Curriculum Vitae et Studiorum

Giacomo Benedetti

: Italiana
:

Posizioni Ricoperte

Visiting Researcher presso il Dipartimento di Computer Science della North Carolina State University, Raleigh, North Carolina, USA
[19/09/2023 – Attuale]
Attività di ricerca nell'ambito del progetto finanziato dalla National Science Foundation (NSF) CNS-2207008 - "Enabling a Secure and Trustworthy Software Supply Chain":

- Ho partecipato a Summit di interesse del programma di ricerca.
- Ho collaborato con altre università partecipanti al programma di ricerca.
- Sto collaborando nell'ambito della ricerca su Reproducible Builds e sofware supply chain security.

Dottorando presso il Dipartimento di Informatica, Bioingegneria, Robotica e Ingegneria dei Sistemi (DIBRIS) dell'Università degli Studi di Genova, Genova
[01/11/2021 – 31/10/2024]
Attività di ricerca e tematiche affrontate nell'ambito software supply chain security:

- Ho investigato e definito nuove tecniche di modellazione della software supply chain di sofware open-source.
- Ho investigato e sviluppato sistemi di testing automatico per GitHub Actions.
- Ho investigato e proposto nuove techniche per la generazione del Software Bill of Materials (SBOM) nell'ecosistema Python.
- Ho condotto un'analisi empirica su Reproducible Builds nel contesto di ecosistemi software.

Sviluppatore Software presso Talos s.r.l.s., Genova
[01/08/2021 – 31/10/2021]
Attività di sviluppo su prodotti software per la sicurezza dei dispositivi mobili:

- Ho implementato una pipeline di automazione permettendo l'utilizzo del prodotto software nel rispetto del paradigma DevSecOps.
- Ho implementato la distribuzione sicura di token di autenticazione per gli utenti del prodotto software.
- Ho utilizzato framework come Django per lo sviluppo della piattaforma web e GitHub Actions per automatizzare i processi.
- Ho utilizzato Python e JavaScript per lo sviluppo dei diversi componenti coinvolti nell'attività.

Sviluppatore Software presso Humana Vox s.r.l., Genova
[01/02/2020 – 31/07/2020]
Attività di sviluppo web di una piattaforma di telemedicina:

- Ho utilizzato il framework Web2Py per lo sviluppo full-stack della piattaforma.
- Ho gestito l'interazione con il cliente per l'acquisizione del requisiti funzionali e di sicurezza della piattaforma.

ISTRUZIONE E FORMAZIONE

Dottorato in Sicurezza, Rischio, e Vulnerabilità – XXXVII Ciclo, Curriculum in Cybersecurity and Reliable AI, DIBRIS, Università degli Studi di Genova, Genova
[11/2019 – 11/2022]
Sviluppo Tesi di Dottorato dal titolo "Improving Transparency, Automation, and Trust in the Software Supply Chain".
La Tesi propone metodologie e tecniche per il miglioramento di tre proprietà fondamentali della software supply chain: trasparenza, automazione e software trust. A tal fine ho condotto studi nella modellazione e rappresentazione della software supply chain di software open-source, creando modelli Neo4J. Questi permettono l'analisi dei componenti di terze parti nel software. In questo senso ho inoltre sviluppato e proposto una tecnologia built-in nel package manager di Python per la generazione dello Software Bill of Material di progetti Python. Ho sviluppato strumenti per l'analisi automatiche di pipeline di sviluppo. Questi tool sono stati validati in contesti non controllati (in-the-wild) e hanno permesso l'identificazioni di reali vulnerabilità all'interno delle GitHub Actions. Ho condotto un'analisi di riproducibilità delle build del software in ecosistemi open-source, identificando le principali cause di non riproducibilità inserite dai rispettivi package managers, e proponendo soluzioni a queste problematiche.
Relatore: Luca Verderame

Laurea Magistrale in Computer Science (LM-18), DIBRIS, Università degli Studi di Genova, Genova
[09/2019 – 07/2021]
Sviluppo Tesi Magistrale dal titolo "Enabling next-generation cyber ranges with mobile security components".
La Tesi estende lo stato dell'arte sui cyber range includendo ecosistemi mobile. Il sistema sviluppato offre supporto per la simulazione del comportamento degli utenti, proponendo un toolset per la gestione di scenari di attacco tramite Ansible.
Voto: 110/110 cum laude
Relatori: Alessio Merlo, Enrico Russo

Laurea Triennale in Informatica (L-31), DIBRIS, Università degli Studi di Genova, Genova
[09/2016 – 07/2019]
Sviluppo Tesi Triennale dal titolo "Application of Adversarial Machine Learning to Malware Detection".
La Tesi studia lo stato dell'arte dei classificatori malware (antivirus) che sfruttano modelli di machine learning. Ho implementato un attacco di adversarial machine learning contenuto all'interno della letteratura scientifica. L'attacco sfruttava l'inutilizzo funzionale del DOS header nei PE di Windows per produrre un attacco untargeted al modello. Ho sfruttato framework come Keras e TensorFlow.
Voto: 103/110
Relatori: Giovanni Lagorio, Luca Demetrio

Diploma di Scuola Superiore, I.T.T.L. Nautico San Giorgio, Genova
[09/2011 – 06/2016]

ATTIVITÀ DI INSEGNAMENTO

Assistenza alla Didattica per "Mobile Security", Corso di Laurea Magistrale in Ingegneria Informatica, DIBRIS, Università degli Studi di Genova, Genova
[03/2024 - 07/2024]
Titolare del corso: Dott. Luca Verderame

Assistenza alla Didattica per "Distributed Computing", Corso di Laurea Magistrale in Computer Science, DIBRIS, Università degli Studi di Genova, Genova
[10/2022 - 03/2023]
Titolare del corso: Dott. Matteo Dell'Amico

Assistenza alla Didattica per "Computer Security", Corso di Laurea Magistrale in Ingegneria Informatica, DIBRIS, Università degli Studi di Genova, Genova
[09/2021 - 03/2023]

Titolare del corso: Prof. Alessandro Armando

SINTESI DELL'ATTIVITÀ DI RICERCA

La mia ricerca di dottorato presso l'Università degli Studi di Genova si divide in tre parti principali: (i) Modellazione della software supply chain; (ii) sicurezza di GitHub Actions; e (iii) reproducible builds negli ecosistemi di packaging del software open-source.
Ho studiato tecniche di modellazione della struttura della software supply chain con lo scopo di identificare relazioni tra i componenti e il conseguente rischio di sicurezza che ne deriva [CI5]. Mentre alcuni componenti della supply chain sono facilmente identificabili, ad esempio le dipendenze software, altri richiedono un'analisi più approfondita del prodotto software. Questa analisi include l'indagine di informazioni disponibili pubblicamente, per esempio vendor delle dipendenze, licenze utilizzate e popolarità. Questo studio ha portato allo sviluppo di un proof of concept rivelando quanto possa essere difficile ricostruire l'intera supply chain di un software. In particolare, è stato possibile identificare un'evidentente mancanza di tracciabilità nella maggior parte degli ecosistemi software. Ho studiato come le dipendenze del software possono essere rappresentate tramite un Software Bill of Materials (SBOM) e le implicazioni di esso sull'analisi di sicurezza [SR2]. Questo studio ha portato allo sviluppo di PIP-sbom [SW1], un'estensione del package manager di Python, PIP, per la generazione dello SBOM. Ho inoltre studiato la relazione tra l'ecosistema Python e i tool di generazione dello SBOM [CI2].
Ho studiato quali sono i principali problemi di sicurezza che una GitHub Actions può esporre e le rispettive mitigazioni [CI4]. Ho sviluppato GHAST [SW2], un tool per analizzare e identificare vulnerabilità e misconfigurations all'interno delle GitHub Actions. Il tool sfrutta tecniche di pattern matching per identificare specifici costrutti che rappresentano la vulnerabilità stessa, come una command injection, oppure possono abilitare un vettore di attacco, come una configurazione sbagliata dei permessi. GHAST è stato utilizzato in combinazione con il generatore del modello della software supply chain sviluppato in precedenza. I dati ottenuti hanno mostrato che esiste un effettivo rischio di sicurezza in ambienti reali.
Nell'ambito di un periodo di visiting presso il WSPR Lab alla North Carolina State University ho studiato come i package manager influenzano la riproducibilità delle build del software in ecosistemi di packaging [CI1]. Tramite l'individuazione delle cause è stato possibile proporre raccomandazioni specifiche e soluzioni pratiche per rendere le build riproducibili senza l'intervento dello sviluppatore. Questa attività è inoltre parte del progetto Frontiers: Enabling a Secure and Trustworthy Software Supply Chain (Progetto di Ricerca NSF - CNS-2207008). Sempre nel contesto di questo progetto ho investigato le principali direzioni di ricerca nella software supply chain security [SR1], individuando quali possono essere le più promettenti e necessarie per un corretto sviluppo accademico e industriale.

COMPETENZE TECNICHE

Ottima conoscenza di:

- Ciclo sicuro di sviluppo del software (DevSecOps).
- Design sicuro di GitHub Actions.
- Analisi delle dipendenze e debloating.
- Riproducibilità della build del software.
- Linguaggi di programmazione: Python, Go, JavaScript, C, C++, Java.
- Linguaggi di marcatura: LaTeX, HTML, Markdown.
- Pacchetto Office: Word, Excel, PowerPoint.
- Sistemi operativi: macOS, Linux (Ubuntu, Debian, Arch, Fedora), Windows.
- Sistemi di virtualizzazione e containerizzazione: Docker, VirtualBox, VMWare.

COMPETENZE LINGUISTICHE

Lingua madre: **italiano**
Altre lingue: **inglese**. Ascolto, lettura, scrittura, produzione orale, interazione orale: **C1**

PARTECIPAZIONI A PROGETTI

Frontiers: Enabling a Secure and Trustworthy Software Supply Chain (Progetto di Ricerca NSF - CNS-2207008)
[14/09/2023 - Attuale]
Nell'ambito del progetto sto studiando l'adozione e la distribuzione di Reproducible Builds all'interno di ecosistemi software.

Partenariato Esteso Cybersecurity, Nuove Tecnologie e Tutela dei Diritti (PE00000014 - PNRR MUR)
[01/04/2022 – 30/09/2022]
Nell'ambito delle attività progettuali dello Spoke 4 - Operating Systems and Virtualization Security (progetto SecCo), ho partecipato alla stesura del progetto di ricerca e alle discussioni di inizio progetto per la gestione dei work packages.

PARTECIPAZIONI A CONFERENZE E WORKSHOP

Relatore del lavoro [CI3]
al 1st Workshop DevSecOps Research and Opportunities, Delft, Netherlands, Luglio 2023.

Relatore del lavoro [CI4]
alla The Italian Conference on CyberSecurity, Bari, Italia, Maggio 2023.

Relatore del lavoro [CI4]
al 1st ACM Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses, Los Angeles, CA, USA, Novembre 2022.

Relatore del lavoro [CI5]
alla 15th International Conference on the Quality of Information and Communications Technology, Talavera de la Reina, Spagna, Settembre 2022.

COLLABORAZIONI

- Prof. Mauro Conti (Università di Padova): attività di ricerca sull'impatto del Software Bill of Materials nell'analisi di sicurezza del software.
- Dott. Matteo Dell'Amico (Università degli Studi di Genova): attività di ricerca sulla generazione del Software Bill of Materials nell'ecosistema Python.
- Prof. William Enck (North Carolina State University): attività di ricerca su Reproducible Builds all'interno di ecosistemi software.
- Prof. Laurie Williams (North Carolina State University): attività di ricerca sull'analisi delle necessità della software supply chain security.
- Prof. Christian Kaestner (Carnegie Mellon University): attività di ricerca su Reproducible Builds.

ATTIVITÀ EDITORIALE

- Membro della Shadow Program Committee della 18th European Conference on Computer Systems (EuroSys), Rome, 2023.

ELENCO DEI LAVORI SCIENTIFICI

PUBBLICAZIONI IN ATTI DI CONFERENZE INTERNAZIONALI

[CI1] **G. Benedetti**, O. Solarin, C. Miller, G. Tystahl, W. Enck, C. Kaestner, A. Kapravelos, A. Merlo, L. Verderame, "An Empirical Study on Reproducible Packaging in Open-Source Ecosystems", 2025 47th IEEE/ACM International Conference on Software Engineering (ICSE), 27 Aprile - 3 Maggio 2025, Ottawa, Canada.

[CI2] S. Cofano, **G. Benedetti**, M. Dell'Amico, "SBOM Generation Tools in the Python Ecosystem: an In-Detail Analysis", 2024 23rd IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 17 - 21 Dicembre 2024, Sanya, Cina.

doi: 10.48550/arXiv.2409.01214

[CI3] **G. Benedetti**, L. Verderame, A. Merlo, "A Preliminary Study of Privilege Life Cycle in Software Management Platform Automation Workflows", Proceedings of the 2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), all'interno del 2023 8th IEEE European Symposium on Security and Privacy (EuroS&P), pp. 21-28, Delft, Netherlands, 3-7 Luglio 2023.

doi: 10.1109/EuroSPW59978.2023.00007

[CI4] **G. Benedetti**, L. Verderame, A. Merlo, "Automatic security assessment of github actions workflows", Proceedings of the 2022 ACM Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses, all'interno della 2022 29th ACM Computer and Communications Security Conference (CCS), pp. 37-45, Los Angeles, CA, USA 07-11 Novembre 2022.

doi: 10.1145/3560835.3564554

[CI5] **G. Benedetti**, L. Verderame, A. Merlo, "Alice in (Software Supply) Chains: Risk Identification and Evaluation", International Conference on the Quality of Information and Communications Technology (QUATIC), pp. 281-295, Talavera de la Reina, Spagna, 12-14 Settembre 2022.

doi: 10.1007/978-3-031-14179-9_19

PUBBLICAZIONI IN FASE DI REVISIONE

[SR1] L. Williams, **G. Benedetti**, S. Hamer, R. Paramitha, I. Rahman, M. Tamanna, G. Tystahl, N. Zahan, P. Morrison, Y. Acar, M. Cukier, C. Kaestner, A. Kapravelos, D. Wermke, W. Enck"Research Directions in Software Supply Chain Security", ACM Transactions on Software Engineering and Methodology (TOSEM).

[SR2] **G. Benedetti**, S. Cofano, A. Brighente, M. Conti, "The Impact of SBOM Generators on Vulnerability Assessment in Python: A Comparison and a Novel Approach", 2025 23rd International Conference on Applied Cryptography and Network Security.

doi: 10.48550/arXiv.2409.06390

POSTER

[P1] **G. Benedetti**, "Software Supply Chain Security", 1st Poster Session of the PhD Program in Security, Risk, and Vulnerability, Università degli Studi di Genova, Genova, Italia, 15 Febbraio 2023.

ELENCO DEI PRODOTTI SOFTWARE

[SW1] **PIP-sbom**: ho contribuito allo sviluppo di questo tool in linguaggio Python per la generazione di Software Bill of Materials (SBOM) di pacchetti Python sfruttando il processo di risoluzione delle dipendenze nativo del package manager.

Documentato nella pubblicazione [SR2].

Rilasciato con Licenza MIT.

link:`https://github.com/giacomobenedetti/pip-sbom`

[SW2] **GHAST**: ho contribuito allo sviluppo di questo tool in linguaggio Python per l'analisi di sicurezza di GitHub Actions.

Documentato nella pubblicazione [CI4].

Rilasciato con Licenza AGPL-3.0.

link:`https://github.com/Mobile-IoT-Security-Lab/GHAST`

INFORMAZIONI AGGIUNTIVE

Revisore di articoli scientifici

- Riviste internazionali quali IEEE Transactions on Information Forensics and Security (editore: IEEE), International Journal of Computers and Applications (editore: Taylor & Francis), e Computer Networks (editore: Elsevier).

Relatore di seminari su software supply chain security

- WSPR Lab, North Carolina State University, NC, USA.
- DIBRIS, Università degli Studi di Genova, Genova.
- UnigeSenior, Università degli Studi di Genova, Genova.

Data, Luogo

5 novembre 2024, Genova

Firma (Giacomo Renato Benedetti)

(firmato digitalmente)

Autorizzo il trattamento dei miei dati personali presenti nel curriculum vitae ai sensi del Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" e dell'art. 13 del GDPR (Regolamento UE 2016/679).