Curriculum Vitæ

Dr. Giancarlo Pellegrino

November 20, 2023

General Information

Name: Giancarlo Pellegrino

Education

02/2010–11/2013	**PhD in Computer Science and Networks** (with distinction), *Eurecom*, Biot, France. Thesis title: Detection of Logic Flaws in Multi-party Business Applications via Security Testing. Supervisor: Prof. Dr. Davide Balzarotti
10/2006–02/2009	**MSc in Computer Science** (110/110 cum laude), *University of Catania*, Catania, Italy.
10/2001–11/2006	**BSc in Computer Science**, *University of Catania*, Catania, Italy.

Employment

05/2023–current	**Tenured Faculty** CISPA Helmholtz Center for Information Security, Saarbrücken, Germany
10/2019–05/2023	**Tenure-Track Faculty** (Fast track), CISPA Helmholtz Center for Information Security, Saarbrücken, Germany
02/2019–02/2021	**Visiting Assistant Professor**, Yokohama National University, Yokohama, Japan
10/2017–09/2019	**Visiting Assistant Professor**, Stanford University, USA
10/2017–09/2019	**Research Group Leader**, CISPA Helmholtz Center for Information Security, Saarbrücken, Germany
01/2015–09/2017	**Postdoctoral Researcher**, CISPA/Saarland University, Saarbrücken, Germany
01/2014–12/2015	**Postdoctoral Researcher**, TU Darmstadt, Darmstadt, Germany
09/2009–08/2013	**Research Associate**, SAP Research, Mougins, France, and Karlsuhe, Germany

Research Group

Giancarlo Pellegrino leads the Application Security (AppSec, in short) research group at CISPA. His team addresses the pressing challenges of identifying, studying, and solving vulnerabilities in modern and future web-based application software. The AppSec group current researchinterests include the analysis of new web vulnerabilities, program analysis (static, dynamic, and hybrid) that operates at scale, application of ML/AI to web application security, and the security and privacy of future application software systems, including immersive web applications.

Grants

- Semantic Models and Agents for Security Testing of Web Applications; DFG; PI; Duration: 36M (2021-24); Budget: 348.453€.
- TESTABLE: Testability Pattern-Driven Web Application Security and Privacy Testing; H2020; Scientific coordinator and PI; Duration: 36M (2021-24); Budget (CISPA / Total): 721.639€ / 4.835.135€;
- ESCUDO-CLOUD: Enforceable Security in the Cloud to Uphold Data Ownership; H2020; PI; Duration: 36M (2015-17); Budget (TU Darmstadt): ca. 600.000€;

Publication List

Conference Proceedings

[1] S. Khodayari and G. Pellegrino, "It's (DOM) clobbering time: Attack techniques, prevalence, and defenses," in *Proceeding of the 44th IEEE Symposium on Security & Privacy*, ser. IEEE SP 2023, IEEE, 2023.

[2] J. Rautenstrauch, G. Pellegrino, and B. Stock, "The leaky web: Automated discovery of cross-site information leaks in browsers and the web," in *Proceedings of the 44rd IEEE Symposium on Security & Privacy*, ser. IEEE SP 2023, IEEE, 2023.

[0] G. Stivala, S. Abdelnabi, A. Mengascini, M. Graziano, M. Fritz, and G. Pellegrino, "From attachments to seo: Click here to learn more about clickbait pdfs!" *ACSAC'23*, 2023.

[3] S. Khodayari and G. Pellegrino, "The state of the samesite: Studying the usage, effectiveness, and adequacy of samesite cookies," in *Proceeding of the 43rd IEEE Symposium on Security & Privacy*, ser. IEEE SP 2022, IEEE, 2022.

[4] B. Eriksson, G. Pellegrino, and A. Sabelfeld, "Black widow: Blackbox data-driven web scanning," in *2021 IEEE Symposium on Security and Privacy (SP)*, ser. IEEE SP 2021, IEEE, 2021.

[5] S. Khodayari and G. Pellegrino, "Jaw: Studying client-side csrf with hybrid property graphs and declarative traversals," in *30th USENIX Security Symposium*, ser. USENIX Security 21, 2021.

[6] X. Likaj, S. Khodayari, and G. Pellegrino, "Where we stand (or fall): An analysis of csrf defenses in web frameworks," in *Symposium on Research in Attacks, Intrusions and Defenses (RAID'21), San Sebastian, Spain, October 6-8, 2021*, ACM, 2021.

[7] E. Chou, F. Tramèr, and G. Pellegrino, "Sentinet: Detecting localized universal attack against deep learning systems," in *2021 IEEE Symposium on Security & Privacy Workshops (SPW)*, ser. IEEE SPW 2020, IEEE, 2020.

[8] S. Koch, T. Sauer, M. Johns, and G. Pellegrino, "Raccoon: Automated verification of guarded race conditions in web applications," in *Proceedings of the 35th Annual ACM Symposium on Applied Computing*, 2020, pp. 1678–1687.

[9] G. Stivala and G. Pellegrino, "Deceptive previews: A study of the link preview trustworthiness in social platforms," in *2020 Network and Distributed System Security Symposium*, ser. NDSS 2020, NDSS, 2020.

[10] Q. Zhao, C. Zuo, B. Dolan-Gavitt, G. Pellegrino, and Z. Lin, "Automatic uncovering of hidden behaviors from input validation in mobile apps," in *2020 IEEE Symposium on Security and Privacy (SP)*, ser. IEEE SP 2020, IEEE, 2020.

[11] S. Eskandarian, J. Cogan, S. Birnbaum, *et al.*, "Fidelius: Protecting user secrets from compromised browsers," in *IEEE Symposium on Security & Privacy, May 2019*, ser. IEEE SP 19, IEEE, 2019.

[12] F. Tramèr, P. Dupré, G. Rusak, G. Pellegrino, and D. Boneh, "Adversarial: Perceptual ad blocking meets adversarial machine learning," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '19, 2019.

[13] Q. Zhao, C. Zuo, G. Pellegrino, and Z. Lin, "Geo-locating drivers: A study of sensitive data leakage in ride-hailing services," in *2019 Network and Distributed System Security symposium*, ser. NDSS 2019, Internet Society, 2019.

[14] M. Oltrogge, E. Derr, C. Stransky, S. Fahl, Y. Acar, C. Rossow, G. Pellegrino, S. Bugiel, and M. Backes, "The rise of the citizen developer: Assessing the security impact of online app generators," in *Proceeding of the 39th IEEE Symposium on Security and Privacy*, ser. IEEE SP 18, IEEE, 2018.

[15] P. Speicher, M. Steinmetz, R. Kuennemann, M. Simeonovski, G. Pellegrino, J. Hoffmann, and M. Backes, "Formally reasoning about the cost and efficacy of securing the email infrastructure," in *Proceeding of the 3rd IEEE European Symposium on Security and Privacy*, ser. EURO SP 2018, IEEE, 2018.

[16] B. Stock, G. Pellegrino, F. Li, M. Backes, and C. Rossow, "Didn't you hear me? - towards more successful web vulnerability notifications," in *2018 Network and Distributed System Security Symposium*, ser. NDSS 2018, NDSS, 2018.

[17] G. Pellegrino, M. Johns, S. Koch, M. Backes, and C. Rossow, "Deemon: Detecting csrf with dynamic analysis and property graphs," in *2017 ACM Conference on Computer and Communications Security*, ACM, 2017.

[18] G. Pellegrino, O. Catakoglu, D. Balzarotti, and C. Rossow, "Uses and Abuses of Server-Side Requests," in *19th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2016)*, 2016.

[19] M. Simeonovski, G. Pellegrino, C. Rossow, and M. Backes, "Who Controls the Internet? Analyzing Global Threats using Property Graph Traversals," in *26th International World Wide Web Conference, 2017 (WWW 2016)*, 2016.

[20] B. Stock, G. Pellegrino, C. Rossow, M. Johns, and M. Backes, "Poster: Mapping the landscape of large-scale vulnerability notifications," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 1787–1789.

[21] B. Stock, G. Pellegrino, C. Rossow, M. Johns, and M. Backes, "Hey, You Have a Problem: On the Feasibility of Large-Scale Web Vulnerability Notification," in *25th USENIX Security Symposium (USENIX Security 16)*, 2016.

[22] G. Pellegrino, D. Balzarotti, S. Winter, and N. Suri, "In the Compression Hornet's Nest: A Security Study of Data Compression in Network Services," in *24th USENIX Security Symposium (USENIX Security 15)*, 2015.

[23] G. Pellegrino, C. Rossow, F. J. Ryba, T. C. Schmidt, and M. Wählisch, "Cashing Out the Great Cannon? On Browser-Based DDoS Attacks and Economics," in *9th USENIX Workshop on Offensive Technologies, WOOT '15*, 2015.

[24] G. Pellegrino, C. Tschürtz, E. Bodden, and C. Rossow, "jÄk: Using Dynamic Analysis to Crawl and Test Modern Web Applications," in *18th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2015)*, 2015.

[25] G. Pellegrino and D. Balzarotti, "Toward Black-Box Detection of Logic Flaws in Web Applications," in *2014 Network and Distributed System Security Symposium*, ser. NDSS 2014, San Diego (USA), 2014.

[26] T. Vateva-Gurova, J. Luna, G. Pellegrino, and N. Suri, "On the feasibility of side-channel attacks in a virtualized environment," in *International Conference on E-Business and Telecommunications*, Springer, 2014, pp. 319–339.

[27] T. Vateva-Gurova, J. Luna, G. Pellegrino, and N. Suri, "Towards a framework for assessing the feasibility of side-channel attacks in virtualized environments," in *2014 11th international conference on security and cryptography (SECRYPT)*, IEEE, 2014, pp. 1–12.

[28] G. Pellegrino, L. Compagna, and T. Morreggia, "A Tool for Supporting Developers in Analyzing the Security of Web-based Security Protocols," in *25th IFIP International Conference on Testing Software and Systems (ICTSS'13)*, 2013.

[29] A. Armando, W. Arsac, T. Avanesov, *et al.*, "The avantssar platform for the automated validation of trust and security of service-oriented architectures," in *TACAS*, C. Flanagan and B. König, Eds., ser. Lecture Notes in Computer Science, vol. 7214, Springer, 2012, pp. 267–282.

[30] A. Armando, G. Pellegrino, R. Carbone, A. Merlo, and D. Balzarotti, "From Model-Checking to Automated Testing of Security Protocols: Bridging the Gap," in *TAP*, A. D. Brucker and J. Julliand, Eds., ser. Lecture Notes in Computer Science, vol. 7305, Springer, 2012, pp. 3–18.

[31] A. Armando, R. Carbone, L. Compagna, J. Cuéllar, G. Pellegrino, and A. Sorniotti, "From multiple credentials to browser-based single sign-on: Are we more secure?" In *SEC*, J. Camenisch, S. Fischer-Hübner, Y. Murayama, A. Portmann, and C. Rieder, Eds., ser. IFIP Advances in Information and Communication Technology, vol. 354, Springer, 2011, pp. 68–79.

[32] W. Arsac, L. Compagna, G. Pellegrino, and S. E. Ponta, "Security validation of business processes via model-checking," in *International Symposium on Engineering Secure Software and Systems*, Springer, 2011, pp. 29–42.

[33] A. Armando, R. Carbone, L. Compagna, K. Li, and G. Pellegrino, "Model-Checking Driven Security Testing of Web-Based Applications," in *ICST Workshops*, IEEE Computer Society, 2010, pp. 361–370.

Articles in Journals

[34] A. Armando, R. Carbone, L. Compagna, J. Cuéllar, G. Pellegrino, and A. Sorniotti, "An Authentication Flaw in Browser-based Single Sign-On Protocols: Impact and Remediations," *Computers & Security*, vol. 33, pp. 41–58, 2013.

Book Chapters

[35] G. L. Mikkelsen, K. Damgård, H. Guldager, J. L. Jensen, J. G. Luna, J. D. Nielsen, P. Paillier, G. Pellegrino, M. B. Stausholm, N. Suri, *et al.*, "Attribute-based credentials for trust: Technical implementation and feasibility," in *Attribute-based Credentials for Trust*, Springer, 2015, pp. 255–317.

[36] A. Armando, R. Carbone, L. Compagna, and G. Pellegrino, "Automatic security analysis of saml-based single sign-on protocols," in *Digital Identity and Access Management: Technologies and Framework, Business Science Reference*, IGI Global, 2011.

Other Publications

[37] E. Chou, F. Tramèr, G. Pellegrino, and D. Boneh, "Sentinet: Detecting physical attacks against deep learning systems," in *Arxiv*, Arxiv, 2018.

[38] A. Cosimo, A. Leonardo, A. Arije, A. Alessandro, A. Rocco, B. Marco, R. Baldoni, B. Antonio, B. Massimo, B. Cataldo, *et al.*, “Il futuro della cybersecurity in italia: Ambiti progettuali strategici,” 2018.

[39] P. Speicher, M. Steinmetz, R. Künnemann, M. Simeonovski, G. Pellegrino, J. Hoffmann, and M. Backes, “Formally reasoning about the cost and efficacy of securing the email infrastructure (full version),” *Extended Version of EuroS&P 2018 Paper*, 2018.

Patents granted

[40] G. Pellegrino, K. Li, and L. Compagna, *Options detection in security protocols*, US Patent App. 13/542,258, 2014.

Teaching

2023 WS	Core Lecture - Security - Saarland University
2023 WS	Seminar - The Web Security Seminar - Saarland University
2023 WS	Lecture Series - Perspectives of Cyber Security - Saarland University
2023 SS	Seminar - The Web Security Seminar - Saarland University
2022 WS	Seminar - Machine Learning for Program Analysis - Saarland University
2022 WS	Seminar - The Web Security Seminar - Saarland University
2022 WS	Lecture Series - Perspectives of Cyber Security - Saarland University
2022 SS	Advance Lecture - Secure Web Development – Saarland University
2021 WS	Lecture Series - Perspectives of Cyber Security - Saarland University
2021 SS	Pro/Seminar - (p)SADWeb: (Pro)Seminar on Attacks and Defense on the Web – Saarland University
2020 WS	Core Lecture - Security - Saarland University
2020 WS	Lecture Series - Perspectives of Cyber Security - Saarland University
2020 SS	Advance Lecture - Secure Web Development – Saarland University
2020 SS	Seminar - INPAWS: INfluential PApers in Web Security – Saarland University
2019 WS	Core Lecture - Security - Saarland University
2019 WS	Seminar - JAWS: Joint Advances in Web Security - Saarland University
2017 SS	Core Lecture - Foundations of Cyber Security II - Saarland University.
2016 SS	Advanced Lecture - Secure Software Engineering - Saarland University
2015 SS	Seminar - Web Security Seminar - Saarland University
2014 SS	Advance Lecture - Operating Systems II: Dependability and Trust - TU Darmstadt

PhD Students

- **Giada Martina Stivala**, PhD student, June 2019 - ongoing
- **Soheil Khodayari**, PhD student, July 2019 - ongoing
- **Aleksei Stafeev**, PhD student, August 2021 - ongoing
- **Andrea Mengascini**, PhD student, November 2021 - ongoing
- **Gianluca De Stefano**, PhD student, August 2022 - ongoing
- **Sepehr Mirzaei**, PhD prep. phase, February 2023 - ongoing

Community Service

Chairs and Non-TPC roles

Vice PC Chair for Usenix Security (2024, 2023), **"Voice of Institutional Wisdom"** of IEEE Euro S&P, **General co-chair** of IEEE Euro S&P (2020), **Member of the Invited Talks Committee** of Usenix (2019, 2021), **Publicity chair** for ACM CCS (2017), **Publication chair** for DIMVA (2021, 2022), and **Program co-chair** of SECTEST (2015)

Technical Program Committee Member

Usenix Security (2022, 2021, 2020, 2019), **IEEE S&P** (2024, 2023, 2022, 2021), **ACM CCS** (2023, 2021, 2020, 2018) , **IEEE EURO S&P** (2023, 2022, 2020), **ACM AsiaCCS** (2022, 2021, 2020, 2019), **ACSAC** (2023, 2022, 2021, 2020, 2019, 2018, 2017), **The Web Conference (former WWW)** (2023, 2022, 2021, 2020), **DIMVA** (2023, 2022, 2021, 2020), EuroSec (2023, 2022, 2021, 2020, 2019), RAID (2022), ACM CCS Poster (2016), SecWeb (2023, 2022, 2020), ECOOP/ISSTA 2021 Doctoral Symposium (2021), ISC (2019), CARDS (2019), Usenix WOOT (2018), IWCC (2016, 2015), DEPEND (2016, 2015), WTMC (2016), STAST (2014), and NBiS (2014)

Journal Reviewer

ACM Computing Surveys, ACM Transactions on Software Engineering and Methodology (TOSEM), IEEE Transactions on Cloud Computing (TCC), and Transactions on Dependable and Secure Computing (TDSC)

Awards

- Distinguished Paper Award, IEEE S&P 2023, "It's (DOM) Clobbering Time: Attack Techniques, Prevalence, and Defense"
- Distinguished Paper Award, IEEE S&P 2023, "The Leaky Web: Automated Discovery of Cross-Site Information Leaks in Browsers and the Web"
- Foundations of CyberSecurity II, "Busy Beaver Award", the best basic lecture of summer semester 2017 (co-taught with Christian Rossow)