume: 22
ISSN (Print): 0926-227X
Ratings:
BFI (2018): BFI-level 2
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 2
BFI (2016): BFI-level 2
Scopus rating (2016): SJR 0.373 SNIP 0.999 CiteScore 1.17
BFI (2015): BFI-level 2
Scopus rating (2015): SJR 0.508 SNIP 1.174 CiteScore 1.12
BFI (2014): BFI-level 2
Scopus rating (2014): SJR 0.625 SNIP 1.78 CiteScore 1.62
BFI (2013): BFI-level 2
Scopus rating (2013): SJR 0.784 SNIP 1.955 CiteScore 1.91
ISI indexed (2013): ISI indexed no
BFI (2012): BFI-level 2
Scopus rating (2012): SJR 0.863 SNIP 2.352 CiteScore 2.03
ISI indexed (2012): ISI indexed no
BFI (2011): BFI-level 2
Scopus rating (2011): SJR 0.71 SNIP 1.713 CiteScore 1.65
ISI indexed (2011): ISI indexed no
BFI (2010): BFI-level 2
Scopus rating (2010): SJR 0.811 SNIP 2.413
BFI (2009): BFI-level 2
Scopus rating (2009): SJR 0.866 SNIP 2.184
BFI (2008): BFI-level 2
Scopus rating (2008): SJR 0.93 SNIP 2.105
Scopus rating (2007): SJR 1.057 SNIP 1.857
Scopus rating (2006): SJR 1.677 SNIP 2.356
Scopus rating (2005): SJR 1.362 SNIP 3.439
Scopus rating (2004): SJR 1.361 SNIP 3.135
Scopus rating (2003): SJR 1.717 SNIP 4.999
Scopus rating (2002): SJR 1.483 SNIP 2.898
Hardware Realization of an FPGA Processor – Operating System Call Offload and Experiences

Field-programmable gate arrays, FPGAs, are attractive implementation platforms for low-volume signal and image processing applications.

The structure of FPGAs allows for an efficient implementation of parallel algorithms. Sequential algorithms, on the other hand, often perform better on a microprocessor. It is therefore convenient for many applications to employ a synthesizable microprocessor to execute sequential tasks and custom hardware structures to accelerate parallel sections of an algorithm. In this paper, we discuss the hardware realization of Tinuso-I, a small synthesizable processor core that can be integrated in many signal and data processing platforms on FPGAs. We also show how we allow the processor to use operating system services. For a set of SPLASH-2 and SPEC CPU2006 benchmarks we show a speedup of up to 64% over a similar Xilinx MicroBlaze implementation while using 27% to 35% fewer hardware resources.

ICT-powered Health Care Processes

The efficient use of health care resources requires the use of Information and Communication Technology (ICT). During a treatment process, patients have often been tested and partially treated with different diagnoses in mind before the precise diagnosis is identified. To use resources well it becomes necessary to adapt the prescribed treatments to make use of the tests and partial treatments already performed, rather than always starting from square one. We propose to facilitate this through the design of declarative process models accounting for the involvement of distributed groups of medical specialists and the adaptation of treatments, and through the evaluation of the trustworthiness of models taking account of test results and actual treatments compared to the clinical guidelines.
Invalidating Policies using Structural Information

Insider threats are a major threat to many organisations. Even worse, insider attacks are usually hard to detect, especially if an attack is based on actions that the attacker has the right to perform. In this paper we present a step towards detecting the risk for this kind of attacks by invalidating policies using structural information of the organisational model. Based on this structural information and a description of the organisation’s policies, our approach invalidates the policies and identifies exemplary sequences of actions that lead to a violation of the policy in question. Based on these examples, the organisation can identify real attack vectors that might result in an insider attack. This information can be used to refine access control systems or policies. We provide case studies showing how mechanical verification tools, i.e. modelchecking with MCMAS and interactive theorem proving in Isabelle/HOL, can be applied to support the invalidation and thereby the identification of the attack vectors.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, Middlesex University
Authors: Kammuller, F. (Ekstern), Probst, C. W. (Intern)
Pages: 59-79
Publication date: 2014
Main Research Area: Technical/natural sciences

Publication information
Journal: Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications
Volume: 5
Issue number: 2
ISSN (Print): 2093-5374
Ratings:
- Scopus rating (2016): CiteScore 1.62
- Scopus rating (2015): CiteScore 1.2
- Scopus rating (2014): CiteScore 1.1
- Scopus rating (2013): CiteScore 1.49
- ISI indexed (2013): ISI indexed no
Original language: English
organisational structure, policies, formal methods
Electronic versions:
- jowua_v5n2_4.pdf
Source: PublicationPreSubmission
Source-ID: 100963101
Publication: Research - peer-review › Journal article – Annual report year: 2014

Model-based Abstraction of Data Provenance
Identifying provenance of data provides insights to the origin of data and intermediate results, and has recently gained increased interest due to data-centric applications. In this work we extend a data-centric system view with actors handling the data and policies restricting actions. This extension is based on provenance analysis performed on system models. System models have been introduced to model and analyse spatial and organisational aspects of organisations, to identify, e.g., potential insider threats. Both the models and analyses are naturally modular; models can be combined to
bigger models, and the analyses adapt accordingly. Our approach extends provenance both with the origin of data, the actors and processes involved in the handling of data, and policies applied while doing so. The model and corresponding analyses are based on a formal model of spatial and organisational aspects, and static analyses of permissible actions in the models. While currently applied to organisational models, our approach can also be extended to work flows, thus targeting a more traditional model of provenance.

**General information**
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, Aalborg University
Authors: Probst, C. W. (Intern), Hansen, R. R. (Ekstern)
Number of pages: 4
Publication date: 2014

**Host publication information**
Title of host publication: Proceedings of the 6th USENIX Workshop on the Theory and Practice of Provenance (TaPP '14)
Publisher: USENIX Association
Main Research Area: Technical/natural sciences
Workshop: 6th USENIX Workshop on the Theory and Practice of Provenance (TaPP '14), Cologne, Germany, 12/06/2014 - 12/06/2014
Electronic versions:
tapp14_paper_probst.pdf
Links:
https://www.usenix.org/conference/tapp2014/agenda/presentation/probst
Source: PublicationPreSubmission
Source-ID: 100963123

Modeling Human Behaviour with Higher Order Logic: Insider Threats
In this paper, we approach the problem of modeling the human component in technical systems with a view on the difference between the use of model and theory in sociology and computer science. One aim of this essay is to show that building of theories and models for sociology can be compared to and implemented in Higher Order Logic. We validate this working hypothesis by revisiting Weber’s understanding explanation. We focus on constructive realism in the context of logical explanation. We review Higher Order Logic (HOL) as a foundation for computer science and summarize its use of theories relating it to the sociological process of logical explanation. As a case study on modeling human behaviour, we present the modeling and analysis of insider threats as a Higher Order Logic theory in Isabelle/HOL. We show how each of the three step process of sociological explanation can be seen in our modeling of insider’s state, its context within an organisation and the effects on security as outcomes of a theorem proving analysis.

**General information**
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, Middlesex University
Authors: Boender, J. (Ekstern), Ivanova, M. G. (Intern), Kammuller, F. (Ekstern), Primiero, G. (Ekstern)
Number of pages: 8
Pages: 31 - 39
Publication date: 2014

**Host publication information**
Title of host publication: Proceedings of the 4th workshop on Socio-Technical Aspects of Security and Trust, STAST 2014
Publisher: IEEE
Main Research Area: Technical/natural sciences
Workshop: 4th Workshop on Socio-Technical Aspects of Security and Trust (STAST 2014), Vienna, Austria, 18/07/2014
DOIs:
10.1109/STAST.2014.13
Source: PublicationPreSubmission
Source-ID: 101358922
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

Pareto Efficient Solutions of Attack Trees

**General information**
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology
These are the proceedings of the Third Workshop on GRAPH Inspection and Traversal Engineering (GRAPHITE 2014), which took place on April 5, 2014 in Grenoble, France, as a satellite event of the 17th European Joint Conferences on Theory and Practice of Software (ETAPS 2014).

The aim of GRAPHITE is to foster the convergence on research interests from several communities dealing with graph analysis in all its forms in computer science, with a particular attention to software development and analysis. Graphs are used to represent data and processes in many application areas, and they are subjected to various computational algorithms in order to analyze them. Just restricting the attention to the analysis of software, graph analysis algorithms are used, for instance, to verify properties using model checking techniques that explore the system's state space graph or static analysis techniques based on control flow graphs. Further application domains include games, planning, and network analysis. Very often, graph problems and their algorithmic solutions have common characteristics, independent of their application domain. The goal of this event is to gather scientists from different communities, who do research on graph analysis algorithms, such that awareness of each others' work is increased.

Proceedings of the 7th Interaction and Concurrency Experience (ICE 2014)

This volume contains the proceedings of ICE 2014, the 7th Interaction and Concurrency Experience, which was held in Berlin, Germany on the 6th of June 2014 as a satellite event of DisCoTec 2014. The ICE procedure for paper selection allows PC members to interact, anonymously, with authors. During the review phase, each submitted paper is published on a Wiki and associated with a discussion forum whose access is restricted to the authors and to all the PC members not declaring a conflict of interests. The PC members post comments and questions that the authors reply to. Each paper was reviewed by three PC members, and altogether 8 papers (including 3 short papers) were accepted for publication. We were proud to host two invited talks, by Pavol Cerny and Kim Larsen, whose abstracts are included in this volume together with the regular papers.
Quantitative modelling and analysis of a Chinese smart grid: a stochastic model checking case study

Cyber-physical systems integrate information and communication technology with the physical elements of a system, mainly for monitoring and controlling purposes. The conversion of traditional power grid into a smart grid, a fundamental example of a cyber-physical system, raises a number of issues that require novel methods and applications. One of the important issues in this context is the verification of certain quantitative properties of the system. In this paper, we consider a specific Chinese smart grid implementation as a case study and address the verification problem for performance and energy consumption. We employ stochastic model checking approach and present our modelling and analysis study using PRISM model checker.
Smartphones as pocketable labs: Visions for mobile brain imaging and neurofeedback

Mobile brain imaging solutions, such as the Smartphone Brain Scanner, which combines low cost wireless EEG sensors with open source software for real-time neuroimaging, may transform neuroscience experimental paradigms. Normally subject to the physical constraints in labs, neuroscience experimental paradigms can be transformed into dynamic environments allowing for the capturing of brain signals in everyday contexts. Using smartphones or tablets to access text or images may enable experimental design capable of tracing emotional responses when shopping or consuming media, incorporating sensorimotor responses reflecting our actions into brain machine interfaces, and facilitating neurofeedback training over extended periods. Even though the quality of consumer neuroheadsets is still lower than laboratory equipment and susceptible to environmental noise, we show that mobile neuroimaging solutions, like the Smartphone Brain Scanner, complemented by 3D reconstruction or source separation techniques may support a range of neuroimaging applications and thus become a valuable addition to high-end neuroimaging solutions.
Sufficient Conditions for Vertical Composition of Security Protocols (Extended Version)

Vertical composition of security protocols means that an application protocol (e.g., a banking service) runs over a channel established by another protocol (e.g., a secure channel provided by TLS). This naturally gives rise to a compositionality question: given a secure protocol P1 that provides a certain kind of channel as a goal and another secure protocol P2 that assumes this kind of channel, can we then derive that their vertical composition P2[P1] is secure? It is well known that protocol composition can lead to attacks even when the individual protocols are all secure in isolation. In this paper, we formalize seven easy-to-check static conditions that support a large class of channels and applications and that we prove to be sufficient for vertical security protocol composition.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, King’s College London
Authors: Mödersheim, S. A. (Intern), Viganò, L. (Ekstern)
Number of pages: 20
Publication date: 2014

Publication information
Publisher: DTU Compute
Original language: English
The logic of XACML
We study the international standard XACML 3.0 for describing security access control policies in a compositional way. Our main contributions are (i) to derive a logic that precisely captures the intentions of the standard, (ii) to formally define a semantics for the XACML 3.0 component evaluation, and (iii) to define a semantics for the XACML 3.0 standard combining operators. To guard against modeling artefacts we provide an alternative lattice based way of characterizing the policy combining operators and we formally prove the equivalence of these approaches thereby increasing our faith in either one. We then discuss several ways of extending XACML: one direction is to extend XACML with new combining operators, and
another direction is to incorporate the notion of conflict into XACML. We conclude by discussing the possibility of analysing XACML policies for gaps and conflicts.
The stochastic quality calculus

We introduce the Stochastic Quality Calculus in order to model and reason about distributed processes that rely on each other in order to achieve their overall behaviour. The calculus supports broadcast communication in a truly concurrent setting. Generally distributed delays are associated with the outputs and at the same time the inputs impose constraints on the waiting times. Consequently, the expected inputs may not be available when needed and therefore the calculus allows to express the absence of data. The communication delays are expressed by general distributions and the resulting semantics is given in terms of Generalised Semi-Markov Decision Processes. By restricting the distributions to be continuous and by allowing truly concurrent communication we eliminate the non-determinism and arrive at Generalised Semi-Markov Processes (GSMPs); further restriction to exponential distributions gives rise to numerically analysable GSMPs, in particular using techniques from stochastic model checking.

Uniform Protection for Multi-exposed Targets

Ensuring that information is protected proportionately to its value is a major challenge in the development of robust distributed systems, where code complexity and technological constraints might allow reaching a key functionality along various paths. We propose a protection analysis over the Quality Calculus that computes the combinations of data required to reach a program point and relates them to a notion of cost. In this way, we can compare the security deployed on different paths that expose the same resource. The analysis is formalised in terms of flow logic, and is implemented as an optimisation problem encoded into Satisfiability Modulo Theories, allowing us to deal with complex cost structures. The usefulness of the approach is demonstrated on the study of password recovery systems.
Verification of Stateful Protocols - Set-Based Abstractions in the Applied Pi-Calculus

A calculus for quality

A main challenge of programming component-based software is to ensure that the components continue to behave in a reasonable manner even when communication becomes unreliable. We propose a process calculus, the Quality Calculus, for programming software components where it becomes natural to plan for default behaviour in case the ideal behaviour fails due to unreliable communication and thereby to increase the quality of service offered by the systems. The development is facilitated by a SAT-based robustness analysis to determine whether or not the code is vulnerable to unreliable communication. This is illustrated on the design of a fragment of a wireless sensor network.
An algebraic approach to analysis of recursive and concurrent programs

This thesis focuses on formal techniques based on static program analysis, model checking and abstract interpretation that offer means for reasoning about software, verification of its properties and discovering potential bugs.

First, we investigate an algebraic approach to static analysis and explore its connections to abstract interpretation framework. We introduce the notion of a flow algebra, which is an algebraic structure similar to semirings, but closer to the classical monotone frameworks. We also generalize Galois connections to flow algebras and discuss when a flow algebra is an upper-approximation of (or induced from) another flow algebra.

Furthermore, we show how flow algebras can be used in communicating or weighted pushdown systems. To achieve that, we show that it is possible to relax some of the requirements imposed by original formulation of those techniques without compromising the soundness or completeness results.

Moreover, we present a new application of pushdown systems in the context of an aspect-oriented process calculus. The addition of aspect-oriented features makes it possible for a process to exhibit a recursive structure. We show how one can faithfully model and analyze such a language.

We also introduce an abstract domain that symbolically represents the messages sent between the concurrently executing processes. It stores prefixes or suffixes of communication traces including various constraints imposed on the messages. Since the problem has exponential complexity, we also present a compact data structure as well as efficient algorithms for the semiring operations.

Apart from that, we discuss an improvement to Pre* and Post* algorithms for pushdown systems, making it possible to directly use program representations such as program graphs. We present a modular library implementing those algorithms, which also provides a lot of flexibility with respect to, e.g., various constraints solvers.

Finally, we describe one such experimental solver based on Newton’s method. It allows solving equation systems over abstract domains that were not accommodated by other solving techniques, e.g., Kleene iteration. We present such a domain and provide a preliminary evaluation of our implementation.

To conclude, we believe the thesis presents a number of contributions interesting both from the theoretical point of view as well as from an implementation one.
A tighter bound for the self-stabilization time in Herman's algorithm
We study the expected self-stabilization time of Herman's algorithm. For N processors the lower bound is 427N^2
(0.148N^2), and an upper bound of 0.64N^2 is presented in Kiefer et al. (2011) [4]. In this paper we give a tighter upper
bound 0.521N^2. © 2013 Published by Elsevier B.V.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, University of
Technology, Sydney
Authors: Feng, Y. (Ekstern), Zhang, L. (Intern)
Pages: 486-488
Publication date: 2013
Main Research Area: Technical/natural sciences

Publication information
Journal: Information Processing Letters
Volume: 113
Issue number: 13
ISSN (Print): 0020-0190
Ratings:
BFI (2018): BFI-level 2
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 2
Web of Science (2017): Indexed Yes
BFI (2016): BFI-level 2
Scopus rating (2016): SJR 0.57 SNIP 0.967 CiteScore 1.02
BFI (2015): BFI-level 2
Scopus rating (2015): SJR 0.602 SNIP 1.167 CiteScore 0.93
BFI (2014): BFI-level 2
Scopus rating (2014): SJR 0.593 SNIP 0.934 CiteScore 0.94
Web of Science (2014): Indexed yes
BFI (2013): BFI-level 2
Scopus rating (2013): SJR 0.609 SNIP 1.047 CiteScore 0.95
ISI indexed (2013): ISI indexed yes
Web of Science (2013): Indexed yes
BFI (2012): BFI-level 2
Scopus rating (2012): SJR 0.603 SNIP 1.037 CiteScore 0.92
ISI indexed (2012): ISI indexed yes
Web of Science (2012): Indexed yes
BFI (2011): BFI-level 2
Scopus rating (2011): SJR 0.612 SNIP 0.929 CiteScore 0.85
ISI indexed (2011): ISI indexed yes
Web of Science (2011): Indexed yes
BFI (2010): BFI-level 2
Scopus rating (2010): SJR 0.625 SNIP 1.016
Web of Science (2010): Indexed yes
BFI (2009): BFI-level 2
Scopus rating (2009): SJR 0.708 SNIP 1.062
BFI (2008): BFI-level 1
Scopus rating (2008): SJR 0.837 SNIP 1.161
Web of Science (2008): Indexed yes
Scopus rating (2007): SJR 0.76 SNIP 1.144
Web of Science (2007): Indexed yes
Scopus rating (2006): SJR 0.699 SNIP 1.193
Scopus rating (2005): SJR 0.614 SNIP 1.189
Scopus rating (2004): SJR 0.652 SNIP 1.171
Scopus rating (2003): SJR 0.726 SNIP 1.248
Bisimulations meet PCTL equivalences for probabilistic automata

Probabilistic automata (PAs) have been successfully applied in formal verification of concurrent and stochastic systems. Efficient model checking algorithms have been studied, where the most often used logics for expressing properties are based on probabilistic computation tree logic (PCTL) and its extension PCTL*. Various behavioral equivalences are proposed, as a powerful tool for abstraction and compositional minimization for PAs. Unfortunately, the equivalences are well-known to be sound, but not complete with respect to the logical equivalences induced by PCTL or PCTL*. The desire of a both sound and complete behavioral equivalence has been pointed out by Segala in [34], but remains open throughout the years. In this paper we introduce novel notions of strong bisimulation relations, which characterize PCTL and PCTL* exactly. We extend weak bisimulations that characterize PCTL and PCTL* without next operator, respectively. Further, we also extend the framework to simulation preorders. Thus, our paper bridges the gap between logical and behavioral equivalences and preorders in this setting.
Broadcast, Denial-of-Service, and Secure Communication

A main challenge in the design of wireless-based Cyber-Physical Systems consists in balancing the need for security and the effect of broadcast communication with the limited capabilities and reliability of sensor nodes. We present a calculus of broadcasting processes that enables to reason about unsolicited messages and lacking of expected communication. Moreover, standard cryptographic mechanisms can be implemented in the calculus via term rewriting. The modelling framework is complemented by an executable specification of the semantics of the calculus in Maude, thereby facilitating solving a number of simple reachability problems.

Deciding bisimilarities on distributions

Probabilistic automata (PA) are a prominent compositional concurrency model. As a way to justify property-preserving abstractions, in the last years, bisimulation relations over probability distributions have been proposed both in the strong and the weak setting. Different to the usual bisimulation relations, which are defined over states, an algorithmic treatment
of these relations is inherently hard, as their carrier set is uncountable, even for finite PAs. The coarsest of these relation, weak distribution bisimulation, stands out from the others in that no equivalent state-based characterisation is known so far. This paper presents an equivalent state-based reformulation for weak distribution bisimulation, rendering it amenable for algorithmic treatment. Then, decision procedures for the probability distribution-based bisimulation relations are presented.

**General information**

State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, Saarland University
Authors: Eisentraut, C. (Ekstern), Hermanns, H. (Intern), Krämer, J. (Ekstern), Turrini, A. (Ekstern), Zhang, L. (Intern)
Pages: 72-88
Publication date: 2013

**Host publication information**

Publisher: Springer
ISBN (Print): 978-3-642-40195-4
ISBN (Electronic): 978-3-642-40196-1

**Defining Privacy Is Supposed to Be Easy**

Formally specifying privacy goals is not trivial. The most widely used approach in formal methods is based on the static equivalence of frames in the applied pi-calculus, basically asking whether or not the intruder is able to distinguish two given worlds. A subtle question is how we can be sure that we have specified all pairs of worlds to properly reflect our intuitive privacy goal. To address this problem, we introduce in this paper a novel and declarative way to specify privacy goals, called α-β privacy, and relate it to static equivalence. This new approach is based on specifying two formulae α and β in first-order logic with Herbrand universes, where α reflects the intentionally released information and β includes the actual cryptographic (“technical”) messages the intruder can see. Then α-β privacy means that the intruder cannot derive any “non-technical” statement from β that he cannot derive from α already. We describe by a variety of examples how this notion can be used in practice. Even though α-β privacy does not directly contain a notion of distinguishing between worlds, there is a close relationship to static equivalence of frames that we investigate formally. This allows us to justify (and criticize) the specifications that are currently used in verification tools, and obtain partial tool support for α-β privacy.

**General information**

State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, Newcastle University, King’s College London
Authors: Mödersheim, S. A. (Intern), Gross, T. (Ekstern), Viganò, L. (Ekstern)
Pages: 619-635
Publication date: 2013

**Host publication information**

Publisher: Springer
ISBN (Print): 978-3-642-45220-8
ISBN (Electronic): 978-3-642-45221-5

Series: Lecture Notes in Computer Science
Volume: 8312
ISSN: 0302-9743
BFI conference series: International Conferences on Logic for Programming, Artificial Intelligence and Reasoning (5020047)
Design-Efficiency in Security
In this document, we present our applied results on balancing security and performance using a running example, which is based on sensor networks. These results are forming a basis for a new approach to balance security and performance, and therefore provide design-efficiency of key updates. We employ probabilistic model checking approach and present our modelling and analysis study using PRISM model checker.

Detecting and Preventing Beacon Replay Attacks in Receiver-Initiated MAC Protocols for Energy Efficient WSNs
In receiver-initiated MAC protocols for Wireless Sensor Networks (WSNs), communication is initiated by the receiver of the data through beacons containing the receiver's identity. In this paper, we consider the case of a network intruder that captures and replays such beacons towards legitimate nodes, pretending to have a fake identity within the network. To prevent this attack we propose RAP, a challenge-response authentication protocol that is able to detect and prevent the beacon replay attack. The effectiveness of the protocol is formally verified using OFMC and ProVerif. Furthermore, we provide an analysis that highlights the trade-offs between the energy consumption and the level of security, defined as the resilience of the protocol to space exhaustion.
ELB-trees: an efficient and lock-free B-tree derivative

As computer systems scale in the number of processors, scalable data structures with good parallel performance become increasingly important. Lock-free data structures promise such improved parallel performance at the expense of higher algorithmic complexity and higher sequential execution time overhead. All lock-free data structures are based on simple atomic operations that, though supported by modern processors, are expensive in execution time. We present a lock-free data structure, ELB-trees, which under certain assumptions can be used as multimaps as well as priority queues. Specifically it cannot store duplicate key-value pairs, and it is not linearizable. Compared to existing data structures, ELB-trees require fewer atomic operations leading to improved performance. We measure the parallel performance of ELB-trees using a set of benchmarks and observe that ELB-trees are up to almost 30 times faster than library multimap implementations.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering, Language-Based Technology
Authors: Bonnichsen, L. F. (Intern), Karlsson, S. (Intern), Probst, C. W. (Intern)
Number of pages: 10
Publication date: 2013

Host publication information
Publisher: IEEE
Main Research Area: Technical/natural sciences
DOIs: 10.1109/MuCoCoS.2013.6633606
Source: dtu
Source-ID: n::oai:DTIC-ART:iel/409579987::34994
Publication: Research - peer-review › Article in proceedings – Annual report year: 2013

ELB-trees - Efficient Lock-free B+trees

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, Embedded Systems Engineering
Authors: Bonnichsen, L. F. (Intern), Karlsson, S. (Intern), Probst, C. W. (Intern)
Number of pages: 1
Publication date: 2013
Main Research Area: Technical/natural sciences
Electronic versions:
actualPoster_EBL_trees.pdf
Source: PublicationPreSubmission
Source-ID: 102244024
Publication: Research › Poster – Annual report year: 2014

Externalizing Behaviour for Analysing System Models

System models have recently been introduced to model organisations and evaluate their vulnerability to threats and especially insider threats. Especially for the latter these models are very suitable, since insiders can be assumed to have more knowledge about the attacked organisation than outside attackers. Therefore, many attacks are considerably easier to be performed for insiders than for outsiders. However, current models do not support explicit specification of different behaviours. Instead, behaviour is deeply embedded in the analyses supported by the models, meaning that it is a
complex, if not impossible task to change behaviours. Especially when considering social engineering or the human factor in general, the ability to use different kinds of behaviours is essential. In this work we present an approach to make the behaviour a separate component in system models, and explore how to integrate in existing models.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, Aalborg University, Middlesex University
Authors: Ivanova, M. G. (Intern), Probst, C. W. (Intern), Hansen, R. R. (Ekstern), Kammuller, F. (Ekstern)
Pages: 52-62
Publication date: 2013
Main Research Area: Technical/natural sciences

Publication information
Journal: Journal of Internet Services and Information Security
Volume: 3
Issue number: 3/4
ISSN (Print): 2182-2069
Ratings:
ISI indexed (2013): ISI indexed no
Original language: English
system models, static analysis, human behaviour
Electronic versions:
jenis_2013_vol3_no34_05.pdf
Source: PublicationPreSubmission
Source-ID: 100963113
Publication: Research - peer-review › Journal article – Annual report year: 2014

Foreword: Science of Computer Programming, special section from the Principles and Practice of Programming in Java conference

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, ABB Corporate Research, Vienna University of Technology, Johannes Kepler University of Linz, University of Calgary
Authors: Aleksy, M. (Ekstern), Gitzel, R. (Ekstern), Krall, A. (Ekstern), Mössenböck, H. (Ekstern), Probst, C. W. (Intern), Stephenson, B. (Ekstern)
Pages: 423-424
Publication date: 2013
Main Research Area: Technical/natural sciences

Publication information
Journal: Science of Computer Programming
Volume: 78
ISSN (Print): 0167-6423
Ratings:
BFI (2018): BFI-level 2
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 2
Web of Science (2017): Indexed yes
BFI (2016): BFI-level 2
Scopus rating (2016): CiteScore 1.36 SJR 0.454 SNIP 1.271
Web of Science (2016): Indexed yes
BFI (2015): BFI-level 2
Scopus rating (2015): SJR 0.442 SNIP 1.182 CiteScore 1.18
Web of Science (2015): Indexed yes
BFI (2014): BFI-level 2
Scopus rating (2014): SJR 0.438 SNIP 1.479 CiteScore 1.2
Web of Science (2014): Indexed yes
BFI (2013): BFI-level 2
Scopus rating (2013): SJR 0.528 SNIP 1.551 CiteScore 1.3
Invalidating Policies using Structural Information

Insider threats are a major threat to many organisations. Even worse, insider attacks are usually hard to detect, especially if an attack is based on actions that the attacker has the right to perform. In this paper we present a step towards detecting the risk for this kind of attacks by invalidating policies using structural information of the organisational model. Based on this structural information and a description of the organisation's policies, our approach invalidates the policies and identifies exemplary sequences of actions that lead to a violation of the policy in question. Based on these examples, the organisation can identify real attack vectors that might result in an insider attack. This information can be used to refine access control system or policies.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, Middlesex University
Authors: Kammuller, F. (Ekstern), Probst, C. W. (Intern)
Pages: 76-81
Publication date: 2013

Host publication information
Title of host publication: 2013 IEEE Security and Privacy Workshops
Publisher: IEEE
ISBN (Print): 978-1-4799-0458-7
Main Research Area: Technical/natural sciences
Workshop: 2013 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, United States, 23/05/2013 - 23/05/2013
DOIs: 10.1109/SPW.2013.36
Source: dtu
Source-ID: n:oai:DTIC-ART:inspec/390690650::35345
Lazy Mobile Intruders
We present a new technique for analyzing platforms that execute potentially malicious code, such as web-browsers, mobile phones, or virtualized infrastructures. Rather than analyzing given code, we ask what code an intruder could create to break a security goal of the platform. To avoid searching the infinite space of programs that the intruder could come up with (given some initial knowledge) we adapt the lazy intruder technique from protocol verification: the code is initially just a process variable that is getting instantiated in a demand-driven way during its execution. We also take into account that by communication, the malicious code can learn new information that it can use in subsequent operations, or that we may have several pieces of malicious code that can exchange information if they "meet". To formalize both the platform and the malicious code we use the mobile ambient calculus, since it provides a small, abstract formalism that models the essence of mobile code. We provide a decision procedure for security against arbitrary intruder processes when the honest processes can only perform a bounded number of steps and without path constraints in communication. We show that this problem is NP-complete.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology
Authors: Mödersheim, S. A. (Intern), Nielson, F. (Intern), Nielson, H. R. (Intern)
Pages: 147-166
Publication date: 2013

Model checking conditional CSL for continuous-time Markov chains
In this paper, we consider the model-checking problem of continuous-time Markov chains (CTMCs) with respect to conditional logic. To the end, we extend Continuous Stochastic Logic introduced in Aziz et al. (2000) [1] to Conditional Continuous Stochastic Logic (CCSL) by introducing a conditional probabilistic operator. CCSL allows us to express a richer class of properties for CTMCs. Based on a parameterized product obtained from the CTMC and an automaton extracted from a given CCSL formula, we propose an approximate model checking algorithm and analyse its complexity.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, Chinese Academy of Sciences, East China Normal University
Authors: Gao, Y. (Ekstern), Xu, M. (Ekstern), Zhan, N. (Ekstern), Zhang, L. (Intern)
Pages: 44-50
Publication date: 2013
Main Research Area: Technical/natural sciences

Publication information
Journal: Information Processing Letters
Volume: 113
Issue number: 1-2
ISSN (Print): 0020-0190
Ratings:
BFI (2018): BFI-level 2
On Building Secure Communication Systems

This thesis presents the Guided System Development (GSD) framework, which aims at supporting the development of secure communication systems.
A communication system is specified in a language similar to the Alice and Bob notation, a simple and intuitive language used to describe the global perspective of the communications between different principals. The notation used in the GSD framework extends that notation with constructs that allow the security requirements of the messages to be described.

From that specification, the developer is guided through a semi-automatic translation that enables the verification and implementation of the system. The translation is semi-automatic because the developer has the option of choosing which implementation to use in order to achieve the specified security requirements. The implementation options are given by plugins defined in the framework. The framework’s flexibility allows for the addition of constructs that model new security properties as well as new plugins that implement the security properties.

In order to provide higher security assurances, the system specification can be verified by formal methods tools such as the Beliefs and Knowledge (BAK) tool — developed specifically for the GSD framework —, LySatool and OFMC. The framework’s flexibility and the existence of the system model in different perspectives — an overall global perspective and an endpoint perspective — allow the connection to new formal methods tools.

The modeled system is also translated into code that implements the communication skeleton of the system and can then be used by the system designer. New output languages can also easily be added to the GSD framework.

Additionally, a prototype of the GSD framework was implemented and an example of using the GSD framework in a real world system is presented.

**General information**

State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology
Authors: Carvalho Quaresma, J. N. (Intern), Probst, C. W. (Intern), Nielson, F. (Intern)
Number of pages: 139
Publication date: 2013

**Publication information**

Place of publication: Kgs. Lyngby
Publisher: Technical University of Denmark (DTU)
Original language: English

Series: PHD-2013
Number: 313
ISSN: 0909-3192
Main Research Area: Technical/natural sciences
Electronic versions:

On the relationship between LTL normal forms and Büchi automata
In this paper, we revisit the problem of translating LTL formulas to Büchi automata. We first translate the given LTL formula into a special disjunctive-normal form (DNF). The formula will be part of the state, and its DNF normal form specifies the atomic properties that should hold immediately (labels of the transitions) and the formula that should hold afterwards (the corresponding successor state). If the given formula is Until-free or Release-free, the Büchi automaton can be obtained directly in this manner. For a general formula, the construction is more involved: an additional component will be needed for each formula that helps us to identify the set of accepting states. Notably, our construction is an on-the-fly construction, which starts with the given formula and explores successor states according to the normal forms. We implement our construction and compare the tool with SPOT [3]. The comparison results are very encouraging and show our construction is quite innovative.

**General information**

State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, East China Normal University, Aalborg University
Authors: Li, J. (Ekstern), Pu, G. (Ekstern), Zhang, L. (Intern), Wang, Z. (Ekstern), He, J. (Ekstern), Guldstrand Larsen, K. (Ekstern)
Pages: 256-270
Publication date: 2013

**Host publication information**

Title of host publication: Theories of Programming and Formal Methods: Essays Dedicated to Jifeng He on the Occasion of His 70th Birthday
Publisher: Springer
ISBN (Print): 978-3-642-39697-7
Predictive access control for distributed computation

We show how to use aspect-oriented programming to separate security and trust issues from the logical design of mobile, distributed systems. The main challenge is how to enforce various types of security policies, in particular predictive access control policies — policies based on the future behavior of a program. A novel feature of our approach is that we can define policies concerning secondary use of data.

General information

State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, Imperial College London
Authors: Yang, F. (Intern), Hankin, C. (Ekstern), Nielson, F. (Intern), Nielson, H. R. (Intern)
Pages: 1264-1277
Publication date: 2013
Main Research Area: Technical/natural sciences
Probabilistic Analysis of the Quality Calculus

We consider a fragment of the Quality Calculus, previously introduced for defensive programming of software components such that it becomes natural to plan for default behaviour in case the ideal behaviour fails due to unreliable communication. This paper develops a probabilistically based trust analysis supporting the Quality Calculus. It uses information about the probabilities that expected input will be absent in order to determine the trustworthiness of the data used for controlling the distributed system; the main challenge is to take accord of the stochastic dependency between some of the inputs. This takes the form of a relational static analysis dealing with quantitative information.

General information

State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology
Authors: Nielsen, H. R. (Intern), Nielsen, F. (Intern)
Pages: 258-272
Publication date: 2013
Reachability-based impact as a measure for insiderness

Insider threats pose a difficult problem for many organisations. While organisations in principle would like to judge the risk posed by a specific insider threat, this is in general not possible. This limitation is caused partly by the lack of models for human behaviour, partly by restrictions on how much and what may be monitored, and by our inability to identify relevant features in large amounts of logged data. To overcome this, the notion of insiderness has been proposed, which measures the degree of access an actor has to a certain resource. We extend this notion with the concept of impact of an insider, and present different realisations of impact. The suggested approach results in readily usable techniques that allow to get a quick overview of potential insider threats based on locations and assets reachable by employees. We present several variations ranging from pure reachability to potential damage to assets causable by an insider.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, Aalborg University
Authors: Probst, C. W. (Intern), Hansen, R. R. (Intern)
Pages: 38-48
Publication date: 2013
Main Research Area: Technical/natural sciences

Publication information
Journal: Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications
Volume: 4
Issue number: 4
ISSN (Print): 2093-5374
Ratings:
Scopus rating (2016): CiteScore 1.62
Scopus rating (2015): CiteScore 1.2
Scopus rating (2014): CiteScore 1.1
Scopus rating (2013): CiteScore 1.49
ISI indexed (2013): ISI indexed no
Original language: English
Insider threats, Insiderness, System models
Electronic versions:
jowua_v4n4_3.pdf
Links:
http://isyou.info/jowua/abstracts/jowua-v4n4-3.htm
Source: FindIt
Source-ID: 258736231
Publication: Research - peer-review › Journal article – Annual report year: 2014

Reachability for Finite-state Process Algebras Using Horn Clauses

In this work we present an algorithm for solving the reachability problem in finite systems that are modelled with process algebras. Our method is based on Static Analysis, in particular, Data Flow Analysis, of the syntax of a process algebraic system with multi-way synchronisation. The results of the Data Flow Analysis are used in order to build a set of Horn clauses whose least model corresponds to an overapproximation of the reachable states. The computed model can be refined after each transition, and the algorithm runs until either a state whose reachability should be checked is encountered or it is not in the least model for all constructed states and thus is definitely unreachable. The advantages of the algorithm are that in many cases only a part of the Labelled Transition System will be built which leads to lower time and memory consumption. Also, it is not necessary to save all the encountered states which leads to further reduction of the memory requirements of the algorithm.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology
Authors: Skrypnyuk, N. (Intern), Nielson, F. (Intern)
Pages: 283-302
Publication date: 2013
Main Research Area: Technical/natural sciences

Publication information
Volume: 24
Revisiting Weak Simulation for Substochastic Markov Chains

The spectrum of branching-time relations for probabilistic systems has been investigated thoroughly by Baier, Hermanns, Katoen and Wolf (2003, 2005), including weak simulation for systems involving substochastic distributions. Weak simulation was proven to be sound w.r.t. the liveness fragment of the logic PCTLx, and its completeness was conjectured. We revisit this result and show that soundness does not hold in general, but only for Markov chains without divergence. It is refuted for some systems with substochastic distributions. Moreover, we provide a counterexample to completeness. In this paper, we present a novel definition that is sound for live PCTLx, and a variant that is both sound and complete. A long version of this article containing full proofs is available from [11].

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, Radboud University Nijmegen, Max Planck Institute
Authors: Jansen, D. N. (Ekstern), Song, L. (Ekstern), Zhang, L. (Intern)
Safety versus Security in the Quality Calculus

Safety and security are both needed for ensuring that cyber-physical systems live up to expectations, but often an intelligent trade-off is called for, because sometimes it is impossible to obtain optimal safety at the same time as optimal security. In the context of the Quality Calculus we develop a type system for checking the extent to which safety and security goals have been met. Safety goals include showing that certain error configurations are in fact not reachable and hence do not require intelligent error handling. Security goals include showing that highly trusted communications can only be performed in highly trusted contexts. This is potentially too demanding and the Quality Calculus is therefore extended with a primitive for endorsing data to a higher trust level (accepting violations of the explicit flow) and for temporarily asserting a higher trust in the context (accepting violations of the implicit flow). This is illustrated on a worked example taken from the automotive sector and we conclude with a discussion of the theoretical properties of the type system.
Security Games for Cyber-Physical Systems
The development of quantitative security analyses that consider both active attackers and reactive defenders is a main challenge in the design of trustworthy Cyber-Physical Systems. We propose a game-theoretic approach where it is natural to model attacker's and defender's actions explicitly, associating costs to attacks and countermeasures. Cost considerations enable to contrast different strategies on the basis of their effectiveness and efficiency, paving the way to a multi-objective notion of optimality. Moreover, the framework allows expressing the probabilistic nature of the environment and of the attack detection process. Finally, a solver is presented to compute strategies and their costs, resorting to a recent combination of strategy iteration with linear programming.

Spatio temporal media components for neurofeedback
A class of Brain Computer Interfaces (BCI) involves interfaces for neurofeedback training, where a user can learn to self-regulate brain activity based on real-time feedback. These particular interfaces are constructed from audio-visual components and temporal settings, which appear to have a strong influence on the ability to control brain activity. Therefore, identifying the different interface components and exploring their individual effects might be key for constructing new interfaces that support more efficient neurofeedback training. We discuss experiments involving two different designs of neurofeedback interfaces and suggest further research to clarify the influence of different audiovisual components and temporal settings on neurofeedback effect.
The Quest for Minimal Quotients for Probabilistic Automata

One of the prevailing ideas in applied concurrency theory and verification is the concept of automata minimization with respect to strong or weak bisimilarity. The minimal automata can be seen as canonical representations of the behaviour modulo the bisimilarity considered. Together with congruence results wrt. process algebraic operators, this can be exploited to alleviate the notorious state space explosion problem. In this paper, we aim at identifying minimal automata and canonical representations for concurrent probabilistic models. We present minimality and canonicity results for probabilistic automata wrt. strong and weak bisimilarity, together with polynomial time minimization algorithms.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, Saarland University, University of the Federal Armed Forces Munich
Authors: Eisentraut, C. (Ekstern), Hermanns, H. (Ekstern), Schuster, J. (Ekstern), Turrini, A. (Ekstern), Zhang, L. (Intern)
Pages: 16-31
Publication date: 2013
Logics and Models for Stochastic Analysis Beyond Markov Chains

Within the last twenty years, logics and models for stochastic analysis of information systems have been widely studied in both theory and practice. The quantitative properties, such as performance and reliability, are evaluated over discrete–time and continuous–time Markov chains. This thesis lifts the stochastic analysis techniques from the class of Markov chains to the more general classes of stochastic processes having PHase–type (PH) distributions and Matrix–Exponential (ME) distributions, such that a Markov renewal process with ME kernels that cannot be formulated as a Markov process with finite or countable state space.

PH distributions are known for many explicit analytic properties, such that systems having PH distributed components can still be formulated as Markov chains. This thesis presents several results related to PH distributions. We first show how to use the explicit analytic form of discrete PH distributions as computational vehicle on measuring the performance of concurrent wireless sensor networks. Secondly, choosing stochastic process algebras as a widely accepted formalism, we study the compositionaliy of continuous PH distributions in order to support modelling concurrent stochastic systems having PH representations as building blocks. At last, we consider discrete–time point processes having PH distributed interarrival times with multiple marks, we propose time-lapse bisimulation, a state-based characterisation of the equivalence relation between the point processes. We clarify that time-lapse bisimulation is a new contribution to the existing bisimulation family, which captures probabilistic behaviour over time for labelled discrete–time Markov chains.

ME distributions is a strictly larger class than PH distributions, such that many results from PH distributions also are valid for ME distributions. ME distributions have a very appealing property, called minimality property: generally a ME representation of a PH distribution will be of lower dimension than PH representations, and one can always find a ME representation with the minimal dimension. However, because of the generality of ME distributions, we have to leave the world of Markov chains. To support ME distributions with multiple exits, we introduce a multi-exits ME distribution together with a process algebra MEME to express the systems having the semantics as Markov renewal processes with ME kernels. The most appealing feature is that all the components before and after compositions are secured to have a minimal state space representation. To support quantitative verification, we also propose stochastic model checking algorithms to our problem.
Safety Verification for Probabilistic Hybrid Systems

The interplay of random phenomena and continuous dynamics deserves increased attention, especially in the context of wireless sensing and control applications. Safety verification for such systems thus needs to consider probabilistic variants of systems with hybrid dynamics. In safety verification of classical hybrid systems, we are interested in whether a certain set of unsafe system states can be reached from a set of initial states. In the probabilistic setting, we may ask instead whether the probability of reaching unsafe states is below some given threshold. In this paper, we consider probabilistic hybrid systems and develop a general abstraction technique for verifying probabilistic safety problems. This gives rise to the first mechanisable technique that can, in practice, formally verify safety properties of non-trivial continuous-time stochastic hybrid systems. Moreover, being based on abstractions computed by tools for the analysis of non-probabilistic hybrid systems, improvements in effectivity of such tools directly carry over to improvements in effectivity of the technique we describe. We demonstrate the applicability of our approach on a number of case studies, tackled using a prototypical implementation.
Smart Grid Security A Smart Meter-Centric Perspective

The electricity grid is a key infrastructure for our society, therefore its security is a critical public concern. This physical system is becoming more and more complex as it is coupled with a cyber layer carrying information about power usage and control instructions for intelligent appliances, leading to what is known as the Smart Grid. The development of this Cyber-Physical System introduces new security issues, thus calling for efforts in studying possible attacks and devising suitable countermeasures. In this paper, we review a generic model for the Smart Grid, and present possible attacks and countermeasures focusing on a key component of the Smart Grid: the Smart Meter.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology
Authors: Vigo, R. (Intern), Yuksel, E. (Intern), Ramli, C. D. P. K. (Intern)
Pages: 127-130
Publication date: 2012

Host publication information
Title of host publication: 2012 20th Telecommunications Forum (TELFOR)
Publisher: IEEE
ISBN (Print): 978-1-4673-2983-5
Main Research Area: Technical/natural sciences
Conference: 20th Telecommunications Forum (TELFOR 2012), Belgrade, Serbia, 20/11/2012 - 20/11/2012
Cyber-Physical System, Cyber security, Home area network, Smart grid, Smart meter
DOIs:
10.1109/TELFOR.2012.6419164
Source: dtu
Source-ID: n:oai:DTIC-ART:iel/378375919::25723
Publication: Research - peer-review › Article in proceedings – Annual report year: 2013

Activities:

CryptoForma Workshop
Period: 13 Jul 2015
Omar Almousa (Speaker)
Department of Applied Mathematics and Computer Science
Language-Based Technology

Description

Related event

CryptoForma Workshop
13/07/2015 → 14/07/2015
Verona, Italy
Activity: Talks and presentations › Conference presentations

Adaptivity Framework: libpappadapt
Period: 22 Jan 2014
Lars Frydendal Bonnichsen (Speaker)
Department of Applied Mathematics and Computer Science
Language-Based Technology
Embedded Systems Engineering

Description
Præsentation af adaptivity biblioteket libpappadapt udviklet i PaPP projektet

PaPP tutorial presentation ved HiPEAC'14, se: http://www.hipeac.net/conference/vienna/tutorial/papp
Documents:
PaPP_Adaptivity_0.50_speed

Related external organisation

Unknown external organisation
Activity: Talks and presentations › Conference presentations

Prizes:

Otto Mønsteds Fund: Travel grant
Hugo-Andrés López-Acosta (Recipient)
Department of Applied Mathematics and Computer Science, Language-Based Technology

Description
Travel grant to support the presentation of a paper at the 2015 ACM SIGPLAN International Conference on Object-Oriented Programming, Systems, Languages, and Applications, OOPSLA 2015, part of {SLASH} 2015. Pittsburgh, PA, USA, October 25-30, 2015

Details
Awarded date: 25 Oct 2015
Granting Organisations: Otto Mønsteds Fond
Prize: Prizes, scholarships, distinctions