Christian W. Probst - DTU Orbit (25/02/2018)

Christian W. Probst

Organisations

**Associate Professor, Department of Applied Mathematics and Computer Science**
27/12/2012 → 27/12/2017 Former
cwpr@dtu.dk
VIP

**Department of Applied Mathematics and Computer Science**
15/12/2017 → 27/12/2017 Former
cwpr@dtu.dk
VIP

**Department of Informatics and Mathematical Modeling**
19/05/2005 → 07/04/2016 Former
probst@imm.dtu.dk
VIP

**Associate Professor, Department of Informatics and Mathematical Modeling**
04/11/2005 → 07/04/2016 Former
probst@imm.dtu.dk
VIP

**Formal Methods**
23/02/2016 → 03/12/2016 Former
VIP

**Language-Based Technology**
18/02/2013 → 13/01/2016 Former
VIP

**Cyber Security**
03/12/2016 → 17/12/2017 Former
VIP

**Computer Science and Engineering**
25/02/2012 → 18/02/2013 Former
VIP

**Language-Based Technology**
25/02/2012 → 18/02/2013 Former
VIP

Publications:

**Architecturally Significant Requirements Identification, Classification and Change Management for Multi-tenant Cloud-Based Systems**

Involvement of numerous stakeholders in cloud-based systems’ design and usage with varying degrees of nonfunctional requirements makes Architecturally Significant Requirements (ASRs) identification and management a challenge undertaking. The aim of the research presented in this chapter is to identify different types of design-time and run-time ASRs of the cloud-based systems, provide an ASRs classification scheme and present a framework to manage the requirements’ variability during life cycle of the cloud-based systems. We have used a multifaceted research approach to address the ASRs identification, classification, and change management challenges. We have explored findings from systematic as well as structured reviews of the literature on quality requirements of the cloud-based systems including but not limited to security, availability, scalability, privacy, and multi-tenancy. We have presented a framework for requirements classification and change management focusing on distributed Platform as a Service (PaaS) and Software as a Service (SaaS) systems as well as complex software ecosystems that are built using PaaS and SaaS, such as Tools as a Service (TaaS). We have demonstrated applicability of the framework on a selected set of the requirements for the cloud-based systems. The results of the research presented in this chapter show that key quality requirements of the cloud-based systems, for example, multi-tenancy and security, have a significant impact on how other quality requirements (such as scalability, reliability, and interoperability) are handled in the overall architecture design of a cloud-based system. It is important to distinguish tenant-specific run-time architecturally significant quality requirements and corresponding cloud-based systems’ components so that run-time status of the tenant-specific architecture quality requirements can be monitored and system configurations can be adjusted accordingly. For the systems that can be used...
by multiple tenants, the requirements change management framework should consider if the addition or modification (triggered by a specific tenant) of a quality requirement can impact quality requirements of other tenants, and whether or not a trade-off point should be introduced in the architecture (corresponding to the requirements). The trade-off point can also be referred as a variability point, that is, a compromise has to be made among the number of quality requirements and only some of the requirements can be satisfied. System analysts and software architects can use the proposed taxonomy and the management framework for identifying relevant quality requirements for multi-tenant cloud-based systems, for analyzing impact of changes in the requirements on the overall system architecture, and for managing variability of the architecturally significant requirements.

**General information**

State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security
Authors: Chauhan, M. A. (Intern), Probst, C. W. (Intern)
Pages: 181-205
Publication date: 2017

**Host publication information**

Title of host publication: Requirements Engineering for Service and Cloud Computing
Publisher: Springer
ISBN (Print): 9783319513096
Chapter: 8
Series: Requirements Engineering for Service and Cloud Computing
Main Research Area: Technical/natural sciences
Computer Science, Computer Communication Networks, Software Engineering, Business Process Management, Cloud computing, Platform as a service (PaaS), Software as a service (SaaS), Architecturally significant requirements (ARSs), Requirements classification, Requirements change management, Architecture quality
DOI: 10.1007/978-3-319-51310-2_8
Source: FindIt
Source-ID: 2372098636
Publication: Research - peer-review › Book chapter – Annual report year: 2017

**Do we educate engineers that can engineer?**

Since 2008, the Bachelor of Engineering education at the Technical University of Denmark has been CDIO-based, including the software technology and IT and economics study lines. Consequently, the study plans of these study lines were revised to include cross-disciplinary CDIO projects in each of the first four semesters. These projects replaced 11 smaller, course-specific projects in the old study plans. The first three semesters contain design-build projects spanning several courses, and the fourth semester centers around a stand-alone CDIO project. These team-based projects aim at training the students' engineering skills (CDIO competence category 4) and at improving the students' skills in CDIO competence categories 2 and 3. In the tenth year of operation, we now decided to investigate, how content students and employers are with our students' engineering skills. To this end we have designed a survey to provide us with insights for improving our study lines and to address the question: "Are we educating engineers who can engineer?" The questionnaire is aligned with the CDIO syllabus and can also serve for surveying other study lines, since it is not study line specific. To obtain meaningful results, we decided to target students who have at least passed the first four terms, and companies that have hosted a significant number of students in the last 3 years in internships or for the final thesis. These companies interact with the students for almost one year at the end of their studies, providing a good foundation for the company supervisors to answer questions about the students' abilities as an engineer. In this paper, we discuss the design and result of the questionnaire, and the obtained results. As mentioned above, the survey will give us and the CDIO community detailed insights as to how our students and their employers experience the result of our education.

**General information**

State: Published
Organisations: Department of Applied Mathematics and Computer Science, Software Engineering, Cyber Security
Authors: Nyborg, M. (Intern), Probst, C. W. (Intern)
Pages: 12
Publication date: 2017

**Host publication information**

Title of host publication: Proceedings of the 13th International CDIO Conference
Main Research Area: Technical/natural sciences
Conference: 13th International CDIO Conference, Calgary, Canada, 18/06/2017 - 18/06/2017
CDIO-based study programs, Stakeholder involvement, Program evaluation, Standards: 1, 2, 3, 12
Electronic versions:
PAPERDoweducateengineersthatcanengineer.pdf
Formal Analysis of Graphical Security Models
The increasing usage of computer-based systems in almost every aspect of our daily life makes more and more dangerous the threat posed by potential attackers, and more and more rewarding a successful attack. Moreover, the complexity of these systems is also increasing, including physical devices, software components and human actors interacting with each other to form so-called socio-technical systems. The importance of socio-technical systems to modern societies requires verifying their security properties formally, while their inherent complexity makes manual analyses impracticable.

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

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

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

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

Publication information
Place of publication: Kgs. Lyngby
Publisher: Technical University of Denmark (DTU)
Original language: English
Series: DTU Compute PHD-2016
Number: 421
ISSN: 0909-3192
Main Research Area: Technical/natural sciences
Electronic versions: phd421_Aslanyan_Z.pdf

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

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

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

Automatic optimizations often fail for theoretical and practical reasons. When they fail we argue that a hybrid approach can be effective. Using compiler feedback, we propose to use the programmer’s intuition and insight to achieve high performance. Compiler feedback enlightens the programmer why a given optimization was not applied, and suggest how to change the source code to make it more amenable to optimizations. We show how this can yield significant speedups and achieve 2.4 faster execution on a real industrial use case.
To aid in parallel debugging we propose the prescriptive debugging model, which is a user-guided model that allows the programmer to use his intuition to diagnose bugs in parallel programs. The model is scalable, yet capable enough, to be general-purpose. In our evaluation we demonstrate low run time overhead and logarithmic scalability. This enable the model to be used on extremely large parallel systems.

**General information**

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

**Publication information**

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

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

**Relations**

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

**Modeling and Verification of Insider Threats Using Logical Analysis**

In this paper, we combine formal modeling and analysis of infrastructures of organizations with sociological explanation to provide a framework for insider threat analysis. We use the higher order logic (HOL) proof assistant Isabelle/HOL to support this framework. In the formal model, we exhibit and use a common trick from the formal verification of security protocols, showing that it is applicable to insider threats. We introduce briefly a three-step process of social explanation, illustrating that it can be applied fruitfully to the characterization of insider threats. We introduce the insider theory constructed in Isabelle that implements this process of social explanation. To validate that the social explanation is generally useful for the analysis of insider threats and to demonstrate our framework, we model and verify the insider threat patterns of entitled independent and Ambitious Leader in our Isabelle/HOL framework.

**General information**

State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, Middlesex University
Authors: Kammuller, F. (Ekstern), Probst, C. W. (Intern)
Number of pages: 12
Pages: 534-545
Publication date: 2017
Main Research Area: Technical/natural sciences

**Publication information**

Journal: IEEE Systems Journal
Volume: 11
Issue number: 2
ISSN (Print): 1932-8184
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 2.36 SJR 0.489 SNIP 1.147
BFI (2015): BFI-level 1
An Adaptive Middleware for Improved Computational Performance

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

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

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, Embedded Systems Engineering
Authors: Bonnichsen, L. F. (Intern), Probst, C. W. (Intern), Karlsson, S. (Intern)
Number of pages: 134
Publication date: 2016

Publication information
Place of publication: Kgs. Lyngby
Publisher: Technical University of Denmark (DTU)
Original language: English
A Process Framework for Designing Software Reference Architectures for Providing Tools as a Service

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

General information

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

Host publication information

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

Series: Lecture Notes in Computer Science
Volume: 10027
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
Cloud Computing, Software Reference Architecture (SRA), Tools as a Service (TaaS), Architecture Design, Architecture evaluation
Electronic versions:
ChauhanBabarProbst_AProcessFrameworkForDesigningSoftwareReferenceArchitecturesForProvidingToolsAsAService.pdf
DOIs:
10.1007/978-3-319-49094-6_8
Source: PublicationPreSubmission
Source-ID: 127557178
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

Attack tree analysis for insider threats on the IoT using isabelle

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

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

Host publication information
Title of host publication: Human Aspects of Information Security, Privacy, and Trust: 4th International Conference, HAS
2016, Held as Part of HCI International 2016, Toronto, ON, Canada, July 17-22, 2016, Proceedings
Volume: 9750
Publisher: Springer
Editor: Tryfonas, T.
ISBN (Print): 978-3-319-39380-3
ISBN (Electronic): 978-3-319-39381-0

Series: Lecture Notes in Computer Science
ISSN: 0302-9743
BFI conference series: Human-Computer Interaction (5000411)
Main Research Area: Technical/natural sciences
Conference: 4th International Conference on Human Aspects of Information Security, Privacy and Trust (HAS 2016),
Toronto, Canada, 17/07/2016 - 17/07/2016
DOIs: 10.1007/978-3-319-39381-0_21
Source: FindIt
Source-ID: 2307015849
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

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

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Formal Methods, Aalborg University,
Middlesex University
Authors: Probst, C. W. (Intern), Kammüller, F. (Ekstern), Hansen, R. R. (Ekstern)
Pages: 54-73
Publication date: 2016

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

Series: Lecture Notes in Computer Science
Volume: 9560
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
Electronic versions:
Guaranteeing Privacy-Observing Data Exchange

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

Model Based Analysis of Insider Threats

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

Identification of threats to organisations and risk assessment often take into consideration the pure technical aspects, overlooking the vulnerabilities originating from attacks on a social level, for example social engineering, and abstracting away the physical infrastructure. However, attacks on organisations are far from being purely technical. After all, organisations consist of employees. Often the human factor appears to be the weakest point in the security of organisations. It may be easier to break through a system using a social engineering attack rather than a pure technological one. The StuxNet attack is only one of the many examples showing that vulnerabilities of organisations are increasingly exploited on different levels including the human factor. There is an urgent need for integration between the technical and social aspects of systems in assessing their security. Such an integration would close this gap, however, it would also result in complicating the formal treatment and automatic identification of attacks.

This dissertation shows that applying a system modelling approach to sociotechnical systems can be used for identifying attacks on organisations, which exploit various levels of the vulnerabilities of the systems. In support of this claim we present a modelling framework, which combines many features. Based on a graph, the framework presents the physical infrastructure of an organisation, where actors and data are modelled as nodes in this graph. Based on the semantics of the underlying process calculus, we develop a formal analytical approach that generates attack trees from the model.

The overall goal of the framework is to predict, prioritise and minimise the vulnerabilities in organisations by prohibiting the overall attack or at least increasing the difficulty and cost of fulfilling it. We validate our approach using scenarios from IPTV and Cloud Infrastructure case studies.

Secure Refactoring with Java Information Flow

Refactoring means that a program is changed without changing its behaviour from an observer's point of view. Does the change of behaviour also imply that the security of the program is not affected by the changes? Using Myers and Liskov's distributed information flow control model DLM and its Java implementation Jif, we explore this question practically on common patterns of Refactoring as known from Fowler. We first illustrate on an example the "Extract method" refactoring and how it can endanger confidentiality. We then show how to construct a secure version of this major refactoring pattern by employing Jif to control information flows. Finally, we can show that security leaks as encountered at the outset are not
The attack navigator

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

General information

State: Published
Organisations: Department of Applied Mathematics and Computer Science , Cyber Security, Brandenburgische Technische Universität Cottbus-Senftenberg, Middlesex University
Authors: Helke, S. (Ekstern), Kammüunietd kller, F. (Ekstern), Probst, C. W. (Intern)
Number of pages: 9
Pages: 264-272
Publication date: 2016

Host publication information

Title of host publication: Data Privacy Management, and Security Assurance
Publisher: Springer
Editors: Garcia-Alfaro, J., Navarro-Arribas, G., Aldini, A., Martinelli, F., Suri, N.
ISBN (Print): 978-3-319-29882-5
ISBN (Electronic): 978-3-319-29883-2
Series: Lecture Notes in Computer Science
Volume: 9481
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
Workshop: 10th International Workshop, DPM 2015, and 4th International Workshop, QASA 2015, Vienna, Austria, 21/09/2015 - 21/09/2015
Computer Science (all), Theoretical Computer Science, Artificial intelligence, Computer science, Computers, Control information, Distributed information, Information flows, Java implementation, Refactorings, Security leak, Data privacy, Data security, Object-oriented programming, Software engineering techniques, Java, security of data, software maintenance, Java information flow, secure refactoring, program security, information flow control model, DLM, Jif, security leaks
DOIs: 10.1007/978-3-319-29883-2_19
Source: FindIt
Source-ID: 2304473884
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

The attack navigator

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

General information

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

Host publication information

Title of host publication: Revised Selected Papers from the 2nd International Workshop on Graphical Models for Security (GraMSec 2015)
Publisher: Springer
ISBN (Print): 978-3-319-29967-9
ISBN (Electronic): 978-3-319-29968-6
Series: Lecture Notes in Computer Science
Volume: 9390
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
Electronic versions:
The Navigation Metaphor in Security Economics

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

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

Publication information
Volume: 14
Issue number: 3
ISSN (Print): 1540-7993
Ratings:
BFI (2018): BFI-level 1
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 1
Web of Science (2017): Indexed Yes
BFI (2016): BFI-level 1
Scopus rating (2016): SJR 0.355 SNIP 1.243 CiteScore 1.39
Web of Science (2016): Indexed yes
BFI (2015): BFI-level 1
Scopus rating (2015): SJR 0.561 SNIP 1.408 CiteScore 1.14
BFI (2014): BFI-level 1
Scopus rating (2014): SJR 0.369 SNIP 1.448 CiteScore 1.06
BFI (2013): BFI-level 1
Scopus rating (2013): SJR 0.458 SNIP 1.827 CiteScore 1.58
ISI indexed (2013): ISI indexed yes
BFI (2012): BFI-level 1
Scopus rating (2012): SJR 0.488 SNIP 1.953 CiteScore 1.84
ISI indexed (2012): ISI indexed yes
BFI (2011): BFI-level 1
Scopus rating (2011): SJR 0.458 SNIP 2.203 CiteScore 1.69
ISI indexed (2011): ISI indexed yes
BFI (2010): BFI-level 1
Scopus rating (2010): SJR 0.471 SNIP 1.581
BFI (2009): BFI-level 1
Scopus rating (2009): SJR 0.469 SNIP 1.41
BFI (2008): BFI-level 1
Scopus rating (2008): SJR 0.614 SNIP 1.477
Scopus rating (2007): SJR 1.025 SNIP 2.538
Scopus rating (2006): SJR 0.967 SNIP 2.651
Towards Formal Analysis of Insider Threats for Auctions

This paper brings together the world of insider threats and auctions. For online-auction systems, like eBay, but also for high-value one-off auction algorithms as they are used for selling radio wave frequencies, the use of rigorous machine supported modelling and verification techniques is meaningful to prove correctness and scrutinize vulnerability to security and privacy attacks. Surveying the threats in auctions and insider collusions, we present an approach to model and analyze auction protocols for insider threats using the interactive theorem prover Isabelle. As a case study, we use the cocaine auction protocol that represents a nice combination of cryptographic techniques, protocols, and privacy goals suitable for highlighting insider threats for auctions.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, University of Birmingham, Middlesex University
Authors: Kammueller, F. (Ekstern), Kerber, M. (Ekstern), Probst, C. W. (Intern)
Pages: 23-34
Publication date: 2016

Host publication information
Title of host publication: Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats, MIST '16
Publisher: Association for Computing Machinery
ISBN (Print): 978-1-4503-4571-2
Main Research Area: Technical/natural sciences
Insider Threat, Auctions, Formal Methods
DOIs:
10.1145/2995959.2995963
Publication: Research - peer-review › Article in proceedings – Annual report year: 2017
Understanding How Components of Organisations Contribute to Attacks

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

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

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

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

Series: Lecture Notes in Computer Science
Volume: 9190
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
Conference: 3rd International Conference on Human Aspects of Information Security, Privacy and Trust (HAS 2015), Los Angeles, United States, 02/08/2015 - 02/08/2015

Electronic versions:
20150409_Chen_Kammueller_Nemli_Probst_ProbabilisticAnalysisFramework.pdf
DOIs:
10.1007/978-3-319-20376-8_16
Source: PublicationPreSubmission
Source-ID: 116483718
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

Attack Tree Generation by Policy Invalidation

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

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, Middlesex University, Aalborg University
Authors: Ivanova, M. G. (Intern), Probst, C. W. (Intern), Hansen, R. R. (Ekstern), Kammuller, F. (Ekstern)
Pages: 249-259
Publication date: 2015

Host publication information
Title of host publication: Proceedings of the 9th IFIP WG 11.2 International Conference on Information Security Theory and Practice, WISTP 2015
Publisher: Springer
Editors: Akram, R. N., Jajodia, S.
ISBN (Print): 978-3-319-24017-6
ISBN (Electronic): 978-3-319-24018-3

Series: Lecture Notes in Computer Science
Developing merged CDIO based curricula for diploma (B.Eng.) IT study programs at DTU

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

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

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

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

- The design process used to develop the new merged study programs;
- Involvement of stakeholders in designing the new curricula;
- Introduction of a common interdisciplinary innovation course in the programs; and
- Education of teaching staff: Integration into one organization.

Hardware Transactional Memory Optimization Guidelines, Applied to Ordered Maps

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

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology, Embedded Systems Engineering
Authors: Bonnichsen, L. F. (Intern), Probst, C. W. (Intern), Karlsson, S. (Intern)
Pages: 124-131
Publication date: 2015

Host publication information
Title of host publication: Proceedings of the 13th IEEE International Symposium on Parallel and Distributed Processing with Applications (ISPA 2015)
Volume: 3
Publisher: IEEE
ISBN (Print): 978-1-4673-7951-9
Main Research Area: Technical/natural sciences
Conference: 13th IEEE International Symposium on Parallel and Distributed Processing with Applications (ISPA 2015), Helsinki, Finland, 20/08/2015 - 20/08/2015
DOIs: 10.1109/Trustcom.2015.621
Source: PublicationPreSubmission
Source-ID: 119054342
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

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

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

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

Host publication information
Title of host publication: Proceedings of the 1st International Workshop on Socio-Technical Perspective in IS Development (STPIS'15)
Editors: Kowalski, S., Bednar, P., Bider, I.
Series: CEUR Workshop Proceedings
Volume: 1374
Number: urn:nbn:de:0074-1374-8
ISSN: 1613-0073
Main Research Area: Technical/natural sciences
Workshop: 1st International Workshop on Socio-Technical Perspective in IS Development (STPIS'15), Stockholm, Sweden, 09/06/2015
Electronic versions: paper11.pdf
Modelling Social–Technical Attacks with Timed Automata

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

Semantics, Logics, and Calculi: Essays Dedicated to Hanne Riis Nielson and Flemming Nielson on the Occasion of Their 60th Birthdays

Hanne Riis Nielson and Flemming Nielson turned 60 in 2014 and 2015, respectively. Congratulations! To celebrate the 60th birthdays, and to honor the birthday children, a colloquium was held at the Technical University of Denmark on January 8, 2016, to deliver the Festschrift and presentations of most contributions as our birthday presents.

This volume is dedicated to Hanne and Flemming and to their work. The Festschrift features contributions from colleagues who have worked together with Hanne and Flemming through their scientific life.

We would like to thank all the contributors to this Festschrift — for their hard work, for their both scientifically interesting and individual articles, as well as for their enthusiasm to contribute. The mix of articles resembles very nicely the impressively wide area in which Hanne and Flemming have worked and made fundamental contributions. Both the Festschrift and the colloquium were a wonderful way to celebrate them.

Our thanks also go to all the reviewers whose support made excellent articles even better. We are also indebted to Alfred Hofmann at Springer for his feedback and advice on our project, and to Anna Kramer from Springer for her fast responses to all our questions about Festschriften and all matters around them.
Tool-based Risk Assessment of Cloud Infrastructures as Socio-Technical Systems
Assessing risk in cloud infrastructures is difficult. Typical cloud infrastructures contain potentially thousands of nodes that are highly interconnected and dynamic. Another important component is the set of human actors who get access to data and computing infrastructure. The cloud infrastructure therefore constitutes a socio-technical system. Attacks on socio-technical systems are still mostly identified through expert brainstorming. However, formal risk assessment for systems including human actors requires modeling human behavior, which is difficult at best. In this chapter, we present a modeling exercise for cloud infrastructures using the socio-technical model developed in the TRESPASS project; after showing how to model typical components of a cloud infrastructure, we show how attacks are identified on this model and discuss their connection to risk assessment. The technical part of the model is extracted automatically from the configuration of the cloud infrastructure, which is especially important for systems so dynamic and complex.
Code Commentary and Automatic Refactorings using Feedback from Multiple Compilers

Optimizing compilers are essential to the performance of parallel programs on multi-core systems. It is attractive to expose parallelism to the compiler letting it do the heavy lifting. Unfortunately, it is hard to write code that compilers are able to optimize aggressively and therefore tools exist that can guide programmers with refactorings allowing the compilers to optimize more aggressively. We target the problem with many false positives that these tools often generate, where the amount of feedback can be overwhelming for the programmer. Our approach is to use a filtering scheme based on feedback from multiple compilers and show how we are able to filter out 87.6% of the comments by only showing the most promising comments.

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

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

Collaborative Compiler Vectorization

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

Bibliographical note
Poster at the HiPEAC’14 Poster Session
Source: PublicationPreSubmission
Source-ID: 102241744
Publication: Research › Poster – Annual report year: 2014
Combining Generated Data Models with Formal Invalidation for Insider Threat Analysis

In this paper we revisit the advances made on invalidation policies to explore attack possibilities in organizational models. One aspect that has so far eloped systematic analysis of insider threat is the integration of data into attack scenarios and its exploitation for analyzing the models. We draw from recent insights into generation of insider data to complement a logic based mechanical approach. We show how insider analysis can be traced back to the early days of security verification and the Lowe-attack on NSPK. The invalidation of policies allows modelchecking organizational structures to detect insider attacks. Integration of higher order logic specification techniques allows the use of data refinement to explore attack possibilities beyond the initial system specification. We illustrate this combined invalidation technique on the classical example of the naughty lottery fairy. Data generation techniques support the automatic generation of insider attack data for research. The data generation is however always based on human generated insider attack scenarios that have to be designed based on domain knowledge of counter-intelligence experts. Introducing data refinement and invalidation techniques here allows the systematic exploration of such scenarios and exploit data centric views into insider threat analysis.

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

Host publication information
Title of host publication: 2014 IEEE Security and Privacy Workshops (SPW)
Publisher: IEEE
Main Research Area: Technical/natural sciences
Conference: 2014 IEEE Security and Privacy Workshops (SPW), San Jose, California, United States, 17/05/2014 - 17/05/2014
Insider threats, policies, formal methods
Electronic versions:
KammuellerProbst_MIST14_CombiningGeneratedDataModelsWithFormalInvalidationForInsiderThreatAnalysis.pdf
DOIs:
10.1109/SPW.2014.45
Links:

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

Compiler Feedback using Continuous Dynamic Compilation during Development

Optimizing compilers are vital for performance. However, compilers ability to optimize aggressively is limited in some cases. To address this limitation, we have developed a compiler guiding the programmer in making small source code changes, potentially making the source code more amenable to optimization. This tool can help programmers understand what the optimizing compiler has done and suggest automatic source code changes in cases where the compiler refrains from optimizing. We have integrated our tool into an integrated development environment, interactively giving feedback as part of the programmers development flow.

We have evaluated our preliminary implementation and show it can guide to a 12% improvement in performance. Furthermore the tool can be used as an interactive optimization adviser improving the performance of the code generated by a production compiler. Here it can lead to a 153% improvement in performance, indicating the feasibility of the tool as a performance adviser for a production compiler.

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

Host publication information
Title of host publication: Proceedings - Workshop on Dynamic Compilation Everywhere
Main Research Area: Technical/natural sciences

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

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

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

ELB-trees - Efficient Lock-free B+trees

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

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

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

**Exploring adaptive program behavior**

**General information**
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology
Authors: Bonnichsen, L. F. (Intern), Probst, C. W. (Intern)
Number of pages: 1
Publication date: 2014
Main Research Area: Technical/natural sciences
Electronic versions:
poster3.pdf

**Bibliographical note**
Poster at the CGO2014 student research competition.
Source: PublicationPreSubmission
Source-ID: 102243579
Publication: Research - peer-review » Poster – Annual report year: 2014

**Exploring Adaptive Program Behavior**
Modern computer systems are increasingly complex, with ever changing bottlenecks. This makes it difficult to ensure consistent performance when porting software, or even running it. Adaptivity, i.e., switching between program variations, and dynamic recompilation have been suggested as solutions. Both solutions come at a cost; adaptivity issues a runtime overhead and requires more design effort, while dynamic recompilation takes time to perform. In this project, we plan to investigate the possibilities, limitations, and benefits of these techniques. This abstract covers our thoughts on how adaptivity and dynamic recompilation can be integrated and evaluated.

**General information**
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology
Authors: Bonnichsen, L. F. (Intern), Probst, C. W. (Intern)
Number of pages: 3
Publication date: 2014
Main Research Area: Technical/natural sciences
Electronic versions:
ExploringAdaptivePrograms.pdf

**Bibliographical note**
Invalidating Policies using Structural Information

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

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

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

Model-based Abstraction of Data Provenance

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

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

In a world that increasingly relies on the Internet to function, application developers rely on the implementations of protocols to guarantee the security of data transferred. Whether a chosen protocol gives the required guarantees, and whether the implementation does the same, is usually unclear. The Guided System Development framework contributes to more secure communication systems by aiding the development of such systems. The framework features a simple modelling language, step-wise refinement from models to implementation, interfaces to security verification tools, and code generation from the verified specification. The refinement process carries thus security properties from the model to the implementation. Our approach also supports verification of systems previously developed and deployed. Internally, the reasoning in our framework is based on the Beliefs and Knowledge tool, a verification tool based on belief logics and explicit attacker knowledge.

ELB-trees an efficient and lock-free B-tree derivative

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

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

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

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

Publication information
Journal: Journal of Internet Services and Information Security
Volume: 3
Issue number: 3/4
ISSN (Print): 2182-2069
Ratings:
ISI indexed (2013): ISI indexed no
Invalidating Policies using Structural Information

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

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

On Building Secure Communication Systems

This thesis presents the Guided System Development (GSD) framework, which aims at supporting the development of secure communication systems.

A communication system is specified in a language similar to the Alice and Bob notation, a simple and intuitive language used to describe the global perspective of the communications between different principals. The notation used in the GSD framework extends that notation with constructs that allow the security requirements of the messages to be described.

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

In order to provide higher security assurances, the system specification can be verified by formal methods tools such as the Beliefs and Knowledge (BAK) tool — developed specifically for the GSD framework —, LySatool and OFMC. The framework’s flexibility and the existence of the system model in different perspectives — an overall global perspective and an endpoint perspective — allow the connection to new formal methods tools.
The modeled system is also translated into code that implements the communication skeleton of the system and can then be used by the system designer. New output languages can also easily be added to the GSD framework.

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

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

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

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

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

**Publication information**
Journal: Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications
Volume: 4
Issue number: 4
ISSN (Print): 2093-5374
Ratings:
Scopus rating (2016): CiteScore 1.62
Scopus rating (2015): CiteScore 1.2
Scopus rating (2014): CiteScore 1.1
Scopus rating (2013): CiteScore 1.49
ISI indexed (2013): ISI indexed no
Original language: English
Insider threats, Insiderness, System models
Electronic versions: jowua_v4n4_3.pdf
Links:
http://isyou.info/jowua/abstracts/jowua-v4n4-3.htm
A Move in the Security Measurement Stalemate: Elo-Style Ratings to Quantify Vulnerability

One of the big problems of risk assessment in information security is the quantification of risk-related properties, such as vulnerability. Vulnerability expresses the likelihood that a threat agent acting against an asset will cause impact, for example, the likelihood that an attacker will be able to crack a password or break into a system. This likelihood depends on the capabilities of the threat agent and the strength of the controls in place. In this paper, we provide a framework for estimating these three variables based on the Elo rating used for chess players. This framework re-interprets security from the field of Item Response Theory. By observing the success of threat agents against assets, one can rate the strength of threats and controls, and predict the vulnerability of systems to particular threats. The application of Item Response Theory to the field of risk is new, but analogous to its application to children solving math problems. It provides an innovative and sound way to quantify vulnerability in models of (information) security.

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling, Computer Science and Engineering, Language-Based Technology, Delft University of Technology, University of Amsterdam
Authors: Pieters, W. (Ekstern), van der Ven, S. H. (Ekstern), Probst, C. W. (Intern)
Pages: 1-14
Publication date: 2012

Host publication information
Title of host publication: Proceedings of the 2012 workshop on New security paradigms
Publisher: Association for Computing Machinery
ISBN (Print): 978-1-4503-1794-8
BFI conference series: New Security Paradigms Workshop (5010167)
Main Research Area: Technical/natural sciences
DOIs:
10.1145/2413296.2413298
Source: Bibtex
Source-ID: urn:c8e72bfcb0a6436f6c7b26591c50de5d
Publication: Research - peer-review › Article in proceedings – Annual report year: 2012

Privacy Penetration Testing: How to Establish Trust in Your Cloud Provider

In the age of cloud computing, IT infrastructure becomes virtualised and takes the form of services. This virtualisation results in an increasing de-perimeterisation, where the location of data and computation is irrelevant from a user’s point of view. This irrelevance means that private and institutional users no longer have a concept of where their data is stored, and whether they can trust in cloud providers to protect their data. In this chapter, we investigate methods for increasing customers’ trust into cloud providers, and suggest a public penetration-testing agency as an essential component in a
Adapt or Become Extinct!: The Case for a Unified Framework for Deployment-Time Optimization

The High-Performance Computing ecosystem consists of a large variety of execution platforms that demonstrate a wide diversity in hardware characteristics such as CPU architecture, memory organization, interconnection network, accelerators, etc. This environment also presents a number of hard boundaries (walls) for applications which limit software development (parallel programming wall), performance (memory wall, communication wall) and viability (power wall). The only way to survive in such a demanding environment is by adaptation. In this paper we discuss how dynamic information collected during the execution of an application can be utilized to adapt the execution context and may lead to performance gains beyond those provided by static information and compile-time adaptation. We consider specialization based on dynamic information like user input, architectural characteristics such as the memory hierarchy organization, and the execution profile of the application as obtained from the execution platform's performance monitoring units. One of the challenges of future execution platforms is to allow the seamless integration of these various kinds of information with information obtained from static analysis (either during ahead-of-time or just-in-time) compilation. We extend the notion of information-driven adaptation and outline the architecture of an infrastructure designed to enable information ow and adaptation throughout the life-cycle of an application.

Bibliographical note
© ACM, 2011. This is the author's version of the work. It is posted here by permission of ACM for your personal use. Not for redistribution. The definitive version was published in EXADAPT '11, http://doi.acm.org/10.1145/2000417.2000422
A Framework for Constraint-Programming based Configuration

Product configuration systems play an important role in the development of Mass Customisation, allowing the companies to reduce their costs while offering highly customised products. Such systems are often based on a configuration model, representing the product knowledge necessary to perform the configuration task. Several challenges arise when dealing with product configuration. One of those issues concerns how to model a configurable product family, i.e. how to represent the different types of configuration knowledge and their interactions. Another challenge is to provide adequate formalisms and efficient algorithms to solve the dependencies of the models at runtime. In this dissertation, we present a constraint-based framework for configuration. The design of this framework is partly based on a study of product configuration requirements as well as a comparison of several general modelling languages. We then develop ProCoLa, a configuration-specific modelling language based on a conceptual framework that synthesizes, unifies and extends several approaches to modelling configuration in different design disciplines, e.g. physical products, software or services. A rigorous formalisation of the ProCoLa language is given and used to verify and analyse the configuration models. Another goal of this dissertation is to describe the semantics of ProCoLa by providing a translation to a Constraint Satisfaction Problem (CSP) representation. For that purpose, several CSP formalisms are discussed and a new algorithm DnSTR is developed in order to solve the dynamic addition and retraction of table constraints at runtime. Finally, we present and evaluate a prototype implementation of ProCoLa and the configuration framework, including the integration in a development environment, tool support and interaction with UML, databases and spreadsheet applications.
Hardware Support for Dynamic Languages

In recent years, dynamic programming languages have enjoyed increasing popularity. For example, JavaScript has become one of the most popular programming languages on the web. As the complexity of web applications is growing, compute-intensive workloads are increasingly handed off to the client side. While a lot of effort is put in increasing the performance of web browsers, we aim for multicore systems with dedicated cores to effectively support dynamic languages. We have designed Tinuso, a highly flexible core for experimentation that is optimized for high performance when implemented on FPGA. We composed a scalable multicore configuration where we study how hardware support for software speculation can be used to increase the performance of dynamic languages.

General information
State: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling, Language-Based Technology
Authors: Schleuniger, P. (Intern), Karlsson, S. (Intern), Probst, C. W. (Intern)
Publication date: 2011

Host publication information
Title of host publication: ACACES 2011 Seventh International Summer School on Advanced Computer Architecture and Compilation for High-Performance and Embedded Systems
Main Research Area: Technical/natural sciences
Electronic versions:
acaces_abstract_pass.pdf
Links:
http://www.hipeac.net/summerschool/
Source: orbit
Source-ID: 314922
Publication: Research - peer-review › Article in proceedings – Annual report year: 2011
Identifying and Mitigating Insider Threats
Organisations face many threats that coarsely can be separated in inside threats and outside threats. Threats from insiders are especially hard to counter since insiders have special knowledge and privileges. Therefore, malicious insider actions are hard to distinguish from benign actions. After discussing new definitions of insiders and insider threats, this article gives an overview of how to mitigate insider threats and discusses conflicting goals when dealing with insider threats.

Insiders and Insider Threats: An Overview of Definitions and Mitigation Techniques
Threats from the inside of an organization’s perimeters are a significant problem, since it is difficult to distinguish them from benign activity. In this overview article we discuss defining properties of insiders and insider threats. After presenting definitions of these terms, we go on to discuss a number of approaches from the technological, the sociological, and the socio-technical domain. We draw two main conclusions. Tackling insider threats requires a combination of techniques from the technical, the sociological, and the socio-technical domain, to enable qualified detection of threats, and their mitigation. Another important observation is that the distinction between insiders and outsiders seems to loose significance as IT infrastructure is used in performing insider attacks.
Modelling Configuration Knowledge in Heterogeneous Product Families

Product configuration systems play an important role in the development of Mass Customisation. The configuration of complex product families may nowadays involve multiple design disciplines, e.g. hardware, software and services. In this paper, we present a conceptual approach for modelling the variability in such heterogeneous product families. Our approach is based on a framework that aims to cater for the different stakeholders involved in the modelling and management of the product family. The modelling approach is centred around the concepts of views, types and constraints and is illustrated by a motivation example. Furthermore, as a proof of concept, a prototype has been implemented for configuring a non-trivial heterogeneous product family.

The Guided System Development Framework

The Service-Oriented Computing paradigm has had significant influence on the Internet. With the emergence of this paradigm, it is important to provide tools that help developers designing and verifying such systems. In this article, we present the Guided System Development (GSD) Framework that aids and guides the developer on the specification of the system being developed, on choosing the appropriate standard protocols suites that achieve the required security properties, on providing an implementation of the specified system, and also on allowing the verification of its security properties.
Towards a Time-predictable Dual-Issue Microprocessor: The Patmos Approach

Current processors are optimized for average case performance, often leading to a high worst-case execution time (WCET). Many architectural features that increase the average case performance are hard to be modeled for the WCET analysis. In this paper we present Patmos, a processor optimized for low WCET bounds rather than high average case performance. Patmos is a dualissue, statically scheduled RISC processor. The instruction cache is organized as a method cache and the data cache is organized as a split cache in order to simplify the cache WCET analysis. To fill the dual-issue pipeline with enough useful instructions, Patmos relies on a customized compiler. The compiler also plays a central role in optimizing the application for the WCET instead of average case performance.

Aspects of Insider Threats

The insider threat has received considerable attention, and is often cited as the most serious security problem. It is also considered the most difficult problem to deal with, because an "insider" has information and capabilities not known to external attackers. The difficulty in handling the insider threat is unsurprising under those circumstances; if one cannot define a problem precisely, how can one approach a solution, let alone know when the problem is solved? This chapter presents some aspects of insider threats, collected at an inter-disciplinary workshop in 2008.
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.
Insider Threats in Cyber Security

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling
Number of pages: 244
Publication date: 2010

Publication information
Publisher: Springer
ISBN (Print): 978-1-4419-7132-6
Original language: English
Series: Advances in Information Security
Number: 49
Main Research Area: Technical/natural sciences
Links:
Source: orbit
Source-ID: 270784
Publication: Research - peer-review › Book – Annual report year: 2010

Maintaining Arc Consistency in Non-Binary Dynamic CSPs using Simple Tabular Reduction
Constraint Satisfaction Problems (CSPs) are well known models used in Artificial Intelligence. In order to represent real world systems, CSPs have been extended to Dynamic CSPs (DCSPs), which support adding and removing constraints at runtime. Some approaches to the NP-complete problem of solving CSPs use filtering techniques such as arc consistency, which also have been adapted to handle DCSPs with binary constraints. However, there exists only one algorithm targeting non-binary DCSPs (DnGAC4). In this paper we present a new algorithm DnSTR for maintaining arc consistency in DCSPs with non-binary constraints. Our algorithm is based on Simple Tabular Reduction for Table Constraints, a technique that dynamically maintains the tables of supports within the constraints. Initial results show that our algorithm...
outperforms DnGAC4 both for addition and removal of constraints.

**General information**

State: Published

Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling, Microsoft Development Center Copenhagen

Authors: Queva, M. S. B. (Intern), Probst, C. W. (Intern), Ricci, L. (Ekstern)

Publication date: 2010

**Host publication information**

Title of host publication: Proceedings of the Fifth European Starting Al Researcher Symposium (STAIRS 2010)

Main Research Area: Technical/natural sciences

Conference: European Starting AI Researcher Symposium, Lisbon, Portugal, 01/01/2010

Simple Tabular Reduction, Arc consistency, Table constraints, Dynamic Constraint Satisfaction Problems

Source: orbit

Source-ID: 269125

Publication: Research - peer-review › Article in proceedings – Annual report year: 2010

**Protocol Implementation Generator**

Users expect communication systems to guarantee, amongst others, privacy and integrity of their data. These can be ensured by using well-established protocols; the best protocol, however, is useless if not all parties involved in a communication have a correct implementation of the protocol and all necessary tools. In this paper, we present the Protocol Implementation Generator (PiG), a framework that can be used to add protocol generation to protocol negotiation, or to easily share and implement new protocols throughout a network. PiG enables the sharing, verification, and translation of communication protocols. With it, partners can suggest a new protocol by sending its specification. After formally verifying the specification, each partner generates an implementation, which can then be used for establishing communication. We also present a practical realisation of the Protocol Implementation Generator framework based on the LySatool and a translator from the LySa language into C or Java.

**General information**

State: Published

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

Authors: Carvalho Quaresma, J. N. (Intern), Probst, C. W. (Intern)

Publication date: 2010

**Host publication information**

Title of host publication: Proceedings of The 15th Nordic Conference on Secure IT Systems

Main Research Area: Technical/natural sciences

Conference: The 15th Nordic Conference on Secure IT Systems, Espoo, Finland, 27/10/2010 - 27/10/2010

Source: orbit

Source-ID: 269273

Publication: Research - peer-review › Article in proceedings – Annual report year: 2010

**Security audits of multi-tier virtual infrastructures in public infrastructure clouds**

Cloud computing has gained remarkable popularity in the recent years by a wide spectrum of consumers, ranging from small start-ups to governments. However, its benefits in terms of flexibility, scalability, and low upfront investments, are shadowed by security challenges which inhibit its adoption. Managed through a web-services interface, users can configure highly flexible but complex cloud computing environments. Furthermore, users misconfiguring such cloud services poses a severe security risk that can lead to security incidents, e.g., erroneous exposure of services due to faulty network security configurations. In this article we present a novel approach in the security assessment of the end-user configuration of multi-tier architectures deployed on infrastructure clouds such as Amazon EC2. In order to perform this assessment for the currently deployed configuration, we automated the process of extracting the configuration using the Amazon API. In the assessment we focused on the reachability and vulnerability of services in the virtual infrastructure, and presented a way for the visualization and automated analysis based on reachability and attack graphs. We proposed a query and policy language for the analysis which can be used to obtain insights into the configuration and to specify desired and undesired configurations. We have implemented the security assessment in a prototype and evaluated it for practical scenarios. Our approach effectively allows to remediate today’s security concerns through validation of configurations of complex cloud infrastructures.

**General information**

State: Published

Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling, IBM Research, IBM Thomas J. Watson Research Center, InfraSight Labs

Authors: Bleikertz, S. (Ekstern), Schunter, M. (Ekstern), Probst, C. W. (Intern), Pendarakis, D. (Ekstern), Eriksson, K. (Ekstern)
The Risk of Risk Analysis

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling
Authors: Probst, C. W. (Intern), Hunker, J. (Ekstern)
Pages: 279-299
Publication date: 2010

Analysing Access Control Specifications
When prosecuting crimes, the main question to answer is often who had a motive and the possibility to commit the crime. When investigating cyber crimes, the question of possibility is often hard to answer, as in a networked system almost any location can be accessed from almost anywhere. The most common tool to answer this question, analysis of log files, faces the problem that the amount of logged data may be overwhelming. This problem gets even worse in the case of insider attacks, where the attacker’s actions usually will be logged as permissible, standard actions—if they are logged at all. Recent events have revealed intimate knowledge of surveillance and control systems on the side of the attacker, making it often impossible to deduce the identity of an inside attacker from logged data. In this work we present an approach that analyses the access control configuration to identify the set of credentials needed to reach a certain location in a system. This knowledge allows to identify a set of (inside) actors who have the possibility to commit an insider attack at that location. This has immediate applications in analysing log files, but also nontechnical applications such as identifying possible suspects, or, beyond cyber crimes, picking the “best” actor for a certain task. We also sketch an online analysis that identifies where an actor can be located based on observed actions.

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling
Authors: Probst, C. W. (Intern), Hansen, R. R. (Intern)
Publication date: 2009

Host publication information
Title of host publication: Proceedings of the Fourth International IEEE Workshop on Systematic Approaches to Digital Forensic Engineering
Publisher: IEEE
ISBN (Print): 978-0-7695-3792-4
Main Research Area: Technical/natural sciences
Conference: Fourth International IEEE Workshop on Systematic Approaches to Digital Forensic Engineering, 01/01/2009
Electronic versions:
Probst.pdf
DOIs:
10.1109/SADFE.2009.13

Bibliographical note
Fluid Information Systems

Networked communication systems and the data they make available have, over the last decades, made their way to the very core of both society and business. Not only do they support everyday life and day-to-day operations, in many cases they enable them in the first place, and often are among the most valuable assets. The flexibility that makes them so valuable in the first place, is also their primary vulnerability: via the network, an entity's data is accessible from almost everywhere, often without the need of physical presence in the entity's perimeter. In this work we propose a new security paradigm, that aims at using the network's flexibility to move data and applications away from potential attackers. We also present a possible realization of the proposed paradigm, based on recent advances in language-based security and static analysis, where data and applications are partitioned ahead-of-time and can be moved automatically based on activity both in the network as well as the real world.

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling
Authors: Probst, C. W. (Intern), Hansen, R. R. (Intern)
Pages: 125-132
Publication date: 2009

Industrial requirements for interactive product configurators

The demand for highly customized products at low cost is driving the industry towards Mass Customization. Interactive product configurators play an essential role in this new trend, and must be able to support more and more complex features. The purpose of this paper is, firstly, to identify requirements for modern interactive configurators. Existing modeling and solving technologies for configuration are then reviewed and their limitations discussed. Finally, a proposition for a future product configuration system is described.

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling, Microsoft Development Center Copenhagen
Authors: Queva, M. S. B. (Intern), Probst, C. W. (Intern), Vikkelsøe, P. (Ekstern)
Pages: 39-46
Publication date: 2009
The Risk of Risk Analysis: And its relation to the Economics of Insider Threats

Insider threats to organisational information security are widely viewed as an important concern, but little is understood as to the pattern of their occurrence. We outline an argument for explaining what originally surprised us: that many practitioners report that their organisations take basic steps to prevent insider attacks, but do not attempt to address more serious attacks. We suggest that an understanding of the true cost of additional policies to control insider threats, and the dynamic nature of potential insider threats together help explain why this observed behaviour is economically rational. This conclusion also suggests that further work needs to be done to understand how better to change underlying motivations of insiders, rather than simply focus on controlling and monitoring their behaviour.

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling, Carnegie Mellon University
Authors: Probst, C. W. (Intern), Hunker, J. (Ekstern)
Publication date: 2009

Host publication information
Title of host publication: Proceedings of The Eighth Workshop on the Economics of Information Security
Main Research Area: Technical/natural sciences
Conference: The Eighth Workshop on the Economics of Information Security, 01/01/2009
Links:
http://weis09.infosecon.net/files/111/paper111.pdf
Source: orbit
Source-ID: 243580
Publication: Research - peer-review › Article in proceedings – Annual report year: 2009

Towards A Comprehensive Study of Supply Chain Integrity

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling, Microsoft, European Network and Information Security Agency, Intel
Authors: Broda, M. (Ekstern), Gorniak, S. (Ekstern), Probst, C. W. (Intern), Vishik, C. (Ekstern)
Publication date: 2009

Host publication information
Title of host publication: Workshop on Telecommunications Infrastructure Protection and Security
Main Research Area: Technical/natural sciences
Conference: Workshop on Telecommunications Infrastructure Protection and Security, 01/01/2009
Source: orbit
Source-ID: 256569
Publication: Research - peer-review › Article in proceedings – Annual report year: 2009

An extensible analysable system model

Analysing real-world systems for vulnerabilities with respect to security and safety threats is a difficult undertaking, not least due to a lack of availability of formalisations for those systems. While both formalisations and analyses can be found for artificial systems such as software, this does not hold for real physical systems. Approaches such as threat modelling try to target the formalisation of the real-world domain, but still are far from the rigid techniques available in security research. Many currently available approaches to assurance of critical infrastructure security are based on (quite successful) ad-hoc techniques. We believe they can be significantly improved beyond the state-of-the-art by pairing them with static analyses techniques. In this paper we present an approach to both formalising those real-world systems, as well as providing an underlying semantics, which allows for easy development of analyses for the abstracted systems. We briefly present one application of our approach, namely the analysis of systems for potential insider threats.

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling, Aalborg University
Authors: Probst, C. W. (Intern), Hansen, R. R. (Ekstern)
Pages: 235-246
Publication date: 2008
Main Research Area: Technical/natural sciences

Publication information
Countering Insider Threats
This article summarizes the objectives and structure of a seminar with the same title, held from July 20th to July 25th, 2008, at Schloss Dagstuhl, Germany. The seminar brought together researchers and policy-makers from all involved communities, to clarify what it is that identifies an insider threat, and to develop a common vision of how an insider can be categorized as well as an integrated approach that allows a qualitative reasoning about the threat and the possibilities of attacks. This report gives an overview of the discussions and presentations during the week, as well as the outcome of these discussions.

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling, Carnegie Mellon University, Technische Universität Hamburg-Harburg, University of California at Davis
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.

Java bytecode verification via static single assignment form
Java Virtual Machines (JVMs) traditionally perform bytecode verification by way of an iterative data-flow analysis. Bytecode verification is necessary to ensure type safety because temporary variables in the JVM are not statically typed. We present an alternative verification mechanism that transforms JVM bytecode into Static Single Assignment Form (SSA) and thereby propagates definitions directly to uses. Type checking at control flow merge points can then be performed in a single pass. Our prototype implementation of the new algorithm is faster than the standard JVM bytecode verifier. It has the additional benefit of generating SSA as a side effect, which may be immediately useful for a subsequent dynamic compilation stage.
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

A new way of estimating compute-boundedness and its application to dynamic voltage scaling
Many dynamic voltage scaling algorithms rely on measuring hardware events (such as cache misses) for predicting how much a workload can be slowed down with acceptable performance loss. The events measured, however, are at best indirectly related to execution time and clock frequency. By relating these two indicators logically, we propose a new way of predicting a workload's compute-boundedness that is based on direct observation, and only requires measuring the total execution cycles for the two highest clock frequencies. Our predictor can be used to develop dynamic voltage scaling algorithms that are more system-aware than current approaches.

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling
Authors: Venkatachalam, V. (Ekstern), Franz, M. (Ekstern), Probst, C. W. (Intern)
Pages: 17-30
Publication date: 2007
Main Research Area: Technical/natural sciences
Automatic Generation of Machine Emulators: Efficient Synthesis of Robust Virtual Machines for Legacy Software Migration

As older mainframe architectures become obsolete, the corresponding legacy software is increasingly executed via platform emulators running on top of more modern commodity hardware. These emulators are virtual machines that often include a combination of interpreters and just-in-time compilers. Implementing interpreters and compilers for each combination of emulated and target platform independently of each other is a redundant and error-prone task. We describe an alternative approach that automatically synthesizes specialized virtual-machine interpreters and just-in-time compilers, which then execute on top of an existing software portability platform such as Java. The result is a considerably reduced implementation effort.

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling, University of California, Irvine
Authors: Franz, M. (Ekstern), Gal, A. (Ekstern), Probst, C. (Intern)
Pages: 83-94
Publication date: 2006

Host publication information
Title of host publication: Proceedings of Software Engineering Conference (SE2007)
Main Research Area: Technical/natural sciences
Conference: Software Engineering, 01/01/2007
Source: orbit
Source-ID: 207848
Publication: Research - peer-review › Article in proceedings – Annual report year: 2007
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

HotpathVM: An Effective JIT for Resource-constrained Devices

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling
Authors: Gal, A. (Ekstern), Franz, M. (Ekstern), Probst, C. (Intern)
Publication date: 2006

Host publication information
Title of host publication: 2nd International Conference on Virtual Execution Environments (VEE 2006)
Main Research Area: Technical/natural sciences
Electronic versions:
imm4746.pdf
Links:
http://www2.imm.dtu.dk/pubdb/p.php?4746
Source: orbit
Source-ID: 191532
Publication: Research - peer-review › Article in proceedings – Annual report year: 2006

Issues in holistic system design
The coordination of layers in computer and software systems is one of the main challenges in designing such systems today. In this paper we consider Holistic System Design as a way of integrating requirements and facilities of different system layers. We also discuss some of the challenges that this kind of system design poses for computer science in general as well as programming languages and operating systems in particular.

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling, University of Southern Denmark, University of Copenhagen
Authors: Lawall, J. L. (Ekstern), Probst, C. W. (Intern), Schultz, U. P. (Ekstern)
Publication date: 2006

Host publication information
Title of host publication: Proceedings of the 3rd workshop on programming languages and operating systems
ISBN (Print): 1-59593-577-0
Main Research Area: Technical/natural sciences
Conference: Programming languages and operating systems : Linguistic support for modern operating systems, San Jose, California, 01/01/2006
DOIs:
10.1145/1215995.1216007
Source: orbit
Source-ID: 229109
Publication: Research - peer-review › Article in proceedings – Annual report year: 2006
Linguistic Support for Modern Operating Systems - Workshop on Programming Languages and Operating Systems (PLOS 2006)

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling
Publication date: 2006

Publication information
Publisher: ACM Digital Library
Original language: English
Main Research Area: Technical/natural sciences
Source: orbit
Source-ID: 195745
Publication: Research - peer-review › Book – Annual report year: 2006

Non-Interference and Erasure Policies for Java Card Bytecode.

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling, Language-Based Technology
Authors: Hansen, R. R. (Intern), Probst, C. W. (Intern)
Publication date: 2006

Host publication information
Title of host publication: 6th International Workshop on Issues in the Theory of Security (WITS '06)
Main Research Area: Technical/natural sciences
Electronic versions:
imm4742.pdf
Links:
http://www2.imm.dtu.dk/pubdb/p.php?4742
Source: orbit
Source-ID: 191540
Publication: Research - peer-review › Article in proceedings – Annual report year: 2006

Program Partitioning using Dynamic Trust Models

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling, System Security
Publication date: 2006

Host publication information
Title of host publication: Workshop on Formal Aspects in Security and Trust (FAST 2006)
Main Research Area: Technical/natural sciences
Conference: Workshop on Formal Aspects in Security and Trust, 01/01/2006
Links:
http://www2.imm.dtu.dk/pubdb/p.php?4745
Source: orbit
Source-ID: 191578
Publication: Research - peer-review › Article in proceedings – Annual report year: 2006

Sandboxing for myKlaim

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling, Language-Based Technology
Authors: Hansen, R. R. (Intern), Probst, C. W. (Intern), Nielson, F. (Intern)
Publication date: 2006

Host publication information
Sandboxing in myKlaim

The μKlaim calculus is a process algebra designed to study the programming of distributed systems consisting of a number of locations each having their own tuple space and collection of mobile processes. Previous work has explored how to incorporate a notion of capabilities to be enforced dynamically by means of a reference monitor. Our first contribution is to describe a sandboxing semantics for the remote evaluation of mobile code; we then develop a succinct flow logic for statically guaranteeing the properties enforced by the reference monitor and hence for dispensing with the overhead of a dynamic reference monitor. Our second contribution is an extension of the calculus to interact with an environment; processes enter the system from the environment and we develop an entry-condition that is sufficient for ensuring that the resulting system continues to guarantee the properties that would otherwise need to be dynamically enforced by the reference monitor. We call the resulting calculus myKlaim.

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

Host publication information
Publisher: IEEE
ISBN (Print): 0-7695-2567-9
Main Research Area: Technical/natural sciences
Electronic versions:
Hansen.pdf
DOIs:
10.1109/ARES.2006.115

Bibliographical note
Copyright: 2006 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
Source: orbit
Source-ID: 252753
Publication: Research - peer-review › Article in proceedings – Annual report year: 2006

Where can an Insider attack?

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling
Authors: Probst, C. W. (Intern), Hansen, R. R. (Intern), Nielson, F. (Intern)
Publication date: 2006

Host publication information
Title of host publication: Workshop on Formal Aspects in Security and Trust (FAST 2006)
Publisher: Springer
Main Research Area: Technical/natural sciences
Links:
http://www2.imm.dtu.dk/pubdb/p.php?4747
A Multilevel Introspective Dynamic Optimization System For Holistic Power-Aware Computing

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling
Authors: Venkatachalam, V. (Ekstern), Probst, C. (Intern), Franz, M. (Ekstern)
Publication date: 2005

Host publication information
Title of host publication: Dagstuhl Seminar Proceedings
Main Research Area: Technical/natural sciences
Electronic versions:
imm4153.pdf
Links:
http://www2.imm.dtu.dk/pubdb/p.php?4153
Source: orbit
Source-ID: 185759
Publication: Research - peer-review › Article in proceedings – Annual report year: 2005

A portable virtual machine target for proof-carrying code
Virtual Machines (VMs) and Proof-Carrying Code (PCC) are two techniques that have been used independently to provide safety for (mobile) code. Existing virtual machines, such as the Java VM, have several drawbacks: First, the effort required for safety verification is considerable. Second and more subtly, the need to provide such verification by the code consumer inhibits the amount of optimization that can be performed by the code producer. This in turn makes just-in-time compilation surprisingly expensive. Proof-Carrying Code, on the other hand, has its own set of limitations, among which are the sizes of the proofs and the fact that the certified code is no longer machine-independent. In this paper, we describe work in progress on combining these approaches. Our hybrid safe-code solution uses a virtual machine that has been designed specifically to support proof-carrying code, while simultaneously providing efficient just-in-time compilation and target-machine independence. In particular, our approach reduces the complexity of the required proofs, resulting in fewer proof obligations that need to be discharged at the target machine.

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling, University of California, Irvine, University of Nottingham
Authors: Franz, M. (Ekstern), Chandra, D. (Ekstern), Gal, A. (Ekstern), Haldar, V. (Ekstern), Probst, C. W. (Intern), Reig, F. (Ekstern), Wang, N. (Ekstern)
Pages: 275-294
Publication date: 2005
Main Research Area: Technical/natural sciences

Publication information
Journal: Science of Computer Programming
Volume: 57
Issue number: 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
Average Case vs. Worst Case-Margins of Safety in System Design

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling
Authors: Probst, C. (Intern), Gal, A. (Ekstern), Franz, M. (Ekstern)
Publication date: 2005

Host publication information
Title of host publication: New Security Paradigms Workshop
Main Research Area: Technical/natural sciences
Electronic versions: imm4149.pdf
Links:
http://www2.imm.dtu.dk/pubdb/p.php?4149
Source: orbit
Source-ID: 185741
Publication: Research - peer-review › Article in proceedings – Annual report year: 2005
Power-aware computing systems

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling
Authors: Benini, L. (Ekstern), Kremer, U. (Ekstern), Probst, C. (Intern), Schelkens, P. (Ekstern)
Publication date: 2005

Host publication information
Title of host publication: Dagstuhl Seminar Proceedings, Internationales Begegnungs- und Forschungszentrum (IBFI), Schloss Dagstuhl, Germany
Main Research Area: Technical/natural sciences
Electronic versions: imm4152.pdf
Links: http://www2.imm.dtu.dk/pubdb/p.php?4152
Source: orbit
Source-ID: 185666
Publication: Research - peer-review › Article in proceedings – Annual report year: 2005

Secure Dynamic Program Repartitioning

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling
Authors: Hansen, R. R. (Ekstern), Probst, C. (Intern)
Publication date: 2005

Host publication information
Title of host publication: Nordic Workshop in Secure IT-Systems
Main Research Area: Technical/natural sciences
Electronic versions: imm4154.pdf
Source: orbit
Source-ID: 185694
Publication: Research - peer-review › Article in proceedings – Annual report year: 2005

Structural Encoding of Static Single Assignment Form
Static Single Assignment (SSA) form is often used as an intermediate representation during code optimization in Java Virtual Machines. Recently, SSA has successfully been used for bytecode verification. However, constructing SSA at the code consumer is costly. SSA-based mobile code transport formats have been shown to eliminate this cost by shifting SSA creation to the code producer. These new formats, however, are not backward compatible with the established Java class-file format. We propose a novel approach to transport SSA information implicitly through structural code properties of standard Java bytecode. While the resulting bytecode sequence can still be directly executed by traditional Virtual Machines, our novel VM can infer SSA form and confirm its safety with virtually no overhead.

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling
Authors: Gal, A. (Ekstern), Probst, C. (Intern), Franz, M. (Ekstern)
Pages: 85-102
Publication date: 2005
Main Research Area: Technical/natural sciences

Publication information
Journal: Electronic Notes in Theoretical Computer Science
Volume: 141
Issue number: 2
ISSN (Print): 1571-0661
Untyped Memory in the Java Virtual Machine

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling
Authors: Gal, A. (Ekstern), Probst, C. (Intern), Franz, M. (Ekstern)
Publication date: 2005

Host publication information
Title of host publication: ECOOP Workshop on Programming Languages and Operating Systems
Main Research Area: Technical/natural sciences
Electronic versions:
Modular Control Flow Analysis for Libraries

One problem in analyzing object oriented languages is that the exact control flow graph is not known statically due to dynamic dispatching. However, this is needed in order to apply the large class of known interprocedural analysis. Control Flow Analysis in the object oriented setting aims at determining run-time types of variables, thus allowing to possibly targeted method implementations. We present a flow sensitive analysis that allows separate handling of libraries and thereby efficient analysis of whole programs.

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling
Authors: Probst, C. W. (Intern)
Publication date: 2002

Host publication information
Title of host publication: Proceedings of the 9th International Symposium on Static Analysis
Main Research Area: Technical/natural sciences
DOIs: 10.1007/3-540-45789-5_14

Projects:

Security in Fog Computing
Technical University of Denmark
Period: 01/09/2017 → 31/08/2020
Number of participants: 3
Phd Student: De Donno, Michele (Intern)
Supervisor: Probst, Christian W. (Intern)
Main Supervisor: Dragoni, Nicola (Intern)

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

Typing for Secure Composition of Distributed Systems
Technical University of Denmark
Period: 01/06/2016 → 01/10/2019
Number of participants: 3
Phd Student: Laursen, Kasper (Intern)
Supervisor: Probst, Christian W. (Intern)
Main Supervisor: Mödersheim, Sebastian Alexander (Intern)

Financing sources
Principles for Scalable Many-core Operating Systems

Technical University of Denmark
Period: 15/01/2014 → 12/01/2018
Number of participants: 3
PhD Student:
Walter, Maxwell (Intern)
Supervisor:
Probst, Christian W. (Intern)
Main Supervisor:
Karlsson, Sven (Intern)

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

Cognitive and Perceptive Cameras - System software and execution platform

Technical University of Denmark
Period: 01/11/2013 → 30/11/2015
Number of participants: 3
PhD Student:
Hindborg, Andreas Erik (Intern)
Supervisor:
Probst, Christian W. (Intern)
Main Supervisor:
Karlsson, Sven (Intern)

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

Cognitive and Perceptive Cameras - Compilation system

Technical University of Denmark
Period: 01/10/2013 → 18/01/2017
Number of participants: 6
PhD Student:
Jensen, Nicklas Bo (Intern)
Supervisor:
Karlsson, Sven (Intern)
Main Supervisor:
Probst, Christian W. (Intern)
Examiner:
Lluch Lafuente, Alberto (Intern)
Kessler, Christoph W. (Ekstern)
Sestoft, Peter (Intern)

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

Relations
Publications:
High Performance with Prescriptive Optimization and Debugging
Stochastic Model Checking of Socio-Technical Models
Technical University of Denmark
Period: 01/07/2013 → 23/11/2016
Number of participants: 6
Phd Student:
Aslanyan, Zaruhi (Intern)
Supervisor:
Probst, Christian W. (Intern)
Main Supervisor:
Nielsen, Flemming (Intern)
Examiner:
Lluch Lafuente, Alberto (Intern)
Hansen, René Rydhof (Intern)
Legay, Axel (Ekstern)

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

Relations
Publications:
Formal Analysis of Graphical Security Models
Project: PhD

Graphical passwords user authentication
Technical University of Denmark
Period: 15/05/2013 → 11/05/2017
Number of participants: 5
Phd Student:
Elaswad, Othoman (Intern)
Main Supervisor:
Jensen, Christian D. (Intern)
Examiner:
Probst, Christian W. (Intern)
Kamala, Mumtaz A. (Ekstern)
Khajuria, Samant (Ekstern)

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

Relations
Publications:
Authentication for E-Government in Developing Countries - With special focus on the North Africa Countries
Project: PhD

Modelling Socio-Technical Aspects of Organizational Security
Technical University of Denmark
Period: 15/01/2013 → 20/04/2016
Number of participants: 5
Phd Student:
Ivanova, Marieta Georgieva (Intern)
Main Supervisor:
Probst, Christian W. (Intern)
Examiner:
Lluch Lafuente, Alberto (Intern)
Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security

Information security threats to organisations have changed completely over the last decade, due to the complexity and dynamic nature of infrastructures and attacks. Successful attacks cost society billions a year, impacting vital services and the economy. Examples include StuxNet, using infected USB sticks to sabotage nuclear plants, and the DigiNotar attack, using fake digital certificates to spy on website traffic. New attacks cleverly exploit multiple organisational vulnerabilities, involving physical security and human behaviour. Defenders need to make rapid decisions regarding which attacks to block, as both infrastructure and attacker knowledge change rapidly.

Current risk management methods provide descriptive tools for assessing threats by systematic brainstorming. Attack opportunities will be identified and prevented only if people can conceive them. In today’s dynamic attack landscape, this process is too slow and exceeds the limits of human imaginative capability. Emerging security risks demand tool support
to predict, prioritise, and prevent complex attacks systematically. The TREsPASS project will make this possible, by building an “attack navigator”. This navigator makes it possible to say which attack opportunities are possible, which of them are the most urgent, and which countermeasures are most effective. To this end, the project combines knowledge from technical sciences (how vulnerable are protocols and software), social sciences (how likely are people to succumb to social engineering), and state-of-the-art industry processes and tools. By integrating European expertise on socio-technical security into a widely applicable and standardised framework, TREsPASS will reduce security incidents in Europe, and allow organisations and their customers to make informed decisions about security investments. This increased resilience of European businesses both large and small is vital to safeguarding the social and economic prospects of Europe.

Department of Informatics and Mathematical Modeling

Language-Based Technology
Period: 01/11/2012 → 31/10/2016
Number of participants: 1
Acronym: TREsPASS
Project participant:
Probst, Christian W. (Intern)

Financing sources
Source: EU research programme (public)
Name of research programme: FP7-ICT-2011-8
Year of approval: 2012
Project

Portable and Predictable Performance Heterogeneous Embedded Manycores - Upper Level System stack

Technical University of Denmark
Period: 01/10/2012 → 21/01/2016
Number of participants: 6
Phd Student:
Bonnichsen, Lars Frydendal (Intern)
Supervisor:
Karlsson, Sven (Intern)
Main Supervisor:
Probst, Christian W. (Intern)
Examiner:
Lluch Lafuente, Alberto (Intern)
Assmann, Uwe (Ekstern)
Hansen, René Rydhof (Intern)

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

Relations
Publications:
An Adaptive Middleware for Improved Computational Performance
Project: PhD

SESAMO: Security and Safety Modelling

Technical University of Denmark
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**
Technical University of Denmark
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

**Adaptive Security in Energy Harvesting Wireless Sensor Networks**
Technical University of Denmark
Period: 15/08/2011 → 19/12/2014
Number of participants: 6
Phd Student:
Di Mauro, Alessio (Intern)
Supervisor:
Probst, Christian W. (Intern)
Main Supervisor:
Dragoni, Nicola (Intern)
Examiner:
Schoeberl, Martin (Intern)
Gaspari, Mauro (Ekstern)
Mazzara, Manuel (Ekstern)

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

**Resilient Infrastructure and Building Security**
Technical University of Denmark
Period: 15/12/2010 → 21/09/2015
Number of participants: 5
Phd Student: Ingwar, Mads Ingerslew (Intern)
Main Supervisor: Jensen, Christian D. (Intern)
Examiner: Probst, Christian W. (Intern)
Moeslund, Thomas (Ekstern)
Terzis, Sotirios (Ekstern)

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

Conflict Management in Aspect Policies
Technical University of Denmark
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

Round-trip Engineering of Service-Oriented Architectures
Department of Informatics and Mathematical Modeling
Period: 01/09/2010 → 22/11/2013
Number of participants: 6
Phd Student: Carvalho Quaresma, Jose Nuno (Intern)
Supervisor: Nielson, Flemming (Intern)
Main Supervisor: Probst, Christian W. (Intern)
Examiner: Dragoni, Nicola (Intern)
Gollmann, Dieter (Ekstern)
Kammüller, Florian (Ekstern)

Financing sources
Source: Internal funding (public)
Name of research programme: Institut stipendie (DTU)
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
Project: PhD
A Framework for Constraint-Programming based Configuration

Department of Informatics and Mathematical Modeling
Period: 01/03/2008 → 28/09/2011
Number of participants: 7
Phd Student:
Queva, Matthieu Stéphane Benoit (Intern)
 Supervisor:
Clausen, Jens (Intern)
Ricci, Laurent (Ekstern)
Main Supervisor:
Probst, Christian W. (Intern)
Examiner:
Fischer, Paul (Intern)
Felfernig, Alexander (Ekstern)
Hotz, Lothar (Ekstern)

Financing sources
Source: Internal funding (public)
Name of research programme: ErhvervsPhD-ordningen VTU
Project: PhD

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:
Nielsøn, 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
Project: PhD

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)

Financing sources
Tools for model-based software descriptions

Department of Informatics and Mathematical Modeling
Period: 01/02/2007 → 31/08/2011
Number of participants: 6
Phd Student:
Larsen, Per (Intern)
Supervisor:
Madsen, Jan (Intern)
Main Supervisor:
Karlsson, Sven (Intern)
Examiner:
Probst, Christian W. (Intern)
Cohen, Albert (Ekstern)
Stenström, Per (Ekstern)

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

Systemarkitekturer baseret på Network-on-Chip

Department of Informatics and Mathematical Modeling
Period: 01/10/2006 → 29/09/2010
Number of participants: 7
Phd Student:
Rasmussen, Morten Sleth (Intern)
Supervisor:
Karlsson, Sven (Intern)
Madsen, Jan (Intern)
Main Supervisor:
Sparsø, Jens (Intern)
Examiner:
Probst, Christian W. (Intern)
Grahn, Håkan (Ekstern)
Nurmi, Jari Antero (Ekstern)

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

Relations

Publications:
Support for Programming Models in Network-on-Chip-based Many-core Systems
Project: PhD