Erin Avllazagaj, PhD

Senior Vuln. Researcher I @ John Hopkins APL | albocoder@gmail.com | https://albocoder.github.io/

Professional Experience

JHU APL, Offensive Cyber Capabilities | *Senior Vuln. Researcher I* | *Laurel, MD, USA* Oct 2024 – **present**

Meta Platforms, Inc | *PhD Security Engineer Intern* | *California, USA* June 2022 – September 2022

- Migrated the an old Zoncolan static analysis pipeline while maintaining 100% uptime.
- Investigated all the customers and the use case of the pipeline on their end.
- Maintained excellent communication with our customers, the privacy team to ensure backwards compatability and seamless integration without the need to change their workflow.
- Automated the data transfer across tables in the big data management tools such as Dataswarm, Hive, Spark.
- Performed A/B testing to ensure seamless integration with our customers' needs.

EURECOM | *Visiting Scientist* | *Nice, France* July 2018 – August 2018

- Analyzed malware behavior data in the wild and performed case studies to highlight their variability.
- Identified the sources of noise in the dataset and sanitized the data.

Maryland Cybersecurity Center | *Research Intern* | *Maryland, USA* June 2017 – August 2017

- Investigated code reuse of exploits in the wild through case studies.
- Implemented prior papers and used their static analysis techniques to measure closeness of code snippets parsed with Joern.
- Derived a general high-level representation of the exploit development cycle in the wild, through case studies.

4S (contractor for HavelSan) | *Vulnerability Research* | *Ankara, Turkey* July 2016 – August 2016

- Tested a mission-critical Unity based simulation for security vulnerabilities.
- Used DevXUnityUnpacker, Cheat Engine and IDA Pro to statically and dynamically analyze the binary.

Education

University of Maryland, College Park Maryland, USA
Ph.D. *in Electrical and Computer Engineering* *Aug. 2018 – Aug. 2024*
* Advisors: Prof. Tudor Dumitraş, (co) Prof. Yonghwi Kwon

University of Maryland, College Park Maryland, USA
M.Sc. *in Electrical and Computer Engineering* *May 2024*

Bilkent University Ankara, Turkey
B.S. *in Computer Science* *Aug. 2014 – May 2018*

- Scholarly paper: "Privacy-Related Consequences of Turkish Citizen Database Leak"
  - Advisors: Prof. Erman Ayday, Prof. Ercüment Çiçek
- Senior Project: "Andlit"
  - Advisor: Prof. Ibrahim Körpeoğlu
  - The project is a social network of AI models that perform face recognition in real-time. It's designed to help the visually impaired recognise their environment, the friends and the *friends of their friends*. The project was called a "third eye" by various Turkish media agencies [1*] [2] [3] [4].

Honors and Awards

Fellowships

Clark Doctoral Fellowship GRA/GTA support (4 years)	2018
Clark Doctoral Fellowship stipend (first 2 semesters)	2018
Clark Doctoral Fellowship travel grant (4 years)	2018
Bilkent University full (Tuition + Accommodation) scholarship (all 4 years)	2014

Awards

1^{st} place in CSAW Applied Research Competition	2021
2^{nd} place in Informatics Olympiad of Tirana	2013

Projects

SCAVY: Discovery of Memory Corruption Targets in kernel for Privesc

Status: Paper accepted to USENIX Security 2024

- Developed *SCAVY*, a framework to discover memory corruption targets for privilege escalation in the Linux kernel
- Evaluated SCAVY by exploiting 10 CVEs using various memory targets
- Achieved a full end-to-end privilege escalation on one CVE without needing KASLR bypass and published a write-up of the exploit on *my blog*

Analysis of malware behavior in the wild

Status: Paper accepted to USENIX Security 2021

- Conducted first quantitative analysis of behavioral variability in malware, PUP, and benign samples
- Used a novel dataset of 7.6M execution traces from 5.4M real hosts across 113 countries and showed how behaviors change across hosts and time
- Demonstrated the impact on the effectiveness of malware detection using behavioral rules

Technical Skills

Languages: Python, C/C++, Java, SQL (Postgres), JS, R
Frameworks: LLVM, Flask, PyTorch, JUnit
Developer Tools: Git, Docker, TravisCI, VS Code, Visual Studio, PyCharm, Eclipse
Software analysis: American Fuzzy Lop (AFL)++, angr, Z3, LLVM, IDA Pro
Pen. testing: Metasploit, Armitage, Burp Suite, nmap, Wireshark

Publications

Conferences

∗ **E. Avllazagaj**, Y. Kwon, T. Dumitraş, "SCAVY: Automated Discovery of Memory Corruption Targets in Linux Kernel for Privilege Escalation", In USENIX Security 24, 2024

∗ **E. Avllazagaj**, Z. Zhu, L. Bilge, D. Balzarotti, T. Dumitraş, "When Malware Changed Its Mind: An Empirical Study of Variable Program Behaviors in the Real World", In 30th USENIX Security Symposium (USENIX Security 21), 2021

- 1^{st} *place winner* of CSAW21' Applied Research competition [certificate]
- Press highlights: [CSO-DE] [Cyberwire] [CSO-EN] [UMIACS]

Workshops

∗ N. Garg, I. Shahid, **E. Avllazagaj**, J. Hill, J. Han, N. Roy, "Thermware: Toward side-channel defense for tiny iot devices", The 24th International Workshop on Mobile Computing Systems and Applications (HotMobile' 23), 2023

∗ **E. Avllazagaj**, E. Ayday, E. Çiçek, "Privacy-Related Consequences of Turkish Citizen Database Leak", In International Workshop on Inference & Privacy in a Hyperconnected World (INFER' 16), 2016

Posters

∗ O. Suciu, **E. Avllazagaj**, T. Dumitraş, "The Secret Life of Pwns: Characterizing and Predicting Exploit Weaponization", In Conference on Applied Machine Learning for Information Security (CAMLIS' 19), 2019

Personal Blog (only featured publications)

∗ "SyzGPT: When the fuzzer meets the LLM"

∗ "CVE-2022-27666: My file your memory"

∗ "Inside commercial malware sandboxes"

Services

Program Committee

[Artifact Evaluation] Usenix Security	2021 – 2024
[Full PC Member] CSAW	2022, 2023
[Artifact Evaluation] PoPETS	2021 – 2023
[Journal Reviewer] IEEE ISCC	2022
[Journal Reviewer] Computer Science Review	2021

External reviewer

IEEE Security and Privacy (S&P)	2022 – 2023
USENIX Security Symposium (USENIX)	2019, 2023
Network and Distributed System Security Symposium (NDSS)	2020
ACM Conference on Computer and Communications Security (CCS)	2019 – 2020
International Symposium on Research in Attacks, Intrusions and Defenses (RAID)	2018 – 2019