PAUL FITERĂU-BROŞTEAN

Telephone: +40 720 114646 ⋄ Email: paul.fiterau_brostean@it.uu.se
Website: https://paulfiterau.github.io/ ⋄ Address: Portalgatan 30, Uppsala, Sweden

WORK EXPERIENCE

Uppsala University September 2018 -
Postdoctoral Researcher *Uppsala, Sweden*

· Developed techniques and tools for testing network protocol implementations based on model learning and symbolic execution.

Quintiq February 2018 - September 2018
Software Developer *'s Hertogenbosch, Netherlands*

· Developed and maintained tooling connecting a complex server application to external endpoints such as file systems, message queues and SOAP servers.

Radboud University, Nijmegen November 2013 - November 2017
PhD Candidate *Nijmegen, Netherlands*

· Improved model learning techniques, tools in their application to testing network protocol implementations.

EDUCATION

Radboud University, Nijmegen 2013-2018
PhD in Computer Science
PhD Thesis on applying active automata learning techniques to network protocols.
Supervisor: Prof. Frits W. Vaandrager

Politehnica University, Timişoara 2011-2013
Master in Software Engineering
Master's Thesis on the semi-automatic generation of drivers for connecting systems to automata learning tools, graded with 10.
Supervisor: Prof. Ioana Şora

Radboud University, Nijmegen 2012-2013
Erasmus exchange student for one semester

Politehnica University, Timişoara 2007-2011
Bachelor in Computers and Information Technology
Bachelor's Thesis on extending the Fractal architecture description language as to enable description of reconfiguration operations, graded with 10.
Supervisor: Prof. Ioana Şora

PUBLICATIONS

[1] Paul Fiterău-Broştean, Bengt Jonsson, Konstantinos Sagonas, and Fredrik Tåkvist. Automata-based automated detection of state machine bugs in protocol implementations. In *Network and Distributed System Security Symposium 2023 (NDSS)*, 2023. to appear.

[2] Hooman Asadian, Paul Fiterău-Broştean, Bengt Jonsson, and Konstantinos Sagonas. Applying symbolic execution to test implementations of a network protocol against its specification. In *2022 IEEE Conference on Software Testing, Verification and Validation (ICST)*, pages 70–81. IEEE, 2022.

[3] Paul Fiterău-Broştean, Bengt Jonsson, Konstantinos Sagonas, and Fredrik Tåkvist. DTLS-Fuzzer: A DTLS protocol state fuzzer. In *2022 IEEE Conference on Software Testing, Verification and Validation (ICST)*, pages 456–458. IEEE, 2022.

[4] Paul Fiterău-Broştean, Bengt Jonsson, Robert Merget, Joeri de Ruiter, Konstantinos Sagonas, and Juraj Somorovsky. Analysis of DTLS implementations using protocol state fuzzing. In *29th USENIX Security Symposium (USENIX Security 20)*, 2020.

[5] Paul Fiterău-Broştean. *Active Model Learning for the Analysis of Network Protocols*. PhD thesis, Radboud University Nijmegen, 2018.

[6] Rick Smetsers, Paul Fiterău-Broştean, and Frits Vaandrager. Model learning as a satisfiability modulo theories problem. In *International Conference on Language and Automata Theory and Applications*, pages 182–194. Springer, 2018.

[7] Paul Fiterău-Broştean and Falk Howar. Learning-based testing the sliding window behavior of TCP implementations. In *Critical Systems: Formal Methods and Automated Verification*, pages 185–200. Springer, 2017.

[8] Paul Fiterău-Broştean, Toon Lenaerts, Erik Poll, Joeri de Ruiter, Frits Vaandrager, and Patrick Verleg. Model learning and model checking of SSH implementations. In *Proceedings of the 24th ACM SIGSOFT International SPIN Symposium on Model Checking of Software*, SPIN 2017, pages 142–151. ACM, 2017.

[9] Paul Fiterău-Broştean, Ramon Janssen, and Frits Vaandrager. Combining model learning and model checking to analyze TCP implementations. In *CAV 2016*, volume 9780 of *LNCS*, pages 454–471. Springer, 2016.

[10] Fides Aarts, Paul Fiterău-Broştean, Harco Kuppens, and Frits Vaandrager. Learning register automata with fresh value generation. In *ICTAC 2015*, volume 9399 of *LNCS*, pages 165–183. Springer, 2015.

[11] Paul Fiterău-Broştean, Ramon Janssen, and Frits Vaandrager. Learning fragments of the TCP network protocol. In *FMICS 2014*, volume 8718 of *LNCS*, pages 78–93. Springer, 2014.

RESEARCH SUMMARY

Model Learning for Network Protocol Testing We used (active) model learning to test implementations of essential network protocols such as TCP [11, 9, 7], SSH [8] and DTLS [4, 1]. These works uncovered bugs, including vulnerabilities, leading to fixes in important libraries such as Java's TLS implementation and the Linux TCP stack. Our works also addressed challenges arising in model learning applications. We automated analysis of learned models using model checking of requirements encoded by linear temporal logic [9, 8], and more recently, by deterministic finite automata [1]. We also improved model learning algorithms and tools for register automata [10, 7], a rich formalism that can better capture the behavior of complex systems compared to the finite state automata traditionally supported by model learning. In a related work [6], we developed an extensible model learning framework based on SMT solvers, which supports a wider range of formalisms.

Symbolic Execution for Network Protocol Testing We present a methodology which leverages symbolic execution to test implementations of network protocols [6]. The idea is to guide symbolic execution, using assertions and assumptions, towards paths in the SUT that violate protocol requirements. We implement our methodology using the KLEE symbolic execution engine and apply it to test DTLS implementations. Our testing revealed bugs in all four libraries tested, including a promptly-fixed memory bug in OpenSSL.

TEACHING

Lecturer for the Secure Computer Systems course, academic year 2021-2022.
Lecturer for the Programming Embedded Systems course, academic year 2019-2020.
Teaching assistant for the Computer Networking course for three consecutive years 2014-2017.
Teaching assistant for the Testing Techniques course, academic year 2014-2015.

SUPERVISION

Fredrik Tåkvist, PhD Student since February 2022.
Hooman Asadian, PhD Student since September 2019.
Rahbar Ghori, 2021, Master's Thesis *Protocol-aware fuzzing of DTLS*.
Fredrik Tåkvist, 2020, Bachelor's Thesis *Analysis of DTLS Implementations Using State Fuzzing*.
Toon Laenarts, 2017, Bachelor's Thesis *Improving Protocol State Fuzzing of SSH*.
Ramon Jansen, 2015, Master's Thesis *Learning and Model Checking Real-world TCP Implementations*.

RESEARCH INTERESTS

Network Protocol Testing
Active and Passive Model Learning
Symbolic Execution
Application of Formal Methods

SERVICE

(Sub-)Reviewer for Computer Networks 2022, FM 2021 and 2019, Computer Communications Journal 2018, ICFEM 2017 and MARS 2017.

AWARDS

VERSEN PhD Award 2019, First Place.

JUNIOR WORK EXPERIENCE

Alcatel Lucent February 2013 - April 2013
Junior Software Developer *Timişoara*

· Contributed to the development of a license manager tool.

e-Austria July 2012 - August 2013
Junior Researcher *Timişoara*

· Developed framework for automatically generating model learning setups for Java and web applications.

Alcatel Lucent October 2011 - July 2012
Junior Software Developer *Timişoara*

· Contributed to the development of a radio network planning tool.

LANGUAGES

Romanian	native
English	full working proficiency
Dutch	basic