HADJER BENKRAOUDA

E-mail: hadjerb2(at)illinois.edu
Mobile: +1 (217) 417-9093

RESEARCH INTERESTS

- Binary analysis
- Machine learning for binary analysis
- Machine learning for security
- Systems security

EDUCATION

University of Illinois at Urbana-Champaign, USA GPA: 4/4 *August '20-Present*
Ph.D. in Computer Science

New York University, USA GPA: 3.83/4 *January '17*
Master of Science in Cybersecurity

United Arab Emirates University, UAE GPA: 3.86/4 *January '15*
Bachelors of Science in Electrical Engineering

New York University Abu Dhabi, UAE *May '13*
Sheikh Mohamed Ben Zayed's Scholars Program

RESEARCH EXPERIENCE

University of Illinois at Urbana-Champaign, USA *August '20-Present*
Research Assistant
Projects
Supervisor: *Gang Wang*

1. Machine Learning for Binary Analysis *Fall '21-Present*
   - Porting NLP techniques for code and data separation in non-standard binary formats.

Supervisor: *Klara Nahrstedt*

1. Attacks on Partitioned Enclave Execution for Neural Networks *Fall '20-Summer '21*
   - Developed an attack on distributed ML systems that can recover private images from embeddings/Intermediate representation
2. Simulating Backdoor Attacks using Packet Dropping *Spring '20-Fall 2021*
   - Created a dataset of triggered images using packet drops and trained a backdoored ML model to cause mis-classifications

Center for Cyber Security, NYUAD, UAE *August '18-August '20*
Research Assistant
Projects
Supervisor: *Michail Maniatakos*

1. Binary Analysis of IEC 61131-3 compliant PLC Control Applications *May '19-August '20*
   - Created and compiled a database of PLC control applications and performed binary analysis to identify security vulnerabilities in PLC applications
2. Automated Generation of Attacks on Industrial Control Systems *January '19-August '19*
   - Tested and developed a machine learning-based industrial process classifier using real-world PLC application binaries
3. Secure Firmware Updates for legacy PLCs *April '19-October '19*
   - Evaluated the firmware update process for legacy PLCs and proposed an online solution for preventing malicious firmware updates

JOURNAL PUBLICATION

1. Sarkar, E., **Benkraouda, H.**, Maniatakos, M. "FaceHack: Attacking Facial Recognition Systems using Malicious Facial Characteristics." *In IEEE Transactions on Biometrics, Behavior, and Identity Science, 2021*

2. Barka, E., Kerrache, C., **Benkraouda, H.**, Shuaib, K., Ahmad, F., Kurugollu, F. "Towards a trusted unmanned aerial system using blockchain (BUAS) for the protection of critical infrastructure." *Wiley Transactions of emerging technologies. 2019*

CONFERENCE AND WORKSHOP PROCEEDINGS

1. Wang, C., Jia, Z., **Benkraouda, H.**, Zevnik, C., Heuermann, N., Foulger, R., Handler, J., Wang, G. "VeriSMS: A Message Verification System for Inclusive Patient Outreach against Phishing Attacks." *In Proceedings of ACM CHI Conference on Human Factors in Computing Systems (CHI), 2024.*
2. **Benkraouda, H.**, Agrawal, A., Tychalas, D., Sazos, M., Maniatakos, M. 2023. Towards PLC-Specific Binary Analysis Tools: An Investigation of Codesys-Compiled PLC Software Applications. *In Proceedings of the 5th Workshop on CPS&IoT Security and Privacy (CPSIoTSec '23).*
3. Mink, J., **Benkraouda, H.**, Yang, L., Ciptadi, A., Ahmadzadeh, A., Votipka, D., Wang, G. "Everybody's Got ML, Tell Me What Else You Have: Practitioners' Perception of ML-Based Security Tools and Explanations." *In Proceedings of the 44th IEEE Symposium on Security and Privacy, 2023 (IEEE S&P).*
4. Tychalas, D., **Benkraouda, H.**, Maniatakos, M. "ICSFuzz: Manipulating I/Os and Repurposing Binary Code to Enable Instrumented Fuzzing in ICS Control Applications." *In Proceedings of The 30th USENIX Security Symposium (USENIX Security), 2021.*
5. **Benkraouda, H.** and Qian, J. and Hung Tran, H., Kaplan, B. "Attacks on Visualization-Based Malware Detection: Balancing Effectiveness and Executability." *MLHat: International Workshop on Deployable Machine Learning for Security Defense, ACM SIGKDD. 2021.*
6. **Benkraouda, H.**, Nahrstedt, K. "Image Reconstruction Attacks on Distributed Machine Learning Models." DistributedML Workshop co-located with *The 17th International Conference on emerging Networking EXperiments and Technologies (CoNext '21).*
7. Sarkar, E., **Benkraouda, H.**, Maniatakos, M. "On Process-independent Automated Generation of Attacks on Industrial Control Systems." *In the proceedings of the ACM ASIA Conference on Computer and Communications Security. 2020*
8. **Benkraouda, H.**, Chakkantakath, M., Keliris, A., Maniatakos, M. "SNIFU: Secure Network Interception for Firmware Updates in Legacy PLCs." *In IEEE VLSI Test Symposium (VTS). 2020*
9. **Benkraouda, H.**, Diwan, N., Wang, G. "Code and Data separation for Non-Standard Binary File Formats Using Instruction Embedding." [In progress]

TEACHING AND MENTORING EXPERIENCE

University of Illinois Urbana-Champaign

1. *Teaching Assistant* *Fall '23*
   CS 562: Advanced Topics in Security, Privacy, and Machine Learning

Polygence

1. *Project Mentor* *Summer-Fall '22*
   Project: A User-study on perceptions of security and privacy among high-school students
2. *Project Mentor* *Summer-Fall '22*
   Project: A survey on efficient cryptographic schemes for low-resource devices

New York University Abu Dhabi

1. *Summer Internship Mentor* *Summer '20*
   Project: Code and Data separation for Unknown Binary File Formats Using Semantic Segmentation

2. *Summer Internship Mentor* *Summer '19*
   Project: Reverse Engineering Programmable Logic Controllers' Binaries
3. *Teaching Assistant* *Spring '19, Spring '20, Summer '20*
   CDAD-UH 1037Q: Cyberwarfare

PROFESSIONAL EXPERIENCE

Bloomberg L.P., Bloomberg New Energy Finance, USA *August '17-January '18*
Research Analyst

- Carried-out thorough research about cybersecurity vulnerabilities and solutions in industrial control systems (ICSs) and published professional reports highlighting findings
- Performed research interviews and client meetings with project stakeholders through emails, calls, and in person meetings

PROFESSIONAL REPORTS

1. **Benkraouda, H.**, Curry, C., Wilshire, M. "Industrial Cybersecurity: An Urgent Need." *Bloomberg New Energy Finance Journal. 2018*
2. **Benkraouda, H.**, Curry, C., Wilshire, M. "The Growing Cybersecurity Risks in Energy." *Bloomberg New Energy Finance Journal. 2017*

AWARDS AND HONORS

iMentor Workshop Travel Grant *Nov 23*
ACM CCS Student Travel Grant *Nov 23*
Grainger Engineering Diversity Ambassadors Scholarship *Fall '23- Spring '25*
ACM CCS Student Travel Grant *Nov 22*
Illinois Cyber Security Scholars Program (ICSSP) - *Declined* *Fall '21 - Spring 24*
IEEE Symposium on Security and Privacy Student Travel Grant *May 21*
ACM SIGSOFT CAPS - ICSE 21 *May 21*
NYU Merit based Scholarship Award *Spring '15-Fall '16*
United Arab Emirates University Honors Graduate *Fall '14*
Sheikh Mohamed Ben Zayed's Scholar *Fall '12-Spring '13*

PROFESSIONAL SOCIETY MEMBERSHIPS

Arab American Association of Engineers and Architects
IEEE Student Fellow
IEEE Women in Engineering Society

REFERENCES

Gang Wang, Assistant Professor
Department of Computer Science, University of Illinois at Urbana-Champaign
Phone: +1 217-244-1008, Email: gangw@illinois.edu
Klara Nahrstedt, Ralph M. and Catherine V. Fisher Professor
Department of Computer Science, University of Illinois at Urbana-Champaign
Phone: +1 217-244-6624, Email: klara@illinois.edu
Michail Maniatakos, Associate Professor
Electrical and Computer Engineering Department, New York University Abu Dhabi
Phone: +9712-628-4591, Email: michail.maniatakos@nyu.edu