Dr. Van-Thuan Pham

Address	COM1, 13 Computing Drive Singapore 117417	**Email**	thuanpv@comp.nus.edu.sg
		Homepage	http://comp.nus.edu.sg/~thuanpv
Contact number	+65 9352 1211	**Linkedin profile**	www.linkedin.com/in/thuanpv

Summary

Van-Thuan Pham is working at NUS (as a Research Fellow) and he is the Technology Lead of Test1080, a deep-tech startup from NUS which provides an automated mobile testing solution based on a patented technology. He is passionate about doing R&D on automated testing to improve the reliability of software systems running on all types of computing devices such as embedded systems, mobile devices, personal computers and servers. Currently, he is working on (security) testing for Android apps and device drivers. He has just finished his PhD studies at NUS. In his thesis work, he designed and developed enhanced fuzz testing techniques (black-box, coverage-based grey-box and symbolic-execution based white-box fuzzing) and applied these techniques to vulnerability detection, crash reproduction and debugging. Beside his academic research work, he also has experiences in working and collaborating with industry in other projects in embedded systems, image processing, manufacturing management systems and simulation.

Education

2012-2017 Doctor of Philosophy in Computer Science - National University of Singapore

Thesis: Enhancing Directed Search in Black-box, Grey-box and White-box Fuzz Testing

2007-2009 Master in Information Processing and Communications - Hanoi University of Technology

Thesis: Optimizing routing protocol for wireless sensor network

2002-2007 Engineer in Information Technology - Hanoi University of Technology

Thesis: Designing image processing algorithms for automatic steel bar counting
First Class Honours - ranked 2/57

Publications

- **Directed Greybox Fuzzing**
  Marcel Böhme, Van-Thuan Pham, Manh-Dung Nguyen and Abhik Roychoudhury
  (One-line abstract) Directed Fuzzing without expensive program analysis
  ACM Conference on Computer and Communications Security (CCS) 2017

- **Bucketing Failing Tests via Symbolic Analysis**
  Van-Thuan Pham, Sakaar Khurana, Subhajit Roy and Abhik Roychoudhury
  (One-line abstract) Remarkably reduce number of failing tests to be debugged
  International Conference on Fundamental Approaches to Software Engineering (FASE) 2017

- **Coverage-based Greybox Fuzzing as Markov Chain**
  Marcel Böhme, Van-Thuan Pham and Abhik Roychoudhury
  (One-line abstract) Effective path exploration without program analysis
  ACM Conference on Computer and Communications Security (CCS) 2016

- **Model-based Whitebox Fuzzing for Program Binaries**
  Van-Thuan Pham, Marcel Böhme and Abhik Roychoudhury
  (One-line abstract) Hybrid fuzzing for programs taking complex file inputs (e.g, PDF or PNG)
  IEEE/ACM International Conference on Automated Software Engineering (ASE) 2016

- **Hercules: Reproducing Crashes in Real-World Application Binaries**
  Van-Thuan Pham, Wei Boon Ng, Konstantin Rubinov and Abhik Roychoudhury
  (One-line abstract) Symbolic execution for multi-module program binaries (e.g, Adobe Reader)
  ACM/IEEE International Conference on Software Engineering (ICSE) 2015

- **Integrated Timing Analysis of Application and Operating Systems Code**
  Lee Kee Chong, Clement Ballabriga, Van-Thuan Pham, Sudipta Chattopadhyay and Abhik Roychoudhury
  (One-line abstract) Integrated WCET analyis on full software & hardware stack
  IEEE Real-time Systems Symposium (RTSS) 2013

- **A General Solution supporting Real-time and Remote Electrocardiogram Diagnostic**
  Dung Cao Tuan, Thuan Pham Van and Viet Hoang Anh
  (One-line abstract) Remote electrocardiogram (ECG) monitoring and diagnosis system
  International Symposium on Information and Communication Technology (SoICT) 2012

Patent Application

- **Autonomous reasoning system for vulnerability analysis**
  Praveen Murthy, Bogdan Copos, Thuan Pham
  (One-line abstract) Automatic vulnerability detection and repair for program binaries
  United States Patent Application - US20160259943

Work Experience

August 2017 - Present School of Computing, National University of Singapore, Singapore
Research Fellow
Doing research on software testing in general and Android app testing in particular.
Technologies: Mobile testing, Fuzz Testing.

April 2017 - Aug 2017 School of Computing, National University of Singapore, Singapore
Research Associate
Doing research on software testing in general and Android app testing in particular.
Technologies: Mobile testing, Fuzz Testing.

May 2016 - March 2017 School of Computing, National University of Singapore, Singapore
Research Assistant
Doing research on Fuzz testing techniques for vulnerability detection & crash reproduction.
Technologies: Binary program analysis, Symbolic Execution, Fuzz Testing.

Feb 2015 - May 2015 Fujitsu Laboratories of America, California, United States
Research Intern
Involved in a team to build an automated Cyber Reasoning System (CRS) to participate in the DARPA Cyber Grand Challenge - The World's first all-machine hacking tournament.
Technologies: Binary program analysis, Fuzz Testing.

Aug 2007 - Jul 2012 Hanoi University of Science and Technology, Hanoi, Vietnam
Lecturer
Taught courses in subjects such as Microprocessors, Embedded Systems, Microsoft .NET Framework and involved in R&D and technonogy transfers activities .
Technologies: Computer architecture, Embedded Systems, Databases.

May 2011 - Jul 2012 Embedded247 Training Center, Hanoi, Vietnam
Co-Founder & Trainer
Designed courses and involved in training & management activities.
Technologies: Embedded Systems, Embedded OS.

Aug 2009 - Jul 2012 Mimas Solutions and Services jsc, Hanoi, Vietnam
Co-Founder & Research Lead
Designed and developed prototypes for emotion & image recognition systems.
Technologies: Brain Computer Interface, Image processing.

Aug 2010 - Aug 2011 DKS Manufacturing and Trading jsc, Hanoi, Vietnam
Software Architect
Designed and developed electric/pneumatic/hydraulic simulators.
Technologies: Simulation, Object Oriented Design.

Feb 2009 - Jul 2009 Orange France Telecom laboratories, Grenoble, France
Research Intern
Designed and evaluated routing protocols for wireless sensor networks.
Technologies: Wireless Sensor Network, Simulation.

Aug 2005 - Aug 2006 FPT Software, Hanoi, Vietnam
Developed automation test tools for embedded systems.
Ported Kaffe JVM to a ARM board & developed an automation test tools for a FPGA prototype.
Technologies: Embedded Systems, Test Automation.

Other experience

- **Lab instructor**
  24-hour Fuzzing Hackathon at Fuzz Testing for Finding Vulnerabilities Workshop – 2nd Singapore Cyber Security R&D Conference (SG-CRC) 2017.
- **External reviewer**
  ICSE'16, CCS'16.
- **Lab tutor**
  Software security course (CS 4329) at NUS.

Honors & Awards

- **Research Achievement Award AY2014/2015, School of Computing, NUS**
  Presented to PhD students who have achieved outstanding research performance.
- **3rd prize VIFOTEC Scientific and Technological Innovation Award**
  For an automatic mirror-rotation based Goniophotometer hardware & software system. The product was bought by Rang Dong Lighting Ltd., one of the most famous lighting companies in Vietnam.
- **Top 5 Intel & DST Asia Pacific Challenge 2011 (Bangalore, India)**
  For a Brain-Computer-Interace (BCI) based emotion recognition system.
- **1st prize Vietnamese Talents Award**
  For a system helping disabled people control electronic/electrical devices via brain signals.

Engineering Skills

- **Programming Languages**
  C, C++, C#, Python, Visual Basic, Java, Assembly (x86-ARM-MIPS), Bash Shell
- **Working Tools**
  Fuzzing tools: AFL, LibFuzzer, Peach Fuzzer, zzuf
  Symbolic execution engines: S2E, KLEE
  Program analysis/debugging tools: IDA Pro, Intel Pin, BAP, radare2, Valgrind, GDB
  Signal processing & machine learning tools: MATLAB
- **Embedded System**
  PCB Design, Embedded Linux, RTOS, Wireless Sensor Network
  Microcontroller Programming (ARM, MIPS, PIC, AVR, Intel-8051)
- **Database Management Systems**
  Microsoft SQL Server, MySQL
- **Web programming & Web Design**
  PHP, HTML, CSS, JavaScript
- **Miscellaneous**
  Docker, LXC container

Practical Security Impact

- **42 CVEs assigned**
  CVE-2016-2226, CVE-2016-4487, CVE-2016-4488, CVE-2016-4489, CVE-2016-4490, CVE-2016-4491, CVE-2016-4492, CVE-2016-4493, CVE-2016-6131, CVE-2017-6965, CVE-2017-6966, CVE-2017-6969, CVE-2017-7209, CVE-2017-7210, CVE-2017- 7223, CVE-2017-7224, CVE-2017-7225, CVE-2017-7226, CVE-2017-7227, CVE-2017-7299, CVE-2017-7300, CVE-2017-7301, CVE-2017-7302, CVE-2017-7303, CVE-2017-7304, CVE-2017-7578, CVE-2017-8392, CVE-2017-8393, CVE-2017-8394, CVE-2017-8395, CVE-2017-8396, CVE-2017-8397, CVE-2017-8398, CVE-2017-9047, CVE-2017-9048, CVE-2017-9049, CVE-2017-9050, CVE-2017-9051, CVE-2017-9052, CVE-2017-9053, CVE-2017-9054, CVE-2017-9055

Referees

Name	Prof. Abhik Roychoudhury	**Name**	Assoc. Prof. Liang Zhenkai
Company	National University of Singapore.	**Company**	National University of Singapore.
Contact	abhik@comp.nus.edu.sg	**Contact**	liangzk@comp.nus.edu.sg