Net4Society

Artificial Intelligence for Secure and Human-Centric Digital Systems

Giovanni Apruzzese, PhD

Assistant Professor – Reykjavik University

(Formerly University of Liechtenstein)

Giovanni Apruzzese, PhD
giovannia@ru.is

My Expertise

- Expertise at the intersection of:
  - Cybersecurity & AI/ML (adversarial ML, phishing, intrusion detection)
  - Trustworthy & Robust AI systems
  - Human factors in security (user perception, awareness, socio-technical risks)

I have published peer-reviewed papers in each of these fields!
(Google Scholar: https://scholar.google.com/citations?user=X2DCBhsAAAAJ&hl=en)

- Project Vision:
  - Developing Human-Centric, Secure and Regulation-Ready AI Systems
  - Bridging technical AI innovation with societal, regulatory and behavioral dimensions

Giovanni Apruzzese, PhD
giovannia@ru.is

Topics of Interest & Potential Contribution

- Relevant Horizon Europe AI–SSH Themes:
  - Trustworthy AI & AI Security
  - AI robustness, resilience & adversarial threats
  - Human oversight, AI governance & compliance (AI Act)
  - Societal impact of AI-driven decision systems

- Potential Contribution:
  - WP leadership on AI robustness & security evaluation
  - Design of realistic adversarial & threat models
  - Human-in-the-loop validation & behavioral studies
  - Evaluation frameworks for regulatory compliance & risk assessment

Giovanni Apruzzese, PhD
giovannia@ru.is

Role in STEM–SSH Collaboration

- As a STEM expert with strong socio-technical focus, I provide:
  - Technical expertise in secure & adversarial ML
  - Empirical evaluation of AI systems in real-world contexts
  - Experience analyzing practitioner and user perception of AI
- Seeking SSH collaboration in:
  - Ethics, governance & AI policy analysis
  - Legal compliance (AI Act, cybersecurity regulation)
  - Socio-economic impact & participatory methodologies
- Goal: Integrate technical robustness with social legitimacy & regulatory readiness

Contact

- Giovanni Apruzzese, PhD
  - Assistant Professor – Department of Computer Science
  - Reykjavik University (Iceland)
  - Nature of Organisation: Academic Institution

  - Email: giovannia@ru.is
  - Website: https://giovanniapruzzese.com
  - ORCID: 0000-0002-6890-9611

Thank you for listening!

Net4Society