Vivek C. Nair, Ph.D.

CURRICULUM VITAE

Washington, D.C.

TS/SCI w/ FS

Schedule a meeting →

I am passionate about defending our digital world and have spent over a decade researching applied cryptographic techniques to secure critical systems. I previously served as a Technical Lead within elite cyber units of the Department of Defense (DOD) and Central Intelligence Agency (CIA), where I received the directorate's Exceptional Performance Award for advancing the frontiers of US cyber operations. I completed my Ph.D. in Computer Science at UC Berkeley at the age of 22, supported by prestigious fellowships from the National Science Foundation, the National Physical Science Consortium, and the Fannie and John Hertz Foundation.

Email	Website	GitHub	LinkedIn	Google Scholar
vivek@nair.me	nair.me	/VCNinc	/nair	6BgkAeQAAAAJ

Experience

US Government, *Cyber Researcher*

- **Central Intelligence Agency (CIA)**: 2023–2025
- **Department of Defense (DOD)**: 2020–2021

UC Berkeley, *Computer Security Researcher*

- **Center for Responsible Decentralized Intelligence (RDI)**: 2022–2023
- **Initiative for CryptoCurrencies & Contracts (IC3)**: 2021–2022

Solid Security, *Authentication Consultant*

2015–2020

Holmusk, *Software Engineer*

2015–2015

VCNinc, *Software Engineer*

2014–2015

Education

University of California, Berkeley

- Ph.D. in Computer Science

University of Illinois Urbana-Champaign

- Master's Degree in Computer Science
- Bachelor's Degree in Computer Science

Awards

Central Intelligence Agency (CIA)

- Exceptional Performance Award
  Awarded for extraordinary contributions to US national security.

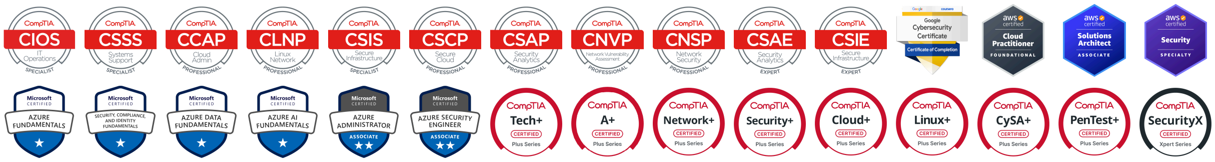
University of California, Berkeley

- Tong Leong Lim Pre-Doctoral Prize
  Awarded annually to the student who achieves the highest distinction in the pre-doctoral examination.
- Fannie and John Hertz Foundation Fellowship
- National Physical Science Consortium Fellowship

University of Illinois Urbana-Champaign

- National Science Foundation Scholarship

Certifications


CompTIA CIOS IT Operations SPECIALIST
CompTIA CSSS Systems Support SPECIALIST
CompTIA CCAP Cloud Admin PROFESSIONAL
CompTIA CLNP Linux Network PROFESSIONAL
CompTIA CSIS Secure Infrastructure SPECIALIST
CompTIA CSCP Secure Cloud PROFESSIONAL
CompTIA CSAP Security Analytics PROFESSIONAL
CompTIA CNVP Network Vulnerability Assessment PROFESSIONAL
CompTIA CNSP Network Security PROFESSIONAL
CompTIA CSAE Security Analytics EXPERT
CompTIA CSIE Secure Infrastructure EXPERT
Google coursera Google Cybersecurity Certificate Certificate of Completion
aws certified Cloud Practitioner FOUNDATIONAL
aws certified Solutions Architect ASSOCIATE
aws certified Security SPECIALTY
Microsoft CERTIFIED AZURE FUNDAMENTALS
Microsoft CERTIFIED SECURITY, COMPLIANCE, AND IDENTITY FUNDAMENTALS
Microsoft CERTIFIED AZURE DATA FUNDAMENTALS
Microsoft CERTIFIED AZURE AI FUNDAMENTALS
Microsoft CERTIFIED AZURE ADMINISTRATOR ASSOCIATE
Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE
CompTIA Tech+ CERTIFIED Plus Series
CompTIA A+ CERTIFIED Plus Series
CompTIA Network+ CERTIFIED Plus Series
CompTIA Security+ CERTIFIED Plus Series
CompTIA Cloud+ CERTIFIED Plus Series
CompTIA Linux+ CERTIFIED Plus Series
CompTIA CySA+ CERTIFIED Plus Series
CompTIA PenTest+ CERTIFIED Plus Series
CompTIA SecurityX CERTIFIED Xpert Series

Publications

“**Exploring the Privacy Risks of Adversarial VR Game Design**,” Vivek Nair*, Gonzalo Munilla Garrido*, Dawn Song, and James F. O'Brien in *Proceedings on Privacy Enhancing Technologies*, 2023. [view] [pdf] [video] [code] [site]

“**Multi-Factor Key Derivation Function (MFKDF) for Fast, Flexible, Secure, & Practical Key Management**,” Vivek Nair and Dawn Song in *USENIX Security Symposium*, 2023. [view] [pdf] [video] [code] [site]

🏅 Distinguished Artifact Award

“**Unique Identification of 50,000+ Virtual Reality Users from Head & Hand Motion Data**,” Vivek Nair, Wenbo Guo, Justus Mattern, Rui Wang, James F. O'Brien, Louis Rosenberg, and Dawn Song in *USENIX Security Symposium*, 2023. [view] [pdf] [video] [code] [site]

“**Decentralizing Custodial Wallets with MFKDF**,” Vivek Nair and Dawn Song in *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2023. [view] [code] [site]

“**MEVade: An MEV-Resistant Blockchain Design**,” Julien Piet, Vivek Nair, and Sanjay Subramanian in *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2023. [view]

“**Multi-Factor Credential Hashing for Asymmetric Brute-Force Attack Resistance**,” Vivek Nair and Dawn Song in *IEEE European Symposium on Security and Privacy (EuroS&P)*, 2023. [view] [code] [site]

“**Going Incognito in the Metaverse: Achieving Theoretically Optimal Privacy-Usability Tradeoffs in VR**,” Vivek Nair*, Gonzalo M. Garrido*, and Dawn Song in *ACM Symposium on User Interface Software and Technology (UIST)*, 2023. [view] [pdf] [video] [code] [site]

🏅 Best Paper Award

“**SoK: Data Privacy in Virtual Reality**,” Gonzalo M. Garrido, Vivek Nair, and Dawn Song in *Privacy Enhancing Technologies Symposium (PETS)*, 2024. [view] [pdf] [site]

“**Truth in Motion: The Unprecedented Risks and Opportunities of Extended Reality Motion Data**,” Vivek Nair, Louis Rosenberg, James F. O'Brien, and Dawn Song in *IEEE Security & Privacy (S&P)*, 2024. [view] [pdf] [site]

“**ProtoBlocks: Programming Language for Secure Implementation of Cryptographic Protocols**,” Vivek Nair, William Mullen, and Ethan Lee in *EECS Technical Reports*, 2023. [pdf]

“**MFDPG: Multi-Factor Authenticated Password Management With Zero Stored Secrets**,” Vivek Nair and Dawn Song in *arXiv*, 2023. [view] [pdf] [code]

“**Effect of Duration and Delay on the Identifiability of VR Motion**,” Mark Roman Miller, Vivek Nair, Eugy Han, Cyan DeVeaux, Christian Rack, Rui Wang, Brandon Huang, Marc Erich Latoschik, James F. O'Brien, and Jeremy N. Bailenson in *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 2024. [view] [code]

“**Effect of Data Degradation on Motion Re-Identification**,” Vivek Nair, Mark Roman Miller, Rui Wang, Brandon Huang, Christian Rack, Marc Erich Latoschik, and James F. O'Brien in *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 2024. [view] [code]

“**Fast Anonymous Consensus and Private Authentication in Large Distributed Systems**,” Vivek Nair and Bolton Bailey in *arXiv*, 2023.

“**Results of the 2023 Census of Beat Saber Users**,” Vivek Nair, Viktor Radulov, and James F. O'Brien in *arXiv*, 2023. [view] [pdf]

“**“I Can’t Believe It’s Not Custodial!”: Usable Trustless Decentralized Key Management**,” Tanusree Sharma, Vivek C. Nair, Henry Wang, Yang Wang, and Dawn Song in *ACM Computer-Human Interaction (CHI)*, 2024. [view] [pdf] [video] [code]

“**Inferring Private Personal Attributes of Virtual Reality Users**,” Vivek Nair, Christian Rack, Wenbo Guo, Rui Wang, Shuixian Li, Brandon Huang, Atticus Cull, James F. O'Brien, Marc Latoschik, and Louis Rosenberg in *IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*, 2024. [view] [code] [site]

“**Berkeley Open Extended Reality Recordings 2023 (BOXRR-23)**,” Vivek Nair, Wenbo Guo, Rui Wang, James F. O'Brien, Louis Rosenberg, and Dawn Song in *IEEE Transactions on Visualization and Computer Graphics*, 2024. [view] [code] [site]

“**Deep Motion Masking for Secure, Usable, and Scalable Real-Time Anonymization of Ecological Virtual Reality Motion Data**,” Vivek Nair, Wenbo Guo, James F. O'Brien, Louis Rosenberg, and Dawn Song in *IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*, 2024. [view] [code] [site]

“**Navigating the Kinematic Maze: Analyzing, Standardizing and Unifying XR Motion Datasets**,” Christian Rack, Vivek Nair, Lukas Schach, Felix Foschum, Marcel Roth, and Marc Erich Latoschik in *IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*, 2024. [view] [site]

Patents

Secure System and Method for Managing the Multi-Factor Authentication Data of a User

✓ Granted as *US11483307B2*, 2022. [view]

Secure System and Method for Preventing Cross-Site Credential Reuse

✓ Granted as *US12058121B2*, 2024. [view]

Secure System and Method for Detecting Credential Stuffing Attacks

● Published as *US20230195887A1*, 2023. [view]
○ Pending

Secure System and Method for Sharing Online Accounts

● Published as *US20230254288A1*, 2023. [view]
○ Pending

System and Method for Efficient Cryptographically-Assured Data Access Management for Advanced Data Access Policies

● Published as *US20240070309A1*, 2024. [view]
○ Pending

System and Method for Multi-Factor Key Derivation

● Utility Application *US18/152,660*, 2023.
○ Pending

System and Method for Determining Personal Information from Extended Reality Tracking Data

● Provisional Application *US63/366,499*, 2022.
→ Open-Sourced, 2023.

System and Method for Protecting Personal Information from Extended Reality Devices

● Provisional Application *US63/366,500*, 2022.
→ Open-Sourced, 2023.

Press

Washington Post: Apple's new Vision Pro is a privacy mess waiting to happen

"Apple has very little visibility into what is happening to it after it leaves the device," says one of the researchers, Vivek Nair.
https://www.washingtonpost.com/technology/2024/01/30/apple-vision-pro-privacy/

Forbes: Worried Your Phone Is Spying On You? Just Wait Until You're In The Metaverse

The study published last month by Garrido and Berkeley's Dawn Song and Vivek Nair proves just how easy it is to rapidly and surreptitiously collect dozens of data points from VR users.
https://www.forbes.com/sites/dylansloan/2022/08/09/worried-your-phone-is-spying-on-you-just-wait-until-youre-inside-it/

Bloomberg: VR Headsets Give Enough Data For AI To Accurately Guess Ethnicity, Income and More

"The easy ones for the model are age, gender, ethnicity, country," said lead researcher Vivek Nair at UC Berkeley.
https://www.bloomberg.com/news/articles/2023-08-10/meta-s-virtual-reality-headset-quest-2-has-privacy-concerns

Politico: DeFi vs. the regulators, by the numbers

That's the takeaway from a new pre-print written by a group of (mostly) UC Berkeley researchers that demonstrated, in their words, how "After training a classification model on 5 minutes of data per person, a user can be uniquely identified amongst the entire pool of 50,000+ with 94.33% accuracy from 100 seconds of motion, and with 73.20% accuracy from just 10 seconds of motion."
https://www.politico.com/newsletters/digital-future-daily/2023/02/23/defi-vs-the-regulators-by-the-numbers-00084240

VentureBeat: New research suggests that privacy in the metaverse might be impossible

Led by graduate researcher Vivek Nair, the recently released study was conducted at the Center for Responsible Decentralized Intelligence (RDI) and involved the largest dataset of user interactions in virtual reality (VR) that has ever been analyzed for privacy risks.
https://venturebeat.com/virtual/new-research-suggests-that-privacy-in-the-metaverse-might-be-impossible/

TechRadar: In the Metaverse, your identity can be revealed just by moving

Graduate researcher Vivek Nair led a team at the University of California, Berkley, in the largest VR study of it kind at the Center for Responsible Decentralized Intelligence (RDI), analyzing user interactions with VR to determine the levels of privacy.
https://www.techradar.com/news/in-the-metaverse-your-identity-can-be-revealed-just-by-moving

View all (35) →