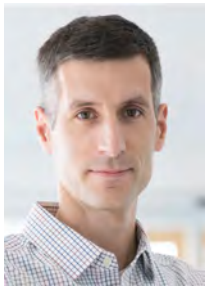
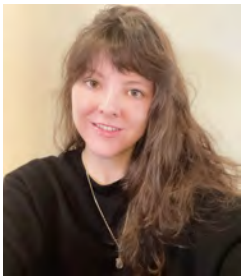
Carnegie Mellon University
Computer Science Department

COMPUTER SECURITY FACULTY

David Andersen



Lujo Bauer



Fraser Brown

Nicolas Christin

Lorrie Cranor

Karl Crary

Giulia Fanti

Aayush Jain

Matt Fredrikson

Vipul Goyal

Limin Jia

Ruben Martins

Roy Maxion

Bryan Parno

Frank Pfenning

Norman Sadeh

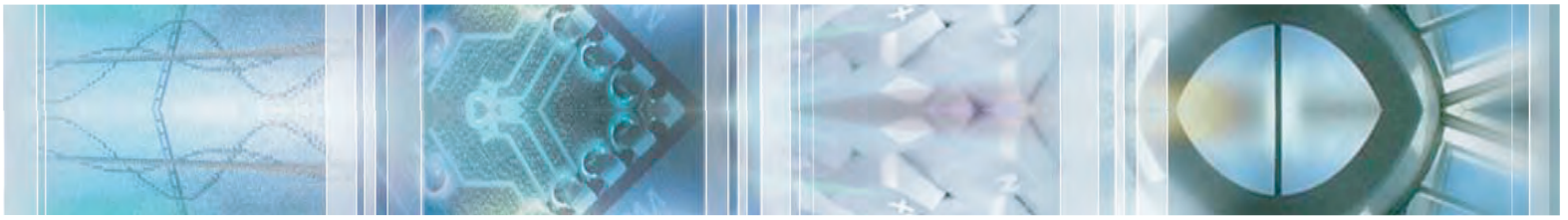
Vyas Sekar

Elaine Shi

Dimitrios Skarlatos

Riad Wahby

Wenting Zheng



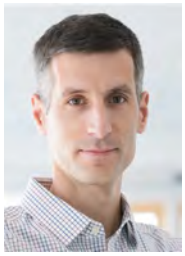
Carnegie Mellon University
Computer Science Department

COMPUTER SECURITY FACULTY

David Andersen, Professor (CS)
dga@cs.cmu.edu
http://www.cs.cmu.edu/~dga/
http://www.csd.cs.cmu.edu/people/faculty/david-andersen

Networks, distributed systems, overlay networks, peer-to-peer, availabilty, Internet measurement, wireless & ad-hoc networks.

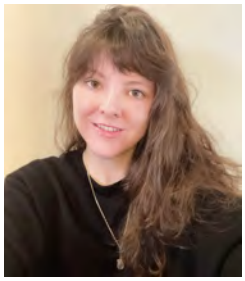
I study the "systems" side of networks: How to improve the availability, performance, and usability of Internet-based and wireless and mobile systems. My research emphasizes building real systems and conducting real-world measurements to provide a better understanding of these networks.



Lujo Bauer, Professor (ECE & ISR)
lbauer@cmu.edu
http://www.ece.cmu.edu/~lbauer/

Software and systems security, usable security and privacy, machine learning and security

My research interests span many areas of computer security and privacy. I like building systems that better protect users' security and privacy, particularly when we can empirically show that these systems actually help users and formally show that the protections are robust. My recent work focuses on understanding the risks of relying on machine learning algorithms, as well as on using machine learning to find software bugs and help users make better security decisions.



Fraser Brown Assistant Professor (ISR)
mlfbrown@stanford.edu

I'm interested in the spectrum of program correctness, from building exploits to finding bugs to verifying (parts of) real systems. Recent projects include compilation tools for cryptographic applications and verified passes in browser just-in-time compilers.

Carnegie Mellon University
Computer Science Department

COMPUTER SECURITY FACULTY

Nicolas Christin, Associate Professor (ISR & EPP)
nicolasc@andrew.cmu.edu
http://www.andrew.cmu.edu/user/nicolasc

Security measurements, human factors

My research interest is in computer and information systems security. Most of my work is at the boundary of systems, networking and policy research. While a good portion of my research activities could be qualified as applied research, I try as much as possible to rely on strong theoretical foundations in my work. In addition, Most of my recent work is informed by empirical data measurements (of users, networks, economic transactions...) so that the term “security analytics” is an appropriate short qualifier.

Lorrie Cranor, Professor (CS & EPP)
Director, CyLab Security and Privacy Institute
Co-director, MSIT-Privacy Engineering masters program
lorrie@cs.cmu.edu
http://lorrie.cranor.org/

Usable privacy and security, technology and public policy

My current projects involve privacy decision making, user-controllable security and privacy, usable cyber trust indicators, and usable and secure passwords.

Karl Crary, Associate Professor (CS)
crary@cs.cmu.edu
http://www.cs.cmu.edu/~crary/
http://www.csd.cs.cmu.edu/people/faculty/karl-crary

Programming languages and security

My research interests are in applying programming language technology to improve the development, maintenance, and performance of software systems. I am particularly interested in the application of type theory to systems programming, in mechanization of the metatheory of programming languages, in type-oriented compilation strategies, in type-based certification of machine code, and in the design of practical, high- or low-level programming languages.

Carnegie Mellon University
Computer Science Department

COMPUTER SECURITY FACULTY

Giulia Fanti, Assistant Professor (ECE & CSD)
gfanti@andrew.cmu.edu
https://www.andrew.cmu.edu/user/gfanti/
https://www.csd.cs.cmu.edu/people/faculty/giulia-fanti

Privacy, Cryptocurrencies, Machine Learning, Networks

I am broadly interested in networked, distributed systems. My research typically involves some combination of designing algorithms, proving theoretical properties about them, and/or testing them in real systems. Some of my recent projects have focused on improving the scalability and privacy of cryptocurrencies at the networking layer, increasing the diversity and robustness of generative adversarial networks, and designing countermeasures for cyberbullying in anonymous online forums.

Aayush Jain, Assistant Professor (CS)
aayushjain1728@gmail.com
https://sites.google.com/view/aayushjain/home

Cryptography and Theoretical Computer Science

I am interested in theoretical and applied cryptography, and its connections with related areas of theoretical computer science. These include (but are not limited to) sum-of-squares and learning algorithms, complexity theory, pseudorandomness and analysis of boolean functions.

Matt Fredrikson, Assistant Professor (CS & ISR)
mfredrik@cs.cmu.edu
http://www.cs.cmu.edu/~mfredrik/
http://www.csd.cs.cmu.edu/people/faculty/matthew-fredrikson

Security and privacy

My research focuses on security and privacy issues that lead to failures in real systems. Some of the key outstanding challenges in this area lie in figuring out why promising theoretical approaches oftentimes do not translate into effective defenses. Much of my work is concerned with developing formal analysis techniques that provide insight into the problems that might exist in a system, building countermeasures that give provable guarantees, and measuring the effectiveness of these solutions in real settings.

Carnegie Mellon University
Computer Science Department

COMPUTER SECURITY FACULTY

Vipul Goyal, Associate Professor (CS)
vipul@cmu.edu
http://www.cs.cmu.edu/~goyal/

Cryptography

I am interested in both theoretical and applied cryptography (and in theoretical computer science in general). I have worked on topics such as blockchains, crypto currencies, zero-knowledge proofs, and attribute-based encryption.

Limin Jia, Associate Research Professor (ECE)
liminjia@cmu.edu
http://www.andrew.cmu.edu/user/liminjia

Mobility, Privacy Protection, Trustworthy Computing Platforms and Devices

My research interests are in formal aspects of software security, in particular applying formal logic and language-based approaches to constructing software systems with known security guarantees.

Ruben Martins, Systems Scientist (CS)
rubenm@cs.cmu.edu
http://www.cs.cmu.edu/~rubenm
https://sat-group.github.io/ruben/

Constraint Programming, Boolean Satisfiability and Optimization, Software Verification, Program Synthesis

The goal of my research is to improve constraint solvers and broaden their applicability in program analysis, synthesis, and security. I have developed several award winning MaxSAT solvers that are widely used in software package upgradeability, computational biology, and course timetabling. My most recent work focuses on program synthesis for data-science-related tasks. Specifically, I am interested in automating a variety of cumbersome data preparation tasks and making the life of data scientists simpler.

Roy Maxion, Research Professor (CS)
maxion@cs.cmu.edu
http://www.cs.cmu.edu/~maxion/
http://www.csd.cs.cmu.edu/people/research-faculty/roy-maxion

Keystroke forensics

My research is on keystroke dynamics/forensics, fault/masquerader/insider/intrusion detection, attacker/defender testbed, measurement and experimental methodology, reliable software/user interfaces.

Carnegie Mellon University
Computer Science Department

COMPUTER SECURITY FACULTY

Bryan Parno, Associate Professor (CS & ECE)
parno@cmu.edu
http://www.andrew.cmu.edu/user/bparno
http://www.csd.cs.cmu.edu/people/faculty/bryan-parno

Security, Systems, Verification, Applied Cryptography

My research is primarily focused on investigating long-term, fundamental improvements in how to design and build secure systems. My work combines theory and practice to provide formal, rigorous security guarantees about concrete systems, with an emphasis on creating solid foundations for practical solutions. I have worked on topics such as network and system security, applied cryptography, usable security, and data privacy.

Frank Pfenning, Professor (CS)
fp@cs.cmu.edu
http://www.cs.cmu.edu/~fp/
http://www.csd.cs.cmu.edu/people/faculty/frank-pfenning

Programming languages, Logic & Type theory

At the heart of my research lies the desire to understand the principles of programming languages. Programming languages are the key to the programming process and therefore of fundamental importance to computer science. Well-designed programming languages allow fast program development, ease software maintenance, and increase confidence in the correctness of implementations.

Norman Sadeh, Professor (ISR, CS & HCII)
sadeh@cs.cmu.edu
www.normsadeh.org

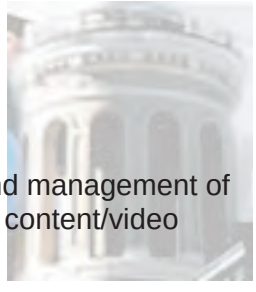
Usable Security and Privacy, Machine Learning, User Modeling, Natural Language Processing, Crowdsourcing, Intelligent Assistants

My research interests lie at the intersection of security, privacy, human computer interaction and artificial intelligence. I am currently leading two of the largest national research projects in privacy, namely "the Usable Privacy Policy Project" and the "Personalized Privacy Assistant Project". These projects focus on helping computers understand the text of privacy policies, discover available privacy settings and learn people's privacy preferences to help them configure available settings. In general, I am always looking for the next research problem to work on. I like problems that are both intellectually challenging and have a practical societal significance.

Vyas Sakar, Professor (ECE & CS)
vyass@cs.cmu.edu
http://www.cs.cmu.edu/~vyass/
http://www.csd.cs.cmu.edu/people/faculty/vyas-sekar

Networking & Security

My research spans networking, security, and systems. This includes work on: design and management of network appliances or "middleboxes", various aspects of network and systems security, content/video delivery systems, and network monitoring and measurement.



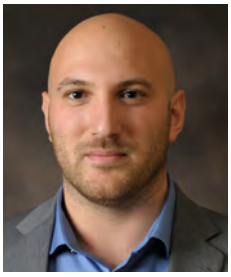
Carnegie Mellon University
Computer Science Department

COMPUTER SECURITY FACULTY

Elaine Shi Associate Professor (CS & ECE)
runting@cs.cmu.edu
elaineshi.com
http://www.csd.cs.cmu.edu/people/faculty/elaine-shi

Cryptography, algorithms, distributed systems

I am broadly interested in cryptography, algorithms, and distributed systems. I've also worked on creating a mathematical foundation for decentralized blockchains, and using programming language techniques to make it easier to program cryptographic systems.



Dimitrios Skarlatos, Professor (CS & ECE)
dskarlat@cs.cmu.edu
http://www.cs.cmu.edu/~dskarlat/

Computer Architecture, Operating Systems, Security

My research bridges computer architecture and operating systems focusing on performance and security. My work follows two central themes: (a) uncovering security vulnerabilities and building defenses at the boundary between hardware and OS, and (b) re-designing abstractions and interfaces between the two layers to improve performance and scalability.

Riad Wahby, Assistant Professor (ECE)
riad@cmu.edu
https://wahby.net

hardware and software security, systems, and applied cryptography

I am interested in building secure software and hardware systems, especially ones that require bridging the gap between theory and practice. Recently I've been thinking about probabilistic proofs, distributed systems, elliptic curves, compilers for cryptographic applications, and blockchain privacy.

Wenting Zheng, Assistant Professor (CS)
wenting@cmu.edu
wzheng.github.io

System Security and Applied Cryptography

I am broadly interested in system security and applied cryptography. I take inspiration from the privacy and security challenges that people face today, and I like to solve such problems by building practical and secure systems via a co-design of systems and cryptography. One of my recent interests is in building systems that enable "sharing without showing": multiple organizations can jointly compute on their collective sensitive data while only learning their own input and the final result. Overall, my goal is to democratize advanced cryptography so that its capabilities are made accessible to everyone.