UNIVERSITÀ DEGLI STUDI DI MILANO

Curriculum vitae

AL MAGNIFICO RETTORE
DELL'UNIVERSITA' DEGLI STUDI DI MILANO **COD. ID: 5420**

Il sottoscritto chiede di essere ammesso a partecipare alla selezione pubblica, per titoli ed esami, per il conferimento di un assegno di ricerca presso il Dipartimento di **Informatica**

Responsabile scientifico: **Prof. Ernesto Damiani**

Lara Mauri

CURRICULUM VITAE

INFORMAZIONI PERSONALI

Cognome	Mauri
Nome	Lara

ISTRUZIONE E FORMAZIONE

Titolo	**Corso di studi**	**Università**	**Anno conseguimento titolo**
Laurea Magistrale o equivalente	Sicurezza Informatica	Università degli Studi di Milano	2017
Dottorato Di Ricerca	Informatica	Università degli Studi di Milano	2022

LINGUE STRANIERE CONOSCIUTE

Lingue	**Livello di conoscenza**
Inglese	Buono
Francese	Autonomo

PREMI, RICONOSCIMENTI E BORSE DI STUDIO

Anno	**Descrizione premio**
2018 – 2021	Borsa di studio del Dottorato di Ricerca, Dipartimento di Informatica, Università degli Studi di Milano

ATTIVITÀ DI RICERCA

ML Security

The research work is in the novel field of *Adversarial machine learning* and focuses on the problem of increasing the robustness of Machine Learning (ML) models against adversarial interference. In particular, I investigated how to improve the resilience of ML models against training-time attacks along two axes. On one hand, by increasing the models' robustness via composite architectures. On the other hand, by enhancing the trustworthiness of data used for training via ad hoc consensus protocol definition. In my doctoral dissertation, I linked the risk of ML training data tampering to the redundancy and diversity in ML model design needed to alleviate it by proposing different defense techniques, under black-box knowledge assumptions on both the attacker and defender, acting at different stages of the learning process.

ATTIVITÀ DI FORMAZIONE O DIDATTICHE

Anno	**Descrizione attività**
A.A. 2021/2022 A.A. 2020/2021 A.A. 2019/2020 A.A. 2018/2019 A.A. 2017/2018	Tutor didattico di *Progettazione di software sicuro*. Corso di Laurea in Sicurezza dei Sistemi e delle Reti Informatiche (edizione on-line), Università degli Studi di Milano. [Art. 45 del Regolamento Generale d'Ateneo]
June 2018 – September 2018	Assegnista di ricerca presso il Dipartimento di Informatica dell'Università degli Studi di Milano nell'ambito del programma di ricerca "Studio di politiche di sicurezza e privacy per gli Enti di formazione e ricerca universitaria conformi alle misure di sicurezza AgID e al regolamento europeo GDPR", sotto la guida del Prof. Ernesto Damiani
March 2018 – June 2018	Attività di tutorato presso il Dipartimento di Informatica dell'Università degli Studi di Milano nell'ambito del programma di addestramento introduttivo alla cybersecurity "Cyberchallenge.IT" organizzato dal Laboratorio Nazionale di Cybersecurity del CINI in collaborazione con il Centro di Ricerca di Cyber Intelligence e Information Security della Sapienza di Roma
October 2017 – December 2017	Collaborazione all'attività di tutorato didattico per gli iscritti ai corsi di laurea specialistica magistrale per l'insegnamento di *Progettazione del software / Progettazione di software sicuro*. Corso di Laurea in Informatica e Corso di Laurea in Sicurezza dei Sistemi e delle Reti Informatiche, Università degli Studi di Milano. [Art. 19 del Regolamento della collaborazione degli studenti ai servizi dell'Università]
March 2017 – April 2017 November 2016 – December 2016	Attività di docenza per la promozione della cultura digitale presso sedi di biblioteche della provincia di Cremona, Associazione Cremasca Studi Universitari

ATTIVITÀ PROGETTUALE

Anno	Progetto
2020–2023	PALM (Prevention and detection of poisoning and adversarial Attacks on Machine Learning Models), DI participates as subcontractor of the Khalifa University of Science and Technology and the Technology Innovation Institute (TII/SSRC/2065/2020)
2020–2021	SEED 2019 (Bando Straordinario per Progetti Interdipartimentali 2019 – Piano di Sostegno alla Ricerca [Linea 3], Università degli Studi di Milano): CRIPTO S.O.S. (Cripto-valute: sfida alla sovranità dello Stato? Un'indagine storico-economica, giuridica e tecnica)
2019–2023	Horizon 2020 (SU-ICT – Boosting the effectiveness of the Security Union): CONCORDIA (Cyber security cOmpeteNce fOr Research anD Innovation)
2019–2022	Horizon 2020 (EU.3.7.4 – Improve cyber security): THREAT-ARREST (Cyber Security Threats and Threat Actors Training - Assurance Driven Multi-Layer, end-to-end Simulation and Training)

CONGRESSI, CONVEGNI E SEMINARI

Data	Titolo	Sede
July 26–28, 2021	IEEE International Conference on Cyber Security and Resilience (CSR 2021)	Virtual conference (due to COVID-19)
October 20, 2020	13th IEEE International Conference on Cloud Computing (CLOUD 2020)	Virtual conference (due to COVID-19)
February 4, 2020	3rd Distributed Ledger Technology Workshop (DLT 2020)	Ancona, Italy
September 16–20, 2019	6th Summer School on Network and Information Security (NIS19)	Heraklion, Greece
June 5–7, 2019	2nd Summer School on Industry Digital Evolution (IDE19)	Carovigno, Italy
February 12, 2019	2nd Distributed Ledger Technology Workshop (DLT 2019)	Pisa, Italy

PUBBLICAZIONI

Articoli su riviste

L. Mauri and E. Damiani. (2022). "Modeling Threats to AI-ML Systems Using STRIDE." *Sensors* 22(17), 6662. doi: 10.3390/s22176662

L. Mauri and E. Damiani. (2021). "Estimating Degradation of Machine Learning Data Assets." *ACM Journal of Data and Information Quality* 14, 2, Article 9 (June 2022), 15 pages. doi: 10.1145/3446331

Capitoli di libri

L. Mauri, S. Cimato, and E. Damiani. (2022). "Untangling the XRP Ledger: Insights and Analysis." In: Furnell, S., Mori, P., Weippl, E., Camp, O. (eds) Information Systems Security and Privacy. ICISSP 2020. *Communications in Computer and Information Science*, vol 1545. Springer, Cham. doi: 10.1007/978-3-030-94900-6_3

Atti di convegni

L. Mauri and E. Damiani. (2021). "STRIDE-AI: An Approach to Identifying Vulnerabilities of Machine Learning Assets." *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, pp. 147-154. doi: 10.1109/CSR51186.2021.9527917

Selezionato tra i migliori paper della conferenza per la pubblicazione di una versione estesa nello Special Issue di Sensors "Selected Papers from the IEEE CSR 2021"

L. Mauri, E. Damiani, and S. Cimato. (2020). "Be Your Neighbor's Miner: Building Trust in Ledger Content via Reciprocally Useful Work." *In 2020 IEEE 13th International Conference on Cloud Computing (CLOUD)*, pp. 53-62, doi: 10.1109/CLOUD49709.2020.00021

L. Mauri, S. Cimato, and E. Damiani. (2020). "A Formal Approach for the Analysis of the XRP Ledger Consensus Protocol." *In Proceedings of the 6th International Conference on Information Systems Security and Privacy*, *ICISSP 2020*, Valletta, Malta, pp. 52-63. doi: 10.5220/0008954200520063

Selezionato tra i migliori paper della conferenza per la pubblicazione di una versione estesa in *Communications in Computer and Information Science (CCIS, vol 1545)*

C. Braghin, S. Cimato, E. Damiani, F. Frati, L. Mauri, and E. Riccobene. (2019). "A Model Driven Approach for Cyber Security Scenarios Deployment." *In Computer Security – ESORICS 2019 International Workshops, IOSec, MSTEC, and FINSEC, Lecture Notes in Computer Science*, vol 11981, pp. 107-122. doi: 10.1007/978-3-030-42051-2_8

C. Braghin, S. Cimato, S. R. Cominesi, E. Damiani, and L. Mauri. (2019). "Towards Blockchain-Based E-Voting Systems." *In Abramowicz, W., Corchuelo, R. (eds) Business Information Systems Workshops, BIS 2019. Lecture Notes in Business Information Processing*, vol 373. doi: 10.1007/978-3-030-36691-9_24

L. Mauri, S. Cimato, and E. Damiani. (2018). "A Comparative Analysis of Current Cryptocurrencies." *In Proceedings of the 4th International Conference on Information Systems Security and Privacy, ICISSP 2018*, Funchal, Madeira – Portugal, pp. 127-138. doi: 10.5220/0006648801270138

Tesi di Dottorato

L. Mauri. (2022). "Data Partitioning and Compensation Techniques for Secure Training of Machine Learning Models." *Scuola di Dottorato in Informatica*, XXXIV ciclo. Università degli Studi di Milano. Settore Scientifico-Disciplinare: INF/01 Informatica. Tutor: Prof. Ernesto Damiani. Co-tutor: Prof. Bruno Apolloni. Direttore della Scuola di Dottorato: Prof. Paolo Boldi

ALTRE INFORMAZIONI

Organizzazione di conferenze e workshop

Program Committee:

- 2021 IEEE International Conference on Smart Data Services (IEEE SMDS 2021), Virtual conference, September 5–10, 2021
- SEPT (Security, Privacy & Trust in Computing) at 2021 IEEE 45th Signature Conference on Computers, Software, and Applications (COMPSAC 2021), Virtual conference, July 12–16, 2021
- 7th International Conference on Information Systems Security and Privacy (ICISSP 2021), Virtual conference, February 11–13, 2021
- 6th International Conference on Information Systems Security and Privacy (ICISSP 2020), Valletta, Malta, February 25–27, 2020

Organizing Committee:

- "Blockchain technology: una prospettiva accademica ed aziendale", SEED 2019, Via Celoria 18, Milan, November 16, 2021
- "Criptovalute e diritto: problemi attuali e sfide future", SEED 2019, Webinar, March 26, 2021
- "Criptovalute: sfida alla sovranità dello stato? Un'indagine storico-economica, giuridica e tecnica", SEED 2019, Webinar, October 20 and 27, 2020

Referaggio

Journals:

- *IEEE Transactions on Services Computing*
- *IEEE Transactions on Fuzzy Systems*
- *International Journal of Knowledge and Learning*
- *Electronic Commerce Research and Applications*
- *Human-centric Computing and Information Sciences*

- *Multimedia Tools and Applications*
- *Security and Communication Networks*

Conferences:

- ICISSP 2021 - 7th International Conference on Information Systems Security and Privacy, Virtual conference, February 11–13, 2021
- ICISSP 2020 - 6th International Conference on Information Systems Security and Privacy, Valletta, Malta, February 25–27, 2020
- WCNC-SFCS 2019 - IEEE Wireless Communications and Networking Conference, Marrakech, Morocco, April 15–18, 2019
- ICME 2018 - IEEE International Conference on Multimedia and Expo, San Diego, USA, July 23-27, 2018
- SEKE 2018 - 30th International Conference on Software Engineering and Knowledge Engineering, San Francisco Bay, USA, July 1–3, 2018

Le dichiarazioni rese nel presente curriculum sono da ritenersi rilasciate ai sensi degli artt. 46 e 47 del DPR n. 445/2000.

Il presente curriculum, non contiene dati sensibili e dati giudiziari di cui all'art. 4, comma 1, lettere d) ed e) del D.Lgs. 30.6.2003 n. 196.

RICORDIAMO che **i curricula SARANNO RESI PUBBLICI sul sito di Ateneo** e pertanto si prega di non inserire dati sensibili e personali. Il presente modello è già precostruito per soddisfare la necessità di pubblicazione senza dati sensibili.

Si prega pertanto di **NON FIRMARE** il presente modello.

Luogo e data: Milano, 28/9/2022