Stanovisko školitele k doktorské práci Ing. Jakuba Křoustka

Doktorand Ing. Jakub Křoustek pracoval po celou dobu studia velmi aktivně. Zadané téma rozvíjel nejev v rámci vlastního studia, ale zejména v rámci řešení grantu TA ČR řešeného společně s firmou AVG, kde byl vůdčí osobností řešitelského týmu na FIT. Výsledky publikoval zejména na příslušných vědeckých konferencích, které jsou příslušné pro řešené téma a jsou klíčové v oboru. Krom toho ale publikoval i ve vědeckých časopisech. Předložená práce prezentuje výsledky Ing. Jakuba Křoustka v oblasti dynamické analýzy spustitelného kódu a generické dekompilace se zaměřením se na přední část dekompilátoru.

Vzhledem k dosaženým výsledkům doporučuji přijmout předloženou práci k obhajobě.

V Brně, dne 19. listopadu 2014

Dušan Kolář
UIFS FIT VUT v Brně

Následuje seznam publikací, které Ing. Křoustek vytvořil v rámci studia pod mým vedením.

Články v časopisech s impakt faktorem

- J. Křoustek a D. Kolář. Context Parsing (Not Only) of the Object-File-Format Description Language. Computer Science and Information Systems (ComSIS), 10(4):1673–1702, 2013.
- J. Křoustek, F. Pokorný a D. Kolář. A New Approach to Instruction-Idioms Detection in a Retargetable Decompiler. Computer Science and Information Systems (ComSIS), 11(4):1337–1359, 2014.

Články v časopisech bez impakt faktoru

- L. Ďurfina, J. Křoustek, P. Matula a P. Zemek. A Novel Approach to Online Retargetable Machine-Code Decompilation. Journal of Network and Innovative Computing (JNIC), 2(1):224–232, 2014.
- L. Ďurfina, J. Křoustek, P. Zemek, D. Kolář, T. Hruška, K. Masařík a A. Meduna. Design of a Retargetable Decompiler for a Static Platform-Independent Malware Analysis. International Journal of Security and Its Applications (IJSIA), 5(4):91–106, 2011.
  - Citováno v:
    - C. Bo-Chao, et al. A Competent Traffic Classification Mechanism Using Packet Size Distribution and Cumulation. Information (Japan) 17(5):1837–1844, 2014.
    - P. Xie, et al. Eliminate Evading Analysis Tricks in Malware using Dynamic Slicing. International Journal of Security and Its Applica-tions, 7(3):357–364, 2013.
    - K. Yakdan, S. Eschweiler a E. Gerhards-Padilla. REcompile: A decompilation framework for static analysis of binaries. 8th International Conference on Malicious and Unwanted Software (MALWARE), IEEE, 2013.
    - C. L. Yee, et al. A static and dynamic visual debugger for malware analysis. 18th Asia-Pacific Conference on Communications (APCC). IEEE,

2012.
    - C. L. Yee, et al. Architecture of Malware Tracker Visualization for Malware Analysis. Journal of Theoretical and Applied Information Technology 52(1):11–20, 2013.
- J. Křoustek. On Decompilation of VLIW Executable Files. Problems of Programming (ISS), s. 1–8. Přijato, bude publikováno v 2015.
- J. Křoustek a D. Kolář. Approaching Retargetable Static, Dynamic, and Hybrid Executable-Code Analysis. Acta Informatica Pragensia (AIP), 2(1):18–29, 2013.
- J. Křoustek, P. Matula, D. Kolář a M. Zavoral. Advanced Preprocessing of Binary Executable Files and its Usage in Retargetable Decompilation. International Journal on Advances in Software (IJAS), 7(1):112–122, 2014.
- J. Křoustek, S. Židek, D. Kolář a A. Meduna. Scattered Context Grammars with Priority. International Journal of Advanced Research in Computer Science (IJARCS), 2(4):1–6, 2011.
- Z. Přikryl, J. Křoustek, T. Hruška a D. Kolář. Fast Translated Simulation of ASIPs. OpenAccess Series in Informatics (OASIcs), 16(1):93–100, 2011.
- Z. Přikryl, J. Křoustek, T. Hruška, D. Kolář, K. Masařík a A. Husár. Design and Simulation of High Performance Parallel Architectures Using the ISAC Language. GSTF International Journal on Computing (GTSF IJC), 1(2):97–106, 2011.

Příspěvky na mezinárodních konferencích

- L. Ďurfina, J. Křoustek a P. Zemek. Generic Source Code Migration Using Decompilation. 10th Annual Industrial Simulation Conference (ISC'2012), s. 38–42. EUROSIS, 2012.
- L. Ďurfina, J. Křoustek a P. Zemek. Psyb0t Malware: A Step-by-Step Decompilation Case Study. 20th Working Conference on Reverse Engineering (WCRE'13), s. 449–456, Koblenz, DE, 2013. IEEE Computer Society.
- L. Ďurfina, J. Křoustek a P. Zemek. Retargetable Machine-Code Decompilation in Your Web Browser. 3rd IEEE World Congress on Information and Communication Technologies (WICT'13), s. 57–62, Hanoi, VN, 2013. IEEE Computer Society.
- L. Ďurfina, J. Křoustek, P. Zemek a B. Kábele. Accurate Recovery of Functions in a Retargetable Decompiler. 15th International Symposium on Research in Attacks, Intrusions and Defenses (RAID'12), LNCS 7462, s. 390–392, Berlin, Heidelberg, DE, 2012. Springer-Verlag.
- L. Ďurfina, J. Křoustek, P. Zemek a B. Kábele. Detection and Recovery of Functions and Their Arguments in a Retargetable Decompiler. 19th Working Conference on Reverse Engineering (WCRE'12), s. 51–60, Kingston, ON, CA, 2012. IEEE Computer Society.
- L. Ďurfina, J. Křoustek, P. Zemek, B. Kábele a D. Kolář. On Complex Reconstruction of Functions from Binary Executable Files. 8th Doctoral Workshop on Mathematical and Engineering Methods in Computer Science (MEMICS'12), s. 100–101. Masaryk University, 2012.
- L. Ďurfina, J. Křoustek, P. Zemek, D. Kolář, T. Hruška, K. Masařík aA. Meduna. Advanced Static Analysis for Decompilation Using Scattered Context Grammars. Applied Computing Conference (ACC'11), s. 164–169. World Scientific and Engineering Academy and Society (WSEAS), 2011.
    - Citováno v:
        - A. V. Višnekov. Issledovaniye metodov dekompilyatsii programm dlja protsessorov x86. Moscow, RU, 2013
- L. Ďurfina, J. Křoustek, P. Zemek, D. Kolář, T. Hruška, K. Masařík a A. Meduna. Design of a Retargetable Decompiler for a Static Platform-Independent Malware Analysis. 5th International Conference on Information Security and Assurance (ISA'11), s. 72–86, Berlin, Heidelberg, DE, 2011. Springer-Verlag.

- L. Ďurfina, J. Křoustek, P. Zemek, D. Kolář, T. Hruška, K. Masařík a A. Meduna. Design of a Retargetable Decompiler for a Static Platform-Independent Malware Analysis. 7th Doctoral Workshop on Mathematical and Engineering Methods in Computer Science (MEMICS'11), s. 114–114. Masaryk University, 2011.
- L. Ďurfina, J. Křoustek, P. Zemek, D. Kolář, K. Masařík, T. Hruška a A. Meduna. Design of an Automatically Generated Retargetable Decompiler. 2nd European Conference of Computer Science (ECCS'11), s. 199–204. North Atlantic University Union, 2011.
  - Citováno v:
    - M. Berger, et al. Methodology and Toolset for Model Verification, Hardware/Software co-simulation, Performance Optimisation and Customisable Source-code generation. WSEAS Transactions on Information Science and Applications 6(10)169–178, 2013.
- J. Křoustek. Decompilation of VLIW Executable Files — Caveats and Pitfalls. 3nd International Scientific Conference Theoretical and Applied Aspects of Cybernetics (TAAC'13), s. 287–296, Kyiv, UA, 2013. Kyiv: Bukrek.
- J. Křoustek. Usage of Decompilation in Processor Architecture Modeling. 31th International Autumn Colloquium Advanced Simulation of Systems (ASIS'09), s. 64–67. MARQ, 2009.
- J. Křoustek a D. Kolář. Object-File-Format Description Language and ItsUsage in Retargetable Decompilation. Conference Proceedings (SCLIT'12), s. 466–469. American Institute of Physics (AIP), 2012.
- J. Křoustek a D. Kolář. Preprocessing of Binary Executable Files Towards Retargetable Decompilation. 8th International Multi-Conference on Computing in the Global Information Technology (ICCGI'13), s. 259–264, Nice, FR, 2013. International Academy, Research, and Industry Association (IARIA).
- J. Křoustek, P. Matula a L. Ďurfina. Generic Plugin-Based Convertor of Executable File Formats and Its Usage in Retargetable Decompilation. 6th International Scientific and Technical Conference (CSIT'11), s. 127–130. Ministry of Education, Science, Youth and Sports of Ukraine, Lviv Polytechnic National University, Institute of Computer Science and Information Technologies, 2011.
- J. Křoustek, P. Matula, J. Končický a D. Kolář. Accurate Retargetable Decompilation Using Additional Debugging Information. 6th International Conference on Emerging Security Information, Systems and Technologies (SECURWARE'12), s. 79–84. International Academy, Research, and Industry Association (IARIA), 2012.
- J. Křoustek a F. Pokorný. Reconstruction of Instruction Idioms in a Retargetable Decompiler. 4th Workshop on Advances in Programming Languages (WAPL'13), s. 1507–1514, Krakow, PL, 2013. IEEE Computer Society.
- J. Křoustek, Z. Přikryl, D. Kolář a T. Hruška. Retargetable Multi-level Debugging in HW/SW Codesign. 23rd International Conference on Microelectronics (ICM'11), s. 6. Institute of Electrical and Electronics Engineers, 2011.
- J. Křoustek, S. Židek, D. Kolář a A. Meduna. Exploitation of Scattered Context Grammars to Model VLIW Instruction Constraints. 12th Biennial Baltic Electronics Conference (BEC'10), s. 165–168. IEEE Computer Society, 2010.
- Z. Přikryl, J. Křoustek, T. Hruška a D. Kolář. Fast Just-In-Time Translated Simulation for ASIP Design. 14th IEEE International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDCS'11), s. 279–282. IEEE Computer Society, 2011.
- Z. Přikryl, J. Křoustek, T. Hruška a D. Kolář. Fast Translated Simulation of ASIPs. 6th Doctoral Workshop on Mathematical and Engineering Methods in Computer Science (MEMICS'10), s. 135–142. Masaryk University, 2010.
- Z. Přikryl, J. Křoustek, T. Hruška, D. Kolář, K. Masařík a A. Husár. Design and Debugging of Parallel Architectures Using the ISAC Language. Annual

International Conference on Advanced Distributed and Parallel Computing and Real-Time and Embedded Systems (RTES'10), s. 213–221. Global Science and Technology Forum (GTSF), 2010.

Příspěvky na studentských soutěžích

- J. Křoustek a S. Židek. Generating Proper VLIW Assembler Code Using Scattered Context Grammars. 16th Conference and Competition Student (EEICT'10), s. 181–185. Brno University of Technology, 2010.

Seznam vytvořených nástrojů

- J. Křoustek, P. Matula, D. Kolář a K. Masařík. Bintran - nástroj pro konverzi spustitelných souborů. Software, 2013.
- J. Křoustek, M. Zavoral a D. Kolář. Fileinfo - nástroj pro detekci použitého překladače či packeru. Software, 2013.
- L. Ďurfina, J. Křoustek a D. Kolář. LfDComparator - nástroj pro porovnání LfD zdrojových kódů. Software, 2013.
- L. Ďurfina, J. Křoustek, P. Zemek, O. Vrana, P. Matula a D. Kolář. Rekonfigurovatelný zpětný překladač. Software, 2013.

Recenze příspěvků

- Mezinárodní konference:
  - SECURWARE 2013 – 2x
  - ICCGI 2014 – 2x
  - SECURWARE 2014 – 2x

Účast na projektech

- TA ČR TA01010667 Systém pro podporu platformě nezávislé analýzy škodlivého kódu ve spustitelných souborech (2011-2013) – získání, vedení a úspěšné obhájení grantu.
- VUT FEKT/FIT-J-13-2000 Validace spustitelného kódu pro systémy průmyslové automatizace pomocí zpětného překladu (2013) – získání, vedení a úspěšné obhájení grantu.
- VUT FIT-S-10-2 Rozpoznávání a prezentace informací z multimediálních dat (2010) – spoluřešitel.
- VUT FIT-S-11-2 Pokročilé rozpoznávání a prezentace multimediálních dat (2011–2013) – spoluřešitel.

Ocenění

- EEICT 2010 – 2. místo
- MEMICS 2010 – best papers award
- ICCGI 2013 – best papers award

Ostatní

- Členství v programových výborech mezinárodních konferencí SECURWARE (2013, 2014) a ICCGI (2014).
- Vedení ústavního semináře rezerzního inženýrství (2012–2014).