

# Stanford Computer Security

John Mitchell  
Computer Science

---

Stanford

# Stanford Computer Security Laboratory



## Overview

The Security Lab is a part of the [Computer Science Department](#) at [Stanford University](#). Research projects in the group focus on various aspects of network and computer security.

## Courses

[CS55N](#): Freshman seminar: Great Ideas in Computer Security and Cryptography

[CS155](#): Computer and Network Security

[CS255](#): Introduction to Cryptography and Computer Security

[CS259](#): Security Analysis of Network Protocols

[CS355](#): Topics in Cryptography

[CS99J](#): Sophomore seminar: Computer Security and Privacy

[CS142](#): Web Programming and Security

## Seminars

The [Stanford Security Seminar](#) focuses on communication between Stanford and the outside world about computer security. The symposia are open to the public and are generally accessible and interesting to experts and laypeople alike.

[Security Lunch](#) focuses on communication with between students in the security lab and students in related research groups. Typically a student gives a technical presentation about his or her current research.

## Faculty

[Alex Aiken](#)

[Dan Boneh](#)

[David Dill](#)

[Dawson Engler](#)

[Hector Garcia-Molina](#)

[Monica Lam](#)

[Phil Levis](#)

[David Mazieres](#)

[Nick McKeown](#)

[John Mitchell](#)

[Mendel Rosenblum](#)

## Ph.D. Students

[Sergio Benitez](#)

[Henry Corrigan-Gibbs](#)

[Ben Fisch](#)

Sam Kim

[Amit Levy](#)

[Ali Jose Mashtizadeh](#)

[Yan Michalevsky](#)

[Valeria Nikolaenko](#)

[David Terei](#)

[David Wu](#)

[Edward Z Yang](#)

## Post-docs

[Joe Bonneau](#)

## Alumni



## About Us

TRUST is advancing *research* to improve the state-of-the-art in cyberest security; developing *education* programs to teach the next generation of researchers; creating *outreach* opportunities to broaden participation; and pursuing *knowledge transfer* to transition results to end users.

[Learn More >>](#)

1 2 3 4

## Publications & Reports

[More Publications & Reports](#)

## Our Mission

The Team for Research in Ubiquitous Secure Technology (TRUST) is focused on the development of cyber security science and technology that will radically transform the ability of organizations to design, build, and operate trustworthy information systems for the nation's critical infrastructure. Established as a *National Science Foundation* Science and Technology Center, TRUST is addressing technical, operational, legal, policy, and economic issues affecting security, privacy, and data protection as well as the challenges of developing, deploying, and using trustworthy systems.

# Core topics

## Stanford Lab

- Applied Cryptography
- Modeling and Analysis
- Experimental Systems

Computer science group  
partnering with law, others

## TRUST Center

- Financial Infrastructure
- Health Infrastructure
- Physical Infrastructure
- Science of Security

Computer science and legal  
policy expertise

## Research and Publications

[Map of Research Activity](#)[Introduction to the Concept of Cyber-Social Systems](#)[Funded Research](#)[Publications](#)

## Research

Our world has been transformed by a recent wave of technological and social change. The technological wave began with a succession of ever more powerful computers that ushered in the “information age.” It grew bigger with the introduction of the digital networks — notably the Internet and the World Wide Web — and associated browsers that permitted computer users to visit millions of websites around the world in a matter of seconds. Over the last several years, mobile and wearable devices, cloud storage and countless software applications have invited us to leverage the power of networked information and move a rapidly growing portion of our activities from the three-dimensional, physical world into cyberspace. Today one can, for example, advertise, sell, buy, bank, play, meet friends, share confidences, turn on appliances, argue, steal, and even engage in warfare in cyberspace, with the online activity experienced through the two-dimensional screen of one’s networked digital device.





Calendar



Calendar



Calendar Help



Annual Meeting



Career Fair



Workshops



Event Archives

[Join our Mailing List](#)

## Annual Meeting : 2016 Security Workshop

**April 11, 2016****Location: McCaw Hall, [Arrillaga Alumni Center](#)**

8:30am - 9:20am	<b>Check-in &amp; Breakfast</b>	
9:20am - 9:30am	Welcome, <a href="#">Dan Boneh</a> , Stanford	
9:30am - 10:00am	<a href="#">Would That It Were So Simple: Yet Another Privacy Theory</a> , <a href="#">John Mitchell</a> , Stanford	
10:00am - 10:30am	<a href="#">Recent Developments in Cryptography</a> , <a href="#">Dan Boneh</a> , Stanford	
10:30am - 10:50am	<b>Break</b>	
10:50am - 11:20am	<a href="#">Auditing IoT Communications with TLS-RaR</a> , <a href="#">Judson Andrew Wilson</a> , Stanford	
11:20am - 11:50am	<a href="#">Space-Hard Functions for Password Hashing</a> , <a href="#">Henry Corrigan-Gibbs</a> , Stanford	
11:50am - 12:20am	<a href="#">Privacy, Discovery, and Authentication for the Internet of Things</a> , <a href="#">David Wu</a> , Stanford	
12:20am - 1:45pm	<b>Lunch</b>	
1:45pm - 2:15pm	<a href="#">Solvency Proofs for Bitcoin Exchanges</a> , <a href="#">Joe Bonneau</a> , Stanford	
2:15pm - 2:45pm	<a href="#">Verifiable ASICs: Trustworthy Hardware with Untrusted Components</a> , <a href="#">Riad Wahby</a> , Stanford	
2:45pm - 3:15pm	<a href="#">CCFI: Cryptographically Enforced Control Flow Integrity</a> , <a href="#">Ali Mashtizadeh</a> , Stanford	
3:15pm - 3:40pm	<b>Break</b>	
3:40pm - 4:10pm	<a href="#">Building Least Privileged Web Applications with Node.js</a> , <a href="#">Deian Stefan</a> , UC San Diego	
4:10pm - 4:40pm	<a href="#">Stickler: Defending Against Malicious CDNs in an Unmodified Browser</a> , <a href="#">Amit Levy</a> , Stanford	