Ying Yuan

Department of Computer Science
Sapienza University of Rome
Viale Regina Elena 295, Rome, Italy

Email: ying.yuan@uniroma1.it
Web: https://yingyuansec.github.io/

Research Interests

Cybersecurity; Machine Learning; Usable Security.

Work Experience

Sapienza University of Rome, Rome, Italy. Mar. 2025 – Present
Postdoctoral Researcher, Department of Computer Science
Supervisor: Prof. Luigi Vincenzo Mancini

University of Padua, Padua, Italy. Mar. 2024 – Feb. 2025
Postdoctoral Researcher, Department of Mathematics
Supervisor: Prof. Mauro Conti

Education

University of Padua, Padua, Italy. Oct. 2020 – Mar. 2024
Ph. D. in Brain, Mind and Computer Science
Advisor: Mauro Conti

Beijing University of Posts and Telecommunications, Beijing, China. Sep. 2017 – Jun. 2020
Master of Engineering, Cyberspace Security
Advisor: Hongliang Zhu

QiLu University of Technology, Jinan, China. Sep. 2013 – Jun. 2017
Bachelor of Engineering, Computer Science and Technology

Publications

Refereed publications

1. **[WWW '24] Ying Yuan**, Qingying Hao, Giovanni Apruzzese, Mauro Conti, Gang Wang. "'Are Adversarial Phishing Webpages a Threat in Reality?' Understanding the Users' Perception of Adversarial Webpages" In Proc. of *The ACM Web Conference (WWW)*, 2024 (Oral, ACM Artifacts Available badge). Acceptance rate = 20.2%.
2. **[USENIX Security '24]** Qingying Hao, Nirav Diwan, **Ying Yuan**, Giovanni Apruzzese, Mauro Conti, Gang Wang. "It Doesn't Look Like Anything to Me: Using Diffusion Model to Subvert Visual Phishing Detectors." In Proc. of *USENIX Security*, 2024 (Oral). Acceptance rate = 18.3%.
3. **[COSE '24] Ying Yuan**, Giovanni Apruzzese, Mauro Conti. "Beyond the West: Revealing and Bridging the Gap between Western and Chinese Phishing Website Detection." In *(Elsevier) Computers & Security*, 2024.
4. **[DTRAP '23] Ying Yuan**, Giovanni Apruzzese, Mauro Conti. "Multi-SpacePhish: Extending the Evasion-space of Adversarial Attacks against Phishing Website Detectors using Machine Learning." In *ACM Digital Threats: Research and Practice (DTRAP)*, 2023.
5. **[ACSAC '22]** Giovanni Apruzzese*, Mauro Conti, **Ying Yuan***. "SpacePhish: The Evasion-space of Adversarial Attacks against Phishing Website Detectors using Machine Learning." In Proc. of *ACSAC*, 2022 (Oral, ACM Artifacts Reusable, *Equal contribution). Acceptance rate = 24.1%.
6. **[IEEE Access '19]** Hongliang Zhu, **Ying Yuan**, Yuling Chen, Yaxing Zha, Wanying Xi, Bin Jia, and Yang Xin. "A Secure and Efficient Data Integrity Verification Scheme for Cloud-IoT based on Short Signature." In *IEEE Access*, 2019.
7. **[CEA '19] Ying Yuan**, Hongliang Zhu, Yuling Chen, Zhi Ouyang, Yang Xin, Yixian Yang. "Survey of Data Integrity Verification Technology Based on Provable Data Possession." In *Computer Engineering and Applications*, 2019 (in Chinese).

Patent

8. Hongliang Zhu, **Ying Yuan**, Yuling Chen, Ting Han, Yang Xin. "A Remote Data Integrity Verification Method Based on Short Signature." CN.2019101628311, 2019.

Visiting Experience

University of Liechtenstein – Visiting Scholar Sep. 2023

Advisor: Giovanni Apruzzese

- **[COSE'24]** Investigated the gap between Chinese and Western phishing website detection.

University of Illinois at Urbana-Champaign – Visiting Scholar Apr. 2023 – Jun. 2023

Advisor: Gang Wang

- **[WWW'24]** Investigated the threat of adversarial phishing websites in practice.
- **[USENIX'24]** Investigated the effectiveness of logos generated by diffusion model.

Poster & Talk

"Are Adversarial Phishing Webpages a Threat in Reality?" *The ACM Web Conference (WWW)* 2024 (Poster & Oral).

Project

PAAM - Privacy Aware Anti Malware, PNRR 2022 PRIN, Mar. 2024 - Feb. 2025

Code and Dataset Release

- "Beyond the West: Revealing and Bridging the Gap between Western and Chinese Phishing Website Detection." https://github.com/joanyy/ChiPhish
- "'Are Adversarial Phishing Webpages a Threat in Reality?' Understanding the Users' Perception of Adversarial Webpages." https://github.com/hihey54/www24_threatAdvPhish
- "SpacePhish: The Evasion-space of Evasion Attacks against Phishing Website Detectors using Machine Learning." https://github.com/hihey54/acsac22_spacephish

Professional Qualification

CITI IRB Training Completion certificate (Training in the Protection of Human Subjects)

Original Vulnerabilities Contribution

- CNVD-YCIW-201707053840
- CNVD-YCIW-201708048282

Professional Services & Organization

Program Committee Member

- ESORICS, 2026
- USENIX Security Symposium, 2026
- Annual Computer Security Applications Conference (ACSAC), 2025

Artifact Evaluation Committee Member

- USENIX Security Symposium, 2025
- ACM The Web Conference 2024 (Artifacts reviewer)

Technical Program Committee Member

- Workshop on AI for Cyber Threat Intelligence, in conjunction with ACSAC 2024
- Workshop on Machine Learning and Deep Learning for Wireless Security, co-located with IEEE GLOBECOM 2024
- Workshop on DevSecOps Research and Opportunities, co-located with EuroS&P 2025

Journal Reviewer

- IEEE Transactions on Dependable and Secure Computing (TDSC)
- Computer Standards & Interfaces
- IEEE Access

Conference Organization

- Assistant at The 27th International Symposium on Research in Attacks, Intrusions and Defenses (RAID) 2024, Padua, Italy

Summer School

Participate in summer school on real-world crypto and privacy, Jun. 2022, Šibenik, Croatia

Competition

Machine Learning Security Evasion Competition (MLSEC), won the 4th, Aug. 2022 - Sep. 2022

Professional Skills

- **Programming Languages**: Python, Java, HTML, etc;
- **Machine Learning Algorithms**: RF, LR, SVM,XGBoost, CNN, LSTM, etc;
- **Penetration Testing**: BurpSuite, AWVS, Sqlmap, Nmap, etc;
- **Tools and OS**: Jupyter, Pandas, Numpy, Linux, Mysql, Overleaf, Qualtrics, Prolific, etc.
- **Languages**: English (IELTS B2, in 2020; and CEFR C1, in 2022), Chinese (Native)

Awards

Outstanding Graduates of BUPT and Outstanding Graduates of Beijing	Jun. 2020
Cyber Security Scholarship	Oct. 2019
Outstanding Graduates of Shandong	Jun. 2017