Fang Yu

Assistant Professor
Software Security Laboratory
Dept. of Management Information Systems
College of Commerce
National Chengchi University
64 Sec 2, Zhinan Rd.
Taipei City 11605, Taiwan R.O.C.

Home Address:
2F 71 Tong-Bei St.
Taipei City 104, Taiwan R.O.C.
Phone: +886-2-8237-7453
yuf at nccu.edu.tw
http://soslab.nccu.edu.tw

Education

- University of California at Santa Barbara, CA, U.S.
  Ph.D./M.S., Department of Computer Science, June 2010.
  Advisor: Prof. Tevfik Bultan
  Thesis: *Automatic Verification of String Manipulating Programs.*
  ACM Doctoral Dissertation Award Nomination.
- National Taiwan University, Taipei, Taiwan
  M.B.A./B.B.A., Department of Information Management, June 2000.

Work experience

- Fall 2010-Present: Assistant Professor, Dept. of Management Information Systems, National Chengchi University.
- Fall 2006- Summer 2010: Research Assistant under the supervision of Prof. Tevfik Bultan, Dept. of Computer Science, University of California at Santa Barbara.
- Summer 2008: Intern, NEC Laboratories America, Inc. Princeton, NJ. Project: Thread-sensitive Concurrent Data Flow analysis, supervised by Chao Wang.
- Summer 2007: Intern, NEC Laboratories America, Inc. Princeton, NJ. Project: Modular Verification of Web Service Composition, supervised by Chao Wang.
- Fall 2005-Spring 2006: Teaching Assistant, Dept. of Computer Science, University of California at Santa Barbara.
- 2001–2005: Research Assistant, Institute of Information Science, Academia Sinica
- Spring 2004, 2005: Lecturer, Taiwan National Representatives of the International Olympiad in Informatics

Research interests

- String Analysis
- Model Checking
- App/Web/Cloud Security
- Software/Hardware Verification

Awards and Honors

- The 2010 ACM Doctoral Dissertation Award Nomination by UCSB
- 2010: The Outstanding Dissertation Award in Computer Science, UCSB
- 2008-2009: UCSB Deans Fellowship
- 2009: ETAPS Scholarship
- 2008: The SIGSOFT-CAPS Graduate Student Travel Support
- 2008: Adobe Best Paper Award, the 3rd UCSB Graduate Student Workshop on Computing
- 2004: Best Paper Nominee, the 13th World Wide Web Conference

Services

- ◇ Program Co-chair/Committee of the 13th International Workshop on Verification of Infinite State Systems (INFINITY'11)
- ◇ Program Committee of the 9th International Symposium on Automated Technology for Verification and Analysis (ATVA'11)
- ◇ Program Committee of the 3rd/4th UCSB Graduate Student Workshop on Computing (GSWC'08, GSWC'09)
- ◇ Organizing Committee of the 10th International Conference on Developments in Language Theory (DLT'06)

Papers at referred conferences

- ◇ *Symbolic Consistency Checking of OpenMp Parallel Programs*
  Fang Yu, Shun-Ching Yang, Farn Wang, Guan-Cheng Chen, and Che-Chang Chan.
  To appear in the Proceedings of the 15th ACM SIGPLAN/SIGBED Conference on Languages, Compilers, Tools and Theory for Embedded Systems (LCTES 2012), Beijing, China, June 2012.
- ◇ *Enumeration of Reachable and Other States of Simple Version of Systems of Simple Sequential Processes with Resources (S3PR)*
  Daniel Y. Chao, Hung-Yi Chen and Fang Yu.
  To appear in the Proceedings of the 21th IEEE International Symposium on Industrial Electronics (ISIE 2012), Hangzhou, China, May 2012.
- ◇ *Number of Reachable States for Simple Classes of Petri Nets*
  Daniel Y. Chao and Fang Yu.
  In Proceedings of the 37th Annual Conference of the IEEE Industrial Electronics Society (IECON 2011), Melbourne, Australia, Nov. 2011.
- ◇ *A Temporal Logic for the Interaction of Strategies*
  Farn Wang, Chung-Hao Huang and Fang Yu.
  In Proceedings of the 22nd International Conference on Concurrency Theory (CONCUR 2011), Aachen, Germany, Sep. 2011.
- ◇ *String Abstractions for String Verification*
  Fang Yu, Tevfik Bultan and Ben Hardekopf.
  In Proceedings of the 18th International SPIN Workshop on Model Checking of Software (SPIN 2011), Utah, U.S., July 2011.
- ◇ *Patching Vulnerabilities with Sanitization Synthesis*
  Fang Yu, Muath Alkhalaf and Tevfik Bultan.
  In Proceedings of the 33th International Conference on Software Engineering (ICSE 2011), Honolulu, U.S., May 2011.
- ◇ *Relational String Verification Using Multi-Track Automata*
  Fang Yu, Tevfik Bultan and Oscar H. Ibarra.
  In Proceedings of the 15th International Conference on Implementation and Application of Automata (CIAA 2010), LNCS, pages. 290-299.
- ◇ *Modular Verification of Synchronization with Reentrant Locks*
  Tevfik Bultan, Fang Yu and Aysu Betin Can.
  In Proceedings of the 8th ACM/IEEE International Conference on Formal Methods and Models for Codesign (MEMOCODE 2010), pages 59-68.
- ◇ *Stranger: An Automata-based String Analysis Tool for PHP*
  Fang Yu, Muath Alkhalaf, and Tevfik Bultan.
  Tool paper. In Proceedings of the 16th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2010), pages 154-157.
- ◇ *Generating Vulnerability Signatures for String Manipulating Programs Using Automata-based Forward and Backward Symbolic Analyses*
  Fang Yu, Muath Alkhalaf, and Tevfik Bultan.

Short paper. In Proceedings of the 24th IEEE/ACM International Conference on Automated Software Engineering (ASE 2009), pages 605-609.

◇ *Symbolic String Verification: Combining String Analysis and Size Analysis*
Fang Yu, Tevfik Bultan, and Oscar H. Ibarra.
In Proceedings of the 15th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2009), LNCS 5505, pages 322-336, York, UK, Mar. 2009.

◇ *Modular Verification of Web Services Using Efficient Symbolic Encoding and Summarization*
Fang Yu, Chao Wang, Aarti Gupta, and Tevfik Bultan.
In Proceedings of the 16th ACM SIGSOFT Symposium on Foundations of Software Engineering (SIGSOFT 2008/FSE 16), pages 192-202, Atlanta, GA, Nov. 2008.

◇ *Symbolic String Verification: An Automata-based Approach*
Fang Yu, Tevfik Bultan, Marco Cova, Oscar H. Ibarra.
In Proceedings of the 15th International SPIN Workshop on Model Checking of Software (SPIN 2008), LNCS 5156, pages 306-324, Los Angeles, CA, August 2008.

◇ *Automated Size Analysis for OCL*
Fang Yu, Tevfik Bultan, Erik Peterson.
In Proceedings of the 6th joint meeting of the European Software Engineering Conference and the ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC/FSE 2007). pp. 331-340, Dubrovnik, Croatia, Sep. 2007.

◇ *On Spiking Neural P Systems and Partially Blind Counter Machines*
Oscar H. Ibarra, Sara Woodworth, Fang Yu, Andri Paun.
In Proceedings of the 5th International Conference on Unconventional Computation (UC 2006), York, UK, Sep. 2006.

◇ *Efficient Exact Spare Allocation via Boolean Satisfiability*
Fang Yu, Chung-Hung Tsai, Yaw-Wen Huang, Hung-Yau Lin, Der-Tsai Lee, Sy-yen Kuo.
In Proceedings of the 20th IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems (DFT 2005), pages 361-370, Monterey, CA, Oct. 2005.

◇ *Toward Unbounded Model Checking for Region Automata.*
Fang Yu and Bow-Yaw Wang.
In Proceedings of the 2nd International Symposium on Automated Technology for Verification and Analysis (ATVA 2004), LNCS 3299, pages 20-33, Taipei, Taiwan, Oct 2004.

◇ *Bounded Model Checking for Region Automata.*
Fang Yu, Bow-Yaw Wang and Yaw-Wen Huang.
In Proceedings of the Joint Conference on Formal Modelling and Analysis of Timed Systems and Formal Techniques in Real-Time and Fault Tolerant System (FORMATS-FTRTFT 2004), LNCS 3253, pages 246-262, Grenoble, France, Sep 2004.

◇ *Verifying Web Applications Using Bounded Model Checking.*
Yao-Wen Huang, Fang Yu, Christian Hang, Chung-Hung Tsai, Der-Tsai Lee, Sy-Yen Kuo.
In Proceedings of the 2004 International Conference on Dependable Systems and Networks (DSN 2004), pages 199-208, Florence, Italy, Jun 2004.

◇ *Securing Web Application Code by Static Analysis and Runtime Protection.*
Yao-Wen Huang, Fang Yu, Christian Hang, Chung-Hung Tsai, Der-Tsai Lee, Sy-Yen Kuo.
In Proceedings of the 13th International World Wide Web Conference (WWW 2004), pages 40-52, New York, May 2004.
Best Paper Nominee.

◇ *Numerical Coverage Estimation for the Symbolic Simulation of Real-Time Systems.*
Farn Wang, Geng-Dian Huang, and Fang Yu.
In: Proceedings of the 23rd IFIP International Conference on Formal Techniques for Networked and Distributed Systems (FORTE 2003), LNCS 2767, Berlin, Sept.-Oct. 2003.

◇ *TCTL Inevitability Analysis of Dense-time Systems.*
Farn Wang, Geng-Dian Huang, and Fang Yu.
In: Proceedings of the 8th International Conference on Implementation and Application of Automata (CIAA 2003), LNCS 2759, July 2003.

◇ *OVL Assertion Checking of Embedded Software with Dense-Time Semantics.*
Farn Wang and Fang Yu.
In: Proceedings of the 9th International Conference on Real-Time and Embedded Computing Systems and Applications (RTCSA 2003), LNCS 2968, February 2003.

◇ *Symbolic Simulation of Real-Time Concurrent Systems.*
Farn Wang, Geng-Dian Huang, and Fang Yu.
In: Proceedings of the 9th International Conference on Real-Time and Embedded Computing Systems and Applications (RTCSA 2003), LNCS 2968, February 2003.

Papers in referred journals

◇ *A Novel Liveness Condition for S3PGR2*
Daniel Y. Chao, Jiun-Ting Chen, Fang Yu.
Transactions of the Institute of Measurement and Control (TIM)(SCIE), Feb. 2012.

◇ *Relational String Verification Using Multi-track Automata*
Fang Yu, Tevfik Bultan, Oscar H. Ibarra.
International Journal of Foundations of Computer Science (IJFCS) (SCIE), Vol 22 (8), pp. 1909-1924, 2011.

◇ *On Spiking Neural P Systems and Partially Blind Counter Machines*
Oscar H. Ibarra, Sara Woodworth, Fang Yu, Andri Paun.
Natural Computing (NC) (SCIE), Vol. 7, Issue 1, pp. 3-19, March 2008.

◇ *SAT-based Model Checking for Region Automata*
Fang Yu and Bow-Yaw Wang.
The International Journal of Foundations of Computer Science (IJFCS)(SCIE), Vol. 17, No. 4, pp. 775-796, August 2006.

◇ *TCTL Inevitability Analysis of Dense-time Systems: from Theory to Engineering*
Farn Wang, Geng-Dian Huang and Fang Yu.
IEEE Transactions on Software Engineering (TSE)(SCI), Vol. 32, No. 7, pp. 510-526. July 2006. ISSN: 0098-5589 2006.

◇ *BDD-based Safety Analysis of Concurrent Software with Pointer Data Structures using Graph Automorphism Symmetry Reduction.*
Farn Wang, K. Schmidt, Fang Yu, Geng-Dian Huang, Bow-Yaw Wang.
IEEE Transactions on Software Engineering (TSE)(SCI), Vol. 30, No. 6, pp. 403-417, June 2004.

◇ *Symbolic Simulation of Industrial Real-Time and Embedded Systems - Experiments with the Bluetooth baseband communication protocol.*
Farn Wang, Geng-Dian Huang, Fang Yu.
Journal of Embedded Computing (JEC), Cambridge International Science Publishing, Vol. 1, No. 1, 2004.

Patents

◇ *Modular Verication of Web Services Using Efficient Symbolic Encoding and Summarization*
Chao Wang, Fang Yu, Aarti Gupta.
US Patent, Pending, Filed on Mar. 3, 2008, No. 61/033126.

◇ *Systems and Methods for Securing Web Application Code*
Yao-Wen Huang, Fang Yu, Christian Hang, Chung-Hung Tsai, Der-Tsai Lee, Sy-Yen Kuo.
US Patent, Application, No. 20070074188, Mar. 2007.

Research Projects and Tools

◇ 2010 Fall-Present: Automatic Detection and Removal of Web Application Vulnerabilities (NSC 99-2218-E-004-002-MY3)
PI: Fang Yu

This is an NSC granted project- PI: Fang Yu, NT1600,000 , 2010/11- 2013/7. Most critical security vulnerabilities in web applications are caused by inadequate manipulation of nput strings.We investigate symbolic string verification techniques with the aim of developing a formal approach for automatic detection and removal of string related vulnerabilities in Web applications. The main topics include: sanitization synthesis, abstraction, and scalable service development. Parts of the results have been published in international conferences and journals. (ICSE 2011, SPIN 2011, IJFCS 2011)

◇ 2007 Fall-2010 Fall: Symbolic String Verification
Supervisor: Prof. Tevfik Bultan
Collaborators: Prof. Oscar H. Ibarra, Muath Alkhalaf, and Marco Cova
String analysis is a static analysis technique that determines the string values that a variable can hold at specific points in a program. We develop an automata-based string analyzer, called Stranger, to detect and prevent string related web application vulnerabilities, e.g., XSS, SQLCI, MFE attacks. Stranger combines forward and backward symbolic reachability analyses and generates string-based vulnerability signatures, i.e., a characterization that includes all malicious inputs that can be used to generate attacks. Stranger takes advantage on symbolic representation of automata, which allows the practical handling of automata on very large alphabets. Stranger also incorporates various novel approximation techniques and targets on proving the correctness of secured web applications efficiently. We later extend this automata-based approach to verify systems having both string and integer variables. By exchanging length information between string and arithmetic automata, we improve precision of both string and size analysis. Recently, we investigate the essence of string systems, and show the decidability/undecidability results for verification of various string systems. We also investigate relational string analysis and apply the techniques for sanitization synthesis. Finally, we use summarization and abstraction techniques to further facilitate our approach. (SPIN 2008, TACAS 2009, ASE 2009, TACAS 2010, CIAA 2010)

◇ 2008 Summer: Thread-sensitive Concurrent Data Flow Analysis
Supervisor: Dr. Chao Wang
We propose a thread-sensitive concurrent data flow analysis using static single assignments, of which state propagation follows causality consistency. We apply our technique to perform precise constant propagation/code elimination on concurrent C programs, and reduce costs on verifying those programs.

◇ 2007 Summer: Scalable Verification of Service Composition
Supervisor: Dr. Chao Wang
We propose a novel method for modular verification of BPEL service composition. We first derive pre and post conditions for well defined web services based on infinite state model checking techniques. The derived pre and post conditions can be collected and served as the summarization of web services. Modular verification, by composing the summarization of external invocations, can then be applied to achieve scalable verification. (FSE 2008)

◇ 2006 Fall-2007 Winter: Size Analysis
Supervisor: Prof. Tevfik Bultan
Collaborator: Erik Peterson
We aim to verify specifications of object oriented systems based on infinite state model checking techniques. We target on object constraint language and propose size abstraction and size analysis. We conducted a case study on the OCL specifications of Java Card APIs. The experiments indicate our abstraction is precise enough to verify/falsify essential properties, e.g., invariant consistency, while coarse enough to perform complex model checking techniques efficiently. (FSE 2007)

◇ 2006: Characterizing Spiking Neural P Systems
Supervisors: Prof. Oscar H. Ibarra
Collaborators: Sara Woodworth and Andri Paun
Neurons are arguably one of the most interesting cell-types in the human body. A large number of neurons working in a cooperative manner are able to perform tasks that are

not yet matched by the tools we can build with our current technology. Spiking Neuron P-systems(SNPs) incorporate ideas from spiking neurons into membrane computing. In this project, we give characterizations of sets definable by partially blind multicounter machines in terms of k-output SNPs operating in a sequential mode. (UC 2006, NC 2008)

◇ 2004-2005: Spare Allocation
Supervisors: Prof. Der-Tsai Lee and Prof. Sy-Yen Kuo
Collaborators: Yaw-Wen Huang and Chung-Hung Tsai
Fabricating large memory and processor arrays is subject to physical failures resulting in yield degradation. The strategy of incorporating spare rows and columns to obtain reasonable production yields was first proposed in the 1970s, and continues to serve as an important role in recent VLSI developments. Since the spare allocation problem (SAP) is NP-complete but requires solving during fabrication, an efficient exact spare allocation algorithm has great value. In this project, we proposed a novel Boolean encoding to reduce exact SAP to the satisfiablity problem, so that we can leverage the capability of modern SAT solvers. (DFT 2005)

◇ 2002-2005: Web Security (WebSARRI)
Supervisors: Prof. Der-Tsai Lee and Prof. Sy-Yen Kuo
Collaborators: Yaw-Wen Huang, Christian Hang, and Chung-Hung Tsai
WebSSARI, a joint project between Academia Sinica and National Taiwan University, stands for Web application security via Static Analysis and Runtime Inspection. Viewing Web application vulnerabilities as a secure information flow problem, we created a lattice-based static analysis algorithm derived from type systems and typestate. During the analysis, sections of code considered vulnerable are instrumented with runtime guards, thus securing Web applications in the absence of user intervention. Soundness, i.e no false negative, is achieved by applying formal methods including typestate checking and bounded model checking. I worked on designing and developing core checkers including: (1) A Light-weight Type Checker (WWW 2004), and (2) A Heavy-weight Bounded Model Checker (DSN 2004).

◇ 2003-2005: SAT-based Model Checking (xBMC)
Supervisor: Dr. Bow-Yaw Wang
We take advantage on SAT-solvers' capability to support formal verification of discrete/real-time systems. We extend SAT-based bounded model checking techniques to verification of dense-time systems. We discrete dense-time systems using region automata and incorporate induction to prove system correctness. (FORMATS-FTRTFT 2004, ATVA 2004, IJFCS 2006).

◇ 2002-2004: TCTL Model Checking (RED 4.0)
Supervisor: Prof. Farn Wang
Collaborator: Geng-Dian Huang
I was involved in designing and developing *RED 4.0* on top of *RED*, the full Timed-CTL symbolic model checker initiated by Prof. Farn Wang. *RED 4.0* enhanced *RED* in the following directions: (1) Symbolic Simulation (RTCSA 2003), (2) Numerical Coverage Estimation (FORTE 2003), (3) Efficient Greatest Fixpoint Computation (CIAA 2003, IEEE TSE 2006), and (4) Symmetric Analysis with Pointer Data Structure (IEEE TSE 2004).

◇ 2001-2002: Optimized Translation (*time*C)
Supervisor: Prof. Farn Wang
We propose a formal approach to verify real-time systems specified in *time*C. *time*C is a C-like language that combines basic C statements with timed statements and Open Verification Library (OVL) assertions. I developed an optimized translator that automatically translates *time*C+OVL assertions to timed automata+TCTL formula specified as the input language of *RED*. (RTCSA 2003)

References

Prof. Tevfik Bultan
Professor, the Department of Computer Science, University of California, Santa Barbara
`bultan at cs.ucsb.edu`

Address: Department of Computer Science University of California Santa Barbara, CA 93106-5110

Prof. Oscar H. Ibarra
IEEE Fellow, ACM Fellow, AAAS Fellow
Professor, the Department of Computer Science, University of California, Santa Barbara
ibarra at cs.ucsb.edu
Address: Department of Computer Science University of California Santa Barbara, CA 93106-5110

Dr. Chao Wang
Research Staff Member, NEC Laboratories America
chaowang at nec-labs.com
Address: 4 Independence way, suite 200 Princeton, NJ 08540, USA

Prof. Farn Wang
Professor, the Department of Electrical Engineering, National Taiwan University
farn at cc.ee.ntu.edu.tw
Address: National Taiwan University. BL 616. Nr.1, Sec. 4, Roosevelt Rd. Taipei, Taiwan 106, ROC

Dr. Bow-Yaw Wang
Associate Research Fellow, the Institute of Information Science, Academia Sinica
bywang at iis.sinica.edu.tw
Address: 128 Sec 2 Academia Rd Taipei 115, Taiwan