Ly Vu Duc

Curriculum Vitae

(+84) 344282282
vuducly151092@gmail.com
My Webpage
Github Linkedin Skype

Education

10/2017–01/2022 **PhD in Information Engineering and Computer Science**, *University of Trento, Trento, Italy*, Software supply chains security, Automated Program Repair, Open-source Software Security
Thesis title: Towards Understanding and Securing the OSS Supply Chain.
Graduation date: 03/2022.
Advisor: Prof. Fabio Massacci

09/2015–08/2017: **Master of Science**, *Hongik University, Sejong Campus*, South Korea.
Thesis title: Efficient Malware Classification Techniques Using Integrated Static and Dynamic Indicators
Advisor: Prof. Seoung Oun Hwang

2010–2015: **Bachelor of Engineering, Information Technology**, *Posts and Telecommunications Institute of Technology, Ho Chi Minh City*, Vietnam.
Thesis title: The research of rootkit on Windows systems
Advisor: MSc. Phuc Le

Publications

Journal Articles

2023 Duc-Ly Vu Fabio Massacci Quang-Cuong Bui, Ranindya Paramitha and Riccardo Scandariato. Apr4vul: An empirical study of automatic program repair techniques on real-world java vulnerabilities. In *To appear in Empirical Software Engineering journal*, 2023.

2020 Duc-Ly Vu, Trong-Kha Nguyen, Tam V Nguyen, Tu N Nguyen, Fabio Massacci, and Phu H Phung. Hit4mal: Hybrid image transformation for malware classification. *Transactions on Emerging Telecommunications Technologies*, volume 31, page e3789. Wiley Online Library, 2020.

2020 Trong-Kha Nguyen, Duc-Ly Vu, and Seong Oun Hwang. Effective feature selection based on manova. *International Journal of Internet Technology and Secured Transactions*, volume 10, pages 383–395. Inderscience Publishers (IEL), 2020.

2019 Duy-Phuc Pham, Duc-Ly Vu, and Fabio Massacci. Mac-a-mal: macos malware analysis framework resistant to anti evasion techniques. *Journal of Computer Virology and Hacking Techniques*, volume 15, pages 249–257. Springer, 2019.

2018 Trong-Kha Nguyen, Duc-Ly Vu, and Seong Oun Hwang. An efficient neural network model for time series forecasting of malware. *Journal of Intelligent & Fuzzy Systems*, volume 35, pages 6089–6100. IOS Press, 2018.

In Conference Proceedings

2024 Duc-Ly Vu, Trevor Dunlap, Karla Obermeier-Velazquez, Paul Gilbert, John Speed Meyers, and Santiago Torres-Arias. A study of malware prevention in linux distributions. *arXiv preprint arXiv:2411.11017*, 2024.

2024 Thanh-Cong Nguyen, Duc-Ly Vu, and Narayan C Debnath. An analysis of malicious behaviors of open-source packages using dynamic analysis. In *Proceedings of the 37th International Conference on Computer Applications in Industry and Engineering*, 2024.

2023 Duc-Ly Vu, Zachary Newman, and John Speed Meyers. Bad snakes: Understanding and improving python package index malware scanning. In *In Proceedings of the 45th IEEE/ACM International Conference on Software Engineering (ICSE-2023)*, 2023.

2022 Simone Scalco, Ranindya Paramitha, Duc-Ly Vu, and Fabio Massacci. On the feasibility of detecting injections in malicious npm packages. In *Proceedings of the 17th International Conference on Availability, Reliability and Security*, pages 1–8, 2022.

2021 Duc-Ly Vu, Ivan Pashchenko, Fabio Massacci, Henrik Plate, and Antonino Sabetta. Lastpymile: identifying the discrepancy between sources and packages. In *Proceedings of the 2021 29th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*. ACM, 2021.

2021 Duc-Ly Vu, Ivan Pashchenko, and Fabio Massacci. Please hold on: more time= more patches? automated program repair as anytime algorithms. In *Proceedings of the IEEE/ACM 43nd International Conference on Software Engineering Workshops*. IEEE Press, 2021.

2021 Duc-Ly Vu. py2src: Towards the automatic (and reliable) identification of sources for pypi package. In *2021 36th IEEE/ACM International Conference on Automated Software Engineering (ASE)*, pages 1394–1396. IEEE, 2021.

2020 Duc-Ly Vu, Ivan Pashchenko, Fabio Massacci, Henrik Plate, and Antonino Sabetta. Typosquatting and combosquatting attacks on the python ecosystem. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 509–514. IEEE, 2020.

2020 Duc Ly Vu, Ivan Pashchenko, Fabio Massacci, Henrik Plate, and Antonino Sabetta. Towards using source code repositories to identify software supply chain attacks. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, pages 2093–2095. ACM, 2020.

2020 Ivan Pashchenko, Duc-Ly Vu, and Fabio Massacci. A qualitative study of dependency management and its security implications. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, pages 1513–1531. ACM, 2020.

2019 Duc-Ly Vu, Trong-Kha Nguyen, Tam V Nguyen, Tu N Nguyen, Fabio Massacci, and Phu H Phung. A convolutional transformation network for malware classification. In *2019 6th NAFOSTED Conference on Information and Computer Science (NICS)*, pages 234–239. IEEE, 2019.

Experience

Chainguard Inc

04/2024 – Present ***Chainguard Inc***, Visiting Researcher.
Project: Panic at the Distro! project: A study of Malware Prevention in Linux Distributions

Eastern International University

04/2024 – Present ***Eastern International University***, Lecturer at the Computing and Information Technology, Member of the CIT's AI Labs.

Vietnamese-German University

09/2023 – 02/2024 ***Vietnamese-German University***, Visiting Lecturer.
Taught Course: Introduction to Programming with Python

University of Information Technology - VNUHCM

09/2023 – Present ***University of Information Technology***, Visiting Lecturer.
Information Security Department

Chainguard Inc

06/2022 – 10/2022 ***Chainguard Inc***, Visiting Researcher.
Project: Bad Snakes: Understanding and Improving Python Package Index Malware Scanning

FPT University

06/2022 – 09/2023 ***FPT University***, Lecturer, Researcher.
Information Assurance Department

Forescout Technologies B.V.

02/2022 – 05/2022 ***Vedere Labs***, Security Researcher.
Malware Analysis, Malware Sandboxes

AssureMoss Project

2019 – 01/2022 ***Automated Program Repair, Software Supply Chain Attacks, Mining source code repositories***, European H2020 Project.

SAP Security Research, France

June,2019 – August, 2019 ***Open-Source Security: Safeguards and attack surface reduction***.
Developing a method to identify software supply chain attacks in PyPI.

Advisor : Henrik Plate, Antonino Sabetta, *Senior Researcher*, SAP Security Research (*Personal Web-page*)

March,2020 – May, 2020 ***Open-Source Security: Safeguards and attack surface reduction***.
Developing a method to identify software supply chain attacks in PyPI.

Advisor : **Henrik Plate, Antonino Sabetta**, *Senior Researcher*, SAP Security Research (*Personal Web-page*)

European Network for Cyber-security (NECS)

November,2017 – November, 2020 ***Software Vulnerability Analysis***, European Network for Cyber-security.
Qualitative and Quantitive Software Vulnerability Analysis

Advisor : Prof. Fabio Massacci (*Personal Web-page*)

Information Security Machine Learning Lab, Hongik Univeristy, South Korea

2015 – 2017 ***Malware detection using machine learning***.

Advisor : **Dr. Seong Oun Hwang**, *Professor, Department of Computer Science & Engineering*, Gachon University (*Personal Web-page*)

Bach Hung Khang Technology, Vietnam

January,2015 – Dec,2015 ***Developing and pentesting security aws on various systems including Windows, Linux, and Cisco devices***.

Advisor : **Mr. Hung Tran**, *CEO*, BHK Tech (*Personal Web-page*)

Fellowships & Awards

2021 ACM/Microsoft Student Research Competition in the Graduate category

2017 –2020 ***Marie Curie Research Fellowship*** of European Network of Security Project

2015 Receipt of three ***Good students*** scholarship at Posts and Telecommunications Institute of Technology.

Certificates

CCNA by **Cisco**

AI for everone by **deeplearning.ai**

Learning SQL Course by **Codecademy**

Learn the Command Line Course by **Codecademy**

Learn Web Scraping with Beautiful Soup Course by **Codecademy**

C1a English Language by **University of Trento, Itay**

Cleaning Data in Python Course by **DataCamp**

Convolutional Neural Networks in Tensorflow by **deeplearning.ai**

Excel Skills for Business: Intermediate I by **Macquarie Univeristy**

Improving Deep Neural Networks: Hyperparameter tuning, Regularization and Optimization by **deeplearning.ai**

Introduction to TensorFlow for Artificial Intelligence, Machine Learning, and Deep Learning by **deeplearning.ai**

Natural Language Processing in TensorFlow by **deeplearning.ai**

Neural Networks and Deep Learning by **deeplearning.ai**

Programming for Everybody (Getting Started with Python) by **University of Michigan**

Python Data Structures by **University of Michigan**

Statistical Thinking in Python (Part 1) Course by **DataCamp**

Structuring Machine Learning Projects by **deeplearning.ai**

Understanding and Visualizing Data with Python by **University of Michigan**

Write Professional Emails in English by **Georgia Institute of Technology**

pandas Foundations Course by **DataCamp**

Introduction to Open Source Security and Dependency Management by **Endor Labs**

Machine Learning for All by **University of London**

Software

C2Ass in *Simulate assembly code for learning purpose.*

bandit4mal in *A fork of Bandit tool with patterns to identifying malicious python code*

wtfptyhon-vi in *wtfpython in Vietnamese*

virustotalIntellgence in *A scanning tool supports detecting virus/malware by using VirusTotal.*

LastPyMile *A tool to detect code discrepancy in PyPI packages*

p2src *Automatic Identification of Source Code Repositories and Factors for Selecting New PyPI Packages*

Computer skills

Programming Languages	Python, scikit-learn, keras, Rust, Tensorflow, Latex, pandas, Jupyter notebook, matplotlib, pytest, sphinx, HTML
Web Technologies	HTML, CSS, Flask, Web scraping (Selenium, beautifulsoup)
Database	SQL, redis, MongoDB, MySQL
Documentation	Latex, Markdown, MS Words
Security	Ghidra, Yara, Cuckoo, Capstone Disassembler, IDA Disassembler, pestudio, SAST
Networking	TCP/IP, Cisco
Networking and security tools	Wireshark, Burp suite, nmap, Kali, radare, Capstone disassembler, Cuckoo sandbox, Unicorn emulator
Operating system	Linux, MacOS, Windows
Software version control	Git, SVN

Software development tools	Vim, dependency management tools (pipenv)
Forensic tools	PE tools, file, PEiD, strings
Cloud/Virtual machines	Google Cloud, VMWare, VirtualBox

Teaching Experience

Fall, 2024 :	**Networks and Data Communications**, Eastern International University, Vietnam.
Spring, 2024 :	**Advanced Firewall Systems**, Birmingham City University - University of Information Technology (BCU-UIT) , Vietnam.
Fall, 2023 :	**Intrusion Detection and Prevention Systems**, University of Information Technology, Vietnam.
Fall, 2023 :	**Introduction to Networking**, University of Information Technology, Vietnam.
Fall, 2023 :	**Cyber Security**, Birmingham City University - University of Information Technology, Vietnam.
Fall, 2023 :	**Introduction to Programming**, Vietnamese-German University, Vietnam.
Spring, 2023 :	**Database Security**, FPT University, Vietnam.
Spring, 2023 :	**Computer Architecture**, FPT University, Vietnam.
Spring, 2023 :	**Introduction to Computer Science**, FPT University, Vietnam.
Spring, 2023 :	**Introduction to Computing**, FPT University, Vietnam.
Summer, 2022 :	**Malware Analysis and Reverse Engineering**, FPT University, Vietnam.
Spring, 2021 :	**ICT Innovation course**, University of Trento, Italy.
Spring, 2021 :	**Cyber Risk Assesment**, University of Trento, Italy.
2015-2018	**Python Courses for System engineers**, BHK Tech, Vietnam.

Referees

Dr. Fabio Massacci
Professor, Department of Computer Science & Engineering
University of Trento, Italy
✉ fabio.massacci@ieee.org

Dr. Antonino Sabetta
Senior Researcher
SAP Security Research
France
✉ antonino.sabetta@sap.com

Dr. Henrik Plate
Security Researcher
Endor Labs
USA
✉ henrik.plate@sap.com