CURRICULUM VITAE
Luigi Romano

Contact info

Dipartimento di Ingegneria - Università degli Studi di Napoli "Parthenope"
Centro Direzionale di Napoli, Isola C4 - 80143 Napoli
e-mail: luigi.romano@uniparthenope.it; prof.luigi.romano@gmail.com
Tel: +39-081-5476700
Cell: +39-333-3016817
skype: luigi.romano
Web: http://www.fitnesslab.eu/

Dati Personali

È nato a Napoli il 20/07/1968.
È coniugato con due figli.

Posizione Attuale

È Professore Ordinario per il settore scientifico-disciplinare ING-INF05 "Sistemi di elaborazione delle informazioni" presso il Dipartimento di Ingegneria dell'Università degli Studi di Napoli "Parthenope".
È Prorettore alle Tecnologie Informatiche del sopra citato ateneo.

Posizioni Precedenti

2005-2011
Professore Associato del settore scientifico-disciplinare ING-INF05 presso il Dipartimento per le Tecnologie dell'Università degli Studi di Napoli "Parthenope".

2000-2005
Ricercatore del settore scientifico-disciplinare ING-INF05 presso il Dipartimento di Informatica e Sistemistica dell'Università degli Studi di Napoli di "Federico II".

1996 -1998
Visiting Scholar - Visiting Researcher
Center for Reliable and High-Performance Computing - Università dell'Illinois ad Urbana-Champaign

Titoli di Studio

Dottorato di Ricerca in Ingegneria Elettronica ed Informatica – Aprile 1999.
Laurea in Ingegneria Elettronica (indirizzo Informatico) con voti 110/110 e lode – Dicembre 1994.

Attività Professionale, Scientifica e Didattica

È un esperto di livello internazionale di cybersecurity, con particolare riferimento ai sistemi di rete critici, cioè sistemi complessi costituiti da un elevato numero di unità funzionali hardware e software collegate in rete, caratterizzati da requisiti stringenti di sicurezza, affidabilità e prestazioni. Esempi di sistemi di rete critici emergenti sono le applicazioni per: l'Industria 4.0; l'e-banking; l'e-government e l'e-business; la telemedicina e la telesorveglianza; il trasporto multimodale; il controllo del traffico spaziale, aereo e ferroviario.

È uno dei tre esperti nominati dalla European Network and Information Security Agency (ENISA, http://enisa.europa.eu/) per la definizione delle "Recommendations on aligning research programme with policy in the specialized area of NIS[1]".
È stato membro del Priorities of Research On Current and Emerging Network Technologies (PROCENT) Expert Group, un gruppo di esperti nominato da ENISA.

[1] NIS = Network and Information Security

Ha collaborato con ENISA anche sulle tematiche relative alla security della supply chain dell'industria ICT (Information and Communication Technology).

È il Chair del Settore Guida 4 ("Cyber Security") della piattaforma SERIT (Security Research in ITaly). SERIT è la Piattaforma Tecnologica Nazionale sulla Sicurezza promossa congiuntamente da CNR e Finmeccanica (http://www.piattaformaserit.it/).

È membro del gruppo IMG-S TA, un'organizzazione promossa dalla AeroSpace and Defence Industries Association of Europe (ASD, http://www.asd-europe.org/) che ha il compito di formulare proposte per la Commissione Europea riguardo alle linee di finanziamento per la sicurezza informatica.

Ha una consolidata esperienza nella conduzione di progetti di ricerca finanziati dalla Commissione Europea. Di seguito si riportano soltanto quelli relativi alla sicurezza ed all'affidabilità dei sistemi di rete, finanziati nell'ambito del Framework Programme 7 (FP7) e di Horizon 2020 (H2020):

- INSPIRE (INcreasing Security and Protection through Infrastructure Resilience, http://www.inspire-strep.eu/), Grant agreement no.: 225553 - Technical Coordinator del progetto;
- INSPIRE INCO (INSPIRE INternational COoperation), http://www.inspire-inco.eu/), Grant agreement no.: 248737 - Technical Coordinator del progetto;
- INTERSECTION (INfrastructure for heTErogeneous, Resilient, SEcure, Complex, Tightly Inter-Operating Networks, http://www.intersection-project.eu/), Grant agreement no.: 216585 - Technical Lead per il partner CINI;
- STREAM (Scalable Autonomic Streaming Middleware for Real-time Processing of Massive Data Flows, http://www.streamproject.eu/), Grant agreement no.: 216181 - Technical Lead per il partner EPSILON;
- MASSIF (MAnagement of Security information and events in Service InFrastructures), Grant agreement no.: 257475 - Technical Lead per il partner CINI;
- SRT-15 (Subscription Racing Technology for 2015, http://www.srt-15.eu/), Grant agreement no.: 257843 - Technical Lead per il partner EPSILON;
- SAWSOC (Situation AWare Security Operations Center, http://www.sawsoc.eu/) - Grant agreement no.: 313034 - Technical Coordinator del progetto;
- LeanBigData (http://leanbigdata.eu/), Grant agreement no.: 619606 - Technical Lead per il partner EPSILON;
- SERECA (Secure Enclaves for REactive Cloud Applications, http://www.serecaproject.eu/) - Grant agreement no.: 645011 - Technical Lead per il partner EPSILON.
- SECURE BIG DATA PROCESSING IN UNTRUSTED CLOUDS (SecureCloud, https://www.securecloudproject.eu/) - Grant agreement no.: 690111 - Technical Lead per il partner Sync Lab.
- KONFIDO (Secure and Trusted Paradigm for Interoperable eHealth Services, http://www.konfido-project.eu/konfido/) – Topic: DS-3-2016: Increasing digital security of health related data on a systemic level.
- COMPACT (Competitive Methods to protect local Public Administration from Cyber security Threats) – Topic: Cyber Security for SMEs, local public administration and Individuals – Ammesso a finanziamento, inizierà a breve.
- InfraStress (Improving resilience of sensitive industrial plants & infrastructures exposed to cyber-physical threats, by means of an open testbed stress-testing system) - Call: H2020-SU-INFRA-2018-2019-2020 - Topic: SU-INFRA-01-2018 'Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe'. Focus: Sensitive Industrial Plants and Sites.
- 7SHIELD (Safety and Security Standards of Space Systems, ground Segments and Satellite data assets, via prevention, detection, response and mitigation of physical and cyber threats) - Topic SU-INFRA01-2018-2019: Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe.
- INCISIVE (A multimodal AI-based toolbox and an interoperable health imaging repository for the empowerment of imaging analysis related to the diagnosis, prediction and follow-up of cancer) - Topic: DT-TDS-05-2020: AI for Health Imaging.

È stato/é Responsabile di numeroso progetti finanziati da Ministeri, Regioni e enti privati, che si omettono per brevità.

È stato il Direttore del Master sui sistemi di rete critici dal titolo “European Master on Critical Networked Systems”, offerto dalla Facoltà d’Ingegneria dell’ dell’Università degli Studi di Napoli “Parthenope”.

È nei Comitati Organizzatori delle massime conferenze scientifiche internazionali nel settore della sicurezza e dell’affidabilità dei sistemi di rete, tra cui: IEEE/IFIP International Conference on Dependable Systems and Networks.

È Revisore Ufficiale per le massime riviste scientifiche internazionali nel settore della sicurezza e dell’affidabilità dei sistemi di rete, tra cui: IEEE Transactions on Dependable and Secure Computing.

Informazioni Addizionali

Possiede una perfetta padronanza della lingua inglese, sia scritta che parlata, acquisita grazie alla lunga permanenza negli Stati Uniti.
Possiede un’ottima padronanza della lingua spagnola, sia scritta che parlata (livello avanzato – Istituto Cervantes).

Pubblicazioni Scientifiche

L’attività scientifica di Luigi Romano è documentata da circa cento pubblicazioni su riviste e negli atti di conferenze internazionali e nazionali. Di seguito si riportano alcune pubblicazioni selezionate, relative al settore specifico della sicurezza informatica di sistemi complessi:

[1] Luigi Coppolino, Salvatore D’Antonio, Luigi Romano, “Exposing vulnerabilities in electric power grids: An experimental approach”, International Journal of Critical Infrastructure Protection, Vol 7, Issue 1.
[2] Luigi Coppolino, Salvatore D’Antonio, Giovanni Mazzeo, Luigi Romano, “A comprehensive survey of hardware-assisted security: From the edge to the cloud”, Internet of Things, Volume 6, 2019, 100055, ISSN 2542-6605, https://doi.org/10.1016/j.iot.2019.100055. (https://www.sciencedirect.com/science/article/pii/S2542660519300101)
[3] G. Mazzeo, S. Arnautov, C. Fetzer and L. Romano, "SGXTuner: Performance Enhancement of Intel SGX Applications via Stochastic Optimization," IEEE Transactions on Dependable and Secure Computing, doi: 10.1109/TDSC.2021.3064391.
[4] Luigi Coppolino, Salvatore D’Antonio, Giovanni Mazzeo, Luigi Romano, “Cloud security: Emerging threats and current solutions”, Computers & Electrical Engineering, Volume 59, 2017, Pages 126-140, ISSN 0045-7906, https://doi.org/10.1016/j.compeleceng.2016.03.004 (https://www.sciencedirect.com/science/article/pii/S0045790616300544)
[5] "VISE: Combining Intel SGX and Homomorphic Encryption for Cloud Industrial Control Systems," L. Coppolino, S. D’Antonio, V. Formicola, G. Mazzeo, and L. Romano - DOI (identifier) 10.1109/TC.2020.2995638, IEEE Transactions on Computers.

Napoli, li 12/04/2021

Firmato digitalmente da: Luigi Romano
Organizzazione: UNIVERSITA' DEGLI STUDI DI NAPOLI PARTHENOPE/01877320638
Limitazioni d'uso: Explicit Text: Il titolare fa uso del presente certificato solo per le finalità di lavoro per le quali esso è rilasciato. The certificate holder must use the certificate only for the purposes for which it is issued.
Data: 12/04/2021 22:21:33

_____

In relazione all’art. 47 del D.P.R.445/2000: autorizzo il trattamento dei miei dati personali per le vostre esigenze di selezione e comunicazione.