Center for Research and Education in Security and Privacy (CRESP) Overview

Trent Jaeger, UC Riverside

November 14, 2024

CRESP Industry Day 2024

Center for Research and Education in Security and Privacy

Vision

We seek to be a premier center for cybersecurity, designing novel approaches to building secure systems and enabling them to detect and tolerate attacks. We also seek to prepare talented engineers and researchers with the technical and problem solving skills in this area of national need.

Mission

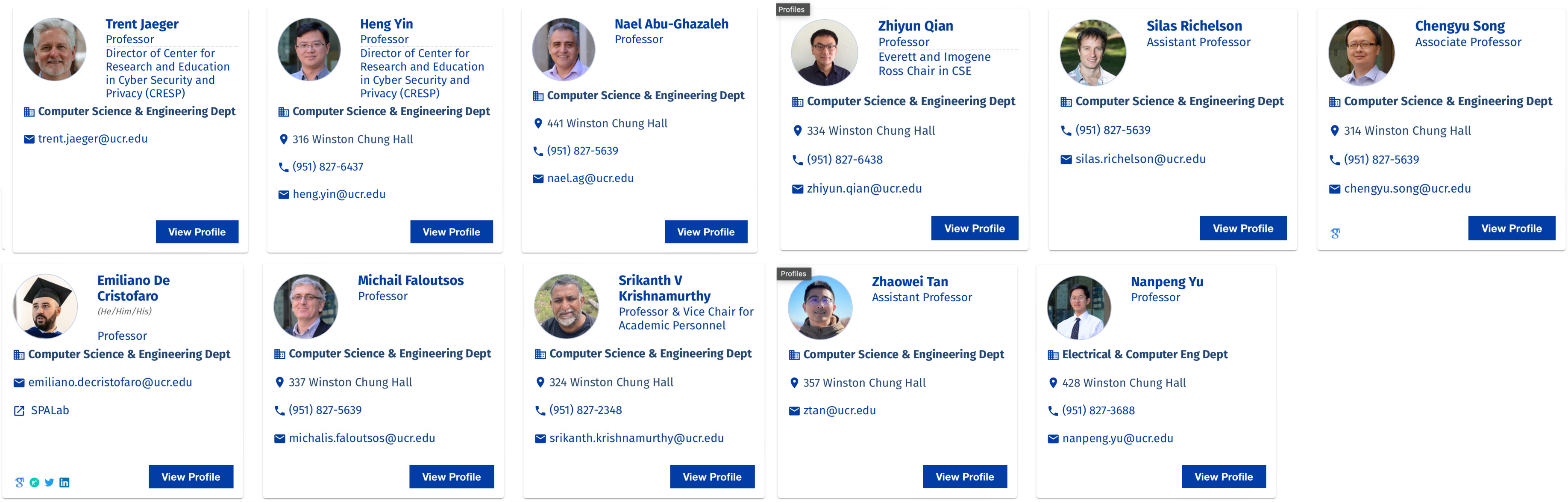
Our mission is to secure everything. We work on building systems that are secure by design, and that resist and tolerate attacks. As computing is becoming pervasive, its essential to build future devices with security and privacy as a first class design consideration.

Research Areas

Our research areas span the full range of computer security and privacy.

UC RIVERSIDE

CRESP Faculty



Trent Jaeger
Professor
Director of Center for Research and Education in Cyber Security and Privacy (CRESP)
Computer Science & Engineering Dept
trent.jaeger@ucr.edu
View Profile

Heng Yin
Professor
Director of Center for Research and Education in Cyber Security and Privacy (CRESP)
Computer Science & Engineering Dept
316 Winston Chung Hall
(951) 827-6437
heng.yin@ucr.edu
View Profile

Nael Abu-Ghazaleh
Professor
Computer Science & Engineering Dept
441 Winston Chung Hall
(951) 827-5639
nael.ag@ucr.edu
View Profile

Profiles
Zhiyun Qian
Professor
Everett and Imogene Ross Chair in CSE
Computer Science & Engineering Dept
334 Winston Chung Hall
(951) 827-6438
zhiyun.qian@ucr.edu
View Profile

Silas Richelson
Assistant Professor
Computer Science & Engineering Dept
(951) 827-5639
silas.richelson@ucr.edu
View Profile

Chengyu Song
Associate Professor
Computer Science & Engineering Dept
314 Winston Chung Hall
(951) 827-5639
chengyu.song@ucr.edu
View Profile

Emiliano De Cristofaro
(He/Him/His)
Professor
Computer Science & Engineering Dept
emiliano.decristofaro@ucr.edu
SPALab
View Profile

Michail Faloutsos
Professor
Computer Science & Engineering Dept
337 Winston Chung Hall
(951) 827-5639
michalis.faloutsos@ucr.edu
View Profile

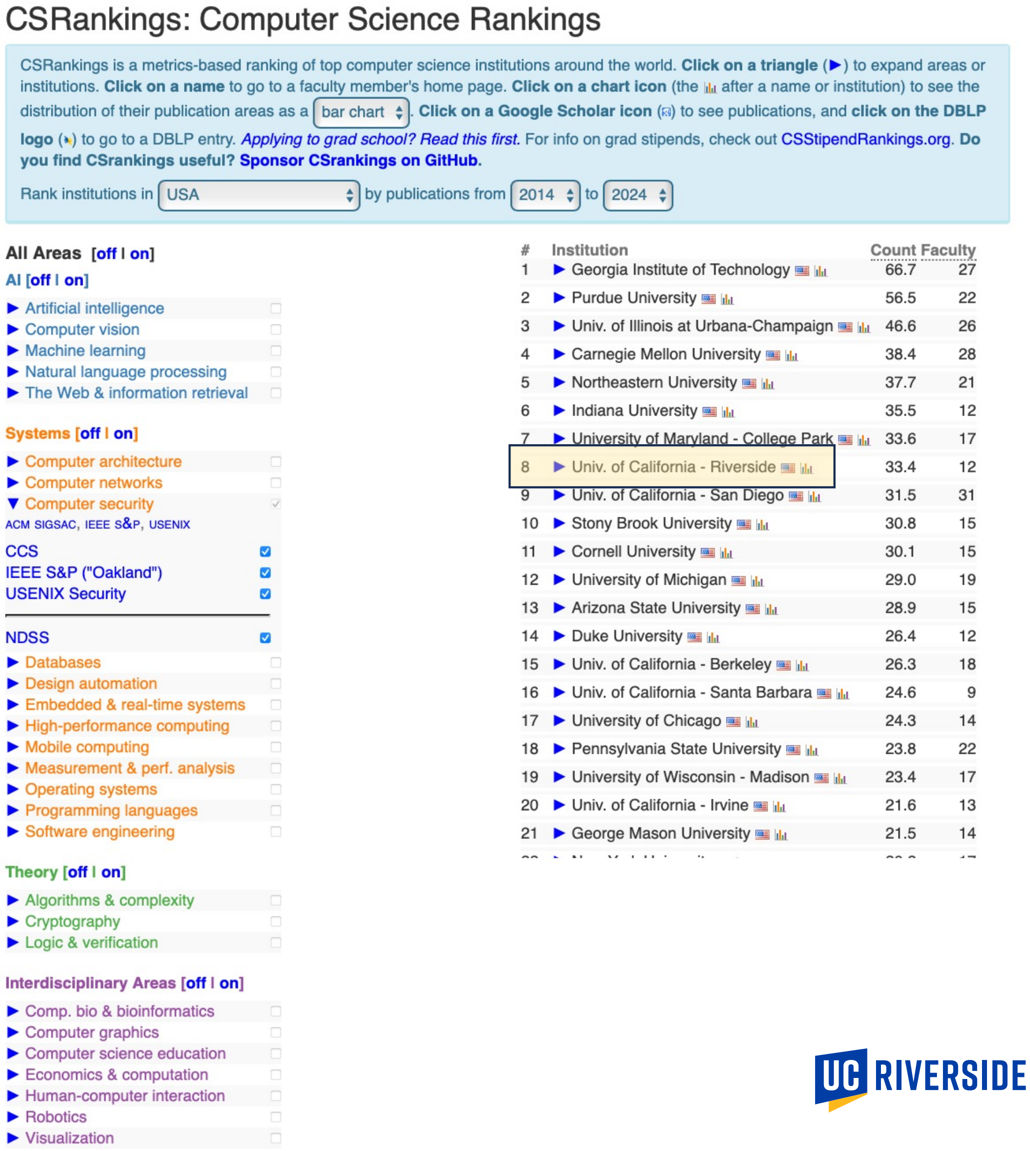
Srikanth V Krishnamurthy
Professor & Vice Chair for Academic Personnel
Computer Science & Engineering Dept
324 Winston Chung Hall
(951) 827-2348
srikanth.krishnamurthy@ucr.edu
View Profile

Profiles
Zhaowei Tan
Assistant Professor
Computer Science & Engineering Dept
357 Winston Chung Hall
ztan@ucr.edu
View Profile

Nanpeng Yu
Professor
Electrical & Computer Eng Dept
428 Winston Chung Hall
(951) 827-3688
nanpeng.yu@ucr.edu
View Profile

Research Quality

- According to the **csrankings.org**, UC Riverside has published the **8th most papers** of any US university in the top-four cybersecurity conferences since 2014
- Despite many other universities having many more faculty publishing in cybersecurity



CSRankings: Computer Science Rankings

CSRankings is a metrics-based ranking of top computer science institutions around the world. **Click on a triangle** (▶) to expand areas or institutions. **Click on a name** to go to a faculty member's home page. **Click on a chart icon** (the 📊 after a name or institution) to see the distribution of their publication areas as a bar chart. **Click on a Google Scholar icon** to see publications, and **click on the DBLP logo** to go to a DBLP entry. *Applying to grad school? Read this first.* For info on grad stipends, check out CSStipendRankings.org. **Do you find CSrankings useful? Sponsor CSrankings on GitHub.**

Rank institutions in USA by publications from 2014 to 2024

All Areas [off | on]

AI [off | on]

- ▶ Artificial intelligence □
- ▶ Computer vision □
- ▶ Machine learning □
- ▶ Natural language processing □
- ▶ The Web & information retrieval □

Systems [off | on]

- ▶ Computer architecture □
- ▶ Computer networks □
- ▼ Computer security ☑
  - ACM SIGSAC, IEEE S&P, USENIX
  - CCS ☑
  - IEEE S&P ("Oakland") ☑
  - USENIX Security ☑
  - NDSS ☑
- ▶ Databases □
- ▶ Design automation □
- ▶ Embedded & real-time systems □
- ▶ High-performance computing □
- ▶ Mobile computing □
- ▶ Measurement & perf. analysis □
- ▶ Operating systems □
- ▶ Programming languages □
- ▶ Software engineering □

Theory [off | on]

- ▶ Algorithms & complexity □
- ▶ Cryptography □
- ▶ Logic & verification □

Interdisciplinary Areas [off | on]

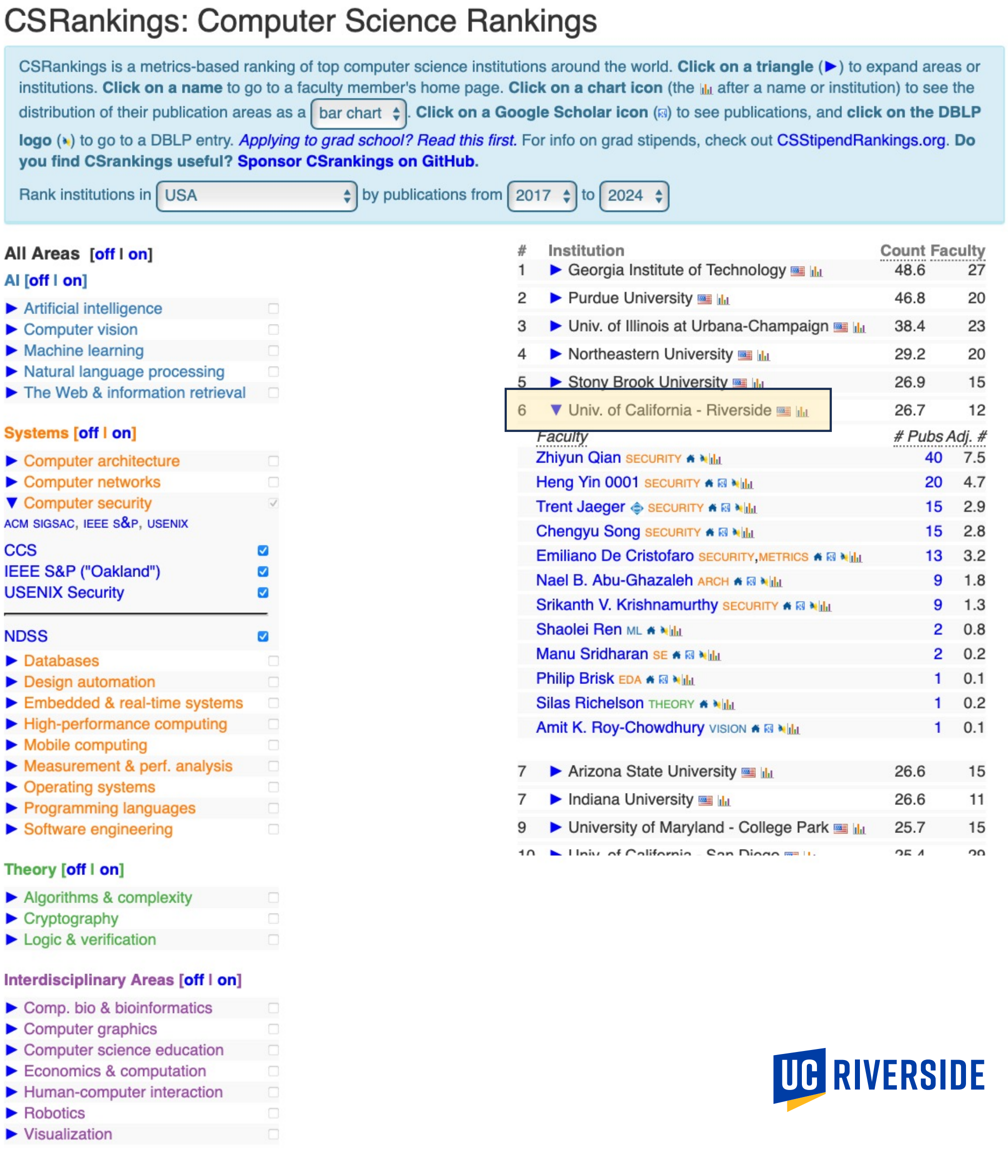
- ▶ Comp. bio & bioinformatics □
- ▶ Computer graphics □
- ▶ Computer science education □
- ▶ Economics & computation □
- ▶ Human-computer interaction □
- ▶ Robotics □
- ▶ Visualization □

#	Institution	Count	Faculty
1	▶ Georgia Institute of Technology	66.7	27
2	▶ Purdue University	56.5	22
3	▶ Univ. of Illinois at Urbana-Champaign	46.6	26
4	▶ Carnegie Mellon University	38.4	28
5	▶ Northeastern University	37.7	21
6	▶ Indiana University	35.5	12
7	▶ University of Maryland - College Park	33.6	17
8	▶ Univ. of California - Riverside	33.4	12
9	▶ Univ. of California - San Diego	31.5	31
10	▶ Stony Brook University	30.8	15
11	▶ Cornell University	30.1	15
12	▶ University of Michigan	29.0	19
13	▶ Arizona State University	28.9	15
14	▶ Duke University	26.4	12
15	▶ Univ. of California - Berkeley	26.3	18
16	▶ Univ. of California - Santa Barbara	24.6	9
17	▶ University of Chicago	24.3	14
18	▶ Pennsylvania State University	23.8	22
19	▶ University of Wisconsin - Madison	23.4	17
20	▶ Univ. of California - Irvine	21.6	13
21	▶ George Mason University	21.5	14

UC RIVERSIDE

Research Quality

- And an even higher productivity rate, if we consider publications from 2017
- **6th most papers** of any US university in the top-four cybersecurity conferences



CSRankings: Computer Science Rankings

CSRankings is a metrics-based ranking of top computer science institutions around the world. **Click on a triangle** (▶) to expand areas or institutions. **Click on a name** to go to a faculty member's home page. **Click on a chart icon** (the 📊 after a name or institution) to see the distribution of their publication areas as a bar chart. **Click on a Google Scholar icon** to see publications, and **click on the DBLP logo** to go to a DBLP entry. *Applying to grad school? Read this first.* For info on grad stipends, check out CSStipendRankings.org. **Do you find CSrankings useful? Sponsor CSrankings on GitHub.**

Rank institutions in USA by publications from 2017 to 2024

All Areas [off | on]

AI [off | on]

- ▶ Artificial intelligence □
- ▶ Computer vision □
- ▶ Machine learning □
- ▶ Natural language processing □
- ▶ The Web & information retrieval □

Systems [off | on]

- ▶ Computer architecture □
- ▶ Computer networks □
- ▼ Computer security ✓

ACM SIGSAC, IEEE S&P, USENIX

- CCS ☑
- IEEE S&P ("Oakland") ☑
- USENIX Security ☑
- NDSS ☑
- ▶ Databases □
- ▶ Design automation □
- ▶ Embedded & real-time systems □
- ▶ High-performance computing □
- ▶ Mobile computing □
- ▶ Measurement & perf. analysis □
- ▶ Operating systems □
- ▶ Programming languages □
- ▶ Software engineering □

Theory [off | on]

- ▶ Algorithms & complexity □
- ▶ Cryptography □
- ▶ Logic & verification □

Interdisciplinary Areas [off | on]

- ▶ Comp. bio & bioinformatics □
- ▶ Computer graphics □
- ▶ Computer science education □
- ▶ Economics & computation □
- ▶ Human-computer interaction □
- ▶ Robotics □
- ▶ Visualization □

#	Institution	Count	Faculty
1	▶ Georgia Institute of Technology	48.6	27
2	▶ Purdue University	46.8	20
3	▶ Univ. of Illinois at Urbana-Champaign	38.4	23
4	▶ Northeastern University	29.2	20
5	▶ Stony Brook University	26.9	15
6	▼ Univ. of California - Riverside	26.7	12

Faculty	*# Pubs*	*Adj. #*
Zhiyun Qian SECURITY	40	7.5
Heng Yin 0001 SECURITY	20	4.7
Trent Jaeger SECURITY	15	2.9
Chengyu Song SECURITY	15	2.8
Emiliano De Cristofaro SECURITY,METRICS	13	3.2
Nael B. Abu-Ghazaleh ARCH	9	1.8
Srikanth V. Krishnamurthy SECURITY	9	1.3
Shaolei Ren ML	2	0.8
Manu Sridharan SE	2	0.2
Philip Brisk EDA	1	0.1
Silas Richelson THEORY	1	0.2
Amit K. Roy-Chowdhury VISION	1	0.1

#	Institution	Count	Faculty
7	▶ Arizona State University	26.6	15
7	▶ Indiana University	26.6	11
9	▶ University of Maryland - College Park	25.7	15
10	▶ Univ. of California - San Diego	25.4	29

UC RIVERSIDE

Software Security Research

Wide ranging work in understanding attacks and developing defenses

- ❑ Automated vulnerability detection and prevention via **static analysis**
- ❑ Fast(est) **concolic execution engine** and use in vulnerability detection
- ❑ Wide variety of open-source research tools for **fuzz testing**
- ❑ Recent work exploring use of **machine learning/LLMs** for security tasks
- ❑ Vast experience in **binary analysis** **– recent Amazon award for AI-Powered Binary Diffing**
- ❑ Built on extensive practical experience in vulnerability discovery and exploitation leading to a variety of real-world impacts

Systems Security Research

Broad experience in the challenges of operating systems security

- ❑ Design and implementation of **security mechanisms** (e.g., access control)
- ❑ **Scalable analysis of operating systems code** to detect flaws, generate exploits, and automate retrofitting with security
- ❑ **Use of recent hardware features** to improve OS security
- ❑ Key research in **file system security,** motivating recent to Linux fixes
- ❑ Security research on **Cloud, AR/VR, autonomous vehicle, Android, CPS, IoT, and power systems**
- ❑ Collaborations with **Microsoft Research, Google,** and **IBM** and more

Hardware Security Research

Hardware security is a key emerging area of research

- ❑ Understanding **vulnerabilities exploiting hardware and architecture** (side channels; fault injection attacks; speculative execution attacks)
- ❑ Designing systems (architecture, software) immune to these attacks
- ❑ **Use and design of hardware features** to improve OS and software security
- ❑ Exploiting and protecting Memory and I/O, e.g., using CHERI, etc.
- ❑ Understanding **heterogeneous system** security
- ❑ Current or recent collaboration with **Intel**, **Nvidia**, and **Meta**

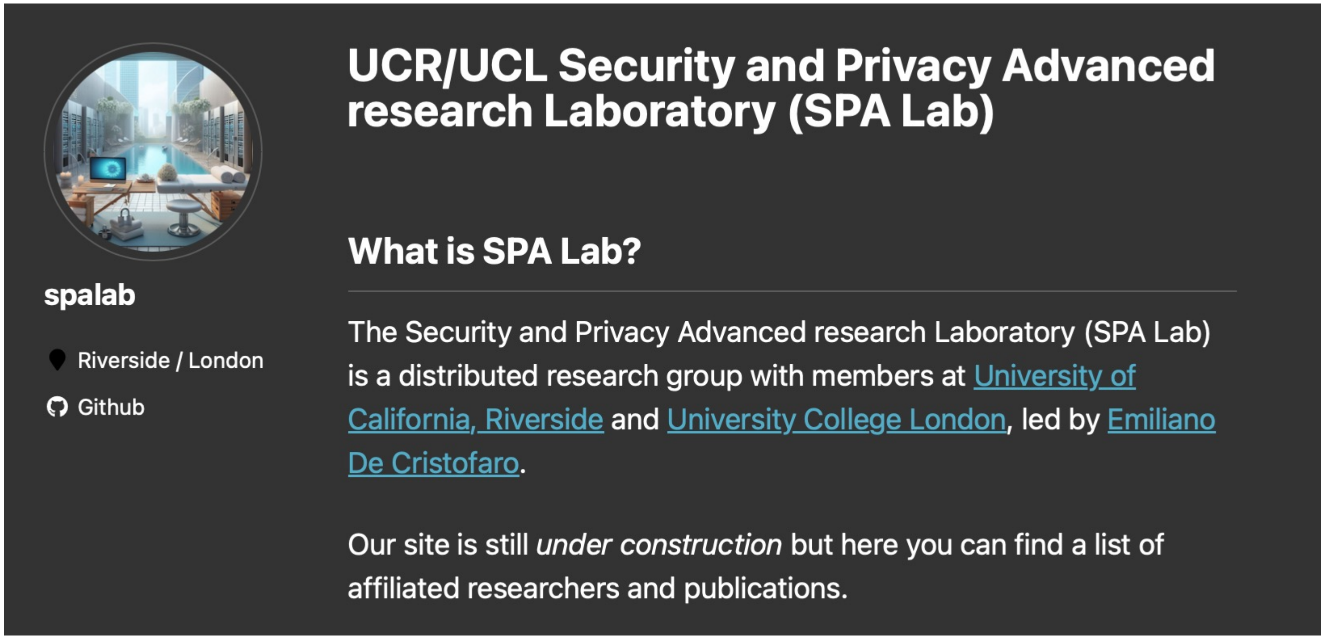
UC RIVERSIDE

Network Security Research

Building performant, intelligent, secure, and resilient networks

- ❑ Research in **wireless and cellular networking**, such as 5G
- ❑ Resurrected research in **network side channels**
- ❑ Vast research in cybersecurity of **web and social media**
- ❑ Variety of research in **ML for security** and **security for ML** in network domain
- ❑ Improve robustness of **firewall** and **SDN** security mechanisms
- ❑ Past experience with startups

Privacy Research



spalab

Riverside / London

Github

UCR/UCL Security and Privacy Advanced research Laboratory (SPA Lab)

What is SPA Lab?

The Security and Privacy Advanced research Laboratory (SPA Lab) is a distributed research group with members at University of California, Riverside and University College London, led by Emiliano De Cristofaro.

Our site is still *under construction* but here you can find a list of affiliated researchers and publications.

CRESP Education

Creating a pipeline of students in cybersecurity

- ❑ Introduce students to cybersecurity early in their undergraduate education
- ❑ Student recruitment from cybersecurity courses to extracurricular activities, including student hacking teams and research
- ❑ Developing collaborations with other universities and government agencies to broaden practical and research opportunities for undergraduates
- ❑ Expand on our already large group of graduate students in cybersecurity
- ❑ Nuture and develop collaborations with government and industry for research for graduate students

CRESP Students

Over 30 Ph.D. students researching cybersecurity

- ❑ Meet many of them at the poster sessions
- ❑ Responsible for the key research tasks
- ❑ Across a wide range of computing domains
- ❑ Placing in many of the top US research labs
- ❑ Scope of faculty to support a pipeline of cybersecurity students from undergrad to Ph.D.

Conclusions

CRESP Is Aiming High in Cybersecurity

- ❑ Among top US universities in cybersecurity research productivity
- ❑ Broad research portfolio covering software, systems, hardware, network, and privacy cybersecurity research areas
- ❑ Great group of research students and increasing undergrad involvement
- ❑ Look forward to research talks from faculty and the poster sessions to learn more!

Questions