Model Checking Safety and Security Systems

Time: 26-27 May 2010

Venue: National University of Singapore, Computing 1, Seminar Room 8

Software Bugs are Costly

- Intel Pentium II chip, released in 1994 produced error in floating point division. **Cost:$475 million**
- Ariane 5 failure: In December 1996, the Ariane 5 rocket exploded 40 seconds after takeoff, by an overflow generated by converting a 64-bit floating-point number into a 16-bit integer. **Cost: $400 million**
- Therac-25 accident: A software failure caused wrong dosages of x-rays. **Cost: Human Loss.**

With the rapid development of IT industry, our reliance on the functioning of software systems is growing rapidly. These systems are becoming more and more complicated and are massively encroaching on daily life. Failure is unacceptable for safety critical systems like electronic commerce, telephone switching networks, air traffic control systems, medical instruments, and numerous other examples. We frequently read of incidents where catastrophic failure is caused by an error in software systems.

Clearly, the need for reliable software systems is crucial. As the involvement of such systems in our lives increases, so does the burden for ensuring their correctness. Therefore, it will become more important to develop methods that increase our confident in the correctness of such systems.

This 2-day training course will focus on the software verification and validation methods to ensure the correctness of safety and security systems, especially using formal methods and model checking techniques. The course will cover the basic knowledge of formal methods and model checking. Participants will get hand-by-hand training of system modeling, simulation and verification using the state-of-the-art model checker PAT. This course also allows you to take any of the two days based on your interests and background.

Register Now

CRITICAL ISSUES &

CHALLENGES TO BE CONSIDERED…

What is formal method and why is it important in software development?

What is software validation and verification and why do we need it?

What are the available software verification techniques and tools?

How to model and verify critical and security systems?

PLUS! HANDS-ON EXERCISES on verifying systems that you are interested.

This practical course will go beyond just theory. It will be delivered through a series of real-world case studies and exercises using PAT tool to let you be ready for verify your own programs.

Model Checking Safety and Security Systems

1 Software Verification is Useful

The principal validation methods for software are simulation, testing, deductive verification, and model checking. Model checking is a push-button method to **automatically** verifying systems properties. The process of model checking can be separated into system modeling, requirement specification and verification. It has a number of advantages over other traditional approaches. This method has been used successfully in practice to verify complex circuit design and communication protocols.

- Windows 7 Hardware Drivers are verified using **Blast**
- Intel i7 CPU is verified using model checking without a single test case

2 Verify your own applications

Software verification is a cool technology, but how to use it in your own application and systems? Our experts will teach you the basic concepts and get your hand on the front research tools using real-world examples.

Attend this interactive 2-day course to obtain in-depth knowledge of software verification and start to verify your own applications

Who Should Attend

This course is specially designed for Senior Software Developers, System Architecture, System Designer and Analysts involved in:

- Safety-critical Software Development
- Cyber/IT/Network/Computer Security
- System Analysis, Testing and Verification

Lead Trainers

Dr. DONG, Jin Song
Associate Professor
NGS PhD Supervisor
School of Computing,
National University of Singapore

Dr. DONG Jin Song received Bachelor and PhD degrees in computing from the University of Queensland (UQ) in 1992 and 1996. He was the winner of the Richard Jago Memorial Prize and Australian Postgraduate Award. From 1995-1998, he was a Research Scientist at the Commonwealth Scientific and Industrial Research Organization (CSIRO) in Australia. Since 1998 he has been in the School of Computing at the National University of Singapore (NUS) where he is currently Associate Professor and PhD Supervisor at NUS Graduate School (NGS). He has won 2004 NUS Young Researcher Award. Jin Song has 100+ international refereed publications in areas of formal methods and software engineering. He is a steering committee member of the International Conference on Formal Engineering Methods (ICFEM) and the Asia Pacific Software engineering Conference (APSEC) series. Jin Song is General/Program Chairs for a number of international conferences and he is also on the editorial board of Formal Aspects of Computing journal and Innovations in Systems and Software Engineering, A NASA Journal. He has been teaching advanced software engineering and formal methods courses for decades.

This course will be jointly conducted with Dr. SUN Jun (LKY Postdoc) and Dr. LIU Yang (Research Associate) from NUS.

Dr. SUN Jun received Bachelor and PhD degree in School of Computing, National University of Singapore (NUS) in 2002 and 2006. Since 2006, he was named a Lee Kuan Yew Postdoctoral fellow at Department of Computer Science, NUS. His research interests are mainly in formal system specification, verification and synthesis. Recently, he founded the PAT framework for model checking. He has more than 40 publications, including articles in IEEE Trans. on SE and ACM Trans. on SE as well as papers in CAV, ICSE and FM.

Dr. LIU Yang received Bachelor and PhD degree in School of Computing, National University of Singapore (NUS) in 2005 and 2010. Since then, he is working as a research associate in NUS on the software verification as the main member in the PAT team. He graduated with 2nd best student for Bachelor degree and the research work won him Microsoft Asia Research Fellowship 2007, Research Achievement Award 2008/2009 and Dean's Graduate Research Excellence Award 2009/2010.

Model Checking Safety and Security Systems

Course Outline

Day 1 Morning:
Introduction to Formal Method

Introduction to formal method specifications and verifications

1. Usages and limitations
   - Brief discussion on industrial/real life examples
2. Formal validation methods
   - Theorem Provers
   - Model Checking
3. Overview and comparison of available tools
4. Introduction to Event based formalism
   - Event, Process and Communications

Day 1 Afternoon:
Introduction to PAT

1. Introduction to PAT
2. The features of PAT
3. The modeling languages supported by PAT
4. Hand-on experiences of using PAT

Day 2 Mornings:
Introduction to Safety and Security Systems

1. Safety and security systems with
   a. Current behaviors
   b. Real-time behaviors
   c. Probabilistic behaviors
2. Modeling of security protocols

Day 2 Afternoon:
Verification of Safety and Security Systems by examples

1. Distributed Systems
   a. Leader Election Algorithms
   b. Shared Stack/Queue
2. Real-time system
   a. A real-time pacemaker
3. Probabilistic system
4. Security Protocols
   a. SSL Protocol
      i. Security Bug
      ii. Verification and Bug fixing

About PAT

Process Analysis Toolkit (**PAT**) is a self-contained framework to support composing, simulating and reasoning of concurrent, real-time and probabilistic systems. PAT implements the state-of-the-art model checking techniques catering for checking deadlock-freeness, reachability, LTL checking, refinement checking and etc. PAT adopts an extensible design, which allows new languages and verification algorithms to be supported easily. Currently, four modules have been developed in PAT. The experiment results show that PAT is capable of verifying systems with large number of states and complements the state-of-the-art model checkers in several aspects.

Model Checking Safety and Security Systems

Registration Form

1 COURSE PRICES

PLEASE ☑ THE APPROPRIATE BOX.

INDIVIDUAL STANDARD PRICE

☐ Individual — S$ 700 (reduced price from S$1,400)

☐ Individual (1-day Course) — S$ 350 (for people who want to attend just the 1st day or just the 2nd day, e.g., participants on the previous verification course may just attend the 2nd day)

GROUP DISCOUNTED PRICES

☐ Group of 3 — S$ 665 per person

☐ Group of 5 — S$ 644 per person

* Course documents, refreshment & lunches are included. Travel and accommodation are NOT included.
* All registration fees are used to support the fourth IEEE International Conference on Secure Software Integration and Reliability Improvement (SSIRI 2010) held in Singapore.

2 DELEGATE DETAILS

PLEASE PHOTOCOPY FOR ADDITIONAL DELEGATES AND/OR DELEGATE WITH DIFFERENT ADDRESSES.

ORGANISATION: _____

DELEGATE 1 ☐ Mr ☐ Mrs ☐ Ms ☐ Dr ☐ Others ☐ Rank _____

First Name: _____ Last Name: _____

Job Title: _____ Department: _____

Email: _____ Phone: _____

DELEGATE 2 ☐ Mr ☐ Mrs ☐ Ms ☐ Dr ☐ Others ☐ Rank _____

First Name: _____ Last Name: _____

Job Title: _____ Department: _____

Email: _____ Phone: _____

DELEGATE 3 ☐ Mr ☐ Mrs ☐ Ms ☐ Dr ☐ Others ☐ Rank _____

First Name: _____ Last Name: _____

Job Title: _____ Department: _____

Email: _____ Phone: _____

PAYMENT / INVOICE CONTACT DETAILS

First Name: _____ Last Name: _____

Job Title: _____ Department: _____

Email: _____ Phone: _____ Fax: _____

Mailing Address: _____

Postal Code: _____ Country: _____

Signature: _____ Date: _____

How to Register

You can pay by **credit card** by filling up the following form.
For other ways of payment (e.g., **bank transfer, cheque**), please contact Registration Chair **Dr. Yang LIU** by
Tel: (+65) 6516 1510
Email: liuyang@comp.nus.edu.sg

GROUP SAVER DISCOUNTS

Learn as a team and enjoy greater saving. Discounts apply only to group bookings from the same organisation at the same time.

- Group of 3 or more: 5%
- Group of 5 or more: 8%

Payment by Credit Card

I, Cardholder's name:

_____, authorize SSIRI 2010 to charge my Credit Card:

- ☐ VISA ☐ MasterCard
- Credit card number:

  _____

  Expiration date (month/year):
  _____/_____
- Security code: _____ (the 3 last numbers on the back of credit card)

for the total amount (in SGD):

_____

Date (day/month/year):
_____/_____/_____

Cardholder Signature :

_____

Pre-Conference Course of SSIRI 2010