Lorenzo De Carli

Department of Electrical and Software Engineering
University of Calgary
622 Collegiate Place NW, Calgary, AB T2N 4V8, Canada

Email: lorenzo.decarli@ucalgary.ca
Web: https://ldklab.github.io

Positions held

Assistant Professor. July 2022–Present
Department of Electrical and Software Engineering, University of Calgary
Calgary, AB, Canada

Assistant Professor. July 2018–June 2022
Department of Computer Science, Worcester Polytechnic Institute
Worcester, MA, USA

Assistant Professor. January 2017–June 2018
Computer Science Department, Colorado State University
Fort Collins, CO, USA

Education

University of Wisconsin-Madison, Madison, WI, USA

Ph.D. in Computer Science, December 2016
Advisor: Professor Somesh Jha

M.Sc. in Computer Science, May 2010

Politecnico di Torino, Torino, Italy

M.Sc. (2007) and B.Sc. (2005) in Computer Engineering

Current Research Interests

Network and IoT security, software security, usable security

Publications

Conferences

[C1] S. Neupane, G. Holmes, E. Wyss, D. Davidson, L. De Carli. Beyond Typosquatting: An In-depth Look at Package Confusion. *USENIX Security 2023. Acceptance rate: 33%*

[C2] T. Ren, R. Williams, S. Ganguly, L. Lu, L. De Carli. Breaking Embedded Software Homogeneity with Protocol Mutations. *EAI SecureComm 2022.*

[C3] S. Neupane, F. Tazi, U. Paudel, F. Veloz Baez, M. Adamjee, L. De Carli, S. Das, I. Ray. On the Data Privacy, Security, and Risk Postures of IoT Mobile Companion Apps. *IFIP DBSec 2022. Acceptance rate: 36%*

[C4] E. Wyss, A. Wittman, D. Davidson, L. De Carli. Wolf at the Door: Preventing Install-Time Attacks in npm with Latch. *ACM AsiaCCS 2022. Acceptance rate: 18%*

[C5] E. Wyss, L. De Carli, D. Davidson. What the Fork? Finding Hidden Code Clones in npm. *IEEE/ACM ICSE 2022. Acceptance rate: 26%*

[C6] L. De Carli, E. Solovey, I. Ray. Stewardship of Smart Devices Security for the Aging Population. *EuroUSEC 2021* **Honorary mention**. *Acceptance rate: (Vision Track) 50%*

[C7] V. Bhosale, L. De Carli, I. Ray. Detection of Anomalous User Activity for Home IoT Devices. *IoTBDS 2021.*

[C8] L. De Carli, A. Mignano. Network Security for Home IoT Devices Must Involve the User: a Position Paper. *FPS 2020.*

[C9] M. Taylor, R. Vaidya, D. Davidson, L. De Carli, V. Rastogi. Defending Against Package Typosquatting. *NSS 2020.*

[C10] F. De Gaspari, D. Hitaj, G. Pagnotta, L. De Carli, L. V. Mancini. EnCoD: Distinguishing Compressed and Encrypted File Fragments. *NSS 2020.*

[C11] N. Hansen, L. De Carli, D. Davidson. Assessing Adaptive Attacks Against Trained JavaScript Classifiers. *EAI SecureComm 2020. Acceptance rate: 36%*

[C12] F. De Gaspari, D. Hitaj, G. Pagnotta, L. De Carli, L. V. Mancini. The Naked Sun: Malicious Cooperation Between Benign-Looking Processes. *ACNS 2020. Acceptance rate: 21%*

[C13] L. De Carli, R. Torres, G. Modelo-Howard, A. Tongaonkar, S. Jha. Kali: Scalable Encryption Fingerprinting in Dynamic Malware Traces. *MALCON 2017. Acceptance rate: 33%*

[C14] V. Rastogi, D. Davidson, L. De Carli, S. Jha, P. McDaniel. Cimplifier: Automatically Debloating Containers. *ACM FSE 2017. Acceptance rate: 24%*

[C15] L. De Carli, R. Torres, G. Modelo-Howard, A. Tongaonkar, S. Jha. Botnet Protocol Inference in the Presence of Encrypted Traffic. *IEEE INFOCOM 2017. Acceptance rate: 21%*

[C16] R. Sommer, M. Vallentin, L. De Carli, V. Paxson. HILTI: An Abstract Execution Environment for Deep, Stateful Network Traffic Analysis. *ACM IMC 2014. Acceptance rate: 23%*

[C17] L. De Carli, R. Sommer, S. Jha. Beyond Pattern Matching: A Concurrency Model for Stateful Deep Packet Inspection. *ACM CCS 2014. Acceptance rate: 20%*

[C18] D. Luchaup, L. De Carli, S. Jha, E. Bach. Deep Packet Inspection with DFA-trees and Parametrized Language Overapproximation. *IEEE INFOCOM 2014. Acceptance rate: 19%*

[C19] S. J. Kim, L. De Carli, K. Sankaralingam, C. Estan. SWSL: SoftWare Synthesis for Network Lookup. *ACM/IEEE ANCS 2013.*

[C20] T. Nowatzki, M. Sartin-Tarm, L. De Carli, K. Sankaralingam, C. Estan, B. Robatmili. A General Constraint-centric Scheduling Framework for Spatial Architectures. *ACM PLDI 2013* **Distinguished paper award**. *Acceptance rate: 17%*

[C21] E. Harris, S. Wasmundt, L. De Carli, K. Sankaralingam, C. Estan. LEAP: Latency- Energy- and Area-optimized Lookup Pipeline. *ACM/IEEE ANCS 2012. Acceptance rate: 28%*

[C22] B. Aggarwal, R. Bhagwan, L. De Carli, V. N. Padmanabhan, K. P. N. Puttaswamy. Deja Vu: Fingerprinting Network Problems. *ACM CoNEXT 2011. Acceptance rate: 19%*

[C23] N. Vaish, T. Kooburat, L. De Carli, K. Sankaralingam, C. Estan. Experiences in Co-designing a Packet Classification Algorithm and a Flexible Hardware Platform. *ACM/IEEE ANCS 2011. Acceptance rate: 32%*

[C24] A. Kumar, L. De Carli, S. J. Kim, M. de Kruijf, K. Sankaralingam, C. Estan, S. Jha. Design and Implementation of the PLUG Architecture for Programmable and Efficient Network Lookups. *PACT 2010. Acceptance rate: 17%*

[C25] L. De Carli, Y. Pan, A. Kumar, C. Estan, K. Sankaralingam. PLUG: Flexible Lookup Modules for Rapid Deployment of New Protocols in High-speed Routers. *ACM SIGCOMM 2009. Acceptance rate: 10%*

[C26] A. Baldini, L. De Carli, F. Risso. Increasing Performances of TCP Data Transfers Through Multiple Parallel Connections. *IEEE ISCC 2009.*

Journals

[J1] F. De Gaspari, D. Hitaj, G. Pagnotta, L. De Carli, L. V. Mancini. Reliable Detection of Compressed and Encrypted Data. *Neural Computing and Applications (NCAA)*, July 2022.

[J2] F. De Gaspari, D. Hitaj, G. Pagnotta, L. De Carli, L. V. Mancini. Evading Behavioral Classifiers: A Comprehensive Analysis on Evading Ransomware Detection Techniques. *Neural Computing and Applications (NCAA)*, March 2022.

[J3] R. Williams, T. Ren, L. De Carli, L. Lu, G. Smith. Guided Feature Identification and Removal for Resource-Constrained Firmware. *ACM Trans. Softw. Eng. Methodol. (TOSEM) 31, 2*, April 2022.

[J4] T. Nowatzki, M. Sartin-Tarm, L. De Carli, K. Sankaralingam, C. Estan, B. Robatmili. A Scheduling Framework for Spatial Architectures Across Multiple Constraint-Solving Theories. *ACM Trans. Program. Lang. Syst. (TOPLAS) 37, 1*, November 2014.

[J5] M. Sartin-Tarm, T. Nowatzki, L. De Carli, K. Sankaralingam, C. Estan. Constraint centric scheduling guide. *ACM SIGARCH Computer Architecture News, Volume 41 Issue 2*, May 2013.

Workshops

[W1] E. Wyss, L. De Carli, D. Davidson. (Nothing But) Many Eyes Make All Bugs Shallow. *ACM SCORED (CCS Workshop) 2023. Acceptance rate: 55%*

[W2] S. Bukhari, B. Tan, L. De Carli. Distinguishing AI- and Human-Generated Code: a Case Study. *ACM SCORED (CCS Workshop) 2023. Acceptance rate: 55%*

[W3] F. Tazi, S. Saka, G. Opp, S. Neupane, S. Das, L. De Carli, I. Ray. Accessibility Evaluation of IoT Android Mobile Companion Apps. *CHI LBW Track 2023. Acceptance rate: 34%*

[W4] T. Ren, A. Wittman, L. De Carli, D. Davidson. An Analysis of First-Party Cookie Exfiltration due to CNAME Redirections. *madWEB (NDSS Workshop) 2021* **Best paper award runner-up**.

[W5] E. Zhou, J. Turcotte, L. De Carli. Enabling Security Analysis of IoT Device-to-Cloud Traffic. *IEEE TrustCom IWCSS Workshop 2020.*

[W6] L. De Carli, I. Ray, E. Solovey. Enabling IoT Residential Security Stewardship for the Aging Population (Extended Abstract). *ACM CHI Workshop "Designing Interactions for the Ageing Populations" 2020.*

Grants

[G1] Managing Risks of AI-generated Code in the Software Supply Chain (grant, 06/2024-05/2027). PIs: Rachel Greenstadt (NYU), Benjamin Tan (UCalgary); co-PIs: Brendan Dolan-Gavitt (NYU), Lorenzo De Carli. *Sponsor: NSERC/NSF Collaboration.* Amount: USD $600K + CAD 255K.

[G2] IoT security and privacy for shared habitats (grant, 02/2024-03/2026). PI: Lorenzo De Carli; co-PIs: Ryan Henry (UCalgary), Joel Reardon (UCalgary), Rei Safavi-Naeini (UCalgary). *Sponsor: Concordia University/Volt-Age.* Amount: CAD $200K.

[G3] Democratizing IoT Security (grant, 04/2023-04/2028). PI: Lorenzo De Carli. *Sponsor: NSERC.* Amount: CAD $217K.

[G4] Typosquatting / Malware Detection Research (gift, 07/2021-07/2023). PI: Lorenzo De Carli. *Sponsor: Google Open Source Security Team.* Amount: USD $100K.

[G5] Renewal of the Scholarship for Service (SFS) Program at the Worcester Polytechnic Institute (grant, 01/2021-12/2025). PI: Craig Shue (WPI); co-PIs: Lorenzo De Carli, Robert Walls (WPI), Craig Wills (WPI). *Sponsor: NSF.* Amount: USD $4.8M.

[G6] Worcester Polytechnic Institute DoD Cyber Scholarship (grant, 09/2020-12/2021). PI: Craig Shue (WPI); co-PIs: Lorenzo De Carli, Robert Walls (WPI). *Sponsor: DoD.* Amount: USD $94K.

[G7] Automated Protocol Specialization and Diversification for Individualized Defense (grant, 08/2018-03/2022). PI: Somesh Jha (UW-Madison); co-PIs: Lorenzo De Carli, Vinod Yegneswaran (SRI). *Sponsor: Office of Naval Research.* Amount: USD $373K.

Patents

[P1] K. Sankaralingam, J. Menon, L. De Carli. Memory Processing Core Architecture. *US Patent US10289604B2*, granted 05/2019.

[P2] R. Torres Guerra, G. Modelo-Howard, A. Tongaonkar, L. De Carli, S. Jha. Systems and methods for reverse-engineering malware protocols. *US Patent US10050982B1*, granted 08/2018.

[P3] R. Bhagwan, V. N. Padmanabhan, B. Aggarwal, L. De Carli. Learning signatures for application problems using trace data. *US Patent US8880933B2*, granted 11/2014.

Talks & Presentations

- The Computer Science graduate program at WPI. Providence College, Oct 30th 2019.
- Securing Your Network. WPI A&S Lightning Talk, Sep 16th 2019.
- Adversarial Program Synthesis: Malicious JavaScript and Cross-site Scripting. La Sapienza University of Rome, July 8th 2019.
- Automatic Inference of Malware Protocol Specifications (and Other Adventures in Network Traffic Analysis. La Sapienza University of Rome, June 13th 2018.
- Program analysis for networking problems: parallelization and de-bloating. Politecnico di Torino, May 15th 2018.

- Automatic Inference of Malware Protocol Specifications. Northeastern University, Nov 13th 2017.
- How I learned to stop worrying and love the job search (advice to graduate students who plan to seek academic jobs). Colorado State University, Oct 9th 2017.
- Automatic Inference of Malware Protocol Specifications. Politecnico di Torino, Sep 5th 2017.
- Increasing Flexibility in Network Traffic Analysis. Colorado State University, Feb 6th 2017.
- Efficient and Flexible Traffic Analysis. Brown University, Jan 31st 2017.

Teaching Experience

University of Calgary:

- ENSF 619.06 - Elements of Software Security (graduate), Winter 2025
- ENSF 338 - Practical Data Structures and Algorithms, Winter 2023, Winter 2024, Winter 2025
- ENSF 461 - Applied Operating Systems, Fall 2023, Fall 2024

Worcester Polytechnic Institute:

- CS 3516 - Computer Networks, B-Term 2019, B-Term 2021, D-Term 2022
- CS 513 - Computer Networks (graduate), Fall 2020, Fall 2021
- CS 4536 - Programming Languages, D-Term 2020
- CS 558 - Computer Network Security (graduate), Fall 2019
- CS 4516 - Advanced Networks, D-Term 2019

Colorado State University:

- CS557 - Advanced Networking (graduate), Fall 2017, Spring 2018

Students Graduated

- Vincenzo Marino (MS, PoliTo) - graduated July 2023. Co-advised with Riccardo Sisto.
- Shradha Neupane (MS, WPI) - graduated May 2023.
- Vishwajeet Bhosale (MS, CSU) - graduated December 2021. Co-advised with Indrakshi Ray.
- Ryan LaPointe (MS, WPI) - graduated May 2021.
- Heshan Perera (MS, WPI) - graduated December 2020. Co-advised with Robert Walls.

Thesis Committees

- PhD thesis committee member for Sarah Shah, University of Calgary (grad. exp. 2024).
- MS thesis internal examiner for Sepideh Bahadoripour, University of Calgary (grad. 2023).
- MS thesis internal examiner for Amirhossein Pakbaz, University of Calgary (grad. 2023).
- MS thesis commitee member for Aadharsh Hariharan, University of Calgary (grad. 2023).
- PhD thesis committee member for Yunsen Lei, WPI (grad. 2023).
- MS thesis committee member for Emad Jabbar, University of Calgary (grad. 2022).
- MS thesis reader for Yunsen Lei, WPI (grad. 2021).
- MS thesis reader for Roger Wirkala, WPI (grad. 2021).
- PhD thesis referee for Jalolliddin Yusupov, Politecnico di Torino (grad. 2020).
- PhD thesis referee for Roberto Bonafiglia, Politecnico di Torino (grad. 2018).

Service

General/PC Chair

- PC co-Chair, ACM Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses (SCORED), 2024.
- General Chair, International Workshop on Cyber-Security in Software-defined and Virtualized Infrastructures (SecSoft), 2024.

Program Committees (selected)

- Annual Computer Security Applications Conference (ACSAC), 2024.
- ACM Internet Measurement Conference (IMC), 2024.
- USENIX Security Symposium (USENIX Security), 2024.
- ACM ASIA Conference on Computer and Communications Security (AsiaCCS), 2024.
- Annual Computer Security Applications Conference (ACSAC), 2023.
- ACM Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses (SCORED), 2023.
- ACM Conference on Computer and Communications Security (CCS), 2023.
- ACM ASIA Conference on Computer and Communications Security (AsiaCCS), 2023.
- Annual Computer Security Applications Conference (ACSAC), 2022.
- ACM Internet Measurement Conference (IMC), 2022.
- ACM Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses (SCORED), 2022.

- ACM Workshop on Forming an Ecosystem Around Software Transformation (FEAST), 2020.
- Research in Attacks, Intrusions and Defenses (RAID), 2020.
- ACM Conference on Computer and Communications Security (CCS), 2019.
- Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA), 2019.
- IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2016.

Journal Reviewer (selected)

IEEE Transactions on Dependable and Secure Computing (TDSC), Elsevier Computer Standards & Interfaces (CSI), IEEE Transactions on Vehicular Technology (TVT), Elsevier Journal of Cloud Computing (JCC), IEEE Transactions on Green Communications and Networking (TGCN), IEEE Transactions on Network and Service Management (TNSM), IEEE/ACM Transactions on Networking (TNET), IEEE Transactions on Industrial Informatics (TII), Elsevier Computers & Security (COSE), IEEE Journal on Selected Areas in Communications (JSAC), IEEE Transactions on Mobile Computing (TMC), ACM Computing Surveys (CSUR), IEEE Access, Elsevier Journal of Information Security and Applications (JISA).

Grant Reviewer

NSF Panel Member (2018, 2021)

Honors & Awards

- Honorable Mention, European Symposium on Usable Security (EuroUSEC), 2021.
- Best Paper Award Runner-Up, NDSS MadWeb Workshop, 2021.
- WARF (Wisconsin Alumni Research Foundation) innovation award finalist (with Karthikeyan Sankaralingam and Jai Menon), Wisconsin Alumni Research Foundation, 2015.
- Distinguished Paper Award, ACM SIGPLAN conference on Programming Language Design and Implementation (PLDI), 2013.