# Table of Contents

11th IEEE High Assurance Systems Engineering Symposium  
HASE 2008

**Message from the Chairs** ............................................................................................................................... x  
**Conference Organization and Committees** ......................................................................................................... xii  
**Reviewers** ................................................................................................................................................... xv

---

**Keynote Speech**

Path Sensitive Analysis for Security Flaws ................................................................................................................... 3  
*Mary Lou Soffa*

Transaction Calculus ..................................................................................................................................................... 4  
*Jifeng He*

Assurance Technology of System Test Based on Operators’ Aspects........................................................................... 5  
*Masayuki Matsumoto*

---

**System Security**

Security Goal Indicator Trees: A Model of Software Features that Supports  
Efficient Security Inspection ......................................................................................................................................... 9  
*Holger Peine, Marek Jawurek, and Stefan Mandel*

Low Cost Secure Computation for the General Client-Server Computation Model ................................................... 19  
*Liangliang Xiao, I-Ling Yen, and Farokh Bastani*

Evaluating Security Risks following a Compliance Perspective ................................................................................... 27  
*Reinaldo de Barros Correia, Luci Pirmez, and Luiz Fernando Rust da Costa Carmo*

---

**Network Security**

On the Comparison of Network Attack Datasets: An Empirical Analysis ................................................................. 39  
*Robin Berthier, Dave Korman, Michel Cukier, Matti Hiltunen, Gregg Vesonder, and Daniel Sheleheda*

On the Use of Security Metrics Based on Intrusion Prevention System Event Data:  
An Empirical Analysis................................................................................................................................................... 49  
*Danielle Chrzan, Michel Cukier, and Gerry Sneeringer*

The Deployment of a Darknet on an Organization-Wide Network: An Empirical Analysis.......................................... 59  
*Robin Berthier and Michel Cukier*
Distributed Systems

A Scalable Checkpoint Encoding Algorithm for Diskless Checkpointing ..............................................................71
Zizhong Chen and Jack Dongarra

HyperMIP: Hypervisor Controlled Mobile IP for Virtual Machine Live Migration across Networks .....................80
Qin Li, Jinpeng Huai, Jianxin Li, Tianyu Wo, and Minxiong Wen

Towards Secure Trust Bootstrapping in Pervasive Computing Environment ..........................................................89
Sheikh I. Ahamed, Endadul Hoque, Farzana Rahman, and Mohammad Zulkernine

Small Logs for Transactional Services: Distinction is Much More Accurate than (Positive) Discrimination .............97
Debmalya Biswas, Blaise Genest, and Thomas Gazagnaire

Embedded Systems

A Low Energy Soft Error-Tolerant Register File Architecture for Embedded Processors ......................................109
M. Fazeli, S.N. Ahmadian, and S.G. Miremadi

Randomization Based Probabilistic Approach to Detect Trojan Circuits .............................................................117
Susmit Jha and Sumit Kumar Jha

On the Integrity of Lightweight Checkpoints ........................................................................................................125
Raul Barbosa and Johan Karlsson

A Fast Performance Analysis Tool for Multicore, Multithreaded Communication Processors ...............................135
Hun Jung, Miao Ju, Hao Che, and Zhijun Wang

Formal Verification, Specification, and Implementation I

Random Relaxation Abstractions for Bounded Reachability Analysis of Linear Hybrid Automata: ..........................147
Sumit Kumar Jha and Susmit Jha

Distributed Randomized Abstractions in Model Checking ......................................................................................147
Sumit Kumar Jha and Susmit Jha

Formal Support for Quantitative Analysis of Residual Risks in Safety-Critical Systems ........................................154
Jonas Elmqvist and Simin Nadjm-Tehrani

A Few Remarks about Formal Development of Secure Systems ........................................................................165
Éric Jaeger and Thérèse Hardin

Formal Verification, Specification, and Implementation II

Verification of Exception Control Flows and Handlers Based on Architectural Scenarios .....................................177
Patrick Henrique da Silva Brito, Rogério de Lemos, and Cecília Mary Fischer Rubira

Localizing Program Errors via Slicing and Reasoning .........................................................................................187
Fei Pu and Yan Zhang

A Timed Extension of Property Sequence Chart ....................................................................................................197
Pengcheng Zhang, Bixin Li, and Mingjie Sun
## Testing

An Interaction-Based Test Sequence Generation Approach for Testing Web Applications ................................................. 209
-Wenhua Wang, Sreedevi Sampath, Yu Lei, and Raghu Kacker

Automated Generation of Test Cases from Contract-Oriented Specifications:
A CSP-Based Approach ......................................................................................................................................................... 219
-Hakim Belhaouari and Frederic Peschanski

Mutation-Based Testing of Format String Bugs ............................................................................................................. 229
-Hossain Shahriar and Mohammad Zulkernine

## Formal Verification, Specification, and Implementation III

Formally Sound Refinement of Spi Calculus Protocol Specifications into Java Code ................................................................. 241
-Alfredo Pironti and Riccardo Sisto

A Multi-Periodic Synchronous Data-Flow Language ........................................................................................................ 251
-Julien Forget, Frédéric Boniol, David Lesens, and Claire Pagetti

Aiding Modular Design and Verification of Safety-Critical Time-Triggered Systems
by Use of Executable Formal Specifications ................................................................................................................... 261
-Kohei Sakurai, Péter Bokor, and Neeraj Suri

## Quality, Reliability, and Safety

At What Level of Granularity Should We be Componentizing for Software Reliability? .......................................................... 273
-Atef Mohamed and Mohammad Zulkernine

A Comparative Study into Architecture-Based Safety Evaluation Methodologies
Using AADL’s Error Annex and Failure Propagation Models ........................................................................................................... 283
-Lars Grunske and Jun Han

Software Quality Improvement via Pattern-Based Model Refactoring..................................................................................... 293
-Dae-Kyoo Kim

A Novel Model for Component-Based Software Reliability Analysis ...................................................................................... 303
-Fan Zhang, Xingshe Zhou, Junwen Chen, and Yunwei Dong

## High Assurance Systems and Programs

Automotive Safety Case — A Qualitative Case Study of Drivers, Usages, and Issues ............................................................... 313
-Fredrik Törner and Peter Öhman

Detection and Diagnosis of Recurrent Faults in Software Systems by Invariant Analysis .......................................................... 323
-Miao Jiang, Mohammad A. Munawar, Thomas Reidemeister, and Paul A.S. Ward

Automated Discovery of Loop Invariants for High-Assurance Programs
Synthesized Using AI Planning Techniques .......................................................................................................................... 333
-Jicheng Fu, Farokh B. Bastani, and I-Ling Yen

Layered Memory Architecture for High IO Intensive Information Services to Achieve Timeliness ........................................ 343
-Hironao Takahashi, Hafiz Farooq Ahmad, and Kinji Mori
Ad Hoc Networks
Securing Sensor Nodes Against Side Channel Attacks ...............................................................353
  Kanthakumar Pongaliur, Zubin Abraham, Alex X. Liu, Li Xiao, and Leo Kempel
Power Optimization in Fault-Tolerant Mobile Ad Hoc Networks.................................................362
  Oliviero Riganelli, Radu Grosu, Samir R. Das, C.R. Ramakrishnan, and Scott A. Smolka

Data Management Systems
A Fine-Grained Damage Management Scheme in a Self-Healing PostgreSQL System ..............373
  Kun Bai and Peng Liu
Secure, Highly Available, and High Performance Peer-to-Peer Storage Systems..........................383
  Yunqi Ye, I-Ling Yen, Liangliang Xiao, and Bhavani Thuraisingham
Privacy, Preservation and Performance: The 3 P’s of Distributed Data Management ......................392
  Bobji Mungamuru and Hector Garcia-Molina

Service-Oriented Computing
A Novel Ripple-Based Context-Cognizant Service Discovery Method
in Autonomous Decentralized Community System .......................................................................405
  Khalid Mahmood, Satoshi Niki, Xiaodong Lu, and Kinji Mori
Architecture Centric System Design for Supporting Reconfiguration of Service Oriented Systems ....414
  Wang Chu and Depei Qian
A Self-Managing Brokerage Model for Quality Assurance in Service-Oriented Systems ..............424
  Daniel Robinson and Gerald Kotonya

Short Papers I
Formalize UML 2 Sequence Diagrams ..........................................................................................437
  Hui Shen, Aliya Virani, and Jianwei Niu
Towards the Service Composition Through Buses .........................................................................441
  Qin Li, Huibiao Zhu, and Jifeng He
Designing, Modelling and Verifying a Container Terminal System Using UPPAAL .......................445
  Quan Zu, Miaomiao Zhang, Jing Liu, and Qingfeng Du
A Grammar-Based Reverse Engineering Framework for Behavior Verification .............................449
  Chunying Zhao and Kang Zhang
Checking Inconsistency of Rule Sets in Active Real-Time Databases ............................................453
  Jian Zhang
An Integrated Model to Analyze Cryptographic Protocols with Colored Petri Nets .......................457
  Jin Wei, Guiping Su, and Meng Xu
Short Papers II

Reliability Design for Large Scale Storage Systems .................................................................463
   Kai Du, Huaimin Wang, Shuqiang Yang, Yingwen Chen, and Yan Wen

A New Fault-Tolerant Wormhole Routing Scheme in Tori with Convex Faults .............................467
   Lingfu Xie, Du Xu, Qing Yao, and Lei Song

Using Multi-Level Security Annotations to Improve Software Assurance ........................................471
   Eryk Kylikowski, Riccardo Scandariato, and Wouter Joosen

DPAC: A Reuse-Oriented Password Authentication Framework for Improving Password Security .................................................................475
   Hua Wang, Yao Guo, and Xiangqun Chen

Synopsis of Evaluating Security Controls Based on Key Performance Indicators and Stakeholder Mission Value .................................................................................................................................479
   Robert K. Abercrombie, Frederick T. Sheldon, and Ali Mili

Methodology for Service-Oriented Management of Security Assurance in Communication Infrastructures .................................................................................................................................483
   Albin Zuccato, Samuel Dubus, and Evren Bulut

Jasmine: A Tool for Model-Driven Runtime Verification with UML Behavioral Models ..................487
   Zhou Zhou, Linzhang Wang, Zhanqi Cui, Xin Chen, and Jianhua Zhao

Author Index ....................................................................................................................................... ........................491