

Proceedings

11th IEEE High Assurance Systems Engineering Symposium

*Nanjing, China
December 3 - 5, 2008*

Sponsored by

IEEE Computer Society

IEEE Reliability Society

Nanjing University



Los Alamitos, California

Washington • Tokyo



TABLE OF CONTENTS

Keynote Speech

Path Sensitive Analysis for Security Flaws	1
<i>Mary Lou Soffa</i>	
Transaction Calculus	2
<i>Jifeng He</i>	
Assurance Technology of System Test Based on Operators' Aspects	3
<i>Masayuki Matsumoto</i>	

System Security

Security Goal Indicator Trees: A Model of Software Features that Supports Efficient Security Inspection	4
<i>Holger Peine, Marek Jawurek, Stefan Mandel</i>	
Low Cost Secure Computation for the General Client-Server Computation Model	14
<i>Liangliang Xiao, I-Ling Yen, Farokh Bastani</i>	
Evaluating Security Risks Following a Compliance Perspective	22
<i>Reinaldo de Barros Correia, Luci Pirmez, Luiz Fernando Rust da Costa Carmo</i>	

Network Security

On the Comparison of Network Attack Datasets: An Empirical Analysis	32
<i>Robin Berthier, Dave Korman, Michel Cukier, Matti Hiltunen, Gregg Vesonder, Daniel Sheleheda</i>	
On the Use of Security Metrics Based on Intrusion Prevention System Event Data: An Empirical Analysis	42
<i>Danielle Chrun, Michel Cukier, Gerry Sneeringer</i>	
The Deployment of a Darknet on an Organization-Wide Network: An Empirical Analysis	52
<i>Robin Berthier, Michel Cukier</i>	

Distributed Systems

A Scalable Checkpoint Encoding Algorithm for Diskless Checkpointing	62
<i>Zizhong Chen, Jack Dongarra</i>	
HyperMIP: Hypervisor Controlled Mobile IP for Virtual Machine Live Migration Across Networks	71
<i>Qin Li, Jinpeng Huai, Jianxin Li, Tianyu Wo, Minxiong Wen</i>	
Towards Secure Trust Bootstrapping in Pervasive Computing Environment	80
<i>Sheikh I. Ahamed, Endadul Hoque, Farzana Rahman, Mohammad Zulkernine</i>	
Small Logs for Transactional Services: Distinction is Much More Accurate than (Positive) Discrimination	88
<i>Debmalya Biswas, Blaise Genest, Thomas Gazagnaire</i>	

Embedded Systems

A Low Energy Soft Error-Tolerant Register File Architecture for Embedded Processors	98
<i>M. Fazeli, S.N. Ahmadian, S.G. Miremadi</i>	

Randomization Based Probabilistic Approach to Detect Trojan Circuits	106
<i>Susmit Jha, Sumit Kumar Jha</i>	

On the Integrity of Lightweight Checkpoints	114
<i>Raul Barbosa, Johan Karlsson</i>	

A Fast Performance Analysis Tool for Multicore, Multithreaded Communication Processors	124
<i>Hun Jung, Miao Ju, Hao Che, Zhijun Wang</i>	

Formal Verification, Specification, and Implementation I

Random Relaxation Abstractions for Bounded Reachability Analysis of Linear Hybrid Automata: Distributed Randomized Abstractions in Model Checking	134
<i>Sumit Kumar Jha, Susmit Jha</i>	

Formal Support for Quantitative Analysis of Residual Risks in Safety-Critical Systems	141
<i>Jonas Elmqvist, Simin Nadjm-Tehrani</i>	

A Few Remarks about Formal Development of Secure Systems	152
<i>Éric Jaeger, Thérèse Hardin</i>	

Formal Verification, Specification, and Implementation II

Verification of Exception Control Flows and Handlers Based on Architectural Scenarios	162
<i>Patrick Henrique da Silva Brito, Rogério de Lemos, Cecília Mary Fischer Rubira</i>	

Localizing Program Errors via Slicing and Reasoning	172
<i>Fei Pu, Yan Zhang</i>	

A Timed Extension of Property Sequence Chart	182
<i>Pengcheng Zhang, Bixin Li, Mingjie Sun</i>	

Testing

An Interaction-Based Test Sequence Generation Approach for Testing Web Applications	192
<i>Wenhua Wang, Sreedevi Sampath, Yu Lei, Raghu Kacker</i>	

Automated Generation of Test Cases from Contract-Oriented Specifications: A CSP-Based Approach	202
<i>Hakim Belhaouari, Frederic Peschanski</i>	

Mutation-Based Testing of Format String Bugs	212
<i>Hossain Shahriar, Mohammad Zulkernine</i>	

Formal Verification, Specification, and Implementation III

Formally Sound Refinement of Spi Calculus Protocol Specifications into Java Code	222
<i>Alfredo Pironti, Riccardo Sisto</i>	

A Multi-Periodic Synchronous Data-Flow Language	232
<i>Julien Forget, Frédéric Boniol, David Lesens, Claire Pagetti</i>	

Aiding Modular Design and Verification of Safety-Critical Time-Triggered Systems by Use of Executable Formal Specifications	242
<i>Kohei Sakurai, Péter Bokor, Neeraj Suri</i>	

Quality, Reliability, and Safety

At What Level of Granularity Should We be Componentizing for Software Reliability?	252
<i>Atef Mohamed, Mohammad Zulkernine</i>	
A Comparative Study into Architecture-Based Safety Evaluation Methodologies Using AADL's Error Annex and Failure Propagation Models	262
<i>Lars Grunske, Jun Han</i>	
Software Quality Improvement via Pattern-Based Model Refactoring	272
<i>Dae-Kyoo Kim</i>	
A Novel Model for Component-Based Software Reliability Analysis	282
<i>Fan Zhang, Xingshe Zhou, Junwen Chen, Yunwei Dong</i>	

High Assurance Systems and Programs

Automotive Safety Case — A Qualitative Case Study of Drivers, Usages, and Issues	289
<i>Fredrik Törner, Peter Öhman</i>	
Detection and Diagnosis of Recurrent Faults in Software Systems by Invariant Analysis	299
<i>Miao Jiang, Mohammad A. Munawar, Thomas Reidemeister, Paul A.S. Ward</i>	
Automated Discovery of Loop Invariants for High-Assurance Programs Synthesized Using AI Planning Techniques	309
<i>Jicheng Fu, Farokh B. Bastani, I-Ling Yen</i>	
Layered Memory Architecture for High IO Intensive Information Services to Achieve Timeliness	319
<i>Hironao Takahashi, Hafiz Farooq Ahmad, Kinji Mori</i>	

Ad Hoc Networks

Securing Sensor Nodes Against Side Channel Attacks	326
<i>Kanthakumar Pongaliur, Zubin Abraham, Alex X. Liu, Li Xiao, Leo Kempel</i>	
Power Optimization in Fault-Tolerant Mobile Ad Hoc Networks	335
<i>Oliviero Riganelli, Radu Grosu, Samir R. Das, C.R. Ramakrishnan, Scott A. Smolka</i>	

Data Management Systems

A Fine-Grained Damage Management Scheme in a Self-Healing PostgreSQL System	344
<i>Kun Bai, Peng Liu</i>	
Secure, Highly Available, and High Performance Peer-to-Peer Storage Systems	354
<i>Yunqi Ye, I-Ling Yen, Liangliang Xiao, Bhavani Thuraisingham</i>	
Privacy, Preservation and Performance: The 3 P's of Distributed Data Management	363
<i>Bobji Mungamuru, Hector Garcia-Molina</i>	

Service-Oriented Computing

A Novel Ripple-Based Context-Cognizant Service Discovery Method in Autonomous Decentralized Community System	373
<i>Khalid Mahmood, Satoshi Niki, Xiaodong Lu, Kinji Mori</i>	
Architecture Centric System Design for Supporting Reconfiguration of Service Oriented Systems	382
<i>Wang Chu, Depei Qian</i>	

A Self-Managing Brokerage Model for Quality Assurance in Service-Oriented Systems	392
<i>Daniel Robinson, Gerald Kotonya</i>	

Short Papers I

Formalize UML 2 Sequence Diagrams	402
<i>Hui Shen, Aliya Virani, Jianwei Niu</i>	
Towards the Service Composition Through Buses	406
<i>Qin Li, Huibiao Zhu, Jifeng He</i>	
Designing, Modelling and Verifying a Container Terminal System Using UPPAAL	410
<i>Quan Zu, Miaomiao Zhang, Jing Liu, Qingfeng Du</i>	
A Grammar-Based Reverse Engineering Framework for Behavior Verification	414
<i>Chunying Zhao, Kang Zhang</i>	
Checking Inconsistency of Rule Sets in Active Real-Time Databases	418
<i>Jian Zhang</i>	
An Integrated Model to Analyze Cryptographic Protocols with Colored Petri Nets	422
<i>Jin Wei, Guiping Su, Meng Xu</i>	

Short Papers II

Reliability Design for Large Scale Storage Systems	426
<i>Kai Du, Huaimin Wang, Shuqiang Yang, Yingwen Chen, Yan Wen</i>	
A New Fault-Tolerant Wormhole Routing Scheme in Tori with Convex Faults	430
<i>Lingfu Xie, Du Xu, Qing Yao, Lei Song</i>	
Using Multi-Level Security Annotations to Improve Software Assurance	434
<i>Eryk Kylikowski, Riccardo Scandariato, Wouter Joosen</i>	
DPAC: A Reuse-Oriented Password Authentication Framework for Improving Password Security	438
<i>Hua Wang, Yao Guo, Xiangqun Chen</i>	
Synopsis of Evaluating Security Controls Based on Key Performance Indicators and Stakeholder Mission Value	442
<i>Robert K. Abercrombie, Frederick T. Sheldon, Ali Mili</i>	
Methodology for Service-Oriented Management of Security Assurance in Communication Infrastructures	446
<i>Albin Zuccato, Samuel Dubus, Evren Bulut</i>	
Jasmine: A Tool for Model-Driven Runtime Verification with UML Behavioral Models	450
<i>Zhou Zhou, Linzhang Wang, Zhanqi Cui, Xin Chen, Jianhua Zhao</i>	

Author Index