Wojciech Wideł

KTH Royal Institute of Technology ◇ Division of Network and Systems Engineering
Malvinas väg 6, floor 4, room A445 ◇ SE-100 44 Stockholm, Sweden
Website ◇ https://wwidel.github.io
Email ◇ widel@kth.se

EDUCATION

Ph.D. in Computer Science December 2019 (expected)
INSA Rennes, IRISA, France
Title of dissertation: *Formal modeling and quantitative analysis of security using attack–defense trees*
Supervisors: Prof. Gildas Avoine and Dr Barbara Kordy

Ph.D. in Mathematics (with distinction) May 2017
AGH University of Science and Technology, Kraków, Poland
Title of dissertation: *Heavy subgraphs and pancyclicity*
Supervisor: Prof. A. Paweł Wojda

M.Sc. in Mathematics July 2014
AGH University of Science and Technology, Kraków, Poland
Major: Mathematics in Computer Science
Title of thesis: *Maximum independent set problem in graphs*
Supervisor: Prof. Ingo Schiermeyer

Technische Universität Bergakademie Freiberg, Freiberg, Germany April - July 2014
I spent the spring semester 2013/2014 at the Department of Discrete Mathematics and Algebra within the Erasmus program. I followed the course *Selected topics in algorithmic graph theory*, took German classes and prepared my master thesis.

B.Sc. in Mathematics July 2012
AGH University of Science and Technology, Kraków, Poland
Title of thesis: *Duże układy równań liniowych z macierza symetryczna* (*Large symmetric systems of linear equations*)
Supervisor: Dr Bogusław Bożek

PROFESSIONAL EXPERIENCE

KTH Royal Institute of Technology October 2019 – Present
Postdoctoral researcher *Stockholm, Sweden*

· As a member of the Division of Network and Systems Engineering, I am working on threat modeling, in particular in the context of cybersecurity of energy infrastructure.

IRISA, INSA Rennes November 2016 – October 2019
Doctoral researcher *Rennes, France*

· As a member of the Embedded Security and Cryptography (EMSEC) team at the Institut de Recherche en Informatique et Systèmes Aléatoires (IRISA), I carried out research on formal foundations of the *attack–defense tree* modeling framework for security, and on related methods for quantitative evaluation of security.

AGH University of Science and Technology October 2014 – November 2016
Doctoral researcher *Kraków, Poland*

· As a member of the Department of Discrete Mathematics at the Faculty of Applied Mathematics, I carried out research resulting in a number of new sufficient conditions for Hamiltonicity and pancyclicity of simple graphs.

AGH University of Science and Technology October 2014 – July 2016
Teaching assistant *Kraków, Poland*

· Calculus, exercise sessions, 1st year of bachelor, 88 hours.
· Extremal Combinatorics, exercise sessions, 2nd year of master, 15 hours.
· Introduction to Discrete Mathematics and Logics, exercise sessions, 1st year of bachelor, 90 hours.
· Linear Algebra and Geometry, exercise sessions, 1st year of bachelor, 40 hours.

SUPERVISION

Master students

Angèle Bossuat University Rennes 1, 2017
Thesis: *Attack–defense trees for computer security: formal modeling of preventive and reactive countermeasures*, co-supervised with Barbara Kordy.

Bachelor and engineer students

Nicolas Huette École Polytechnique (X), 2018
Project: *Linear programming on attack–defense trees*, co-supervised with Barbara Kordy.

Student projects

OptiTool – how to secure your system in an optimal way, INSA Rennes, 2018 – 2019
One year project executed by the 4th year computer science students, co-supervised with Barbara Kordy.

PUBLICATIONS

In peer-reviewed international journals

[1] Wei Zheng, Wojciech Wideł, and Ligong Wang. On implicit heavy subgraphs and hamiltonicity of 2-connected graphs. *Discussiones Mathematicae Graph Theory*. (To appear).

[2] Wojciech Wideł. On implicit degree-type conditions for hamiltonicity in implicit claw-f-heavy graphs. *Ars Combinatoria*. (To appear).

[3] Wojciech Wideł, Maxime Audinot, Barbara Fila, and Sophie Pinchinat. Beyond 2014: Formal methods for attack tree–based security modeling. *ACM Comput. Surv.*, 52(4):75:1–75:36, August 2019.

[4] Wojciech Wideł. Fan's condition on induced subgraphs for circumference and pancyclicity. *Opuscula Mathematica*, 37(4):617–639, 2017.

[5] Wojciech Wideł. A triple of heavy subgraphs ensuring pancyclity of 2-connected graphs. *Discussiones Mathematicae Graph Theory*, 37(2):477–500, 2017.

[6] Wojciech Wideł. A fan-type heavy triple of subgraphs for pancyclicity of 2-connected graphs. *Discrete Mathematics*, 340(7):1639–1644, 2017.

[7] Wojciech Wideł. Clique-heavy subgraphs and pancyclicity of 2-connected graphs. *Information Processing Letters*, 117:6–9, 2017.

[8] Wojciech Wideł. A fan-type heavy pair of subgraphs for pancyclicity of 2-connected graphs. *Discussiones Mathematicae Graph Theory*, 36(1):173–184, 2016.

In peer-reviewed international conferences

[9] Barbara Fila and Wojciech Wideł. Attack–defense trees for abusing optical power meters: A case study and the OSEAD tool experience report. In *Graphical Security Modeling (GraMSec)*, volume 11720 of *LNCS*. Springer, 2019. (To appear).

[10] Barbara Fila and Wojciech Wideł. Efficient attack–defense tree analysis using Pareto attribute domains. In *Computer Security Foundations (CSF)*, pages 200–215. IEEE Computer Society, 2019.

[11] Barbara Kordy and Wojciech Wideł. On quantitative analysis of attack–defense trees with repeated labels. In *Principles of Security and Trust (POST)*, volume 10804 of *LNCS*, pages 325–346. Springer, 2018.

[12] Barbara Kordy and Wojciech Wideł. How well can I secure my system? In *Integrated Formal Methods (iFM)*, volume 10510 of *LNCS*, pages 332–347. Springer, 2017.

SELECTED TALKS

On quantitative analysis of attack–defense trees with repeated labels — April 2018
7th International Conference on Principles of Security and Trust (POST'18),
Thessaloniki, Greece

Attributes' evaluation in attack–defense trees with repeated labels — November 2017
Workshop on Formal Methods for Attack Trees,
Munich, Germany

How well can I secure my system? — September 2017
13th International Conference on Integrated Formal Methods (IFM'17),
Turin, Italy

On optimization problems in attack–defense trees — August 2017
17th International School on Foundations of Security Analysis and Design,
Bertinoro, Italy

Hamiltonicity of 3-connected claw-heavy graphs — November 2015
24th Workshop On Graph Theory "3in1",
Krynica-Zdrój, Poland

Heavy subgraphs and the existence of cycles in 2-connected graphs — September 2015
16th Workshop On Graph Theory "Colourings, Independence and Domination",
Szklarska Poreba, Poland

ACADEMIC DUTIES

Reviewing activities

I have served as an external reviewer for the following:

Journals: Ars Combinatoria, Discussiones Mathematicae Graph Theory, International Journal of Information Security (subreviewer), Frontiers of mathematics in China, Opuscula Mathematica.

Conferences: DBSec 2019 (subreviewer), ESORICS 2018 (subreviewer), GraMSec 2018 (subreviewer), FPS 2017 (subreviewer).

Other responsabilities

I co-organised the 25th Workshop On Graph Theory "3in1", held at Dosłońce, Poland, on 16-19 November 2016.

PROFESSIONAL DEVELOPMENT

Winter School on Mathematical Foundations of Asymmetric Cryptography March 2019
Aussois, France

I participated in 20 hours of lectures focusing on the discrete logarithm problem, lattice-based cryptography and cryptography based on isogeny graphs.

Cryptography I January 2019
Coursera

The course of approximately 35 hours, given by Dan Boneh from Stanford, covered topics such as stream ciphers, block ciphers, authenticated encryption, basic key exchange and public key encryption. Basic notions, constructions and pitfalls were presented, and the knowledge obtained was consolidated by answering quizzes and solving hands-on programming exercises.

Lattice–based cryptography November/December 2018
(*Réseaux Euclidiens pour la cryptographie*) *Rennes, France*

During the 12 hours of this lecture, intended for 2nd year master and doctoral students, the basics of lattices and some of their applications for constructing cryptographic primitives were covered.

Rencontres Entreprises DOCtorants Sécurité (REDOCS) 2018 October 2018
Gif-sur-Yvette, France

I spent a week working in a four-person team on a project entitled "Towards a decentralized identity management solution based on blockchain", proposed by the IDnomic company.

Summer School on Real-World Crypto and Privacy June 2018
Šibenik, Croatia

I participated in 21 hours of lectures on various security- and privacy-related topics, ranging from cryptography (including lattice-based cryptography and cryptography based on eliptic curves), through random numbers generation and security protocols, to selected issues related to hardware security.

RootMe 2017/2018

I have been developing and improving my hacking skills on RootMe, with focus on solving cryptanalysis-related challenges: https://www.root-me.org/wwww?inc=score&lang=en.

International School on Foundations of Security Analysis and Design (FOSAD) August 2017
Bertinoro, Italy

I participated in 28 hours of lectures covering basics of several topics in security. Among them were: cryptocurrencies and transparency systems, verification of security protocols, privacy engineering, information-flow control libraries and privacy-related issues of machine learning.

TECHNICAL SKILLS

I prepare my scientific publications using LaTeX 2_ε. In my everyday work I am using Python. I have developed a Python package for security analysis using attack–defense trees (available at https://github.com/wwidel). I have used it also for solving ethical hacking challenges.

During my bachelor and master studies, I have written some code in C and C++.

LANGUAGE SKILLS

My mother tongue is Polish. I am a fluent English speaker and I have a basic knowledge of French and German.

OUTSIDE INTERESTS

History (most recently: history of China in 20th and 21st century), climbing, chess.