Curriculum vitae

INFORMAZIONI PERSONALI

Ying Yuan

TITOLO DI STUDIO

Phd degree in Brain, Mind and Computer Science

ESPERIENZA PROFESSIONALE

March 2024 – Present

Assegnista di Ricerca

Department of Mathematics at the University of Padua
Advisor: Mauro Conti
Funded by the project PRIN 2022 n. P20225J5YS “PAAM - Privacy Aware Anti Malware".

September 2023

Visiting Scholar

University of Liechtenstein
Advisor: Giovanni Apruzzese
Reveal and bridge the gap between Chinese and Western phishing website detection

April 2023 – June 2023

Visiting Scholar

Department of Computer Science at the University of Illinois at Urbana-Champaign
Advisor: Gang Wang
Measure the threat of adversarial phishing samples in practice

ISTRUZIONE E FORMAZIONE

2020–2024

PhD Degree in Brain, Mind and Computer Science
Curriculum Computer Science for Societal Challenges and Innovation

University of Padua, Italy
Supervisor: Mauro Conti
Thesis Title: “Machine Learning for Phishing Website Detection"

2017–2020

Master of Engineering in Cyberspace Security

School of Cyberspace Security, Beijing University of Posts and Telecommunications, China
Supervisor: Hongliang Zhu

2013–2017

Bachelor of Engineering in Computer Science and Technology

School of Information, QiLu University of Technology, China

COMPETENZE PERSONALI

Lingua madre: Chinese

Altre lingue

	COMPRENSIONE		PARLATO		PRODUZIONE SCRITTA
	Ascolto	Lettura	Interazione	Produzione orale	
English	Utente avanzato	Utente avanzato	Utente autonomo	Utente autonomo	Utente autonomo

Livelli: A1 e A2: Utente base – B1 e B2: Utente autonomo – C1 e C2: Utente avanzato
Quadro Comune Europeo di Riferimento delle Lingue

Competenze comunicative

I possess strong communication skills demonstrated through:

- International Research Collaboration: Collaborating with research teams from different countries during my PhD, successfully managing diverse working styles and cultural perspectives. Effectively coordinated research efforts across time zones and cultural boundaries to achieve shared research objectives.
- Conference Presentations (Oral and Poster): Presented research findings at top-tier international conferences (e.g., WWW'2024), showcasing the ability to communicate complex ideas to expert audiences. Engaged in scholarly discussions and defended my work through Q&A sessions with leading researchers in the field.

Competenze organizzative e gestionali

- I served as an organizing assistant for RAID 2024 (Symposium on Research in Attacks, Intrusions and Defenses).
- I am a Technical Program Committee member for multiple workshops in the field of Cyber Security, for example, Workshop on AI for Cyber Threat Intelligence in conjunction with ACSAC 2024 and IEEE GLOBECOM 2024 Workshop on Machine Learning and Deep Learning for Wireless Security.

Competenze professionali

- Skilled in using Python for data analysis, machine learning, and security research. I successfully developed and released peer-reviewed code for security research projects on GitHub, and received Artifacts Available and Artifacts Reusable badges from WWW 2024 and ACSAC 2022, respectively.
- Provided professional review services for high-impact journals, including Computer Standards & Interfaces, and acted as an Artifact Evaluation Committee member at Usenix Security 2025.

Competenze digitali

Excellent computer skills. Python | Jupyter Notebook | VS code | Git | Overleaf.

ULTERIORI INFORMAZIONI

Pubblicazioni

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)*, Singapore, May 2024 (Oral, Artifacts Available). (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 *the 33rd USENIX Security Symposium (USENIX Security)*, Philadelphia, PA, August 2024. (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 *the 38th Annual Computer Security Applications Conference (ACSAC)*, Austin, TX, December 2022 (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	Hongliang Zhu, **Ying Yuan**, Yuling Chen, Ting Han, Yang Xin. "A Remote Data Integrity Verification Method Based on Short Signature." CN.2019101628311, 2019. (China)
Original Vulnerabilities Contribution	CNVD-2017-21518, CNVD-2017-16452
Presentazioni	"Are Adversarial Phishing Webpages a Threat in Reality?" *The ACM Web Conference (WWW)*, Singapore, May 16 2024. (Conference talk & Poster)
Riconoscimenti e premi	– Jun. 2020, Outstanding Graduates of BUPT and Outstanding Graduates of Beijing
Dati personali	Autorizzo il trattamento dei miei dati personali ai sensi del Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali".