Yohan **Beugin**

Ph.D. Student · Computer Sciences · University of Wisconsin–Madison

1210 W. Dayton Street, Madison, WI 53706-1613, USA

yohan@beugin.org https://yohan.beugin.org yohhaan Yohan Beugin

Research Experience

MadS&P - Security and Privacy Research Group at UW–Madison — *UW–Madison*

Research Assistant — *2022 - Present*

- My research focuses on security of open-source software as well as tracking and privacy in online advertising

Lead Graduate Student — *2024 - Present*

- Mentoring students and managing lab logistics

Systems and Internet Infrastructure Security Laboratory — *Penn State*

Research Assistant — *2019 - 2022*

- Development of CaCTUs, a privacy-preserving smart camera system controlled totally by its users (PETS 2022)
- Collaboration in adversarial machine learning, cloud security, trusted execution environments, and internet of things
- System administration of the lab research cluster (9 DELL Poweredge R640, 1 DELL Poweredge R740XD, and 12 A100 GPUs)

LIRIS Laboratory, École Centrale de Lyon — *Centrale Lyon*

Research Internship — *Summer 2019*

- Development of ReViVD, a tool for exploring and filtering large trajectory-based datasets using virtual reality (IEEE VR 2020)

Education

University of Wisconsin–Madison — *Madison, WI, USA*

Ph.D. in Computer Sciences — *2022 - Present*

- Dissertation Topic: *Measuring and Securing Open-Source Software*
- Advisor: Prof. Patrick McDaniel
- Transfer from Penn State starting Fall 2022

The Pennsylvania State University — *University Park, PA, USA*

Ph.D. in Computer Science and Engineering — *2021 - 2022 (transferred)*

- Advisor: Prof. Patrick McDaniel
- Transfer to UW–Madison starting Fall 2022

The Pennsylvania State University — *University Park, PA, USA*

M.S. in Computer Science and Engineering — *2019 - 2021*

- Thesis: *Building a Secure and Privacy-Preserving Smart Camera System*
- Advisor: Prof. Patrick McDaniel
- Thesis committee: Prof. Patrick McDaniel, Prof. Gang Tan, Prof. Syed Rafiul Hussain

École Centrale de Lyon — *Lyon, France*

Diplôme d'Ingénieur (M.S. and B.S. in Engineering Sciences) — *2017 - 2021*

- French Engineering School
- Multidisciplinary studies: Maths, Physics, Computer Science, Fluid Mechanics, Electrical Engineering, Economics, Management, etc.

Lycée Faidherbe — *Lille, France*

Classe Préparatoire aux Grandes Écoles (equivalent to the first 2 years of B.S. in Engineering Sciences) — *2015 - 2017*

- 2-year intensive program preparing for the national competitive exams for entry to the top French Engineering Schools

Publications

Conferences

- Kunyang Li, Jean-Charles Noirot Ferrand, Ryan Sheatsley, Blaine Hoak, **Yohan Beugin**, Eric Pauley, and Patrick McDaniel. "On the Robustness Tradeoff in Fine-Tuning". In: *2025 International Conference on Computer Vision (ICCV)*. Oct. 2025. DOI: 10.48550/arXiv.2503.14836.
- Quinn Burke, Ryan Sheatsley, **Yohan Beugin**, Eric Pauley, Owen Hines, Michael Swift, and Patrick McDaniel. "Efficient Storage Integrity in Adversarial Settings". In: *2025 IEEE Symposium on Security and Privacy (SP)*. May 2025. DOI: 10.1109/SP61157.2025.00196.
- Eric Pauley, Kyle Domico, Blaine Hoak, Ryan Sheatsley, Quinn Burke, **Yohan Beugin**, Engin Kirda, and Patrick McDaniel. "Secure IP Address Allocation at Cloud Scale". In: *2025 Network and Distributed Systems Security Symposium (NDSS)*. Feb. 2025. DOI: 10.14722/ndss.2025.230374.
- **Yohan Beugin** and Patrick McDaniel. "Interest-disclosing Mechanisms for Advertising are Privacy-Exposing (not Preserving)". In: *Proceedings on Privacy Enhancing Technologies Symposium (PETS)*. July 2024. DOI: 10.56553/popets-2024-0004.
- Ryan V Guide, Eric Pauley, **Yohan Beugin**, Ryan Sheatsley, and Patrick McDaniel. "Characterizing the Modification Space of Signature IDS Rules". In: *2023 IEEE Military Communications Conference (MILCOM)*. Oct. 2023. DOI: 10.1109/MILCOM58377.2023.10356225.
- **Yohan Beugin**, Quinn Burke, Blaine Hoak, Ryan Sheatsley, Eric Pauley, Gang Tan, Syed Rafiul Hussain, and Patrick McDaniel. "Building a Privacy-Preserving Smart Camera System". In: *Proceedings on Privacy Enhancing Technologies Symposium (PETS)*. July 2022. DOI: 10.2478/popets-2022-0034.
- Eric Pauley, Ryan Sheatsley, Blaine Hoak, Quinn Burke, **Yohan Beugin**, and Patrick McDaniel. "Measuring and Mitigating the Risk of IP Reuse on Public Clouds". In: *2022 IEEE Symposium on Security and Privacy (SP)*. Apr. 2022. DOI: 10.1109/SP46214.2022.9833784.
- Ahmed Abdou, Ryan Sheatsley, **Yohan Beugin**, Tyler Shipp, and Patrick McDaniel. "HoneyModels: Machine Learning Honeypots". In: *2021 IEEE Military Communications Conference (MILCOM)*. Nov. 2021. DOI: 10.1109/MILCOM52596.2021.9652947.
- Ryan Sheatsley, Blaine Hoak, Eric Pauley, **Yohan Beugin**, Michael J. Weisman, and Patrick McDaniel. "On the Robustness of Domain Constraints". In: *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (CCS)*. Nov. 2021. DOI: 10.1145/3460120.3484570.
- François Homps, **Yohan Beugin**, and Romain Vuillemot. "ReViVD: Exploration and Filtering of Trajectories in an Immersive Environment using 3D Shapes". In: *2020 IEEE Conference on Virtual Reality and 3D User Interfaces (VR)*. Mar. 2020. DOI: 10.1109/VR46266.2020.00096.

Workshops

- Rachel King, Quinn Burke, **Yohan Beugin**, Blaine Hoak, Kunyang Li, Eric Pauley, Ryan Sheatsley, and Patrick McDaniel. *ParTEETor: A System for Partial Deployments of TEEs within Tor*. Proceedings of the 23rd Workshop on Privacy in the Electronic Society (WPES). Oct. 2024. DOI: 10.48550/arXiv.2408.14646.
- **Yohan Beugin** and Patrick McDaniel. *A Public and Reproducible Assessment of the Topics API on Real Data*. IEEE Security and Privacy Workshops (SPW - SecWeb). May 2024. DOI: 10.48550/arXiv.2403.19577.

Journals

- Quinn Burke, **Yohan Beugin**, Blaine Hoak, Rachel King, Eric Pauley, Ryan Sheatsley, Mingli Yu, Ting He, Thomas La Porta, and Patrick McDaniel. "Securing Cloud File Systems with Trusted Execution". In: *IEEE Transactions on Dependable and Secure Computing (TDSC)* (Sept. 2024). DOI: 10.1109/TDSC.2024.3474423.

Talks

- **Yohan Beugin** and Patrick McDaniel. *The Need for a (Research) Sandstorm through the Privacy Sandbox*. 17th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs 2024). July 2024. URL: https://privacysandstorm.com.
- **Yohan Beugin**. *Privacy-Preserving Protocols for Smart Camera Systems and Other IoT Devices*. June 2022. URL: https://www.usenix.org/conference/pepr22/presentation/beugin.

Preprints

- Jean-Charles Noirot Ferrand, **Yohan Beugin**, Eric Pauley, Ryan Sheatsley, and Patrick McDaniel. *Targeting Alignment: Extracting Safety Classifiers of Aligned LLMs*. 2025. DOI: 10.48550/arXiv.2501.16534.
- Yash Vekaria, **Yohan Beugin**, Shaoor Munir, Gunes Acar, Nataliia Bielova, Steven Englehardt, Umar Iqbal, Alexandros Kapravelos, Pierre Laperdrix, Nick Nikiforakis, Jason Polakis, Franziska Roesner, Zubair Shafiq, and Sebastian Zimmeck. *SoK: Advances and Open Problem in Web Tracking*. 2025. DOI: 10.48550/arXiv.2506.14057.
- Alban Héon, Ryan Sheatsley, Quinn Burke, Blaine Hoak, Eric Pauley, **Yohan Beugin**, and Patrick McDaniel. *Systematic Evaluation of Geolocation Privacy Mechanisms*. 2023. DOI: 10.48550/arXiv.2309.06263.
- **Yohan Beugin**, Quinn Burke, Blaine Hoak, Ryan Sheatsley, Eric Pauley, Gang Tan, Syed Rafiul Hussain, and Patrick McDaniel. *Privacy-Preserving Protocols for Smart Cameras and Other IoT Devices*. 2022. DOI: 10.48550/arXiv.2208.09776.

- Kyle Domico, Ryan Sheatsley, **Yohan Beugin**, Quinn Burke, and Patrick McDaniel. *A Machine Learning and Computer Vision Approach to Geomagnetic Storm Forecasting*. 2022. DOI: `10.48550/arXiv.2204.05780`.

Chapters

- **Yohan Beugin**, Sam Dutton, Yana Dimova, Rowan Merewood, and Barry Pollard. "Cookies". English. In: *The 2024 Web Almanac*. HTTP Archive, 2024. Chap. 21. DOI: `10.5281/zenodo.14065903`. URL: `https://almanac.httparchive.org/en/2024/cookies`.

Thesis

- **Yohan Beugin**. "Building a Secure and Privacy-Preserving Smart Camera System". The Pennsylvania State University, May 2021. URL: `https://etda.libraries.psu.edu/files/final_submissions/23611`.

Honors & Awards

2025	**Distinguished Artifact Reviewer**, PETS
2025	**Google Research Conference on Ads Privacy Travel Award**, Awardee
2025	**SAMSUNG START Research Proposal**, Finalist
2025	**Google Cloud Research Credits**, Awardee
2024	**The Andreas Pfitzmann Best Student Paper Award Runner-up**, PETS
2024	**Distinguished Artifact Reviewer & Award Sub-committee**, USENIX Security
2024	**Ph.D. Student Fellowship**, EPFL Summer Research Institute (SuRI)
2024	**Distinguished Artifact Award Sub-committee**, NDSS
2023	**Distinguished Artifact Reviewer**, USENIX Security
2021	**Centrale Lyon's Student Organizations Commitment Recognition**, Awardee
2015	**Placa de Honor de la Orden Civil de Alfonso X El Sabio**, Awardee (high school's binational section)

Engagement & Public Speaking

- *Privacy & Utility Analysis of the Topics API for the Web [Poster]*. 2025 Google Research Conference on Ads Privacy. June 2025.
- *The Need for a (Research) Sandstorm through the Privacy Sandbox [Poster]*. UW–Madison CS Welcome Week-end. Mar. 2025.
- *The Need for a (Research) Sandstorm through the Privacy Sandbox [Poster]*. UW–Madison CS Research Fair. Oct. 2024.
- *Privacy & Utility Analysis of the Topics API for the Web [Poster]*. 2024 Symposium on Usable Privacy and Security (SOUPS). Aug. 2024.
- *Interest-disclosing Mechanisms for Advertising are Privacy-Exposing (not Preserving)*. 2024 Privacy Enhancing Technologies Symposium (PETS). July 2024.
- *Privacy & Utility Analysis of the Topics API for the Web [Poster]*. 2024 EPFL Summer Research Institute. July 2024.
- *Privacy & Utility Analysis of the Topics API for the Web [Poster]*. 2024 Privacy Enhancing Technologies Symposium (PETS). July 2024.
- *The Need for a (Research) Sandstorm through the Privacy Sandbox*. 17th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs 2024). July 2024.
- *A Public and Reproducible Assessment of the Topics API on Real Data*. 2024 IEEE Security and Privacy Workshops (SPW - SecWeb). May 2024.
- *Analysis of the Topics API for the Web [Poster]*. UW–Madison CS Research Fair. Oct. 2023.
- *Graduate School and Research in the United States*. Dual Degree Information Session for Centrale Lyon's Students. 2022.
- *Building a Privacy-Preserving Smart Camera System*. UW–Madison Security & Privacy Seminar. Sept. 2022.
- *Building a Privacy-Preserving Smart Camera System*. 2022 Privacy Enhancing Technologies Symposium (PETS). July 2022.
- *Privacy-Preserving Protocols for Smart Camera Systems and Other IoT Devices*. 2022 USENIX Conference on Privacy Engineering Practice and Respect (PEPR). June 2022.
- *Building a Privacy-Preserving Smart Camera System*. Penn State Security Reading Group. 2021.
- *Graduate School at Penn State*. Dual Degree Feedback Session for Centrale Lyon's Students. 2021.
- *M.S. in Computer Science and Engineering at Penn State*. Dual Degree Information Session for Centrale Lyon's Students. 2020.
- *ReViVD: Exploration and Filtering of Trajectories in an Immersive Environment using 3D Shapes*. 2020 IEEE Conference on Virtual Reality and 3D User Interfaces (VR). Mar. 2020.

Professional Activities

Teaching Experience

Spring 2025	**CS839 - Emerging Trends in Security & Privacy**, Course Design & Guest Lecturer & Course Assistant	*UW–Madison*
Fall 2024	**CS642 - Introduction to Information Security**, Project Design & Guest Lecturer	*UW–Madison*
Fall 2023	**CS642 - Introduction to Information Security**, Course Design & Guest Lecturer	*UW–Madison*
Fall 2021	**CMPSC297 - Introduction to C Programming**, Course Design & Guest Lecturer & Teaching Assistant	*Penn State*
Fall 2021	**CMPSC311 - Introduction to Systems Programming**, Guest Lecturer & Teaching Assistant	*Penn State*
Fall 2021	**CSE597 - Emerging Trends in Computer Security**, Teaching Assistant	*Penn State*

Reviewer (Conferences)

2026	**Proceedings on Privacy Enhancing Technologies (PoPETs)**, Technical Program Committee
2025	**MADWeb Workshop**, Technical Program Committee
2024	**SecWeb Workshop**, Technical Program Committee
2022-24	**IEEE Symposium on Security and Privacy (IEEE S&P)**, External reviewer
2021-23	**ACM Conference on Computer and Communications Security (ACM CCS)**, External Reviewer
2021-23	**USENIX Security Symposium (USENIX Security)**, External Reviewer
2021	**International Conference on Mobile Computing and Networking (MobiCom)**, External Reviewer
2021	**IEEE Computer Security Foundations Symposium (CSF)**, External Reviewer

Reviewer (Journals)

2025	**IEEE Transactions on Privacy**, Invited Reviewer
2020	**PeerJ Computer Science**, Invited Reviewer

Reviewer (Other)

2025	**IEEE Symposium on Security and Privacy (IEEE S&P)**, Poster Jury
2023-25	**Proceeding of Privacy Enhancing Technologies Symposium (PoPETs)**, Artifact Reviewer
2023-25	**USENIX Security Symposium (USENIX Security)**, Artifact Reviewer
2024	**Network and Distributed System Security Symposium (NDSS)**, Artifact Reviewer

Organization

2026-27	**Proceeding of Privacy Enhancing Technologies Symposium (PoPETs)**, Artifact Chair
2024	**IEEE Symposium on Security and Privacy (IEEE S&P)**, Session Chair
2023-24	**IEEE Conference on Secure and Trustworthy Machine Learning (IEEE SaTML)**, Web Chair
2023	**Secure and Trustworthy Cyberspace Vision 2.0 Workshop (SaTC 2.0)**, Chair Support

Other Service

2023-24	**UW-Madison Security & Privacy Seminar**, Co-organizer
2023-25	**UW-Madison CS Welcome Weekend**, Open Lab and Campus Tour Volunteer
2023-25	**UW-Madison new CS Graduate Students Mentoring Program**, Mentor

Skills

Computing Skills

Languages	C, C++, C#, Bash, Go, Python, Java, Typescript, Matlab, LaTeX, (X)HTML, CSS, JavaScript, SQL, PHP
OS	GNU/Linux (Debian), Windows
Softwares	Docker, Git, Apache, Nginx, MariaDB, Gitlab, Virtual Machine Manager, Iptables, Zabbix, etc.
Others	Ionic, Arduino, Wordpress, Android SDK, Unity

Language Skills

French	Native
English	Fluent
Spanish	Fluent

Extracurricular Activities

ÉCLAIR - IT Student Organization of Centrale Lyon

Centrale Lyon

SYSADMIN, DEVELOPER, AND TEAM LEADER *2018 - 2019*

- Network administration of the on-campus accommodations, about 800 rooms
- Development, maintenance, and hosting of students and other organizations' websites, about 30 websites
- Maintenance of the network, servers, and of the internal payment system on campus, about €100k of revenue per year
- GDPR compliance of the organization, about 3,000 users and 40 services

Challenge Centrale Lyon

Centrale Lyon

ORGANIZER AND DIGITAL MANAGER *2018 - 2019*

- Organizer of the 37th edition of this student-organized sports tournaments, about 3,000 students from 40 different schools
- Development and maintenance of the registration website, the smartphone application, the interactive giant screens display system, and the dispatch algorithm of the participants in the shuttles

Smartphone Application - Challenge Centrale Lyon

Centrale Lyon

DEVELOPER AND PROJECT MANAGER *2017 - 2018*

- Project manager of a team developing a smartphone application for the Challenge Centrale Lyon
- Development and release of the iOS and Android applications in under 3 months to be available to the 3,000 participants

GeoNord - Geocaching Events

France

MAIN ORGANIZER OF THE LARGEST ANNUAL GEOCACHING EVENTS OF FRANCE *Since 2014*

- 6 events organized in 2015, 2016, 2017, 2018, 2022, and 2025 gathering 2,000 to 3,000 participants over 4-5 days
- Creation of an $100\,\mathrm{m}^2$ exhibition about Geocaching
- See `https://www.geonordelements.com/` for more