Luca Invernizzi

Research Scientist Manager, Google

Bio

Luca Invernizzi is a Research Scientist Manager in the Security Research Group at Google, where he focuses on designing better ways to protect people online, advancing cybersecurity through AI, and bettering hardware attacks and defenses.

Luca's research has been featured by CNN, Forbes, Wired, CNET, The Verge, and tech news sites like Ars Technica and TechRepublic. He regularly gives talks at academic and industry conferences and participates in committees like Usenix Security. Luca holds a PhD and Master's in Computer Science from UCSB, an EMBA from Quantic School of Business, a Master's in Robotics from the University of Pisa, and an engineering degree from the Sant'Anna School of Advanced Studies .

Professional Experience

- **Research Scientist Manager** | Google | Switzerland | 2020 - Present
    - Leading research in the Security Research Group, focusing on designing better ways to protect people online, advancing cybersecurity through AI, and implementing hardware attacks and defenses.
    - Contributions include:
        - SecGemini: Google's most advanced AI cybersecurity agent
        - SCAAML: AI models to extract secrets from side-channels in secure chips
        - Magika: Google's filetype detector, powering Gmail, Drive, Virustotal, Cloud, Gemini, and others
        - Gmail's spam/scam detection
        - Google's security keys and their post-quantum crypto support
- **Research Scientist** | Google | USA | 2015 - 2020

    - Conducted research in cybersecurity, focusing on botnet detection, internet measurements, and ransomware analysis.
    - Created automatic detection for leaked credentials and quantified ransomware revenue.
    - Joined Google's anti-abuse team to detect sophisticated cloaking sites.
- **Project Lead** | The Activity Exchange | 2012 - 2015
    - Led the design and operation of a scalable service for collecting and normalizing sensitive health data for over 200,000 users.
- **Research Intern** | Narus | 2013
    - Designed "Nazca," a system to discover and track malicious downloads in ISP network traffic.
- **Engineering Intern, Pentester** | Appfolio | 2011
    - Performed penetration testing on Ruby on Rails web applications, including a payment-processing system.
    - Developed tools to alert developers of potential security vulnerabilities.
- **Engineering Intern** | Google Summer of Code | 2010
    - Extended the "Getting Things GNOME!" task manager to support multiple synchronization services.

Education

- **Executive Master of Business Administration** | Quantic School of Business and Technology | 2018 - 2019
    - *GPA: 95% with honors*
- **Ph.D. in Computer Science, Information Security** | University of California, Santa Barbara | 2010 - 2015
    - *GPA: 4.0/4.0*
    - *Awards: UCSB Computer Science Outstanding Publication Award (2015), CSAW Best Security Paper Finalist (2012)*
- **Master's in Computer Science** | University of California, Santa Barbara | 2010 - 2015
    - *GPA: 4.0/4.0*
- **Master's Degree in Control Engineering** | University of Pisa, Italy | 2007 - 2010
    - *GPA: 110/110 cum laude*
- **Diploma di Licenza** | Sant'Anna University, School of Advanced Studies, Italy | 2004 - 2010

    - *GPA: 100/100 cum laude*
- **Bachelor's Degree in Computer Engineering** | University of Pisa, Italy | 2004 - 2007
    - *GPA: 110/110 cum laude with excellence path*

Publications

- ***Gemini 1.5: Unlocking multimodal understanding across millions of tokens of context*** *Machel Reid, Nikolay Savinov, Denis Teplyashin, Dmitry Lepikhin, Timothy Lillicrap, et al. (606 authors)*
  arXiv, 2024, 1938 citations
- ***Magika: AI-Powered Content-Type Detection*** *Yanick Fratantonio, Luca Invernizzi, Loua Farah, Kurt Thomas, Marina Zhang, Ange Albertini, Francois Galilee, Giancarlo Metitieri, Julien Cretin, Alex Petit-Bianco, David Tao, Elie Bursztein arXiv, 2024*
- ***Generalized power attacks against crypto hardware using long-range deep learning*** *Elie Bursztein, Luca Invernizzi, Karel Král, Daniel Moghimi, Jean-Michel Picod, Marina Zhang arXiv, 2023*
- ***Hybrid Post-Quantum Signatures in Hardware Security Keys*** *Diana Ghinea, Fabian Kaczmarczyck, Jennifer Pullman, Julien Cretin, Stefan Kölbl, Rafael Misoczki, Picod Jean-Michel, Luca Invernizzi, Elie Bursztein ACNS Workshop on Secure Cryptographic Implementation, 2022* 🏆 *Best Paper Award*
- ***CoinPolice: Detecting Hidden Cryptojacking Attacks with Neural Networks*** *Ivan Petrov, Luca Invernizzi, Elie Bursztein ArxiV, 2020*
- ***Spotlight: Malware Lead Generation at Scale****, Fabian Kaczmarczyck, Bernhard Grill, Luca Invernizzi, Jennifer Pullman, Cecilia M. Procopiuc, David Tao, Borbala Benko, Elie Bursztein, Annual Computer Security Applications Conference (ACSAC), 2020*
- ***Protecting accounts from credential stuffing with password breach alerting*** *Kurt Thomas, Jennifer Pullman, Kevin Yeo, Ananth Raghunathan, Patrick Gage Kelley, Luca Invernizzi, Borbala Benko, Tadek Pietraszek, Sarvar Patel, Dan Boneh, Elie Bursztein USENIX Security Symposium, 2019* 🏆 *Best Paper Award*
- ***Five years of the right to be forgotten*** *Theo Bertram, Elie Bursztein, Stephanie Caro, Hubert Chao, Rutledge Chin Feman, Peter Fleischer, Albin Gustafsson, Jess Hemerly, Chris Hibbert, Luca Invernizzi, Lanah Kammourieh Donnelly, Jason Ketover, Jay Laefer, Paul Nicholas, Yuan Niu, Harjinder Obhi, David Price, Andrew*

Strait, Kurt Thomas, Al Verney ACM SIGSAC Conference on Computer and Communications Security, 2019

- ***Serverless Cybersecurity Training*** *Luca Invernizzi, Elie Bursztein TDCommons, 2019*
- ***Tracking ransomware end-to-end*** *Danny Yuxing Huang, Maxwell Matthaios Aliapoulios, Vector Guo Li, Luca Invernizzi, Elie Bursztein, Kylie McRoberts, Jonathan Levin, Kirill Levchenko, Alex C Snoeren, Damon McCoy IEEE Symposium on Security and Privacy (S&P), 2018*
- ***Three years of the Right to be Forgotten*** *Theo Bertram, Elie Bursztein, Stephanie Caro, Hubert Chao, Rutledge Chin Feman, Peter Fleischer, Albin Gustafsson, Jess Hemerly, Chris Hibbert, Luca Invernizzi, LK Donnelly, J Ketover, Jay Laefer, Paul Nicholas, Yuan Niu, Harjinder Obhi, David Price, Andrew Strait, Kurt Thomas, Al Verney ArXiv, 2018*
- ***Understanding the mirai botnet*** *Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J Alex Halderman, Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever, Zane Ma, Joshua Mason, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas, Yi Zhou USENIX security symposium (USENIX Security 17), 2017, 2959 citations*
- ***Data Breaches, Phishing, or Malware?: Understanding the Risks of Stolen Credentials*** *Kurt Thomas, Frank Li, Ali Zand, Jacob Barrett, Juri Ranieri, Luca Invernizzi, Yarik Markov, Oxana Comanescu, Vijay Eranti, Angelika Moscicki, et al ACM SIGSAC Conference on Computer and Communications Security, 2017*
- ***Gossip: Automatically identifying malicious domains from mailing list discussions*** *Cheng Huang, Shuang Hao, Luca Invernizzi, Jiayong Liu, Yong Fang, Christopher Kruegel, Giovanni Vigna ACM on Asia Conference on Computer and Communications Security (AsiaCCS), 2017*
- ***Cloak of Visibility: Detecting When Machines Browse A Different Web*** *Luca Invernizzi, Kurt Thomas, Alexandros Kapravelos, Oxana Comanescu, Jean-Michel Picod, Elie Bursztein IEEE Security and Privacy (S&P), 2016*
- ***What the app is that? deception and countermeasures in the android user interface*** *Antonio Bianchi, Jacopo Corbetta, Luca Invernizzi, Yanick Fratantonio, Christopher Kruegel, Giovanni Vigna IEEE Symposium on Security and Privacy (S&P), 2015*
- ***Baredroid: Large-scale analysis of android apps on real devices*** *Simone Mutti, Yanick Fratantonio, Antonio Bianchi, Luca Invernizzi, Jacopo Corbetta,*

Dhilung Kirat, Christopher Kruegel, Giovanni Vigna Annual Computer Security Applications Conference (ACSAC), 2015

- ***Detecting malware infestations in large-scale networks*** *Luca Invernizzi, Stanislav Miskovic, Ruben Torres, Sabyasachi Saha, Christopher Kruegel, Antonio Nucci, Sung-Ju Lee, Giovanni Vigna US Patent, 2015*
- ***Nazca: Detecting Malware Distribution in Large-Scale Networks.*** *Luca Invernizzi, Stanislav Miskovic, Ruben Torres, Christopher Kruegel, Sabyasachi Saha, Giovanni Vigna, Sung-Ju Lee, Marco Mellia Annual Network and Distributed Systems Security (NDSS), 2014*
- ***Ten Years of {iCTF}: The Good, The Bad, and The Ugly*** *Giovanni Vigna, Kevin Borgolte, Jacopo Corbetta, Adam Doupe, Yanick Fratantonio, Luca Invernizzi, Dhilung Kirat, Yan Shoshitaishvili USENIX Summit on Gaming Games and Gamification in Security Education (3GSE 14), 2014*
- ***Do you feel lucky? A large-scale analysis of risk-rewards trade-offs in cyber security*** *Yan Shoshitaishvili, Luca Invernizzi, Adam Doupe, Giovanni Vigna Annual ACM Symposium on Applied Computing (ACSAC), 2014*
- ***Eyes of a human, eyes of a program: Leveraging different views of the web for analysis and detection*** *Jacopo Corbetta, Luca Invernizzi, Christopher Kruegel, Giovanni Vigna Research in Attacks Intrusions and Defenses (RAID), 2014*
- ***You are what you include: large-scale evaluation of remote javascript inclusions*** *Nick Nikiforakis, Luca Invernizzi, Alexandros Kapravelos, Steven Van Acker, Wouter Joosen, Christopher Kruegel, Frank Piessens, Giovanni Vigna ACM conference on Computer and communications security, 2012*
- ***EVILSEED: A Guided Approach to Finding Malicious Web Pages*** *Luca Invernizzi, UC Santa Barbara, Stefano Benvenuti, Marco Cova, Paolo Milani Comparetti, Christopher Kruegel, Giovanni Vigna IEEE Symposium on Security & Privacy (S&P) and AT&T NYU CSAW best security paper '12 finalist, 2012*
- ***Message In A Bottle: Sailing Past Censorship*** *Luca Invernizzi, Christopher Kruegel, Giovanni Vigna Annual Computer Security Applications Conference (ACSAC) and in HotPETS12 (workshop), 2012*
- ***A geometric approach to trajectory design for an autonomous underwater vehicle: Surveying the bulbous bow of a ship*** *Ryan N Smith, Dario Cazzaro, Luca Invernizzi, Giacomo Marani, Song K Choi, Monique Chyba Acta Applicandae Mathematicae, 2011*

- ***Geometric control for autonomous underwater vehicles: overcoming a thruster failure*** *Michael Andonian, Dario Cazzaro, Luca Invernizzi, Monique Chyba, Sergio Grammatico IEEE Conference on Decision and Control (CDC), 2010*
- ***Trajectory design for autonomous underwater vehicles for basin exploration*** *Monique Chyba, D Cazzaro, L Invernizzi, M Andonian International Conference on Computer and IT Applications in the Maritime Industries (COMPIT), 2010*

Program Committees

- **2025:** USENIX Security, ACSAC
- **2024:** USENIX Security
- **2023:** TheWebConf, IEEE S&P, NDSS MadWeb
- **2022:** CCS, S&P
- **2021:** RAID, NDSS MadWeb
- **2020:** IEEE S&P, CCS, NDSS, RAID, WWW
- **2018:** TheWebConf
- **2017:** TheWebConf
- **2016:** Ecrime

Open Source & Community

- **Core Developer & Mentor** | The GNOME Foundation | 2010 - 2012
    - Core developer of "Getting Things GNOME" and mentored students for Google Summer of Code and Gnome's Outreach Program for Women.
- **Hacking Competitions** | Shellphish Team | 2010 - 2015
    - Participated in numerous hacking competitions, including DEFCON CTF.
    - Helped design and organize the iCTF, a large-scale academic hacking competition.