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.
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
Scopus rating (2008): SJR 0.506 SNIP 1.046
Scopus rating (2007): SJR 0.62 SNIP 1.556
Scopus rating (2006): SJR 0.564 SNIP 0.963
Scopus rating (2005): SJR 0.515 SNIP 1.166
Scopus rating (2004): SJR 0.64 SNIP 0.733
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.
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.
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.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology
Authors: Bruni, A. (Intern), Nielson, F. (Intern), Nielson, H. R. (Intern)
Number of pages: 155
Publication date: 2016

Publication information
Place of publication: Kgs. Lyngby
Publisher: Technical University of Denmark (DTU)
Original language: English
Series: DTU Compute PHD-2016
Number: 389
ISSN: 0909-3192
Main Research Area: Technical/natural sciences
Electronic versions: phd389_Bruni_A.pdf

Relations
Projects:
Analysis of Security Protocols in Embedded Systems
Publication: Research › Ph.D. thesis – Annual report year: 2016

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
Disjunctive Information Flow for Communicating Processes

The security validation of practical computer systems calls for the ability to specify and verify information flow policies that are dependent on data content. Such policies play an important role in concurrent, communicating systems: consider a scenario where messages are sent to different processes according to their tagging. We devise a security type system that enforces content-dependent information flow policies in the presence of communication and concurrency. The type system soundly guarantees a compositional noninterference property. All theoretical results have been formally proved in the Coq proof assistant [9].

General information

State: Published
Organisations: Department of Applied Mathematics and Computer Science, University of Science and Technology of China
Authors: Li, X. (Intern), Nielson, F. (Intern), Nielson, H. R. (Intern), Feng, X. (Ekstern)
Pages: 95-111
Publication date: 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

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

Host publication information
Title of host publication: Proceedings of the 36th IFIP WG 6.1 International Conference on Formal Techniques for Distributed Objects, Components, and Systems (FORTE 2016)
Publisher: Springer
Editors: Albert, E., Lanese, I.
ISBN (Print): 978-3-319-39569-2
ISBN (Electronic): 978-3-319-39570-8

Series: Lecture Notes in Computer Science
Volume: 9688
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
Conference: 36th IFIP WG 6.1 International Conference on Formal Techniques for Distributed Objects, Components, and Systems (FORTE 2016), Heraklion, Crete, Greece, 06/06/2016 - 06/06/2016
Electronic versions:
main.pdf
DOIs:
10.1007/978-3-319-39570-8_13
Source: PublicationPreSubmission
Source-ID: 123902709
Publication: Research - peer-review › Article in proceedings – Annual report year: 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.

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.

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.
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.
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 flaw 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].
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.

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.
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

Availability by Design: A Complementary Approach to Denial-of-Service

In computer security, a Denial-of-Service (DoS) attack aims at making a resource unavailable. DoS attacks to systems of public concern occur increasingly and have become infamous on the Internet, where they have targeted major corporations and institutions, thus reaching the general public. There exist various practical techniques to face DoS attacks and mitigate their effects, yet we witness the successfulness of many.

The need for a renewed investigation of availability gains in relevance when considering that our life is more and more dominated by Cyber-Physical Systems (CPSs), large-scale network of sensors that interact with the physical environment. CPSs are increasingly exploited in the realisation of critical infrastructure, from the power grid to healthcare, traffic control, and defence applications. Such systems are particularly prone to DoS attacks: in addition to classic communication-based attacks, their components can be subject to physical capture. Moreover, sensors are often powered by batteries, and time-limited unavailability is usually a stage planned to prolong their life span.

This dissertation argues that techniques rooted in the theory and practice of programming languages, language-based techniques, offer a unifying framework to deal with the consequences of DoS, thereby encompassing inadvertent and malicious sources of unavailability in a uniform manner.

In support to this claim we develop a family of process calculi, the Quality Calculi, where availability considerations are promoted to be first-class object of the language domain. Moreover, these modelling tools are complemented by static analyses that pinpoint where and why unavailability may occur, leveraging the enhanced expressiveness of the language.

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
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.

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.
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 misconduct 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 trustable re-use of data.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, Department of Informatics and Mathematical Modeling
Authors: Karafili, E. (Intern), Nielson, H. R. (Intern), Nielson, F. (Intern)
Pages: 72-88
Publication date: 2015

Host publication information
Title of host publication: Proceedings of the 11th International Workshop on Security and Trust Management (STM 2015)
Publisher: Springer
Editor: Foresti, S.
ISBN (Print): 978-3-319-24857-8
ISBN (Electronic): 978-3-319-24858-5

Series: Lecture Notes in Computer Science
Volume: 9331
ISSN: 0302-9743
BFI conference series: Security and Trust Management (5010862)
Main Research Area: Technical/natural sciences
Conference: 11th International Workshop on Security and Trust Management (STM 2015), Vienna, Austria, 21/09/2015 - 21/09/2015
DOIs:
10.1007/978-3-319-24858-5_5

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
Editors: Holvoet, T., Viroli, M.
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
DOIs:
10.1007/978-3-319-19282-6_13
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), Nielsen, H. R. (Intern), Nielsen, 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

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.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology
Authors: Bruni, A. (Intern), Mödersheim, S. A. (Intern), Nielson, F. (Intern), Nielson, H. R. (Intern)
Pages: 185-188
Publication date: 2015

Host publication information
Publisher: IEEE

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.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology
Authors: Nielson, F. (Intern), Nielson, H. R. (Intern), Zeng, K. (Intern)
Pages: 522-537
Publication date: 2015

Host publication information
Title of host publication: Software, Services, and Systems: Essays Dedicated to Martin Wirsing on the Occasion of His Retirement from the Chair of Programming and Software Engineering
Publisher: Springer
Editors: De Nicola, R., Hennicker, R.
ISBN (Print): 978-3-319-15544-9
ISBN (Electronic): 978-3-319-15545-6

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.
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.

Availability by Design

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
Editors: Ábrahám, E., Palamidessi, C.
ISBN (Print): 978-3-662-43612-7
ISBN (Electronic): 978-3-662-43613-4
Series: Lecture Notes in Computer Science
Volume: 8461
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
Conference: 34th IFIP WG 6.1 International Conference, FORTE 2014, Berlin, Germany, 03/06/2014 - 03/06/2014
Hybrid systems, Denial-of-service, Safety verification, Inference system
DOIs: 10.1007/978-3-662-43613-4_10
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

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.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, Czech Technical University
Authors: Bruni, A. (Intern), Sojka, M. (Ekstern), Nielson, F. (Intern), Nielson, H. R. (Intern)
Pages: 241-255
Publication date: 2014

Host publication information
Title of host publication: Proceedings of the 11th International Conference on Integrated Formal Methods, IFM 2014
Publisher: Springer
Editors: Albert, E., Sekerinski, E.
ISBN (Print): 978-3-319-10180-4
ISBN (Electronic): 978-3-319-10181-1
Series: Lecture Notes in Computer Science
Volume: 8739
ISSN: 0302-9743
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.

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.
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.

**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)

Pages: 80-105

Publication date: 2014

Main Research Area: Technical/natural sciences

**Publication information**

Journal: Science of Computer Programming

Volume: 83

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
- 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
- ISI indexed (2013): ISI indexed yes
- Web of Science (2013): Indexed yes
- BFI (2012): BFI-level 2
- Scopus rating (2012): SJR 0.626 SNIP 1.85 CiteScore 1.66
- ISI indexed (2012): ISI indexed yes
- BFI (2011): BFI-level 2
- Scopus rating (2011): SJR 0.634 SNIP 1.973 CiteScore 1.81
- ISI indexed (2011): ISI indexed yes
- BFI (2010): BFI-level 2
- Scopus rating (2010): SJR 1.146 SNIP 2.637
- Web of Science (2010): Indexed yes
- BFI (2009): BFI-level 2
- Scopus rating (2009): SJR 0.872 SNIP 1.915
- BFI (2008): BFI-level 2
- Scopus rating (2008): SJR 1.02 SNIP 2.022
- Scopus rating (2007): SJR 0.734 SNIP 1.973
- Scopus rating (2006): SJR 0.615 SNIP 1.547
- Scopus rating (2005): SJR 0.699 SNIP 1.502
- Web of Science (2005): Indexed yes
- Scopus rating (2004): SJR 0.706 SNIP 2.11
- Scopus rating (2003): SJR 0.851 SNIP 1.818
- Web of Science (2003): Indexed yes
- Scopus rating (2002): SJR 1.189 SNIP 1.58
- Scopus rating (2001): SJR 1.171 SNIP 1.912
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.
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.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology
Authors: Nielson, H. R. (Intern), Nielson, F. (Intern), Vigo, R. (Intern)
Pages: 188-204
Publication date: 2013

Host publication information
Title of host publication: Formal Aspects of Component Software : 9th International Symposium, FACS 2012, Mountain View, CA, USA, September 12-14, 2012. Revised Selected Papers
Publisher: Springer
ISBN (Print): 978-3-642-35860-9
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.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology
Authors: Terepeta, M. T. (Intern), Nielson, H. R. (Intern), Nielson, F. (Intern)
Number of pages: 205
Publication date: 2013

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

Series: IMM-PHD-2013
Number: 307
ISSN: 0909-3192
Main Research Area: Technical/natural sciences
Electronic versions: phd307_Terepeta_M.pdf
Publication: Research › Ph.D. thesis – Annual report year: 2013
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.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology
Authors: Vigo, R. (Intern), Nielson, F. (Intern), Nielson, H. R. (Intern)
Pages: 412-427
Publication date: 2013

Host publication information
Title of host publication: Integrated Formal Methods: 10th International Conference, IFM 2013, Turku, Finland, June 10-14, 2013. Proceedings
Publisher: Springer
ISBN (Print): 978-3-642-38612-1
ISBN (Electronic): 978-3-642-38613-8

Series: Lecture Notes in Computer Science
Volume: 7940
ISSN: 0302-9743
BFI conference series: Integrated Formal Methods (5000153)
Main Research Area: Technical/natural sciences
Conference: 10th International Conference on integrated Formal Methods (iFM 2013), Turku, Finland, 10/06/2013 - 10/06/2013
Cyber-Physical Systems, Broadcast communication, Denial-of-Service, Process calculus, Security protocol verification

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.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology
Authors: Yuksel, E. (Intern), Nielson, H. R. (Intern), Nielson, F. (Intern)
Number of pages: 33
Publication date: 2013

Publication information
Place of publication: Kgs. Lyngby
Publisher: Technical University of Denmark (DTU)
Original language: English
Number: 2013-03
ISSN: 1601-2321
Main Research Area: Technical/natural sciences
Electronic versions:
tr13_03_Yuksel_E.pdf
Publication: Research › Report – Annual report year: 2013

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.

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.
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.
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.
XACML 3.0 in Answer Set Programming

We present a systematic technique for transforming XACML 3.0 policies in Answer Set Programming (ASP). We show that the resulting logic program has a unique answer set that directly corresponds to our formalisation of the standard semantics of XACML 3.0 from [9]. We demonstrate how our results make it possible to use off-the-shelf ASP solvers to formally verify properties of access control policies represented in XACML, such as checking the completeness of a set of access control policies and verifying policy properties.

General information

State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology
Authors: Ramli, C. D. P. K. (Intern), Nielsen, H. R. (Intern), Nielsen, F. (Intern)
Pages: 89-105
Publication date: 2013

Host publication information

Title of host publication: Logic-Based Program Synthesis and Transformation: 22nd International Symposium, LOPSTR 2012, Leuven, Belgium, September 18-20, 2012, Revised Selected Papers
Publisher: Springer
ISBN (Print): 978-3-642-38196-6
ISBN (Electronic): 978-3-642-38197-3

Series: Lecture Notes in Computer Science
Volume: 7844
ISSN: 0302-9743
BFI conference series: Logic-Based Program Synthesis and Transformation (5000273)
Main Research Area: Technical/natural sciences
XACML, Access control, Policy language, Answer Set Programming

A Succinct Approach to Static Analysis and Model Checking

In a number of areas software correctness is crucial, therefore it is often desirable to formally verify the presence of various properties or the absence of errors. This thesis presents a framework for concisely expressing static analysis and model checking problems. The framework facilitates rapid prototyping of new analyses and consists of variants of ALFP logic and associated solvers.

First, we present a Lattice based Least Fixed Point Logic (LLFP) that allows interpretations over complete lattices satisfying Ascending Chain Condition. We establish a Moore Family result for LLFP that guarantees that there always is a single best solution for a problem under consideration. We also develop a solving algorithm, based on a dierential worklist, that computes the least solution guaranteed by the Moore Family result.

Furthermore, we present a logic for specifying analysis problems called Layered Fixed Point Logic. Its most prominent
feature is the direct support for both inductive computations of behaviors as well as co-inductive specifications of properties. Two main theoretical contributions are a Moore Family result and a parametrized worst-case time complexity result. We develop a BDD-based solving algorithm, which computes the least solution guaranteed by the Moore Family result with worst-case time complexity as given by the complexity result.

We also present magic set transformation for ALFP, known from deductive databases, which is a clause-rewriting strategy for optimizing query evaluation. In order to compute the answer to a query, the original ALFP clauses are rewritten at compile time, and then the rewritten clauses are evaluated bottom-up. It is usually more efficiently than computing entire solution followed by selection ii of the tuples of interest, which was the case in the classical formulation of ALFP logic.

Finally, we show that the logics and the associated solvers can be used for rapid prototyping. We illustrate that by a variety of case studies from static analysis and model checking.

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling, Language-Based Technology, Computer Science and Engineering
Authors: Filipiuk, P. (Intern), Nielson, H. R. (Intern), Nielson, F. (Intern)
Number of pages: 187
Publication date: 2012

Publication information
Place of publication: Kgs. Lyngby
Publisher: Technical University of Denmark (DTU)
Original language: English
Series: IMM-PHD-2012
Number: 278
ISSN: 2012-268
Main Research Area: Technical/natural sciences
Electronic versions:
phd278_PiotrFilipiuk_net.pdf
Publication: Research › Ph.D. thesis – Annual report year: 2012

Distributed security in closed distributed systems
The goal of the present thesis is to discuss, argue and conclude about ways to provide security to the information travelling around computer systems consisting of several known locations.

When developing software systems, security of the information managed by these plays an important role in their design. There should always exist techniques for ensuring that the required security properties are met. This has been thoroughly investigated through the years, and many varied methodologies have come through. In the case of distributed systems, there are even harder issues to deal with. Many approaches have been taken towards solving security problems, yet many questions remain unanswered. Most of these problems are related to some of the following facts: distributed systems do not usually have any central controller providing security to the entire system; the system heterogeneity is usually reflected in heterogeneous security aims; the software life cycle entails evolution and this includes security expectations; the distribution is useful if the entire system is "open" to new (a priori unknown) interactions; the distribution itself poses intrinsically more complex security-related problems, such as communication, cryptography, performance and reliability. We do not expect to solve all of these, but we shall approach the first three.

In this dissertation, we take the view of a distributed system from a high-level of abstraction. We then focus on the interactions that can take place between the locations, and aim at providing security to each of these individually. The approach taken is by means of access control enforcement mechanisms, providing security to the locations they are related to. We provide a framework for modelling so. All this follows techniques borrowed from the aspect-orientation community.

As this needs to be scaled up to the entire distributed system, we then focus on ways of reasoning about the resulting composition of these individual access control mechanisms. We show how, by means of relying on the semantics of our framework, we can syntactically guarantee some limited set of global security properties. This is also restricted to distributed systems in which the set of locations is known a priori. All this follows techniques borrowed from both the model checking and the static analysis communities.

In the end, we reach a step towards solving the problem of enforcing security in distributed systems. We achieve the goal of showing how this can be done, though we restrict ourselves to closed systems and with a limited set of enforceable security policies. In this setting, our approach proves to be efficient.

Finally, we achieve all this by bringing together several fields of Computer Science. These include aspect orientation, model checking and static analysis, and of course some ingredients of logics and formal methods as well. All this is in an attempt to approach a software engineering problem, such as security in distributed systems. This shows how the full field of Computer Science can benefit from combining its subfields.

General information
Fixpoints vs Moore Families

Model checking and static analysis are both successful approaches to the analysis of IT systems and it has been shown that many static analyses can be reduced to model checking. Recent results show that CTL model checking can be reduced to static analysis and that the set of satisfying states of a CTL formula can be described as the least element in a Moore family of acceptable sets of states for the static analysis. Turning the attention to the μ-calculus we are able to generalise this result to the alternation-free fragment whereas even for the fragment of alternation depth 2 we show that the fixed point characterisation cannot be recast as a Moore family property.

Flow Logic for Process Calculi

Flow Logic is an approach to statically determining the behavior of programs and processes. It borrows methods and techniques from Abstract Interpretation, Data Flow Analysis and Constraint Based Analysis while presenting the analysis
in a style more reminiscent of Type Systems. Traditionally developed for programming languages, this article provides a tutorial development of the approach of Flow Logic for process calculi based on a decade of research.

We first develop a simple analysis for the π-calculus; this consists of the specification, semantic soundness (in the form of subject reduction and adequacy results), and a Moore Family result showing that a least solution always exists, as well as providing insights on how to implement the analysis. We then show how to strengthen the analysis technology by introducing reachability components, interaction points, and localized environments, and finally, we extend it to a relational analysis.

A Flow Logic is a program logic—in the same sense that a Hoare’s logic is. We conclude with an executive summary presenting the highlights of the approach from this perspective including a discussion of theoretical properties as well as implementation considerations.

The electronic supplements present an application of the analysis techniques to a version of the π-calculus incorporating distribution and code mobility; also the proofs of the main results can be found in the electronic supplements.

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling, Computer Science and Engineering
Authors: Nielson, H. R. (Intern), Nielson, F. (Intern), Pilegaard, H. (Intern)
Number of pages: 39
Pages: Article No. 3
Publication date: 2012
Main Research Area: Technical/natural sciences

Publication information
Journal: ACM Computing Surveys
Volume: 44
Issue number: 1
ISSN (Print): 0360-0300
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 2.362 SNIP 6.438 CiteScore 11.16
BFI (2015): BFI-level 2
Scopus rating (2015): SJR 2.664 SNIP 7.615 CiteScore 10.32
BFI (2014): BFI-level 2
Scopus rating (2014): SJR 2.494 SNIP 8.05 CiteScore 8.89
BFI (2013): BFI-level 2
Scopus rating (2013): SJR 2.691 SNIP 9.308 CiteScore 10.95
ISI indexed (2013): ISI indexed yes
BFI (2012): BFI-level 2
Scopus rating (2012): SJR 3.577 SNIP 14.973 CiteScore 13.78
ISI indexed (2012): ISI indexed yes
Web of Science (2012): Indexed yes
BFI (2011): BFI-level 2
Scopus rating (2011): SJR 5.282 SNIP 15.668 CiteScore 18.29
ISI indexed (2011): ISI indexed yes
BFI (2010): BFI-level 2
Scopus rating (2010): SJR 4.536 SNIP 10.659
BFI (2009): BFI-level 2
BFI (2008): BFI-level 2
Scopus rating (2008): SJR 2.832 SNIP 14.598
From Explicit to Symbolic Types for Communication Protocols in CCS

We study communication protocols having several rounds and expressed in value passing CCS. We develop a type-based analysis for providing an explicit record of all communications and show the usual subject reduction result. Since the explicit records can be infinitely large, we also develop a type-based analysis for providing a finite, symbolic record of all communications. We show that it correctly approximates the explicit record and prove an adequacy result for it.

Key Update Assistant for Resource-Constrained Networks

Key update is a challenging task in resource-constrained networks where limitations in terms of computation, memory, and energy restrict the proper use of security mechanisms. We present an automated tool that computes the optimal key update strategy for any given resource-constrained network. We developed a push-button solution - powered by stochastic model checking - that network designers can easily benefit from, and it paves the way for consumers to set up key update related security parameters. Key Update Assistant, as we named it, runs necessary model checking operations and determines the optimal key update strategy that satisfies given security and performance requirements.
Layered Fixed Point Logic

We present a logic for the specification of static analysis problems that goes beyond the logics traditionally used. Its most prominent feature is the direct support for both inductive computations of behaviors as well as co-inductive specifications of properties. Two main theoretical contributions are a Moore Family result and a parametrized worst case time complexity result. We show that the logic and the associated solver can be used for rapid prototyping of analyses and illustrate a wide variety of applications within Static Analysis, Constraint Satisfaction Problems and Model Checking. In all cases the complexity result specializes to the worst case time complexity of the classical methods.

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 ambients when the honest ambients can only perform a bounded number of steps and without path constraints in communication.

General information

State: Published
Organisations: Department of Informatics and Mathematical Modeling, Language-Based Technology
Authors: Filipiuk, P. (Intern), Nielson, F. (Intern), Nielson, H. R. (Intern)
Pages: 45-54
Publication date: 2012
Quantitative techniques have been successfully employed in verification of information and communication systems. However, the use of such techniques are still rare in the area of security. In this paper, we present a toolkit that implements transient analysis on a key update method for wireless sensor networks. The analysis aims to find out the probability of a network key being compromised at a specific time point, which result in fluctuations over time for a specific key update method called Leave-based key update. For such a problem, the use of current tools is limited in many ways such as rapidly constructing a compact formal model, computing the time point where the risk is maximum, or terminating the transient analysis after the fluctuations disappear and system stabilizes. Our toolkit, LBTool, is not only resolving the above-mentioned issues, but also demonstrating how to construct models in an analytical way and how to speed up the analysis by eliminating redundant computations. The toolkit can be generalized to other key update methods by replacing the analytical model construction.

Both model checking and static analysis are prominent approaches to detecting software errors. Model Checking is a successful formal method for verifying properties specified in temporal logics with respect to transition systems. Static analysis is also a powerful method for validating program properties which can predict safe approximations to program behaviors. In this thesis, we have developed several static analysis based techniques to solve model checking problems, aiming at showing the link between static analysis and model checking.

We focus on logical approaches to static analysis. Alternation-free Least Fixed Point Logic (ALFP), an extension of Datalog, has been used as the specification language in most of our research results.

We have first considered the CTL model checking and developed an ALFP-based technique to solve the CTL model checking problem. We have shown that the set of states satisfying a CTL formula can be characterized as the least model of ALFP clauses specifying this CTL formula. The existence of the least model of ALFP clauses is ensured by the Moore Family property of ALFP. Then, we take fairness assumptions in CTL into consideration and have shown that CTL fairness
problems can be encoded into ALFP as well.

To deal with multi-valued model checking problems, we have proposed multivalued ALFP. A Moore Family result for multivalued ALFP is also established, which ensures the existence and uniqueness of the least model. When the truth values in multi-valued ALFP constitute a finite distributive complete lattice, multi-valued ALFP can be reduced to two-valued ALFP. This result enables to implement a solver for multi-valued ALFP by reusing existing solvers for two-valued ALFP. Our ALFP-based technique developed for the two-valued CTL naturally generalizes to a multi-valued setting, and we therefore obtain a multivalued analysis for temporal properties specified by CTL formulas. In particular, we have shown that the three-valued CTL model checking problem over Kripke modal transition systems can be exactly encoded in three-valued ALFP.

Last, we come back to two-valued settings and have considered the model checking for the modal μ-calculus. Our results have shown that ALFP succee to deal with the model checking problem for the alternation-free μ-calculus. However, to deal with the full fragment of the μ-calculus, we need to go beyond ALFP. Therefore, we proposed Succinct Fixed Point Logic (SFP), as an extension of ALFP. We have established a Moore Family result for SFP, which ensures the existence and uniqueness of the intended model of SFP. We have shown that SFP is well suited to specify nested fixed points in the μ-calculus and the model checking problem for the μ-calculus can be encoded as the intended model of SFP.

Our research results have strengthened the link between model checking and static analysis. This provides a theoretical foundation for developing a unified tool for both model checking and static analysis techniques.
Modelling and Analysis of Smart Grid: A Stochastic Model Checking Case Study

Cyber-physical systems integrate information and communication technology functions to the physical elements of a system 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. In this context, an important issue 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.

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling, East China Normal University, Wuxi SensingNet Industrialization Research Institute
Authors: Yuksel, E. (Intern), Zhu, H. (Ekstern), Nielson, H. R. (Intern), Huang, H. (Ekstern), Nielson, F. (Intern)
Number of pages: 8
Pages: 25-32
Publication date: 2012

Host publication information
Title of host publication: 2012 Sixth International Symposium on Theoretical Aspects of Software Engineering (TASE)
Publisher: IEEE
ISBN (Print): 978-1-4673-2353-6
BFI conference series: International Symposium on Theoretical Aspects of Software Engineering (5000148)
Main Research Area: Technical/natural sciences
Conference: 6th International Symposium on Theoretical Aspects of Software Engineering Conference (TASE 2012), Beijing, China, 04/07/2012 - 04/07/2012
Specification and verification, Stochastic model checking, Smart grid
DOIs: 10.1109/TASE.2012.44
Source: dtu
Source-ID: n:oai:DTIC-ART:iel/368070436::26780
Publication: Research - peer-review › Article in proceedings – Annual report year: 2012

Modelling Chinese Smart Grid: A Stochastic Model Checking Case Study

In this document, we consider a specific Chinese Smart Grid implementation and try to address the verification problem for certain quantitative properties including performance and battery consumption. We employ stochastic model checking approach and present our modelling and analysis study using PRISM model checker.

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling, Wuxi SensingNet Industrialization Research Institute, East China Normal University
Authors: Yuksel, E. (Intern), Nielson, H. R. (Intern), Nielson, F. (Intern), Zhu, H. (Ekstern), Huang, H. (Ekstern)
Number of pages: 58
Publication date: 2012

Publication information
Place of publication: Kgs. Lyngby, Denmark
Publisher: Technical University of Denmark, DTU Informatics, Building 321
Original language: English
Number: 2012-02
ISSN: 1601-2321
Recursive Advice for Coordination

Aspect-oriented programming is a programming paradigm that is often praised for the ability to create modular software and separate cross-cutting concerns. Recently aspects have been also considered in the context of coordination languages, offering similar advantages. However, introducing aspects makes analyzing such languages more difficult due to the fact that aspects can be recursive - advice from an aspect must itself be analyzed by aspects - as well as being simultaneously applicable in concurrent threads. Therefore the problem of reachability of various states of a system becomes much more challenging. This is important since ensuring that a system does not contain errors is often equivalent to proving that some states are not reachable. In this paper we show how to solve these challenges by applying a successful technique from the area of software model checking, namely communicating pushdown systems. Even though primarily used for analysis of recursive programs, we are able to adapt them to fit this new context.

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling, Language-Based Technology, Computer Science and Engineering
Authors: Terepeta, M. T. (Intern), Nielson, H. R. (Intern), Nielson, F. (Intern)
Pages: 137-151
Publication date: 2012

Host publication information
Title of host publication: Coordination Models and Languages : 14th International Conference, COORDINATION 2012 Stockholm, Sweden, June 14-15, 2012 Proceedings
Editor: Sirjani, M.
ISBN (Print): 978-3-642-30828-4
ISBN (Electronic): 978-3-642-30829-1

Series: Lecture Notes in Computer Science
Number: 7274
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
Conference: 14th International Conference on Coordination Models and Languages, Stockholm, Sweden, 14/06/2012 - 14/06/2012
DOIs: 10.1007/978-3-642-30829-1_10

Bibliographical note
The research presented in this paper has been supported by MT-LAB, a VKR Centre of Excellence for the Modelling of Information Technology.
Source: dtu
Source-ID: n:oat:DTIC-ART:inspec/366257938::18822
Publication: Research - peer-review » Article in proceedings – Annual report year: 2012
Analysing Protocol Stacks for Services

We show an approach, CaPiTo, to model service-oriented applications using process algebras such that, on the one hand, we can achieve a certain level of abstraction without being overwhelmed by the underlying implementation details and, on the other hand, we respect the concrete industrial standards used for implementing the service-oriented applications. By doing so, we will be able to not only reason about applications at different levels of abstractions, but also to build a bridge between the views of researchers on formal methods and developers in industry. We apply our approach to the financial case study taken from Chapter 0-3. Finally, we develop a static analysis to analyse the security properties as they emerge at the level of concrete industrial protocols.

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling, Language-Based Technology
Authors: Gao, H. (Intern), Nielson, F. (Intern), Nielson, H. R. (Intern)
Number of pages: 736
Pages: 369-389
Publication date: 2011

Host publication information
Title of host publication: Rigorous Software Engineering for Service-Oriented Systems: Results of the SENSORIA Project on Software Engineering for Service-Oriented Computing
Volume: 6582
Publisher: Springer
Editors: Wirsing, M., Hölzl, M.
ISBN (Print): 978-3-642-20400-5
ISBN (Electronic): 978-3-642-20401-2

Series: Lecture Notes in Computer Science
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
Source: orbit
Source-ID: 312440
Publication: Research - peer-review › Book chapter – Annual report year: 2011

CaPiTo: protocol stacks for services
CaPiTo allows the modelling of service-oriented applications using process algebras at three levels of abstraction. The abstract level focuses on the key functionality of the services; the plug-in level shows how to obtain security using standardised protocol stacks; finally, the concrete level allows to consider how security is obtained using asymmetric and symmetric cryptographic primitives. The CaPiTo approach therefore caters for a variety of developers that need to cooperate on designing and implementing service-oriented applications. We show how to formally analyse CaPiTo specifications for ensuring the absence of security flaws. The method used is based on static analysis of the corresponding LySa specifications. We illustrate the development on two industrial case studies; one taken from the banking sector and the other a single sign-on protocol.

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling, Language-Based Technology
Authors: Gao, H. (Intern), Nielson, F. (Intern), Nielson, H. R. (Intern)
**Characteristics of Key Update Strategies for Wireless Sensor Networks**

Wireless sensor networks offer the advantages of simple and low-resource communication. Challenged by this simplicity and low-resources, security is of particular importance in many cases such as transmission of sensitive data or strict requirements of tamper-resistance. Updating the security keys is one of the essential points in security, which restrict the amount of data that may be exposed when a key is compromised. In this paper, we investigate key update methods that may be used in wireless sensor networks, and benefiting from stochastic model checking we derive characteristics of these methods in security perspective.

**General information**

State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling
Authors: Yuksel, E. (Intern), Nielson, H. R. (Intern), Nielson, F. (Intern)
Pages: 132-136
Publication date: 2011

**Host publication information**

Title of host publication: Proceedings of the International Conference on Network Communication and Computer (ICNCC 2011)
Main Research Area: Technical/natural sciences
Conference: International Conference on Network Communication and Computer, New Delhi, India, 01/01/2011
Security, Sensor networks, Verification, Key management
Electronic versions:
EnderICNCC2011-KU_characters.pdf
Links:
http://www.icncc.org/
Source: orbit
Source-ID: 312718
Publication: Research - peer-review › Article in proceedings – Annual report year: 2011

**Combining Static Analysis and Runtime Checking in Security Aspects for Distributed Tuple Spaces**

Enforcing security policies to distributed systems is difficult, in particular, to a system containing untrusted components. We designed AspectKE*, an aspect-oriented programming language based on distributed tuple spaces to tackle this issue. One of the key features in AspectKE* is the program analysis predicates and functions that provide information on future behavior of a program. With a dual value evaluation mechanism that handles results of static analysis and runtime values at the same time, those functions and predicates enable the users to specify security policies in a uniform manner. Our two-staged implementation strategy gathers fundamental static analysis information at load-time, so as to avoid performing all analysis at runtime. We built a compiler for AspectKE*, and successfully implemented security aspects for a distributed chat system and an electronic healthcare record workflow system.

**General information**

State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling, Japan Advanced Institute of Science and Technology, University of Tokyo
Authors: Yang, F. (Intern), Aotani, T. (Ekstern), Masuhara, H. (Ekstern), Nielson, F. (Intern), Nielson, H. R. (Intern)
Pages: 202-218
Publication date: 2011

**Host publication information**

Title of host publication: Coordination Models and Languages : 13th International Conference, COORDINATION 2011, Reykjavik, Iceland, June 6-9, 2011 - Proceedings
Volume: 6721
Publisher: Springer
ISBN (Print): 978-3-642-21463-9

Series: Lecture Notes in Computer Science
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
Conference: 13th International Conference on Coordination Models and Languages, Reykjavik, Iceland, 06/06/2011 - 08/06/2011
DOIs:
10.1007/978-3-642-21464-6_14
Source: orbit
Source-ID: 277825
Controlling Modelling Artifacts

When analysing the performance of a complex system, we typically build abstract models that are small enough to analyse, but still capture the relevant details of the system. But it is difficult to know whether the model accurately describes the real system, or if its behaviour is due to modelling artifacts that were inadvertently introduced. In this paper, we propose a novel methodology to reason about modelling artifacts, given a detailed model and a high-level (more abstract) model of the same system. By a series of automated abstraction steps, we lift the detailed model to the same state space as the high-level model, so that they can be directly compared. There are two key ideas in our approach — a temporal abstraction, where we only look at the state of the system at certain observable points in time, and a spatial abstraction, where we project onto a smaller state space that summarises the possible configurations of the system (for example, by counting the number of components in a certain state). We motivate our methodology with a case study of the LMAC protocol for wireless sensor networks. In particular, we investigate the accuracy of a recently proposed high-level model of LMAC, and identify some modelling artifacts in the model. Since we can apply our abstractions on-the-fly, while exploring the state space of the detailed model, we can analyse larger networks than are possible with existing techniques.

Designing, Capturing and Validating History-Sensitive Security Policies for Distributed Systems

We consider the use of Aspect-oriented techniques as a flexible way to deal with security policies in distributed systems. We follow the approach of attaching security policies to the relevant locations that must be governed by them, and then combining them at runtime according to the interactions that happen. Recent work suggests using Aspects in this way to analyse the future behaviour of programs and to make access control decisions based on this; this gives the flavour of dealing with information flow rather than mere access control. We show in this paper that it is beneficial to augment this approach with history-based components, as is traditional in reference-monitor-based approaches to mandatory access control. Our developments are performed in an Aspect-oriented coordination language, aiming to describe the Bell-LaPadula policy as elegantly as possible. Furthermore, the resulting language has the capability of combining both history-sensitive and future-sensitive policies, providing even more flexibility and power. Moreover, we propose a global Logic for reasoning about the systems designed with this language. We show how the Logic can be used to validate the combination of security policies in a distributed system, either with or without exploring the entire state space.
Galois Connections for Flow Algebras

We generalise Galois connections from complete lattices to flow algebras. Flow algebras are algebraic structures that are less restrictive than idempotent semirings in that they replace distributivity with monotonicity and dispense with the annihilation property; therefore they are closer to the approach taken by Monotone Frameworks and other classical analyses. We present a generic framework for static analysis based on flow algebras and program graphs. Program graphs are often used in Model Checking to model concurrent and distributed systems. The framework allows to induce new flow algebras using Galois connections such that correctness of the analyses is preserved. The approach is illustrated for a mutual exclusion algorithm.

Modal abstractions of concurrent behavior

We present an effective algorithm for the automatic construction of finite modal transition systems as abstractions of potentially infinite concurrent processes. Modal transition systems are recognized as valuable abstractions for model checking because they allow for the validation as well as refutation of safety and liveness properties. However, the
algorithmic construction of finite abstractions from potentially infinite concurrent processes is a missing link that prevents their more widespread usage for model checking of concurrent systems. Our algorithm is a worklist algorithm using concepts from abstract interpretation and operating upon mappings from sets to intervals in order to express simultaneous over- and underapprox-imations of the multisets of process actions available in a particular state. We obtain a finite abstraction that is 3-valued in both states and transitions and that supports the definition of a 3-valued modal logic for validating as well as refuting properties of systems. The construction is illustrated on a few examples, including the Ingemarsson-Tang-Wong key agreement protocol. © 2011 ACM.

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling, Swiss Federal Institute of Technology
Authors: Nielson, F. (Intern), Nanz, S. (Ekstern), Nielson, H. R. (Intern)
Pages: 18
Publication date: 2011
Main Research Area: Technical/natural sciences

Publication information
Journal: A C M Transactions on Computational Logic
Volume: 12
Issue number: 3
ISSN (Print): 1529-3785
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 0.637 SNIP 1.327 CiteScore 1.4
BFI (2015): BFI-level 2
Scopus rating (2015): SJR 0.743 SNIP 2.035 CiteScore 1.61
BFI (2014): BFI-level 2
Scopus rating (2014): SJR 0.756 SNIP 1.699 CiteScore 1.45
BFI (2013): BFI-level 2
Scopus rating (2013): SJR 0.849 SNIP 1.876 CiteScore 1.51
ISI indexed (2013): ISI indexed yes
BFI (2012): BFI-level 2
Scopus rating (2012): SJR 0.884 SNIP 1.839 CiteScore 1.51
ISI indexed (2012): ISI indexed yes
BFI (2011): BFI-level 2
Scopus rating (2011): SJR 0.846 SNIP 1.765 CiteScore 1.44
ISI indexed (2011): ISI indexed yes
Web of Science (2011): Indexed yes
BFI (2010): BFI-level 2
Scopus rating (2010): SJR 1.146 SNIP 2.053
Web of Science (2010): Indexed yes
BFI (2009): BFI-level 2
Scopus rating (2009): SJR 1.283 SNIP 3.376
BFI (2008): BFI-level 2
Scopus rating (2008): SJR 2.139 SNIP 3.048
Scopus rating (2007): SJR 2.226 SNIP 2.777
Scopus rating (2006): SJR 1.251 SNIP 2.12
Scopus rating (2005): SJR 1.072 SNIP 2.852
Scopus rating (2004): SJR 0.833 SNIP 1.776
Original language: English
DOIs:
10.1145/1929954.1929955
Links:
Optimizing Key Updates in Sensor Networks

Sensor networks offer the advantages of simple and low-resource communication. Nevertheless, security is of particular importance in many cases such as when sensitive data is communicated or tamper-resistance is required. Updating the security keys is one of the key points in security, which restrict the amount of data that may be exposed when a key is compromised. In this paper, we propose novel key update methods, and benefiting from stochastic model checking we propose a novel method for determining optimal key update strategies for custom network scenarios. We also present a case study where an application in commercial building automation is considered.

Qualitative and Quantitative Security Analyses for ZigBee Wireless Sensor Networks

Wireless sensor networking is a challenging and emerging technology that will soon become an inevitable part of our modern society. Today wireless sensor networks are broadly used in industrial and civilian application areas including environmental monitoring, surveillance tasks, healthcare applications, home automation, and traffic control. The challenges for research in this area are due to the unique features of wireless sensor devices such as low processing power and associated low energy. On top of this, wireless sensor networks need secure communication as they operate in open fields or unprotected environments and communicate on broadcasting technology. As a result, such systems have to meet a multitude of quantitative constraints (e.g. timing, power consumption, memory usage, communication bandwidth) as well as security requirements (e.g. authenticity, confidentiality, integrity). One of the main challenges arise in dealing with the security needs of such systems where it is less likely that absolute security guarantees can be sustained - because of the need to balance security against energy consumption in wireless sensor network standards like ZigBee.

This dissertation builds on existing methods and techniques in different areas and brings them together to create an efficient verification system. The overall ambition is to provide a wide range of powerful techniques for analyzing models with quantitative and qualitative security information. We stated a new approach that first verifies low level security protocols in a qualitative manner and guarantees absolute security, and then takes these verified protocols as actions of scenarios to be verified in a quantitative manner. Working on the emerging ZigBee wireless sensor networks, we used probabilistic verification that can return probabilistic results with respect to the trade-off between security and performance. Especially in the problem of key update, we believe we have contributed to the solution for not only wireless sensor networks but also many other types of systems that require key updates. Besides we produced automated tools that were intended to demonstrate what kind of tools can developed on different purposes and application domains.
Resilience Analysis of Key Update Strategies for Resource-Constrained Networks

Severe resource limitations in certain types of networks lead to various open issues in security. Since such networks usually operate in unattended or hostile environments, revoking the cryptographic keys and establishing (also distributing) new keys – which we refer to as key update – is a critical security issue. In this paper, we investigate the behaviour of different key update strategies under deviant network conditions. We consider resource-critical networks that employ symmetric cryptography and rely on (shared) network keys. We provide a methodology for quantitative security and performance analysis, and present a case study covering six different key update strategies.

The Logic of XACML

We study the international standard XACML 3.0 for describing security access control policy in a compositional way. Our main contribution is to derive a logic that precisely captures the idea behind the standard and to formally define the semantics of the policy combining algorithms of XACML. To guard against modelling artifacts we provide an alternative way of characterizing the policy combining algorithms and we formally prove the equivalence of these approaches. This allows us to pinpoint the shortcoming of previous approaches to formalization based either on Belnap logic or on D-algebra.
Verification of Stochastic Process Calculi

Stochastic process calculi represent widely accepted formalisms within Computer Science for modelling nondeterministic stochastic systems in a compositional way. Similar to process calculi in general, they are suited for modelling systems in a hierarchical manner, by explicitly specifying subsystems as well as their interdependences and communication channels. Stochastic process calculi incorporate both the quantified uncertainty on probabilities or durations of events and nondeterministic choices between several possible continuations of the system behaviour. Modelling of a system is often performed with the purpose to verify the system. In this dissertation it is argued that the verification techniques that have their origin in the analysis of programming code with the purpose to deduce the properties of the code's execution, i.e. Static Analysis techniques, are transferable to stochastic process calculi. The description of a system in the syntax of a particular stochastic process calculus can be analysed in a compositional way, without expanding the state space by explicitly resolving all the interdependencies between the subsystems which may lead to the state space explosion problem. In support of this claim we have developed analysis methods that belong to a particular type of Static Analysis { Data Flow / Pathway Analysis. These methods have previously been applied to a number of non-stochastic process calculi. In this thesis we are lifting them to the stochastic calculus of Interactive Markov Chains (IMC). We have devised the Pathway Analysis of IMC that is not only correct in the sense of overapproximating all possible behaviour scenarios, as is usual for Static Analysis methods, but is also precise. This gives us the possibility to explicitly decide on the trade-off between precision and complexity while post-processing the analysis results. Another novelty of our methods consists in the kind of properties that we can verify using the results of the Pathway Analysis. We can check both qualitative and quantitative properties of IMC systems. In particular, we have developed algorithms for constructing bisimulation relations, computing (overapproximations of) sets of reachable states and computing the expected time reachability, the last for a linear fragment of IMC. In all the cases we have the complexities of algorithms which are low polynomial in the size of the syntactic description of a system. The presented methods have a clear application in the areas of embedded systems, (randomised) protocols run between a fixed number of parties etc.

A Secure Key Establishment Protocol for ZigBee Wireless Sensor Networks

ZigBee is a wireless sensor network standard that defines network and application layers on top of IEEE 802.15.4's physical and medium access control layers. In the latest version of ZigBee, enhancements are prescribed for the security sublayer but we show in this paper that problems persist. In particular, we show that the end-to-end application key establishment protocol is flawed and we propose a secure protocol instead. We do so by using formal verification techniques based on static program analysis and process algebras. We present a way of using formal methods in wireless network security, and propose a secure key establishment protocol for ZigBee networks.
AspectKE*: Security Aspects with Program Analysis for Distributed Systems

Enforcing security policies to distributed systems is difficult, in particular, when a system contains untrusted components. We designed AspectKE*, a distributed AOP language based on a tuple space, to tackle this issue. In AspectKE*, aspects can enforce access control policies that depend on future behavior of running processes. One of the key language features is the predicates and functions that extract results of static program analysis, which are useful for defining security aspects that have to know about future behavior of a program. AspectKE* also provides a novel variable binding mechanism for pointcuts, so that pointcuts can uniformly specify join points based on both static and dynamic information about the program. Our implementation strategy performs fundamental static analysis at load-time, so as to retain runtime overheads minimal. We implemented a compiler for AspectKE*, and demonstrate usefulness of AspectKE* through a security aspect for a distributed chat system.

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling, University of Tokyo
Authors: Yang, F. (Intern), Masuhara, H. (Ekstern), Aotani, T. (Ekstern), Nielson, F. (Intern), Nielson, H. R. (Intern)
Number of pages: 47
Pages: 27-31
Publication date: 2010

Host publication information
Title of host publication: Proceedings of the 9th Workshop on Aspects, Components, and Patterns for Infrastructure Software (ACP4IS '10)
Publisher: Universitätsverlag Potsdam
Editors: Adams, B., Haupt, M., Lohmann, D.
ISBN (Print): 978-3-86956-043-4
Series: Technische Berichte des Hasso-Plattner-Instituts für Softwaresystemtechnik an der Universität Potsdam
Number: 33
Main Research Area: Technical/natural sciences
Conference: 9th Workshop on Aspects, Components, and Patterns for Infrastructure Software (ACP4IS '10), Rennes, France, 01/01/2010
Aspect Oriented Programming, Program Analysis, Security Policies, Distributed Systems, Tuple Spaces
Electronic versions: tbhpi33_S27_31.pdf
Source: orbit
Source-ID: 259697
Publication: Research - peer-review › Article in proceedings – Annual report year: 2010

AspectKE*: Security Aspects with Program Analysis for Distributed Systems

AspectKE* is the first distributed AOP language based on a tuple space system. It is designed to enforce security policies to applications containing untrusted processes. One of the key features is the high-level predicates that extract results of static program analysis. These predicates provide users an easy way to define aspects by providing information about future behavior of processes, which are shown to be useful to implement security policies such as secrecy and integrity. The users of AspectKE* do not need to write low-level analysis by themselves. In the demonstration, we show basic features of AspectKE* and a case study of building a secure distributed chat application that contains a malicious process.

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling, University of Tokyo
Authors: Yang, F. (Intern), Masuhara, H. (Ekstern), Aotani, T. (Ekstern), Nielson, F. (Intern), Nielson, H. R. (Intern)
Publication date: 2010

Publication information
Original language: English
Place of publication: Demonstration track of the 9th International Conference on Aspect-Oriented Software Development (AOSD'10), Rennes and Saint Malo, France
Main Research Area: Technical/natural sciences
Aspect Oriented Programming, Program Analysis, Distributed Systems, Security Policies, Tuple Spaces
Source: orbit
Source-ID: 259699
Publication: Research › Interactive production – Annual report year: 2010
Aspects with Program Analysis for Security Policies

Enforcing security policies to IT systems, especially for a mobile distributed system, is challenging. As society becomes more IT-savvy, our expectations about security and privacy evolve. This is usually followed by changes in regulation in the form of standards and legislation. In many cases, small modification of the security requirement might lead to substantial changes in a number of modules within a large mobile distributed system. Indeed, security is a crosscutting concern which can spread to many business modules within a system, and is difficult to be integrated in a modular way. This dissertation explores the principles of adding challenging security policies to existing systems with great flexibility and modularity. The policies concerned cover both classical access control and explicit information flow policies. We built our solution by combining aspect-oriented programming techniques with static program analysis techniques. The former technique can separate security concerns out of the main logic, and thus improves system modularity. The latter can analyze the system behavior, and thus helps detect software bugs or potential malicious code. We present AspectKE, an aspect-oriented extension of the process calculus KLAIM that excels at modeling mobile, distributed systems. A novel feature of our approach is that advices are able to analyze the future use of data, which is achieved by using program analysis techniques. We also present AspectK to propose other possible aspect-oriented extensions based on KLAIM, followed by a discussion of open joinpoints that commonly exist in coordination languages such as KLAIM. Based on the idea of AspectKE, we design and implement a proof-of-concept programming language AspectKE*, which enables programmers to easily specify analysis-based security policies with the help of high-level program analysis predicates and functions. The prototype is efficiently realized by a two-stage implementation strategy and a static-dynamic dual value evaluation mechanism. We have performed two case studies to evaluate our programming model and language design. One application is based on a electronic health care workflow system. The other is a distributed chat system. We considered a number of security policies for both primary and secondary use of data, classical access control and predictive access control - control access based on the future behavior of a program. Some of the above mentioned policies can only be enforced by analysis of process continuations.

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling
Authors: Yang, F. (Intern), Nielson, F. (Intern), Nielson, H. R. (Intern)
Publication date: 2010

Publication information
Place of publication: Kgs. Lyngby, Denmark
Publisher: Technical University of Denmark (DTU)
Original language: English
Series: IMM-PHD-2010-239
Main Research Area: Technical/natural sciences
Electronic versions:
phd239_fy.pdf
Source: orbit
Source-ID: 266345
Publication: Research › Ph.D. thesis – Annual report year: 2010

Explicit Versus Symbolic Algorithms for Solving ALFP Constraints

General information
State: E-pub ahead of print
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling
Authors: Filipiuk, P. (Intern), Nielson, H. R. (Intern), Nielson, F. (Intern)
Pages: 15-28
Publication date: 2010

Host publication information
Title of host publication: Electronic Notes in Theoretical Computer Science
Volume: 267
Main Research Area: Technical/natural sciences
DOIs: 10.1016/j.entcs.2010.09.015
Links:
http://www.elsevier.com/locate/entcs
Source: orbit
From Flow Logic to static type systems for coordination languages

Coordination languages are often used to describe open-ended systems. This makes it challenging to develop tools for guaranteeing the security of the coordinated systems and the correctness of their interaction. Successful approaches to this problem have been based on type systems with dynamic checks; therefore, the correctness properties cannot be statically enforced. By contrast, static analysis approaches based on Flow Logic usually guarantee properties statically. In this paper, we show how the insights from the Flow Logic approach can be used to construct a type system for statically ensuring secure access to tuple spaces and safe process migration for an extension of the language KLAIM. (C) 2009 Elsevier B.V. All rights reserved.
High Security at a Low Cost
In the future tiny devices with microcontrollers and sensors will be in charge of numerous activities in our lives. Tracking our energy consumption and CO2 emission, controlling our living conditions, enforcing security, and monitoring our health will be some examples of their functions. These devices will form wireless networks to communicate with one another, moreover their power consumption will be very low. It is not hard to predict that our modern society will depend on the correct operation of these devices, and the security of the network they are operating. Such sensor-based systems, also known as "cyber-physical systems", achieve security by means of cryptographic protocols. In a simplistic setting where the power consumption should be minimum and the processing power is limited, it is more likely that all devices in the network will share the same cryptographic key. In this study, we are working on the trade-off between two challenges: "the cryptographic key should be changed frequently to preserve security" and "the cryptographic key should be changed rarely to save power". We work on the ZigBee wireless sensor network standard, that offers the advantages of simple and low resource communication. We model the system as a continuous-time Markov chain, and analyze it by posing a number of questions shedding light on its behaviour. The properties we are interested in are expressed in continuous stochastic logic, and probabilistic model checker Prism is used in the analysis.

General information
State: E-pub ahead of print
Organisations: Department of Informatics and Mathematical Modeling
Authors: Yuksel, E. (Intern), Nielson, H. R. (Intern), Nielson, F. (Intern)
Publication date: 2010
Main Research Area: Technical/natural sciences
Source: orbit
Source-ID: 263619
Publication: Research - peer-review › Conference article – Annual report year: 2010

Model Checking Is Static Analysis of Modal Logic
Flow Logic is an approach to the static analysis of programs that has been developed for functional, imperative and object-oriented programming languages and for concurrent, distributed, mobile and cryptographic process calculi. In this paper we extend it; to deal with modal logics and prove that it can give an exact characterisation of the semantics of formulae in a modal logic. This shows that model checking can be performed by means of state-of-the-art approaches to static analysis and allow us to conclude that the problems of model checking and static analysis are reducible to each other. In terms of computational complexity we show that model checking by means of static analysis gives the same complexity bounds as are known for traditional approaches to model checking.

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling
Authors: Nielson, F. (Intern), Nielson, H. R. (Intern)
Pages: 191-205
Publication date: 2010
Main Research Area: Technical/natural sciences
Model Checking Multivariate State Rewards

We consider continuous stochastic logics with state rewards that are interpreted over continuous time Markov chains. We show how results from multivariate phase type distributions can be used to obtain higher-order moments for multivariate state rewards (including covariance). We also generalise the treatment of eventuality to unbounded path formulae. For all extensions we show how to obtain closed form definitions that are straightforward to implement and we illustrate our development on a small example.

Optimizing ZigBee Security using Stochastic Model Checking

Probabilistic Aspects: Checking Security in an Imperfect World
Static analysis of topology-dependent broadcast networks

Broadcast semantics poses significant challenges over point-to-point communication when it comes to formal modelling and analysis. Current approaches to analysing broadcast networks have focused on fixed connectivities, but this is unsuitable in the case of wireless networks where the dynamically changing network topology is a crucial ingredient. In this paper, we develop a static analysis that automatically constructs an abstract transition system, labelled by actions and connectivity information, to yield a mobility-preserving finite abstraction of the behaviour of a network expressed in a process calculus with asynchronous local broadcast. Furthermore, we use model checking based on a 3-valued temporal logic to distinguish network behaviour which differs under changing connectivity patterns. (C) 2009 Elsevier Inc. All rights reserved.
A Verifiable Language for Cryptographic Protocols

We develop a formal language for specifying cryptographic protocols in a structured and clear manner, which allows verification of many interesting properties; in particular confidentiality and integrity. The study sheds new light on the problem of creating intuitive and human readable languages, that are analysable with respect to interesting properties. Furthermore it motivates and is an example of, a novel, more general methodology of language design by first verbosely describing the semantics in a mathematical language, e.g. a logic, then restricting the properties of interest to be computable, and finally systematically transforming it into a more intuitive specification language, maintaining this tractability.

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling
Authors: Nielsen, C. R. (Intern), Nielson, F. (Intern), Nielson, H. R. (Intern)
Publication date: May 2009

Publication information
Place of publication: Kgs. Lyngby, Denmark
Publisher: Technical University of Denmark (DTU)
Original language: English
Series: IMM-PHD-2008-210
Main Research Area: Technical/natural sciences
Electronic versions: phd210.pdf
Source: orbit
Source-ID: 229299
Publication: Research › Ph.D. thesis – Annual report year: 2009
A monotone framework for CCS

The calculus of communicating systems, CCS, was introduced by Robin Milner as a calculus for modelling concurrent systems. Subsequently several techniques have been developed for analysing such models in order to get further insight into their dynamic behaviour. In this paper we present a static analysis for approximating the control structure embedded within the models. We formulate the analysis as an instance of a monotone framework and thus draw on techniques that often are associated with the efficient implementation of classical imperative programming languages. We show how to construct a finite automaton that faithfully captures the control structure of a CCS model. Each state in the automaton records a multiset of the enabled actions and appropriate transfer functions are developed for transforming one state into another. A classical worklist algorithm governs the overall construction of the automaton and its termination is ensured using techniques from abstract interpretation.
A Secure Key Establishment Protocol for ZigBee Wireless Sensor Networks

ZigBee is a wireless sensor network standard that defines network and application layers on top of IEEE 802.15.4's physical and medium access control layers. In the latest version of ZigBee, enhancements are prescribed for the security sublayer but we show in this paper that problems persist. In particular we show that the End-to-End Application Key Establishment Protocol is flawed and we propose a secure protocol instead. We do so by using formal verification techniques based on static program analysis and process algebras. We present a way of using formal methods in wireless network security, and propose a secure key establishment protocol for ZigBee networks.

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling
Authors: Yuksel, E. (Intern), Nielson, H. R. (Intern), Nielson, F. (Intern)
Pages: 340-345
Publication date: 2009

Protocol Stacks for Services

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling
Authors: Gao, H. (Intern), Nielson, F. (Intern), Nielson, H. R. (Intern)
Publication date: 2009

Quantitative Security Analysis of ZigBee Key Updates

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling
Analysis of Security Protocols by Annotations

The trend in Information Technology is that distributed systems and networks are becoming increasingly important, as most of the services and opportunities that characterise the modern society are based on these technologies. Communication among agents over networks has therefore acquired a great deal of research interest. In order to provide effective and reliable means of communication, more and more communication protocols are invented, and for most of them, security is a significant goal. It has long been a challenge to determine conclusively whether a given protocol is secure or not. The development of formal techniques, e.g. control flow analyses, that can check various security properties, is an important tool to meet this challenge. The dissertation contributes to the development of such techniques.

In this dissertation, security protocols are modelled in the process calculus LYSA. A variety of interesting security properties that protocols are often expected to have are formalised: authentication, confidentiality, freshness, absence of simple and complex type flaws. Those security properties are explicitly specified as annotations embedded in the LYSA syntax. Finally, a number of automatic techniques for the analysis of system behaviour are developed. These techniques are specified as control flow analyses and are, therefore, guaranteed to terminate. The perspectives for the analysis techniques are discussed. Thus the dissertation marks a step forward both for scientists, who gain a general framework for the study of several interesting security properties, and developers, who get a collection of tools that can validate protocols with respect to various aspects of security.

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling, Language-Based Technology
Authors: Gao, H. (Intern), Nielsen, H. R. (Intern), Nielsen, F. (Intern)
Publication date: May 2008
Advice for Coordination

We show how to extend a coordination language with support for aspect oriented programming. The main challenge is how to properly deal with the trapping of actions before the actual data have been bound to the formal parameters. This necessitates dealing with open joinpoints – which is more demanding than the closed joinpoints in more traditional aspect oriented languages like AspectJ. The usefulness of our approach is demonstrated by mechanisms for discretionary and mandatory access control policies, as usually expressed by reference monitors, as well as mechanisms for logging actions.

From Flow Logic to Static Type Systems in Coordination Languages

Coordination languages are often used to describe open ended systems. This makes it challenging to develop tools for guaranteeing security of the coordinated systems and correctness of their interaction. Successful approaches to this problem have been based on type systems with dynamic checks; therefore, the correctness properties cannot be statically enforced. By contrast, static analysis approaches based on Flow Logic usually guarantee properties statically. In this paper we show how to combine these two approaches to obtain a static type system for describing secure access to tuple spaces and safe process migration for a dialect of the language Klaim.
Iterative Specialisation of Horn Clauses

We present a generic algorithm for solving Horn clauses through iterative specialisation. The algorithm is generic in the sense that it can be instantiated with any decidable fragment of Horn clauses, resulting in a solution scheme for general Horn clauses that guarantees soundness and termination, and furthermore, it presents sufficient criteria for completeness.

We then demonstrate the use of the framework, by creating an instance of it, based on the decidable class $\mathcal{H}_1$, capable of solving a non-trivial protocol analysis problem based on the Yahalom protocol.
Relational Analysis for Delivery of Services

Many techniques exist for statically computing properties of the evolution of processes expressed in process algebras. Static analysis has shown how to obtain useful results that can both be checked and computed in polynomial time. In this paper we develop a static analysis in relational form which substantially improves the precision of the results obtained while being able to deal with the full generality of the syntax of processes. The analysis reveals a feasible complexity for practical examples and gives rise to a fast prototype. We use this prototype to automatically prove the correct delivery of messages for the implementation of an accident service, which is based on multiplexed communication, a crucial feature of global computing applications.
Relational Analysis of Correlation

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling, Language-Based Technology
Authors: Bauer, J. (Intern), Nielson, F. (Intern), Nielson, H. R. (Intern), Pilegaard, H. (Intern)
Pages: 32-46
Publication date: 2008

Host publication information
Title of host publication: Static Analysis : Proceedings of 15th International Symposium, SAS 2008
Publisher: Springer
Editors: Alpuente, M., Vidal, G.

Series: Lecture Notes in Computer Science
Number: 5079
Main Research Area: Technical/natural sciences
Conference: 15th International Static Analysis Symposium , Valencia, Spain, 16/07/2008 - 16/07/2008
Source: orbit
Source-ID: 222468
Publication: Research - peer-review › Article in proceedings – Annual report year: 2008
Static validation of licence conformance policies

Policy conformance is a security property gaining importance due to commercial interest like Digital Rights Management. It is well known that static analysis can be used to validate a number of more classical security policies, such as discretionary and mandatory access control policies, as well as communication protocols using symmetric and asymmetric cryptography. In this work we show how to develop a Flow Logic for validating the conformance of client software with respect to a licence conformance policy. Our approach is sufficiently flexible that it extends to fully open systems that can admit new services on the fly.

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling, Aalborg University
Authors: Hansen, R. R. (Ekstern), Nielson, F. (Intern), Nielson, H. R. (Intern), Probst, C. W. (Intern)
Pages: 1104-1111
Publication date: 2008

Host publication information
Title of host publication: Proceedings of the 3rd International Conference on Availability, Reliability, and Security
Publisher: IEEE Computer Society Press
ISBN (Print): 978-0-7695-3102-1
Main Research Area: Technical/natural sciences
Conference: Third International Conference on Availability, Reliability and Security, 01/01/2008
DOIs:
10.1109/ARES.2008.162
Source: orbit
Source-ID: 229142
Publication: Research - peer-review › Article in proceedings – Annual report year: 2008

ZigBee-2007 Security Essentials

ZigBee is a fairly new but promising standard for wireless networks due to its low resource requirements. As in other wireless network standards, security is an important issue and each new version of the ZigBee Specification enhances the level of the ZigBee security. In this paper, we present the security essentials of the latest ZigBee Specification, ZigBee-2007. We explain the key concepts, protocols, and computations. In addition, we formulate the protocols using standard protocol narrations. Finally, we identify the key challenges to be considered for consolidating ZigBee.

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling
Authors: Yuksel, E. (Intern), Nielson, H. R. (Intern), Nielson, F. (Intern)
Number of pages: 212
Pages: 65-82
Publication date: 2008

Host publication information
Title of host publication: Proceedings of the 13th Nordic Workshop on Secure IT Systems : NordSec 2008
Place of publication: Denmark
Publisher: Technical University of Denmark, DTU Informatics, Building 321
Edition: ISSN 1601-2321
Main Research Area: Technical/natural sciences
Conference: 13th Nordic Workshop on Secure IT Systems, Kongens Lyngby, Denmark, 09/10/2008 - 09/10/2008
Source: orbit
Source-ID: 228698
Publication: Research - peer-review › Article in proceedings – Annual report year: 2008

Language Based Techniques for Systems Biology

Process calculus is the common denominator for a class of compact, idealised, domain-specific formalisms normally associated with the study of reactive concurrent systems within Computer Science. With the rise of the interactioncentred science of Systems Biology a number of bio-inspired process calculi have similarly been used for the study of bio-chemical reactive systems. In this dissertation it is argued that techniques rooted in the theory and practice of programming languages, language based techniques if you will, constitute a strong basis for the investigation of models of biological systems as formalised in a process calculus. In particular it is argued that Static Program Analysis provides a useful approach to the study of qualitative properties of such models. In support of this claim a number of static program analyses are developed for Regev’s BioAmbients – a bio-inspired variant of Cardelli’s Ambient Calculus that incorporates all features of Milner’s π-calculus: The property of spatial reachability, which is related to the function of cellular transport mechanisms, is addressed by two traditional Control Flow Analyses (CFAs). The simpler of the two, a mono-variant
analysis (0CFA), is context insensitive, while the other, a poly-variant analysis (2CFA), is context-sensitive. These analyses compute safe approximations to the set of spatial configurations that are reachable according to a given model. This is useful in the qualitative study of cellular self-organisation and, e.g., the effects of receptor defects or drug delivery mechanisms. The property of sequential realisability, which is closely related to the function of biochemical pathways, is addressed by a variant of traditional Data Flow Analysis (DFA). This so-called 'Pathway Analysis' computes safe approximations to the set of reaction sequences that is realisable according to given model. This is useful in the qualitative study of the metabolic pathways that emerge from a group of connected biochemical agents. Technically, these approaches are complementary, but the analyses overapproximate the set of run-time enabled reactions. This is used in an iterative narrowing scheme that achieves considerable synergy between CFA and DFA, and dramatically improves the results of both. The specified analyses are proved correct with respect to the semantics of Bio-Ambients, and their strength is illustrated by application to abstract models of biological phenomena: One is a model of the LDL degradation pathway, where it is shown that the analyses are able to pinpoint the effects of certain genetic defects that are known to be associated to cardiovascular disease. The other is a model of genetic transcription that relies only on the π calculus fragment of BioAmbients. In both cases the analyses compute very precise estimates of the temporal structure of the underlying pathways; hence they are applicable across a family of widely used bio-ware languages that descend from Milner’s Calculus of Communicating Systems. The presented set of analyses constitutes a nice toolbox for the analysis of biological models. The individual tools range in complexity from low polynomial to exponential, while the precision scales similarly. Thus, the toolbox may provide useful information at all stages of a models lifetime, including development, where one is interested in frequent quick estimates, verification, and prediction, where one is willing to wait longer for more precise estimates.

**General information**

State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling, Language-Based Technology
Authors: Pilegaard, H. (Intern), Nielson, F. (Intern), Nielson, H. R. (Intern)
Publication date: Dec 2007

**Publication information**

Place of publication: Kgs. Lyngby
Publisher: Technical University of Denmark, DTU Informatics, Building 321
Original language: English
Series: IMM-PHD-2008-184
Main Research Area: Technical/natural sciences
Electronic versions:
phd184_hepi-update.pdf
Source: orbit
Source-ID: 210319
Publication: Research › Ph.D. thesis – Annual report year: 2007

**Language-based Security for VHDL**

**General information**

State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling, Language-Based Technology
Authors: Tolstrup, T. K. (Intern), Nielson, H. R. (Intern), Nielson, F. (Intern)
Publication date: Apr 2007

**Publication information**

Original language: English
Series: IMM-PHD
Number: 174
Main Research Area: Technical/natural sciences
Electronic versions:
phd174_tkt.pdf
Source: orbit
Source-ID: 200866
Publication: Research › Ph.D. thesis – Annual report year: 2007

**Active Evaluation Contexts for Reaction Semantics**

**General information**
A Flow-Sensitive Analysis of Privacy Properties
In this paper we consider service oriented architectures where many components interact with one another using a wireless network. We are interested in questions like: ldr Can I be sure that I do not get unsolicited information from some service? - unless I give my permission? ldr Can I be sure that information I send to some service never is leaked to another service? - unless I give my permission? We shall develop a static program analysis for the pi- calculus and show how it can be used to give privacy guarantees like the ones requested above. The analysis records the explicit information flow of the system and keeps track of, not only the potential configurations of the system, but also the order in which they may be encountered.

A formal analysis for capturing replay attacks in cryptographic protocols

Copyright: 2007 IEEE. Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the IEEE

Copyright: 2007 IEEE. Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the IEEE

Copyright: 2007 IEEE. Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the IEEE
Analyzing the Control Structure of PEPA

The Performance Evaluation Process Algebra, PEPA, is introduced by Jane Hillston as a stochastic process algebra for modelling distributed systems and especially suitable for performance evaluation. We present a static analysis that very precisely approximates the control structure of processes expressed in PEPA. The analysis technique we adopted is Data Flow Analysis. We begin the analysis by defining an appropriate transfer function, then with the classical worklist algorithm we construct a finite automaton that captures all possible interactions among processes. By annotating labels and layers to PEPA programs, the approximating result is very precise. Based on the analysis, we also develop algorithms for validating the deadlock property of PEPA programs. The techniques have been implemented in a tool which is able to analyze processes with a control structure that more than one thousand states.

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling, Computer Science and Engineering, Language-Based Technology
Authors: Yang, F. (Intern), Nielsen, H. R. (Intern)
Publication date: 2007
Event: Poster session presented at The 14th International Static Analysis Symposium (SAS 2007), Lyngby, Denmark.
Main Research Area: Technical/natural sciences
PEPA, Data Flow Analysis, Control Structure, Finite Automaton, Deadlock, Static Analysis, Stochastic Process Algebra
Source: orbit
Source-ID: 259698
Publication: Research - peer-review › Poster – Annual report year: 2007

A Secure Simplification of the PKMv2 Protocol in IEEE 802.16e-2005

Static analysis is successfully used for automatically validating security properties of classical cryptographic protocols. In this paper, we shall employ the same technique to a modern security protocol for wireless networks, namely the latest version of the Privacy and Key Management protocol for IEEE 802.16e, PKMv2. This protocol seems to have an exaggerated mixture of security features. Thus, we iteratively investigate which components are necessary for upholding the security properties and which can be omitted safely. This approach is based on the LySa process calculus and employs the corresponding automated analysis tool, the LySaTool.

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling, Istanbul Technical University
Authors: Yuksel, E. (Intern), Nielsen, H. R. (Intern), Nielsen, C. R. (Intern), Orencik, M. B. (Ekstern)
Pages: 149-164
Publication date: 2007

Host publication information
Title of host publication: Proceedings of Joint Workshop on Foundations of Computer Security and Automated Reasoning for Security Protocol Analysis
Editors: Degano, P., Kusters, R., Vigano, L., Zdancewic, S.
Main Research Area: Technical/natural sciences
Source: orbit
Source-ID: 205421
Publication: Research - peer-review › Article in proceedings – Annual report year: 2007

Control Flow Analysis for BioAmbients

This paper presents a static analysis for investigating properties of biological systems specified in BioAmbients. We exploit the control flow analysis to decode the bindings of variables induced by communications and to build a relation of the ambients that can interact with each other. We eventually apply our analysis to an example of gene regulation by positive feedback taken from the literature.
Cryptographic Pattern Matching

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling
Authors: Nielsen, C. R. (Intern), Nielson, F. (Intern), Nielson, H. R. (Intern)
Pages: 91-107
Publication date: 2007
Main Research Area: Technical/natural sciences

Publication information
Journal: Electronic Notes in Theoretical Computer Science
Volume: 168
ISSN (Print): 1571-0661
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 0.256 SNIP 0.609 CiteScore 0.66
Web of Science (2016): Indexed yes
BFI (2015): BFI-level 1
Scopus rating (2015): SJR 0.373 SNIP 0.781 CiteScore 0.67
BFI (2014): BFI-level 1
Scopus rating (2014): SJR 0.382 SNIP 0.771 CiteScore 0.6
BFI (2013): BFI-level 1
Scopus rating (2013): SJR 0.323 SNIP 0.72 CiteScore 0.55
ISI indexed (2013): ISI indexed no
BFI (2012): BFI-level 1
Scopus rating (2012): SJR 0.386 SNIP 0.608 CiteScore 0.55
ISI indexed (2012): ISI indexed no
BFI (2011): BFI-level 1
Scopus rating (2011): SJR 0.325 SNIP 0.582 CiteScore 0.57
ISI indexed (2011): ISI indexed no
BFI (2010): BFI-level 1
Scopus rating (2010): SJR 0.408 SNIP 0.567
BFI (2009): BFI-level 1
Scopus rating (2009): SJR 0.419 SNIP 0.689
BFI (2008): BFI-level 1
Scopus rating (2008): SJR 0.407 SNIP 0.619
Scopus rating (2007): SJR 0.419 SNIP 0.611
Scopus rating (2006): SJR 0.377 SNIP 0.649
Scopus rating (2005): SJR 0.373 SNIP 0.633
Scopus rating (2004): SJR 0.406 SNIP 0.713
Scopus rating (2003): SJR 0.343 SNIP 0.56
Scopus rating (2002): SJR 0.464 SNIP 0.661
Scopus rating (2001): SJR 0.435 SNIP 0.679
Scopus rating (2000): SJR 0.348 SNIP 0.556
Scopus rating (1999): SJR 0.365 SNIP 0.683
Original language: English
Source: orbit
Source-ID: 231118
Publication: Research - peer-review › Conference article – Annual report year: 2007
Data Flow Analysis for {CCS}

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielsen, H. R. (Intern), Nielsen, F. (Intern)
Pages: 311-327
Publication date: 2007

Host publication information
Title of host publication: Lecture Notes in Computer Science
Volume: 4444
Publisher: Springer
Main Research Area: Technical/natural sciences

Heuristics for Safety and Security Constraints

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielsen, F. (Intern), Nielsen, H. R. (Intern)
Pages: 523-543
Publication date: 2007
Main Research Area: Technical/natural sciences

Publication information
Journal: Electronic Notes in Theoretical Computer Science
Volume: 172
ISSN (Print): 1571-0661
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 0.256 SNIP 0.609 CiteScore 0.66
Web of Science (2016): Indexed yes
BFI (2015): BFI-level 1
Scopus rating (2015): SJR 0.373 SNIP 0.781 CiteScore 0.67
BFI (2014): BFI-level 1
Scopus rating (2014): SJR 0.382 SNIP 0.771 CiteScore 0.6
BFI (2013): BFI-level 1
Scopus rating (2013): SJR 0.323 SNIP 0.72 CiteScore 0.55
ISI indexed (2013): ISI indexed no
BFI (2012): BFI-level 1
Scopus rating (2012): SJR 0.386 SNIP 0.608 CiteScore 0.55
ISI indexed (2012): ISI indexed no
BFI (2011): BFI-level 1
Scopus rating (2011): SJR 0.325 SNIP 0.582 CiteScore 0.57
ISI indexed (2011): ISI indexed no
BFI (2010): BFI-level 1
Scopus rating (2010): SJR 0.408 SNIP 0.567
BFI (2009): BFI-level 1
Scopus rating (2009): SJR 0.419 SNIP 0.689
BFI (2008): BFI-level 1
Scopus rating (2008): SJR 0.407 SNIP 0.619
Scopus rating (2007): SJR 0.419 SNIP 0.611
Scopus rating (2006): SJR 0.377 SNIP 0.649
Scopus rating (2005): SJR 0.373 SNIP 0.633
Scopus rating (2004): SJR 0.406 SNIP 0.713
Scopus rating (2003): SJR 0.343 SNIP 0.56
Scopus rating (2002): SJR 0.464 SNIP 0.661
Scopus rating (2001): SJR 0.435 SNIP 0.679
Scopus rating (2000): SJR 0.348 SNIP 0.556
Scopus rating (1999): SJR 0.365 SNIP 0.683

Original language: English
DOIs:
10.1016/j.entcs.2007.02.018

Links:
http://www2.imm.dtu.dk/pubdb/views/publication_details.php?id=5530
Source: orbit
Source-ID: 205554
Publication: Research - peer-review › Journal article – Annual report year: 2007

Semantics with Applications: An Appetizer

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielson, H. R. (Intern), Nielson, F. (Intern)
Publication date: 2007

Publication information
Publisher: Springer
Original language: English
Series: Undergraduate Topics in Computer Science
Main Research Area: Technical/natural sciences
Links:
http://www2.imm.dtu.dk/pubdb/views/publication_details.php?id=5526
Source: orbit
Source-ID: 205570
Publication: Research - peer-review › Book – Annual report year: 2007

Static Analysis: 14th International Symposium, SAS 2007, Kgs. Lyngby, Denmark, August 22-24, proceedings

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling
Authors: Nielson, H. R. (ed.) (Intern), Filé, G. (ed.) (Ekstern)
Publication date: 2007

Publication information
Publisher: Springer
Original language: English
Series: Lecture Notes in Computer Science
Number: 4634
Main Research Area: Technical/natural sciences
Links:
http://www2.imm.dtu.dk/pubdb/views/publication_details.php?id=5544
Source: orbit
Source-ID: 205571
Publication: Research - peer-review › Book – Annual report year: 2007
What is a free name in a process algebra?

State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielson, F. (Intern), Nielson, H. R. (Intern), Pilegaard, H. (Intern)
Pages: 188-194
Publication date: 2007

Main Research Area: Technical/natural sciences
Publication information
Journal: Information Processing Letters
Volume: 103
Issue number: 5
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
Analysis of LYSA-calculus with explicit confidentiality annotations

Recently there has been an increased research interest in applying process calculi in the verification of cryptographic protocols due to their ability to formally model protocols. This work presents LYSA with explicit confidentiality annotations for indicating the expected behavior of target protocols. A static analysis approach is developed for analyzing protocols specified in the extended LYSA. The proposed approach will over-approximate the possible executions of protocols while keeping track of all messages communicated over the network, and furthermore it will capture the potential malicious activities performed by attackers as specified by the confidentiality annotations. The proposed analysis approach is fully automatic without the need of human intervention and has been applied successfully to a number of protocols.
Analyzing security protocols in hierarchical networks
Validating security protocols is a well-known hard problem even in a simple setting of a single global network. But a real network often consists of, besides the public-accessed part, several sub-networks and thereby forms a hierarchical structure. In this paper, we first present a process calculus capturing the characteristics of hierarchical networks and describe the behavior of protocols on such networks. We then develop a static analysis to automate the validation. Finally, we demonstrate how the technique can benefit the protocol development and the design of network systems by presenting a series of experiments we have conducted.

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Zhang, Y. (Intern), Nielson, H. R. (Intern)
Publication date: 2006

Host publication information
Title of host publication: Automated Technology For Verification and Analysis, Proceedings
Place of publication: Berlin
Publisher: Springer-verlag Berlin

Series: Lecture Notes in Computer Science
Number: 4218
Main Research Area: Technical/natural sciences
Source: orbit
Source-ID: 198117
Publication: Research - peer-review › Book chapter – Annual report year: 2006

Context Dependent Analysis of BioAmbients

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling, Computer Science and Engineering
Authors: Pilegaard, H. (Intern), Nielson, F. (Intern), Nielson, H. R. (Intern)
Publication date: 2006

Host publication information
Title of host publication: Emerging Aspects of Abstract Interpretation 2006
Main Research Area: Technical/natural sciences
Links:
http://www2.imm.dtu.dk/pubdb/p.php?4809
Source: orbit
Source-ID: 191561
Publication: Research - peer-review › Article in proceedings – Annual report year: 2006

Enhancing Creativity by Test Diversity

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling, Computer Science and Engineering
Authors: Probst, C. (Intern), Nielson, H. R. (Intern), Nielson, F. (Intern)
Publication date: 2006

Host publication information
Title of host publication: 6th International Workshop on Active Learning in Engineering Education
Main Research Area: Technical/natural sciences
Electronic versions:
imm4741.pdf
Links:
http://www2.imm.dtu.dk/pubdb/p.php?4741
Source: orbit
Source-ID: 191567
Publication: Research - peer-review › Article in proceedings – Annual report year: 2006
Static analysis for blinding

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielsen, C. (Ekstern), Nielson, H. R. (Intern)
Pages: 100-118
Publication date: 2006
Main Research Area: Technical/natural sciences

Publication information
Journal: Nordic Journal of Computing
Volume: 13
Issue number: 1-2
ISSN (Print): 1236-6064
Ratings:
BFI (2016): BFI-level 1
BFI (2015): BFI-level 1
BFI (2014): BFI-level 1
BFI (2013): BFI-level 1
ISI indexed (2013): ISI indexed no
BFI (2012): BFI-level 1
ISI indexed (2012): ISI indexed no
BFI (2011): BFI-level 1
ISI indexed (2011): ISI indexed no
BFI (2010): BFI-level 1
BFI (2009): BFI-level 1
BFI (2008): BFI-level 1
Original language: English
Source: orbit
Source-ID: 194892
Publication: Research - peer-review › Journal article – Annual report year: 2006

Static analysis for blinding
The classical key distribution protocols are based on symmetric and asymmetric encryption as well as digital signatures. Protocols with different purposes often require different cryptographic primitives, an example is electronic voting protocols which are often based on the cryptographic operation blinding. In this paper we study the theoretical foundations for one of the successful approaches to validating cryptographic protocols and we extend it to handle the blinding primitive. Our static analysis approach is based on Flow Logic; this gives us a clean separation between the specification of the analysis and its realization in an automatic tool. We concentrate on the former in the present paper and provide the semantic foundation for our analysis of protocols using blinding - also in the presence of malicious attackers.

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling
Authors: Nielsen, C. R. (Intern), Nielson, H. R. (Intern)
Pages: 98 - 116
Publication date: 2006
Main Research Area: Technical/natural sciences

Publication information
Journal: Nordic Journal of Computing
Volume: 13
Issue number: 1
ISSN (Print): 1236-6064
Ratings:
BFI (2016): BFI-level 1
BFI (2015): BFI-level 1
BFI (2014): BFI-level 1
BFI (2013): BFI-level 1
Heuristics for Enforcing Security Constraints

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielson, F. (Intern), Nielson, H. R. (Intern)
Publication date: 2005

Host publication information
Title of host publication: CPSec Barcelona
Main Research Area: Technical/natural sciences

Information Flow Analysis for VHDL

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling, Computer Science and Engineering
Authors: Tolstrup, T. K. (Intern), Nielson, F. (Intern), Nielson, H. R. (Intern)
Publication date: 2005

Host publication information
Title of host publication: Parallel Computing Technologies
Publisher: Springer
Main Research Area: Technical/natural sciences

On evaluating the performance of security protocols

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling, Computer Science and Engineering
Pages: 1-5
Performance Evaluation of Security Protocols

We use a special operational semantics which drives us in inferring quantitative measures on systems describing cryptographic protocols. We assign rates to transitions by only looking at these labels. The rates reflect the distributed architecture running applications and the use of possibly different cryptosystems. We then map transition systems to Markov chains and evaluate performance of systems, using standard tools.

Performance Evaluation of Security Protocols Specified in LySa

We use a special operational semantics which drives us in inferring quantitative measures on systems describing cryptographic protocols. The transitions of the system carry enhanced labels. We assign rates to transitions by only looking at these labels. The rates reflect the distributed architecture running applications and the use of possibly different cryptosystems. We then map transition systems to Markov chains and evaluate performance of systems, using standard tools.
Static analysis of a Model of the LDL degradation pathway

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling, Computer Science and Engineering
Authors: Pilegaard, H. (Intern), Nielson, F. (Intern), Nielson, H. R. (Intern)
Publication date: 2005

Host publication information
Title of host publication: Third International Workshop on Computational Methods in Systems Biology (CMSB'05)
Publisher: University of Edinburgh
Main Research Area: Technical/natural sciences
Links:
http://www2.imm.dtu.dk/pubdb/p.php?4193
Source: orbit
Source-ID: 185589
Publication: Research - peer-review › Journal article – Annual report year: 2005

Static Validation of a Voting Protocol

General information
State: Published
Static Validation of Security Protocols

We methodically expand protocol narrations into terms of a process algebra in order to specify some of the checks that need to be made in a protocol. We then apply static analysis technology to develop an automatic validation procedure for protocols. Finally, we demonstrate that these techniques suffice to identify several authentication flaws in symmetric and asymmetric key protocols such as Needham-Schroeder symmetric key, Otway-Rees, Yahalom, Andrew secure RPC, Needham-Schroeder asymmetric key, and Beller-Chang-Yacobi MSR.

General information

State: Published
Organisations: Department of Informatics and Mathematical Modeling, Computer Science and Engineering
Authors: Bodei, C. (Ekstern), Buchholtz, M. (Intern), Degano, P. (Ekstern), Nielson, H. R. (Intern), Nielsen, F. (Intern)
Pages: 347-390
Publication date: 2005
Main Research Area: Technical/natural sciences

Publication information

Journal: Journal of Computer Security
Volume: 13
Issue number: 3
ISSN (Print): 0925-227X
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
A Calculus for Control Flow Analysis of Security Protocols

The design of a process calculus for analysing security protocols is governed by three factors: how to express the security protocol in a precise and faithful manner, how to accommodate the variety of attack scenarios, and how to utilise the strengths (and limit the weaknesses) of the underlying analysis methodology. We pursue an analysis methodology based on control flow analysis in flow logic style and we have previously shown its ability to analyse a variety of security protocols. This paper develops a calculus, LysaNS that allows for much greater control and clarity in the description of attack scenarios, that gives a more flexible format for expressing protocols, and that at the same time allows to circumvent

Static Validation of Voting Protocols

Using static analysis to validate the SAML Single Sign-on Protocol
Automated Analysis of Security in Networking Systems

It has for a long time been a challenge to built secure networking systems. One way to counter this problem is to provide developers of software applications for networking systems with easy-to-use tools that can check security properties before the applications ever reach the marked. These tools will both help raise the general level of awareness of the
problems and prevent the most basic flaws from occurring. This thesis contributes to the development of such tools. Networking systems typically try to attain secure communication by applying standard cryptographic techniques. In this thesis such networking systems are modelled in the process calculus LySa. On top of this programming language based formalism an analysis is developed, which relies on techniques from data and control ow analysis. These are techniques that can be fully automated, which make them an ideal basis for tools targeted at non-experts users. The feasibility of the techniques is illustrated by a proof-of-concept implementation of a control ow analysis developed for LySa. From a technical point of view, this implementation also interesting because it encodes in nite sets of algebraic terms, which denote encryption, as a nite number of tree grammar rules. The security of any software application relies crucially on the scenario in which the application is deployed. In contrast to many related analysis approaches, this thesis provides an explicit mechanism for specifying deployment scenarios. Even though these scenarios may be arbitrarily large the analysis techniques can be extended to cope with such scenarios. The analysis techniques are furthermore capable of tackling security issues that arise because of attacks from arbitrary attackers: the analysis can deal with confidentiality and authentication properties, parallel session attacks, and attacks launched by insiders. Finally, the perspectives for the application of the analysis techniques are discussed, thereby, coming a small step closer to providing developers with easy-to-use tools for validating the security of networking applications.

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling, Language-Based Technology
Authors: Buchholtz, M. (Intern), Nielson, H. R. (Intern), Nielson, F. (Intern)
Publication date: 2004

Control Flow Analysis Can Find New Flaws Too
A previous study showed how control flow analysis can be applied to analyse key distribution protocols based on symmetric key cryptography. We have extended both the theoretical treatment and our fully automatic verifier to deal with protocols based on asymmetric cryptography. This paper reports on the application of our technique - exemplified on the Beller-Chang-Yacobi MSR protocol, which uses both symmetric and asymmetric cryptography - and show how we discover an undocumented flaw.

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling, Computer Science and Engineering
Authors: Bodei, C. (Ekstern), Buchholtz, M. (Intern), Degano, P. (Ekstern), Nielson, F. (Intern), Nielson, H. R. (Intern)
Publication date: 2004

Cryptographic Analysis in Cubic Time
The spi-calculus is a variant of the polyadic pi-calculus that admits symmetric cryptography and that admits expressing communication protocols in a precise though still abstract way. This paper shows that context-independent control flow analysis can be calculated in cubic time despite the fact that the spi-calculus operates over an infinite universe of values. Our approach is based on Horn Clauses with Sharing and we develop transformations to pass from the infinite to the finite
and to deal with the polyadic nature of input and output. We prove that this suffices for obtaining a cubic time implementation without sacrificing precision and without making simplifying assumptions on the nature of keys.

**General information**

State: Published

Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling

Authors: Nielson, F. (Intern), Nielson, H. R. (Intern), Seidl, H. (Ekstern)

Pages: 1

Publication date: 2004

Main Research Area: Technical/natural sciences

**Publication information**

Journal: Electronic Notes in Theoretical Computer Science

Volume: 62

Issue number: 17

ISSN (Print): 1571-0661

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 0.256 SNIP 0.609 CiteScore 0.66

Web of Science (2016): Indexed yes

BFI (2015): BFI-level 1

Scopus rating (2015): SJR 0.373 SNIP 0.781 CiteScore 0.67

BFI (2014): BFI-level 1

Scopus rating (2014): SJR 0.382 SNIP 0.771 CiteScore 0.6

BFI (2013): BFI-level 1

Scopus rating (2013): SJR 0.323 SNIP 0.72 CiteScore 0.55

ISI indexed (2013): ISI indexed no

BFI (2012): BFI-level 1

Scopus rating (2012): SJR 0.386 SNIP 0.608 CiteScore 0.55

ISI indexed (2012): ISI indexed no

BFI (2011): BFI-level 1

Scopus rating (2011): SJR 0.325 SNIP 0.582 CiteScore 0.57

ISI indexed (2011): ISI indexed no

BFI (2010): BFI-level 1

Scopus rating (2010): SJR 0.408 SNIP 0.567

BFI (2009): BFI-level 1

Scopus rating (2009): SJR 0.419 SNIP 0.689

BFI (2008): BFI-level 1

Scopus rating (2008): SJR 0.407 SNIP 0.619

Scopus rating (2007): SJR 0.419 SNIP 0.611

Scopus rating (2006): SJR 0.377 SNIP 0.649

Scopus rating (2005): SJR 0.373 SNIP 0.633

Scopus rating (2004): SJR 0.406 SNIP 0.713

Scopus rating (2003): SJR 0.343 SNIP 0.56

Scopus rating (2002): SJR 0.464 SNIP 0.661

Scopus rating (2001): SJR 0.435 SNIP 0.679

Scopus rating (2000): SJR 0.348 SNIP 0.556

Scopus rating (1999): SJR 0.365 SNIP 0.683

Original language: English

DOIs:

10.1016/S1571-0661(04)00316-0

Source: orbit

Source-ID: 58113

Publication: Research - peer-review › Journal article – Annual report year: 2004
Security for Mobility
We show how to use static analysis to provide information about security issues related to mobility. First the syntax and semantics of Mobile Ambients is reviewed and we show how to obtain a so-called 0CFA analysis that can be implemented in polynomial time. Next we consider discretionary access control where we devise Discretionary Ambients, based on Safe Ambients, and we adapt the semantics and 0CFA analysis; to strengthen the analysis we incorporate context-sensitivity to obtain a 1CFA analysis. This paves the way for dealing with mandatory access control where we express both a Bell-LaPadula model for confidentiality as well as a Biba model for integrity. Finally, we use Boxed Ambients as a means for expressing cryptographic key exchange protocols and we adapt the operational semantics and the 0CFA analysis.

Spatial Analysis of BioAmbients
Programming language technology can contribute to the development and understanding of Systems Biology by providing formal calculi for specifying and analysing the dynamic behaviour of biological systems. Our focus is on BioAmbients, a variation of the ambient calculi developed for modelling mobility in computer systems. We present a static analysis for capturing the spatial structure of biological systems and we illustrate it on a few examples.

Static Analysis for Systems Biology
This paper shows how static analysis techniques can help understanding biological systems. Based on a simple example we illustrate the outcome of performing three different analyses extracting information of increasing precision. We conclude by reporting on the potential impact and exploitation of these techniques in systems biology.
The Succinct Solver Suite

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Pages: 251-265
Publication date: 2004

Host publication information
Title of host publication: Proc. of workshop on Systeomatics - dynamic biological systems informatics
Publisher: Computer Science Press, Trinity College Dublin
Main Research Area: Technical/natural sciences
Electronic versions: imm3188.pdf
Source: orbit
Source-ID: 154650
Publication: Research - peer-review › Article in proceedings – Annual report year: 2004

Abstract Interpretation of Mobile Ambients

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielson, F. (Intern), Hansen, R. R. (Intern), Nielson, H. R. (Intern)
Pages: 145-175
Publication date: 2003
Main Research Area: Technical/natural sciences

Publication information
Journal: Science of Computer Programming
Volume: 47
Issue number: 2-3
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
Automatic Validation of Protocol Narration

We perform a systematic expansion of protocol narrations into terms of a process algebra in order to make precise some of the detailed checks that need to be made in a protocol. We then apply static analysis technology to develop an automatic validation procedure for protocols. Finally, we demonstrate that these techniques suffice for identifying a number of authentication flaws in symmetric key protocols such as Needham-Schroeder, Otway-Rees, Yahalom and Andrew Secure RPC.

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling, Computer Science and Engineering
Authors: Bodei, C. (Ekstern), Buchholtz, M. (Intern), Degano, P. (Ekstern), Nielson, F. (Intern), Nielson, H. R. (Intern)
Pages: 126-140
Publication date: 2003
Observation Predicates in Flow Logic
Motivated by the connection between strong and soft type systems we explore flow analyses with hard constraints on the admissible solutions. We show how to use observation predicates and formula rearrangements to map flow analyses with hard constraints into more traditional flow analyses in such a way that the hard constraints are satisfied exactly when the observation predicates report no violations. The development is carried out in a large fragment of a first order logic with negation and also takes care of the transformations necessary in order to adhere to the stratification restrictions inherent in Alternation-free Least Fixed Point Logic and similar formalisms such as Datalog.

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielsen, F. (Intern), Nielsen, H. R. (Intern), Sun, H. (Ekstern)
Publication date: 2003

Publication information
Original language: English
Main Research Area: Technical/natural sciences
Electronic versions: imm2812.pdf
Links:
Source: orbit
Source-ID: 58713
Publication: Research › Report – Annual report year: 2003

A Succinct Solver for ALFP

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielsen, F. (Intern), Nielsen, H. R. (Intern), Seidl, H. (Ekstern)
Pages: 335-372
Publication date: 2002
Main Research Area: Technical/natural sciences

Publication information
Journal: Nordic Journal of Computing
Volume: 9
ISSN (Print): 1236-6064
Ratings:
BFI (2016): BFI-level 1
BFI (2015): BFI-level 1
BFI (2014): BFI-level 1
BFI (2013): BFI-level 1
ISI indexed (2013): ISI indexed no
BFI (2012): BFI-level 1
ISI indexed (2012): ISI indexed no
BFI (2011): BFI-level 1
ISI indexed (2011): ISI indexed no
BFI (2010): BFI-level 1
BFI (2009): BFI-level 1
BFI (2008): BFI-level 1
Original language: English
Source: orbit
Source-ID: 58114
Publication: Research - peer-review › Journal article – Annual report year: 2002

Automatic Complexity Analysis

General information
Host publication information
Title of host publication: Proc. ESOP'02
Publisher: Springer Verlag
Main Research Area: Technical/natural sciences
Links:
Source: orbit
Source-ID: 58205
Publication: Research - peer-review › Article in proceedings – Annual report year: 2002

Data Structures in the Succinct Solver (V1.0)
General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling, Computer Science and Engineering
Authors: Sun, H. Y. (Intern), Nielson, H. R. (Intern), Nielson, F. (Intern)
Publication date: 2002

Publication information
Original language: English
Main Research Area: Technical/natural sciences
Links:
Source: orbit
Source-ID: 58399
Publication: Research › Report – Annual report year: 2002

Experiments with Succinct Solvers
General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling, Computer Science and Engineering
Authors: Buchholtz, M. (Intern), Nielson, H. R. (Intern), Nielson, F. (Intern)
Publication date: 2002

Publication information
Original language: English
Main Research Area: Technical/natural sciences
Electronic versions:
imm919.pdf
Links:
Source: orbit
Source-ID: 58374
Publication: Research - peer-review › Report – Annual report year: 2002

Flow Logic for Dolev-Yao Secrecy in Cryptographic Processes
General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Bodei, C. (Ekstern), Degano, P. (Ekstern), Nielson, H. R. (Intern), Nielson, F. (Intern)
Pages: 747-756
Publication date: 2002
Main Research Area: Technical/natural sciences

Publication information
Flow Logics: a multi-paradigmatic approach to static analysis

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielson, H. R. (Intern), Nielson, F. (Intern)
Pages: 223-244
Publication date: 2002
Security for Mobility

We show how to use static analysis to provide information about security issues related to mobility. First the syntax and semantics of Mobile Ambients is reviewed and we show how to obtain a so-called 0CFA analysis that can be implemented in polynomial time. Next we consider discretionary access control where we devise Discretionary Ambients, based on Safe Ambients, and we adapt the semantics and 0CFA analysis; to strengthen the analysis we incorporate context-sensitivity to obtain a 1CFA analysis. This paves the way for dealing with mandatory access control where we express both a Bell-LaPadula model for confidentiality as well as a Biba model for integrity. Finally, we use Boxed Ambients as a means for expressing cryptographic key exchange protocols and we adapt the operational semantics and the 0CFA analysis.

Validating Firewalls using Flow Logics

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielson, H. R. (Intern), Nielson, F. (Intern), Buchholtz, M. (Intern)
Publication date: 2002

Publication information
Original language: English
Main Research Area: Technical/natural sciences
Electronic versions:
imm1254.pdf
imm1254.ps
Links:
Source: orbit
Source-ID: 58394
Publication: Research › Report – Annual report year: 2002
Kleene's Logic with Equality

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielson, F. (Intern), Nielson, H. R. (Intern), Sagiv, M. (Ekstern)
Pages: 131-137
Publication date: 2001
Main Research Area: Technical/natural sciences

Publication information
Journal: Information Processing Letters
Volume: 80
Issue number: 3
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
Shape analysis for mobile ambients
The ambient calculus is a calculus of computation that allows active processes to move between sites. We present an analysis inspired by state-of-the-art pointer analyses that safely and accurately predicts which processes may turn up at what sites during the execution of a composite system. The analysis models sets of processes by sets of regular tree grammars enhanced with context dependent counts, and it obtains its precision by combining a powerful redex materialisation with a strong redex reduction (in the manner of the strong updates performed in pointer analyses).
Static analysis for secrecy and non-interference in networks of processes

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Bodei, C. (Ekstern), Degano, P. (Ecstern), Nielson, H. R. (Intern), Nielson, F. (Intern)
Pages: 27-41
Publication date: 2001
Host publication information
Title of host publication: Proc. PACT’01
Publisher: Springer
Main Research Area: Technical/natural sciences
Links:
Source: orbit
Source-ID: 57827
Publication: Research - peer-review › Article in proceedings – Annual report year: 2001

Static Analysis for the Pi-calculus with Applications to Security

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Bodei, C. (Ekstern), Degano, P. (Ekstern), Nielson, F. (Intern), Nielson, H. R. (Intern)
Pages: 68-92
Publication date: 2001
Main Research Area: Technical/natural sciences
Publication information
Journal: Information and Computation
Volume: 168
Issue number: 1
ISSN (Print): 0890-5401
Ratings:
BFI (2018): BFI-level 2
A Kleene analysis of Mobile Ambients

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling
Authors: Nielson, F. (Intern), Nielson, H. R. (Intern), Sagiv, M. (Ekstern)
Pages: 305-319
Publication date: 2000

Host publication information
A Kleene analysis of Mobile Ambients
We show how a program analysis technique originally developed for C-like pointer structures can be adapted to analyse the hierarchical structure of processes in the ambient calculus. The technique is based on modeling the semantics of the language in a two-valued logic; by reinterpreting the logical formulae in Kleene's three-valued logic we obtain an analysis allowing us to reason about may as well as must properties. The correctness of the approach follows from a general Embedding Theorem for Kleene's logic; furthermore embeddings allow us to reduce the size of structures so as to control the time and space complexity of the analysis.

Security Analysis using Flow Logics

Shape analysis for Mobile Ambients
The ambient calculus is a calculus of computation that allows active processes to move between sites. We present an analysis inspired by state-of-the-art pointer analyses that safety and accurately predicts which processes may turn up at what sites during the execution of a composite system. The analysis models sets of processes by sets of regular tree grammars enhanced with context-dependent counts, and it obtains its precision by combining a powerful redex materialisation with a strong redex reduction (in the manner of the strong updates performed in pointer analyses). The underlying ideas are flexible and scale up to general tree structures admitting powerful restructuring operations.
Abstract Interpretation of Mobile Ambients

We demonstrate that abstract interpretation is useful for analysing calculi of computation such as the ambient calculus (which is based on the p-calculus); more importantly, we show that the entire development can be expressed in a constraint-based formalism that is becoming exceedingly popular for the analysis of functional and object-oriented languages. The first step of the development is an analysis for counting occurrences of processes inside other processes (for which we show semantic correctness and that solutions constitute a Moore family); the second step is a previously developed control flow analysis that we show how to induce from the counting analysis (and its properties are derived from those of the counting analysis using general results).

Interprocedural Control Flow Analysis

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielson, F. (Intern), Nielson, H. R. (Intern)
Pages: 20-39
Publication date: 1999

Principles of Program Analysis

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielson, F. (Intern), Nielson, H. R. (Intern), Hankin, C. L. (Ekstern)
Publication date: 1999
Static Analysis of Processes for No Read-Up and No Write-Down

We study a variant of the no read-up/no write-down security property of Bell and LaPadula for processes in the π-calculus. Given processes are given levels of security clearance, we statically check that a process at a high level never sends names to processes at a lower level. The static check is based on a Control Flow Analysis for the π-calculus that establishes a super-set of the set of names to which a given name may be bound and of the set of names that may be sent and received along a given channel, taking into account its directionality. The static check is shown to imply the natural dynamic condition.

Type and Effect Systems

Type and Effect Systems: Behaviours for Concurrency

Type and Effect Systems: Correct System Design
Validating Firewalls in Mobile Ambients

The ambient calculus is a calculus of computation that allows active processes (mobile ambients) to move between sites. A firewall is said to be protective whenever it denies entry to attackers not possessing the required passwords. We devise a polynomial time algorithm for rejecting proposed firewalls that are not guaranteed to be protective. This is based on a control flow analysis for recording what processes may turn up inside what other processes; in particular, we develop a syntax-directed system for specifying the acceptability of an analysis, we prove that all acceptable analyses are semantically sound, and we demonstrate that each process admits a least analysis.
Control Flow Analysis for the Pi-calculus

Control Flow Analysis is a static technique for predicting safe and computable approximations to the set of values that the objects of a program may assume during its execution. We present an analysis for the pi-calculus that shows how names will be bound to actual channels at run time. The formulation of the analysis requires no extensions to the pi-calculus, except for assigning "channels" to the occurrences of names within restrictions, and assigning "binders" to the occurrences of names within input prefixes. The result of our analysis establishes a super-set of the set of names to which a given name may be bound and of the set of names that may be sent along a given channel. Applications of our analysis include establishing simple security properties of processes. One example is that $P$ has no leaks, i.e. $P$ offers communication through public channels only, and confines its secret names within itself.

General information

State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Bodei, C. (Ekstern), Degano, P. (Ekstern), Nielson, F. (Intern), Nielson, H. R. (Intern)
Pages: 84-98
Publication date: 1998
Flow Logics and Operational Semantics

Flow logic is a “fast prototyping” approach to program analysis that shows great promise of being able to deal with a wide variety of languages and calculi for computation. However, seemingly innocent choices in the flow logic as well as in the operational semantics may inhibit proving the analysis correct. Our main conclusion is that environment based semantics is more flexible than either substitution based semantics or semantics making use of structural congruences (like alpha-renewing).

General information

State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielson, F. (Intern), Nielson, H. R. (Intern)
Pages: 150-169
Publication date: 1998
Main Research Area: Technical/natural sciences

Publication information

Journal: Electronic Notes in Theoretical Computer Science
Volume: 10
ISSN (Print): 1571-0661
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 0.256 SNIP 0.609 CiteScore 0.66
Web of Science (2016): Indexed yes
BFI (2015): BFI-level 1
Scopus rating (2015): SJR 0.373 SNIP 0.781 CiteScore 0.67
BFI (2014): BFI-level 1
Scopus rating (2014): SJR 0.382 SNIP 0.771 CiteScore 0.6
BFI (2013): BFI-level 1
Scopus rating (2013): SJR 0.323 SNIP 0.72 CiteScore 0.55
ISI indexed (2013): ISI indexed no
BFI (2012): BFI-level 1
Scopus rating (2012): SJR 0.386 SNIP 0.608 CiteScore 0.55
ISI indexed (2012): ISI indexed no
BFI (2011): BFI-level 1
Scopus rating (2011): SJR 0.325 SNIP 0.582 CiteScore 0.57
ISI indexed (2011): ISI indexed no
BFI (2010): BFI-level 1
Scopus rating (2010): SJR 0.408 SNIP 0.567
BFI (2009): BFI-level 1
Scopus rating (2009): SJR 0.419 SNIP 0.689
BFI (2008): BFI-level 1
Scopus rating (2008): SJR 0.407 SNIP 0.619
Scopus rating (2007): SJR 0.419 SNIP 0.611
Scopus rating (2006): SJR 0.377 SNIP 0.649
Scopus rating (2005): SJR 0.373 SNIP 0.633
Scopus rating (2004): SJR 0.406 SNIP 0.713
Flow Logics for Constraint Based Analysis

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielson, H. R. (Intern), Nielson, F. (Intern)
Pages: 109-127
Publication date: 1998

Host publication information
Title of host publication: Proc. CC’98
Publisher: Springer Verlag
Main Research Area: Technical/natural sciences
Source: orbit
Source-ID: 200355
Publication: Research - peer-review › Article in proceedings – Annual report year: 1998

Strictness and Totality Analysis
We define a novel inference system for strictness and totality analysis for the simply-typed lazy lambda-calculus with constants and fixpoints. Strictness information identifies those terms that definitely denote bottom (i.e. do not evaluate to WHNF) whereas totality information identifies those terms that definitely do not denote bottom (i.e. do evaluate to WHNF). The analysis is presented as an annotated type system allowing conjunctions at ?top-level? only. We give examples of its use and prove the correctness with respect to a natural-style operational semantics.

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Solberg, K. L. (Ekstern), Nielson, H. R. (Intern), Nielson, F. (Intern)
Pages: 113-145
Publication date: 1998
Main Research Area: Technical/natural sciences

Publication information
Journal: Science of Computer Programming
Volume: 31
Issue number: 1
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
The Flow Logic of Imperative Objects

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielson, F. (Intern), Nielson, H. R. (Intern)
Pages: 220-228
Publication date: 1998

Host publication information
Title of host publication: Proc. MFCS'98
Publisher: Springer Verlag
Main Research Area: Technical/natural sciences
Conference: Proc. MFCS'98, 01/01/1998
Source: orbit
Source-ID: 200276
Publication: Research - peer-review › Article in proceedings – Annual report year: 1998
Polymorphic Subtyping for Effect Analysis: The Dynamic Semantics

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Amtoft, T. (Ekstern), Nielson, F. (Intern), Nielson, H. R. (Intern), Ammann, J. (Ekstern)
Pages: 172-206
Publication date: 1997

Host publication information
Title of host publication: Analysis and Verification of Multiple-Agent Languages
Main Research Area: Technical/natural sciences
Links:
http://www2.imm.dtu.dk/pubdb/p.php?1573
Source: orbit
Source-ID: 200654
Publication: Research - peer-review › Book chapter – Annual report year: 1997

Polymorphic Subtyping for Effect Analysis: The Static Semantics

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielson, H. R. (Intern), Nielson, F. (Intern), Amtoft, T. (Ekstern)
Pages: 141-171
Publication date: 1997

Host publication information
Title of host publication: Analysis and Verification of Multiple-Agent Languages
Main Research Area: Technical/natural sciences
Links:
http://www2.imm.dtu.dk/pubdb/p.php?1572
Source: orbit
Source-ID: 200625
Publication: Research - peer-review › Book chapter – Annual report year: 1997

Systematic realisation of control flow analyses for CML
We present a methodology for the systematic realisealisation of control flow analyses and illustrate it for Concurrent ML. We start with an abstract specification of the analysis that is next proved semantically sound with respect to a traditional small-step operational semantics; this result holds for terminating as well as non-terminating programs. The analysis is defined coinductively and it is shown that all programs have a least analysis result (that is indeed the best one). To realise the analysis we massage the specification in three stages: (i) to explicitly record reachability of subexpressions, (ii) to be defined in a syntax-directed manner, and (iii) to generate a set of constraints that subsequently can be solved by standard techniques. We prove equivalence results between the different versions of the analysis; in particular it follows that the least solution to the constraints generated will be the least analysis result also to the initial specification.

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Gasser, K. (Ekstern), Nielson, F. (Intern), Nielson, H. R. (Intern)
Pages: 38-51
Publication date: 1997

Host publication information
Title of host publication: Proceedings of the second ACM SIGPLAN international conference on Functional programming
Type and Behaviour Reconstruction for Higher-Order Concurrent Programs

The authors develop a sound and complete type and behaviour inference algorithm for a fragment of CML (Standard ML with primitives for concurrency). Behaviours resemble terms of a process algebra and yield a concise representation of the communications taking place during execution; types are mostly as usual except that function types and ‘delayed communication types’ are labelled by behaviours expressing the communications that will take place if the function is applied or the delayed action is activated. The development of the paper improves a previously published algorithm in achieving completeness as well as soundness; this is due to an alternative strategy for generalising over types and behaviours.
From CML to its Process Algebra

Reppy's (1991) language CML (Concurrent ML) extends the Standard ML of Milner et al. (1990) with primitives for communication. It thus inherits a notion of strong polymorphic typing and may be equipped with a structural operational semantics. As a first step, we formulate an effect system for statically expressing the communication behaviours of CML programs as these are not reflected in the types. As a second step, we adapt the structural operational semantics of CML so as to incorporate behaviours. We then show how types and behaviours evolve in the course of computation: types may decrease and behaviours may lose prefixes as well as decrease. As the syntax of behaviours is rather similar to that of a process algebra, our main result may therefore be viewed as regarding the semantics of a process algebra as an abstraction of the semantics of an underlying programming language. This establishes a new kind of connection between "realistic" concurrent programming languages and "theoretical" process algebras.

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielson, F. (Intern), Nielson, H. R. (Intern)
Publication date: 1996

Publication information
Journal: Theoretical Computer Science
Volume: 155
Issue number: 1
ISSN (Print): 0304-3975
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 0.97 SJR 0.569 SNIP 1.006
Multi-Level Lambda-Calculi: an Algebraic Description

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielson, F. (Intern), Nielson, H. R. (Intern)
Pages: 338-354
Publication date: 1996

Host publication information
Title of host publication: Partial Evaluation
Publisher: Springer Verlag
Operational Semantics of Termination Types

In principle termination analysis is easy: find a well-founded ordering and prove that calls decrease with respect to the ordering. We show how to embed termination information into a polymorphic type system for an eager higher-order functional language allowing multiple-argument functions and algebraic data types. The well-founded orderings are defined by pattern matching against the definition of the algebraic data types. We prove that the analysis is semantically sound with respect to a big-step (or natural) operational semantics. We compare our approach based on operational semantics to one based on denotational semantics and we identify the need for extending the semantic universe with low constructs whose sole purpose is to facilitate the proof. For dealing with partial correctness it suffices to consider approximations that are less defined than the desired fixed points; for dealing with total correctness we introduce functions that are more defined than the fixed points.

Static and Dynamic Processor Allocation for Higher-Order Concurrent Languages

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielson, F. (Intern), Nielson, H. R. (Intern)
Pages: 590-604
Publication date: 1995
Host publication information
Title of host publication: Proc. TAPSOFT
Publisher: Springer Verlag
Main Research Area: Technical/natural sciences
Conference: Proc. TAPSOFT, 01/01/1995
The tensor product in Wadler's analysis of lists

We consider abstract interpretation (in particular strictness analysis) for pairs and lists. We begin by reviewing the well-known fact that the best known description of a pair of elements is obtained using the tensor product rather than the cartesian product. We next present a generalisation of Wadler's strictness analysis for lists (1987) using the notion of open set. Finally, we illustrate the intimate connection between the case analysis implicit in Wadler's strictness analysis and the precision that the tensor product allows for modelling the inverse cons operation.
Finiteness Conditions for Strictness Analysis

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielson, F. (Intern), Nielson, H. R. (Intern)
Pages: 194-205
Publication date: 1993

Host publication information
Title of host publication: Proc. Workshop on Static Program Analysis
Publisher: Springer Verlag
Main Research Area: Technical/natural sciences
Source: orbit
Source-ID: 200284
Publication: Research - peer-review › Article in proceedings – Annual report year: 1993

From CML to Process Algebras

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielson, F. (Intern), Nielson, H. R. (Intern)
Pages: 493-508
Publication date: 1993

Host publication information
Title of host publication: Proc. CONCUR'93
Publisher: Springer Verlag
Main Research Area: Technical/natural sciences
Conference: Proc. CONCUR'93, 01/01/1993
Source: orbit
Source-ID: 200283
Publication: Research - peer-review › Article in proceedings – Annual report year: 1993

Layered Predicates

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielson, F. (Intern), Nielson, H. R. (Intern)
Pages: 425-456
Publication date: 1993

Host publication information
Title of host publication: Proc. REX’92 workshop on Semantics -- foundations and applications
Publisher: Springer Verlag
Main Research Area: Technical/natural sciences
Conference: Proc. REX’92 workshop on Semantics -- foundations and applications, 01/01/1993
Source: orbit
Source-ID: 200282
Publication: Research - peer-review › Article in proceedings – Annual report year: 1993
Bounded Fixed Point Iteration

In the context of abstract interpretation the authors study the number of times a functional needs to be unfolded in order to give the least fixed point. For the cases of total or monotone functions they obtain an exponential bound and in the case of strict and additive (or distributive) functions they obtain a quadratic bound. These bounds are shown to be tight. Specializing the case of strict and additive functions to functionals of a form that would correspond to iterative programs they show that a linear bound is tight. This is related to several analyses studied in the literature (including strictness analysis).
Finiteness Conditions for Fixed Point Iteration

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielson, H. R. (Intern), Nielson, F. (Intern)
Pages: 96-108
Publication date: 1992

Host publication information
Title of host publication: Proc. Lisp and Functional Programming (LFP)
Publisher: ACM Press
Main Research Area: Technical/natural sciences
Conference: Proc. Lisp and Functional Programming (LFP), 01/01/1992
Source: orbit
Source-ID: 200359
Publication: Research - peer-review › Article in proceedings – Annual report year: 1992

Forced Transformations of Occam Programs

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielson, F. (Intern), Nielson, H. R. (Intern)
Pages: 91-96
Publication date: 1992
Main Research Area: Technical/natural sciences

Publication information
Journal: Information and Software Technology
Volume: 34
Issue number: 2
ISSN (Print): 0950-5849
Ratings:
BFI (2018): BFI-level 2
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 2
Inference Systems for Binding Time Analysis

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Solberg, K. L. (Ekstern), Nielson, H. R. (Intern), Nielson, F. (Intern)
Pages: 247-254
Publication date: 1992

Host publication information
Title of host publication: Proc. Workshop on Static Program Analysis
Publisher: University of Bordeaux
Main Research Area: Technical/natural sciences
Conference: Proc. Workshop on Static Program Analysis, 01/01/1992
Source: orbit
Source-ID: 200380
Publication: Research - peer-review › Article in proceedings – Annual report year: 1992
The tensor product in Wadler's analysis of lists

We consider abstract interpretation (in particular strictness analysis) for pairs and lists. We begin by reviewing the well-known fact that the best known description of a pair of elements is obtained using the tensor product rather than the cartesian product. We next present a generalisation of Wadler's strictness analysis for lists using the notion of open set. Finally, we illustrate the intimate connection between the case analysis implicit in Wadler's strictness analysis and the precision that the tensor product allows for modelling the inverse cons operation.
Using Transformations in the Implementation of Higher-order Functions

Many different techniques are needed in an optimising compiler-constant folding, program transformation, semantic analysis and optimisation, code generation and so on. The authors propose a uniform framework for all these activities. Every computation in the program to be compiled is classified as either compile-time or run-time and the run-time parts are translated into an easily manipulable form-categorical combinators. The authors set up a framework for defining operations on these intermediate forms, and show how it can be used to define concisely two forwards analyses (strictness, constant propagation), a backwards analysis (liveness), and even code generation. Both compile- and run-time parts can also be transformed. Every technique presented is illustrated using a simple running example, and the emphasis throughout is on intuition rather than absolute formality.

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielson, H. R. (Intern), Nielson, F. (Intern)
Pages: 459-494
Publication date: 1991
Main Research Area: Technical/natural sciences

Publication Information
Journal: Journal of Functional Programming
Volume: 1
Issue number: 4
ISSN (Print): 0956-7968
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 0.324 SNIP 1.256 CiteScore 0.93
BFI (2015): BFI-level 2
Scopus rating (2015): SJR 0.782 SNIP 1.764 CiteScore 1.39
BFI (2014): BFI-level 2
Scopus rating (2014): SJR 0.492 SNIP 1.127 CiteScore 0.81
BFI (2013): BFI-level 2
Scopus rating (2013): SJR 0.527 SNIP 1.414 CiteScore 1.14
ISI indexed (2013): ISI indexed yes
BFI (2012): BFI-level 2
Scopus rating (2012): SJR 0.681 SNIP 1.702 CiteScore 1.33
ISI indexed (2012): ISI indexed yes
BFI (2011): BFI-level 2
Scopus rating (2011): SJR 0.841 SNIP 1.983 CiteScore 1.49
ISI indexed (2011): ISI indexed yes
BFI (2010): BFI-level 2
Scopus rating (2010): SJR 0.956 SNIP 2.008
BFI (2009): BFI-level 2
Scopus rating (2009): SJR 1.081 SNIP 1.962
BFI (2008): BFI-level 2
Scopus rating (2008): SJR 0.692 SNIP 1.723
Scopus rating (2007): SJR 1.084 SNIP 1.796
Scopus rating (2006): SJR 0.885 SNIP 1.578
Scopus rating (2005): SJR 0.987 SNIP 1.593
Scopus rating (2004): SJR 0.951 SNIP 2.221
Scopus rating (2003): SJR 0.924 SNIP 1.571
Scopus rating (2002): SJR 0.87 SNIP 1.023
Scopus rating (2001): SJR 1.219 SNIP 2.007
Functional completeness of the mixed λ-calculus and combinatory logic

Functional completeness of the combinatory logic means that every lambda-expression may be translated into an equivalent combinator expression and this is the theoretical basis for the implementation of functional languages on combinator-based abstract machines. To obtain efficient implementations it is important to distinguish between early and late binding times, i.e. to distinguish between compile-time and run-time computations. The authors therefore introduce a two-level version of the lambda-calculus where this distinction is made in an explicit way. Turning to the combinatory logic they generate combinator-code for the run-time computations. The two-level version of the combinatory logic therefore is a mixed lambda-calculus and combinatory logic. They extend the mixed lambda-calculus and combinatory logic with a new combinator, Psi, and show that this suffices for the mixed lambda-calculus and combinatory logic to be functionally complete. However, the new combinator may not always be implementable and they therefore discuss conditions under which it can be dispensed with.
Automatic Binding Time Analysis for a Typed Lambda-Calculus

A binding time analysis imposes a distinction between the computations to be performed early (e.g. at compile-time) and those to be performed late (e.g. at run-time). For the lambda-calculus this distinction is formalized by a two-level lambda-calculus. The authors present an algorithm for static analysis of the binding times of a typed lambda-calculus with products, sums, lists and general recursive types. Given partial information about the binding times of some of the subexpressions it will complete that information such that (i) early bindings may be turned into late bindings but not vice versa, (ii) the resulting two-level lambda-expression reflects our intuition about binding times, e.g. that early bindings are
performed before late bindings, and (iii) as few changes as possible have been made compared with the initial binding information. The results can be applied in the implementation of functional languages and in semantics directed compiling.
Automatic Binding Time Analysis for a Typed Lambda-Calculus (Extended Abstract)

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielson, H. R. (Intern), Nielson, F. (Intern)
Pages: 98-106
Publication date: 1988

Host publication information
Title of host publication: Proc. ACM Conference on Principles of Programming Languages (POPL'88)
Main Research Area: Technical/natural sciences
Conference: Proc. ACM Conference on Principles of Programming Languages (POPL'88), 01/01/1988
Source: orbit
Source-ID: 200364
Publication: Research - peer-review › Article in proceedings – Annual report year: 1988

Two-Level Semantics and Code Generation
A two-level denotational metalanguage that is suitable for defining the semantics of Pascal-like languages is presented. The two levels allow for an explicit distinction between computations taking place at compile-time and computations taking place at run-time. While this distinction is perhaps not absolutely necessary for describing the input-output semantics of programming languages, it is necessary when issues such as data flow analysis and code generation are considered. For an example stack-machine, the authors show how to generate code for the run-time computations and still perform the compile-time computations. Using an example, it is argued that compiler-tricks such as the use of activation records suggest how to cope with certain syntactic restrictions in the metalanguage. The correctness of the code generation is proved using Kripke-like relations and using a modified machine that can be made to loop when a certain level of recursion is encountered.

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielson, F. (Intern), Nielson, H. R. (Intern)
Pages: 59-133
Publication date: 1988
Main Research Area: Technical/natural sciences

Publication information
Journal: Theoretical Computer Science
Volume: 56
Issue number: 1
ISSN (Print): 0304-3975
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 0.97 SJR 0.569 SNIP 1.006
Web of Science (2016): Indexed yes
BFI (2015): BFI-level 2
Scopus rating (2015): SJR 0.623 SNIP 1.212 CiteScore 1
Web of Science (2015): Indexed yes
BFI (2014): BFI-level 2
Scopus rating (2014): SJR 0.708 SNIP 1.228 CiteScore 1.08
A Hoare-like proof system for analysing the computation time of programs

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielson, H. R. (Intern)
Pages: 107-136
Publication date: 1987
Main Research Area: Technical/natural sciences

Publication information
Journal: Science of Computer Programming
Volume: 9
Issue number: 2
ISSN (Print): 0167-6423
Ratings:
BFI (2018): BFI-level 2
Web of Science (2018): Indexed yes
Code Generation from Two-Level Denotational Meta-Languages

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielson, F. (Intern), Nielson, H. R. (Intern)
Pages: 192-205
Publication date: 1986

Host publication information
Title of host publication: Programs as Data Objects
Publisher: Springer Verlag
Comments on Georgeff's Transformation and Reduction Strategies for Typed Lambda Expressions

In his recent paper, Georgeff [1] considers the evaluation of lambda expressions (with reducing reflexive types) on a variant of Landin's SECD machine. It is observed that for so-called simple expressions the SECD machine will construct stack-like environment structures, whereas, in general, they are tree-like. Georgeff then explores the idea of transforming any (typed) lambda expression into simple form and then using the SECD machine for these expressions. However, such transformations might be undesirable if the language is going to be interpreted directly. This leads Georgeff to modify the SECD machine such that it constructs stack-like environments for all expressions. Briefly, the idea in this modification is to let the machine construct over-applied closures for function-valued expressions in operand positions and to let it apply the closure in situ in the case of function-valued expressions in operator positions. The construction of overapplied closures implies that tree-like environment structures are avoided. Georgeff claims that by applying expressions in operator positions in situ it is avoided that operand values are “needlessly popped from the stack during creation of the overapplied closure, only to be reinstated on entry to the closure” [1, p. 620]. However, the example of Figure 1 shows that Georgeff's construction does not overcome this problem: the transitions 14, 15, and 16 move the on constant 3 from the stack to the closure and back to the stack. Intuitively, the reason is that the construction does not recognize correctly whether a sub-expression in operator position is in fact “basic-valued.” An expression (or, more precisely, its closure) occurring in operator position will look for its remaining arguments on the current stack and on the stacks of the dump. The prediction of the number of available arguments is important in order to determine whether the expression is “basic-valued,” and should therefore be treated specially. Georgeff suggests the following function for counting the number of available arguments on the stacks:

\[
def \text{totapps} (ST) = (S, E, C, D) = ST \text{ let } n = (\text{napps} C) \text{ if } n = 0 \text{ then } n \text{ else } (+ n (\text{totapps} D)) \text{ end}
\]

where the function (napps C) returns the number of consecutive apply operators at the beginning of the control C. For the configuration of line 14 of Figure 1 this gives totapps (...) = 2 napps (A & A & A) = 1 and totapps (d1) = 1 — this means that the closure ((&bgr;&ggr;&gr;&ggr;), u, (2), e1) can find 2 arguments on the stacks although its functionality is 1! Hence, the predicate, basic-valued, fails, although it ought to succeed. We suggest replacing the function above with def totapps (ST) let (S, E, C, D) = ST let n = (napps C) if length C ≠ n then /B> n else (+ n (totapps D)) end where length C is the length of the list C. The intuition behind this suggestion is that, if the control C of some configuration is not just a list of apply symbols, then the subexpression at hand will be turned into operand position before a basic value can be returned. Returning to the example mentioned above, note that we now get totapps (...) = 1 because napps (A & A & A) = 1 and length (A & A & A) ≠ 1, and the needless movements on the stack are avoided.
Pragmatic Aspects of Two-Level Denotational Meta-Languages

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielson, H. R. (Intern), Nielson, F. (Intern)
Pages: 133-143
Publication date: 1986

Host publication information
Title of host publication: Proc. ESOP'86
Publisher: Springer Verlag
Main Research Area: Technical/natural sciences
Conference: European Symposium on Programming, Saarbrücken, Germany, 17/03/1986 - 17/03/1986
Source: orbit
Source-ID: 200365
Publication: Research - peer-review › Article in proceedings – Annual report year: 1986

Semantics Directed Compiling for Functional Languages

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielson, H. R. (Intern), Nielson, F. (Intern)
Pages: 249-257
Publication date: 1986

Host publication information
Title of host publication: Proc. ACM Conference on LISP and Functional Programming
Main Research Area: Technical/natural sciences
Conference: Proc. ACM Conference on LISP and Functional Programming, 01/01/1986
Source: orbit
A Hoare-like Proof System for Total Correctness of Nested Recursive Procedures

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielson, H. R. (Intern)
Publication date: 1985

Host publication information
Title of host publication: Proc. Fourth Hungarian Computer Science Conference
Main Research Area: Technical/natural sciences
Source: orbit
Source-ID: 200367
Publication: Research - peer-review › Article in proceedings – Annual report year: 1985

Hoare Logic's for Run-time Analysis of Programs

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielson, H. R. (Intern)
Publication date: 1984

Publication information
Original language: English
Main Research Area: Technical/natural sciences

Bibliographical note
Publisher Edinburgh University
Source: orbit
Source-ID: 200850
Publication: Research › Ph.D. thesis – Annual report year: 1984

Computation Sequences: A Way to Characterize Classes of Attribute Grammars
A computation sequence for a derivation tree specifies a way of walking through the tree evaluating all the attributes of all nodes. By requiring that each derivation tree has a computation sequence with a certain property, it is possible to give simple characterizations of well-known subclasses of attribute grammars. Especially the absolutely noncircular attribute grammars are considered

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielson, H. R. (Intern)
Pages: 255-268
Publication date: 1983
Main Research Area: Technical/natural sciences

Publication information
Journal: Acta Informatica
Volume: 19
Issue number: 3
ISSN (Print): 0001-5903
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 0.327 SNIP 0.928 CiteScore 0.97
Proof Systems for Computation Time

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Nielson, H. R. (Intern)
Publication date: 1983

Host publication information
Title of host publication: Proc. Third Conference on Foundations of Software Technology and Theoretical Computer Science
Main Research Area: Technical/natural sciences
Source: orbit
Source-ID: 200368
Publication: Research - peer-review › Article in proceedings – Annual report year: 1983

k-visit Attribute Grammars
It is shown that any well-defined attribute grammar is k-visit for some k. Furthermore, it is shown that given a well-defined grammar G and an integer k, it is decidable whether G is k-visit. Finally it is shown that the k-visit grammars specify a proper hierarchy with respect to translations

General information
State: Published
Abstract Interpretation for Secure Information Flow
Department of Applied Mathematics and Computer Science
Period: 01/09/2016 → 31/08/2019
Number of participants: 3
Phd Student:
Vasilikos, Panagiotis (Intern)
Supervisor:
Nielson, Flemming (Intern)
Main Supervisor:
Nielson, Hanne Riis (Intern)

Financing sources
Source: Internal funding (public)
Name of research programme: Samfinansieret - Andet
Project: PhD

Modeling and Verifying eID Protocols (Future ID)
Department of Applied Mathematics and Computer Science
Period: 15/12/2012 → 24/02/2016
Number of participants: 6
Phd Student:
Almousa, Omar (Intern)
Supervisor:
Nielson, Hanne Riis (Intern)
Main Supervisor:
Mödersheim, Sebastian Alexander (Intern)
Examiner:
Lluch Lafuente, Alberto (Intern)
Brucker, Achim D. (Ekstern)
Sprenger, Christoph (Ekstern)

Financing sources
Source: Internal funding (public)
Name of research programme: Anden EU-finansiering
Project: PhD

SESAMO: Security and Safety Modelling
Department of Applied Mathematics and Computer Science
Period: 01/10/2012 → 21/01/2016
Number of participants: 6
Phd Student:
Li, Ximeng (Intern)
Supervisor:
Nielsen, Hanne Riis (Intern)
Main Supervisor:
Nielsen, Flemming (Intern)
Examiner:
Probst, Christian W. (Intern)
Aceto, Luca (Ekstern)
Mantal, Heiko (Ekstern)

**Financing sources**
Source: Internal funding (public)
Name of research programme: Institut, samfinansiering
Project: PhD

**SESAMO: Security and Safety Modelling**
Department of Applied Mathematics and Computer Science
Period: 01/10/2012 → 31/03/2016
Number of participants: 6
Phd Student:
Bruni, Alessandro (Intern)
Supervisor:
Nielsen, Hanne Riis (Intern)
Main Supervisor:
Nielsen, Flemming (Intern)
Examiner:
Probst, Christian W. (Intern)
Kremer, Steve (Ekstern)
Maffeis, Sergio (Ekstern)

**Financing sources**
Source: Internal funding (public)
Name of research programme: Institut, samfinansiering

**Relations**
Publications:
Analysis of Security Protocols in Embedded Systems
Project: PhD

**Rejseplanen - Next Generation**
Department of Management Engineering
Period: 15/12/2011 → 14/03/2012
Number of participants: 4
Phd Student:
Lins, Thomas Vermehren (Intern)
Supervisor:
Nielsen, Otto Anker (Intern)
Nielsen, Hanne Riis (Intern)
Main Supervisor:
Pisinger, David (Intern)

**Financing sources**
Source: Internal funding (public)
Name of research programme: Institut stipendie (DTU) Samf.
Project: PhD

**Cyber-Physical Systems secure communication protocols**
Department of Applied Mathematics and Computer Science
Period: 01/12/2011 → 04/03/2015
Number of participants: 6
Phd Student:
Vigo, Roberto (Intern)
Supervisor:
Nielson, Hanne Riis (Intern)
Main Supervisor:
Nielson, Flemming (Intern)
Examiner:
Lluch Lafuente, Alberto (Intern)
Victor, Björn (Ekstern)
Viganò, Luca (Ekstern)

Financing sources
Source: Internal funding (public)
Name of research programme: 1/3 FUU, 1/3 inst 1/3 Andet
Project: PhD

Conflict Management in Aspect Policies
Department of Applied Mathematics and Computer Science
Period: 01/09/2010 → 21/09/2015
Number of participants: 6
Phd Student:
Ramli, Carroline Dewi Puspa Kencana (Intern)
Supervisor:
Nielson, Flemming (Intern)
Main Supervisor:
Nielson, Hanne Riis (Intern)
Examiner:
Probst, Christian W. (Intern)
Kammüller, Florian (Ekstern)
Karjoth, Günter (Ekstern)

Financing sources
Source: Internal funding (public)
Name of research programme: 1/3 FUU, 1/3 inst 1/3 Andet
Project: PhD

Static Analysis for Model Checking
Department of Informatics and Mathematical Modeling
Period: 01/08/2010 → 25/10/2013
Number of participants: 6
Phd Student:
Terepeta, Michal Tomasz (Intern)
Supervisor:
Nielson, Flemming (Intern)
Main Supervisor:
Nielson, Hanne Riis (Intern)
Examiner:
Mödersheim, Sebastian Alexander (Intern)
Cortesi, Agostino (Ekstern)
Jensen, Thomas (Intern)

Financing sources
Source: Internal funding (public)
Name of research programme: 1/3 FUU, 1/3 inst 1/3 Andet
Project: PhD
Combined Techniques of Static Analysis and Model Checking

Department of Informatics and Mathematical Modeling
Period: 01/09/2009 → 22/11/2012
Number of participants: 6
Phd Student:
Zhang, Fuyuan (Intern)
Supervisor:
Nielsen, Hanne Riis (Intern)
Main Supervisor:
Nielsen, Flemming (Intern)
Examiner:
Probst, Christian W. (Intern)
Dam, Mads (Ekstern)
Huth, Michael (Ekstern)

Financing sources
Source: Internal funding (public)
Name of research programme: 1/3 FUU, 1/3 inst 1/3 Andet
Project: PhD

Static Analysis and Model Checking of Software Systems

Department of Informatics and Mathematical Modeling
Period: 01/08/2009 → 25/10/2012
Number of participants: 6
Phd Student:
Filipiuk, Piotr (Intern)
Supervisor:
Nielsen, Flemming (Intern)
Main Supervisor:
Nielsen, Hanne Riis (Intern)
Examiner:
Probst, Christian W. (Intern)
Schmidt, David A. (Ekstern)
Seidl, Helmut (Ekstern)

Financing sources
Source: Internal funding (public)
Name of research programme: Institut stipendie (DTU)
Project: PhD

Formal approaches for Aspect-Oriented Systems

Department of Informatics and Mathematical Modeling
Period: 01/06/2009 → 28/09/2012
Number of participants: 6
Phd Student:
Hernandez, Alejandro Mario (Intern)
Supervisor:
Nielsen, Hanne Riis (Intern)
Main Supervisor:
Nielsen, Flemming (Intern)
Examiner:
Probst, Christian W. (Intern)
De Nicola, Rocco (Ekstern)
Hankin, Chris (Ekstern)

Financing sources
Source: Internal funding (public)
Name of research programme: Forskningsrådsfinansiering
**Qualitative and Quantitative Security Analyses for ZigBee Wireless Sensor Networks**

Department of Informatics and Mathematical Modeling  
Period: 01/09/2007 → 30/03/2011  
Number of participants: 6  
Phd Student:  
Yuksel, Ender (Intern)  
Supervisor:  
Nielsen, Flemming (Intern)  
Main Supervisor:  
Nielsen, Hanne Riis (Intern)  
Examiner:  
Madsen, Jan (Intern)  
Gilmore, Stephen (Ekstern)  
Martinelli, Fabio (Ekstern)

**Financing sources**  
Source: Internal funding (public)  
Name of research programme: DTU-lønnet stipendie

**Verification of Stochastic Process Calculi**

Department of Informatics and Mathematical Modeling  
Period: 01/09/2007 → 22/06/2011  
Number of participants: 7  
Phd Student:  
Skrypnyuk, Nataliya (Intern)  
Supervisor:  
Nielsen, Hanne Riis (Intern)  
Seidl, Helmut (Ekstern)  
Main Supervisor:  
Nielsen, Flemming (Intern)  
Examiner:  
Probst, Christian W. (Intern)  
Hankin, Chris (Ekstern)  
Hermanns, Holger (Intern)

**Financing sources**  
Source: Internal funding (public)  
Name of research programme: Forskningsrådsfinansiering

**Aspects for security policies**

Department of Informatics and Mathematical Modeling  
Period: 01/06/2007 → 08/12/2010  
Number of participants: 6  
Phd Student:  
Yang, Fan (Intern)  
Supervisor:  
Nielsen, Hanne Riis (Intern)  
Main Supervisor:  
Nielsen, Flemming (Intern)  
Examiner:  
Probst, Christian W. (Intern)  
De Nicola, Rocco (Ekstern)  
Südholt, Mario (Ekstern)
Validation of Security Properties in Network Systems

Department of Informatics and Mathematical Modeling
Period: 15/09/2005 → 05/05/2009
Number of participants: 6
Phd Student:
Nielsen, Christoffer Rosenkilde (Intern)
Supervisor:
Nielsen, Flemming (Intern)
Main Supervisor:
Nielsen, Hanne Riis (Intern)
Examiner:
Fischer, Paul (Intern)
Mycroft, Alan (Ekstern)
Viganò, Luca (Ekstern)

Financing sources
Source: Internal funding (public)
Name of research programme: DTU-lønnet stipendie
Project: PhD

Statisk analyse af kritiske software systemer

Department of Informatics and Mathematical Modeling
Period: 01/01/2005 → 26/06/2005
Number of participants: 3
Phd Student:
Hansen, Steffen Michael (Ekstern)
Supervisor:
Nielsen, Flemming (Intern)
Main Supervisor:
Nielsen, Hanne Riis (Intern)

Financing sources
Source: Internal funding (public)
Name of research programme: DTU-lønnet stipendie
Project: PhD

Secure Communication Protocols

Department of Informatics and Mathematical Modeling
Period: 01/09/2004 → 29/05/2008
Number of participants: 5
Phd Student:
Gao, Han (Intern)
Main Supervisor:
Nielsen, Hanne Riis (Intern)
Examiner:
Baumeister, Hubert (Intern)
Cortesi, Agostino (Ekstern)
Gilmore, Stephen (Ekstern)

Financing sources
Source: Internal funding (public)
Name of research programme: Programbevilling
Project: PhD
Specification and Programming Languages for Biological Systems

Department of Informatics and Mathematical Modeling
Period: 01/10/2003 → 13/12/2007
Number of participants: 5
Phd Student:
Pilegaard, Henrik (Intern)
Supervisor:
Nielson, Hanne Riis (Intern)
Main Supervisor:
Nielson, Flemming (Intern)
Examiner:
Hillston, Jane (Ekstern)
Ingolfsdottir, Anna (Ekstern)

Financing sources
Source: Internal funding (public)
Name of research programme: DTU-lønnet stipendie
Project: PhD

Statisk program analyse af VHDL

Department of Informatics and Mathematical Modeling
Period: 01/04/2003 → 18/04/2007
Number of participants: 6
Phd Student:
Tolstrup, Terkel Kristian (Intern)
Supervisor:
Nielson, Flemming (Intern)
Main Supervisor:
Nielson, Hanne Riis (Intern)
Examiner:
Madsen, Jan (Intern)
Banerjee, Anindya (Ekstern)
Sabelfeld, Andrei (Ekstern)

Financing sources
Source: Internal funding (public)
Name of research programme: DTU-lønnet stipendie
Project: PhD

Modellering og analyse af globale applikationer

Department of Informatics and Mathematical Modeling
Period: 01/01/2002 → 12/07/2005
Number of participants: 6
Phd Student:
Buchholtz, Mikael (Intern)
Supervisor:
Nielson, Flemming (Intern)
Main Supervisor:
Nielson, Hanne Riis (Intern)
Examiner:
Haxthausen, Anne Elisabeth (Intern)
Focardi, Riccardo (Ekstern)
Guttman, Joshua D. (Ekstern)

Financing sources
Source: Internal funding (public)
Name of research programme: Eksternt EU-finansieret
**Security and Safety of Computer Systems**

Static analysis is a proven technology in the implementation of compilers and interpreters. Recent years have begun to see the application of static analysis techniques in novel areas such as software validation (for example, Ariane V) and software re-engineering (for example, the Y2K problem). This project will demonstrate that static analysis facilitates the validation of the security and safety of internet based computer systems.

Department of Informatics and Mathematical Modeling

Imperial College of Science, Technology and Medicine

French National Institute for Computer Science and Applied Mathematics

**Trusted Logic**

Period: 01/12/2000 → 31/12/2002

Number of participants: 5

Project participant:

Nielson, Hanne Riis (Intern)

Hankin, Chris (Ekstern)

Jensen, Thomas (Ekstern)

Marlet, Renaud (Ekstern)

Project Manager, organisational:

Nielson, Flemming (Intern)

---

**Secure and Safe Systems based on Static Analysis**

Static analysis of programs is a proven technology in the implementation of compilers and interpreters. Recent years have begun to see application of static analysis techniques in novel areas such as software validation and software re-engineering. This project will demonstrate that static analysis technology facilitates the validation of systems based on the internet and on smart cards.

Department of Informatics and Mathematical Modeling

Period: 01/08/2000 → 01/10/2003

Number of participants: 2

Project participant:

Nielson, Hanne Riis (Intern)

Project Manager, organisational:

Nielson, Flemming (Intern)

---

**Types for DSP Assembler Programs**

Department of Informatics and Mathematical Modeling

Period: 01/04/1999 → 26/02/2004

Number of participants: 6

Phd Student:

Larsen, Ken (Intern)

Supervisor:

Sestoft, Peter (Intern)

Main Supervisor:

Sparse, Jens (Intern)

Examiner:

Nielson, Hanne Riis (Intern)

Hankin, Chris (Ekstern)

Morrisett, Greg (Ekstern)

Financing sources

Source: Internal funding (public)

Name of research programme: Forskerakademiets Samfinansier

Project: PhD