

# UC Davis

## UC Davis Previously Published Works

### Title

Selected Papers from the 2017 IEEE Symposium on Security and Privacy

### Permalink

<https://escholarship.org/uc/item/00p380wh>

### Journal

IEEE Security & Privacy, 16(1)

### ISSN

1540-7993

### Authors

Benzel, Terry  
Peisert, Sean

### Publication Date

2018

### DOI

10.1109/msp.2018.1331038

Peer reviewed

## FPO

# Selected Papers from the 2017 IEEE Symposium on Security and Privacy

**Terry Benzel** | University of Southern California Information Sciences Institute  
**Sean Peisert** | Lawrence Berkeley National Laboratory, CENIC, and University of California, Davis

**F**or 38 years, the IEEE Symposium on Security and Privacy has been the premier forum for presenting computer security and electronic privacy developments and for bringing together leading researchers and practitioners. The topics covered at the symposium have varied over the years, but the work presented has always been considered some of the best, most timely research in the field.

In an effort to bring some of the symposium and the workshops to a wider audience, *IEEE Security & Privacy* magazine's editorial board devotes one special issue each year to highlight selected papers. This special issue is the fourth such instantiation.

### Selecting Papers

To put together this special issue, we surveyed the papers and, together with the program chairs of the 2017 IEEE Symposium on Security and Privacy, Úlfar Erlingsson and Bryan Parno, chose the papers we felt had the broadest potential interest and accessibility. Based on this, we invited authors to submit revised versions of their symposium papers, recast as articles suitable for publication in *IEEE Security & Privacy* magazine. Specifically, we asked the original authors to revise their papers to speak to the magazine's audience, which goes beyond the symposium's traditional academically focused audience to also include policymakers and practitioners.

### Articles in This Issue

We are pleased to publish this month's feature article, "Science of Security: Combining Theory and Measurement to Reflect the Observable," by Cormac Herley and Paul Van Oorschot. In their piece, Herley and Van Oorschot describe their views on what a "Science of Security" would

look like. In a highly entertaining romp through both the history of security research and the history of science, starting with the Greeks and Bacon, Newton, Kant, Feynman, and through to the recent JASON “Science of Security” report, the NSF/NSA/IARPA, LASER, and CSET workshops on cybersecurity experimentation, and more, Herley and Van Oorschot give a readable and compelling view about what has and has not worked in the history of cybersecurity—and why—and how we need to think about science and security in the future to make meaningful progress. This article is a must-read for any security researcher, practitioner, or policymaker.

In “Toward Continual Measurement of Global Network-Level Censorship,” Paul Pearce, Roya Ensafi, Frank Li, Nick Feamster, and Vern Paxson look at censorship on Internet via an intriguing and novel approach they call “Augur” that measures the reachability of websites from a variety of vantage points. This work not only demonstrates a valuable methodology but also, via a longitudinal study, describes a fascinating set of results about the prevalence and patterns of global Internet censorship, enlightening readers with valuable insight into what governments are actually doing to block access to online content for their citizens.

What’s better than data? More data, right? Data may be a “toxic asset,” according to Bruce Schneier, but even so, what has the alternative ever been, if accurate prediction is required? In “Enhancing Selectivity in Big Data,” Mathias Lecuyer, Riley Spahn, Roxana Geambasu, Tzu-Kuo Huang, and Siddhartha Sen challenge the notion that more data is always necessary to produce accurate results. Their work provides substantial evidence that could ultimately improve security and privacy around the world by showing data-collecting companies that not only is more not always better, but it’s not always even necessary, thereby justifying how companies can reduce their exposure to “toxic assets.”

Augmented reality (AR) has long been a vision of the future in *Star Trek*-style science fiction. However, AR is now becoming mainstream with head-mounted displays as well as displays in ordinary automobiles. With such new technologies, however, come new security perils. In “Arya: Operating System Support for Securely Augmenting Reality,” Kiron Lebeck, Kimberly Ruth, Tadayoshi Kohno, and Franziska Roesner examine the risks to AR outputs, such as ways in which AR users can be misled or distracted by output that has been manipulated to affect their perception, and, by extension, potentially even their safety. The authors provide key insight into problems with existing systems and provide numerous pieces of guidance for the design of future AR systems.

For most of the existence of computer systems, we have viewed the effects of cyberattacks as being

confined to computer systems. Vulnerabilities in networked industrial control systems, such as the uranium enrichment centrifuges attacked by Stuxnet, showed us that cyberattacks could have physical consequences as well. The Internet of Things—essentially a term that has come to refer to an explosion in mainstream adoption of networked sensors and actuators installed in everyday life—has brought new risk to societies relying on such technologies. In “IoT Goes Nuclear: Creating a Zigbee Chain Reaction,” Eyal Ronen, Colin O’Flynn, Adi Shamir, and Achi-Or Weingarten describe attacks and weaknesses in the popular Zigbee wireless protocol. Through their experimental results, they show that the vulnerability has the potential to infect in a large-scale installation of “smart” lighting leveraging the protocol.

This mobile app needs access to your camera. And your address book. And your calendar. And your email. But wait—what does the app really need that access for, and is that really okay? In “Dynamically Regulating Mobile Application Permissions,” by Primal Wijesekera, Arjun Baokar, Lynn Tsai, Joel Reardon, Serge Egelman, David Wagner, and Konstantin Beznosov describe a user study that bridges the gap between expectations between smartphone users and reality to help those users better make decisions about when access needs to be granted and when it does not, thereby helping users make decisions that mitigate loss of privacy to smartphone apps.

Every May, the IEEE Symposium on Security and Privacy remains a highlight for academic security researchers around the world. It is our hope that by bringing a selection of the symposium’s program to this magazine again this year, the symposium and some of the work presented there will reach an additional part of the community, who will enjoy and learn from that work. We look forward to seeing you at the symposium if you’re able to attend, and connecting with you through the pages of the magazine throughout the year. ■

---

**Terry Benzel** is the director of the Internet and Networked Systems Division at the University of Southern California Information Sciences Institute. Contact her at [tbenzel@isi.edu](mailto:tbenzel@isi.edu).

---

**Sean Peisert** is a staff scientist at Lawrence Berkeley National Laboratory, Chief Cybersecurity Strategist at CENIC, and is an adjunct associate professor at the University of California, Davis. Contact him at [speisert@lbl.gov](mailto:speisert@lbl.gov).

myCS

Read your subscriptions through  
the myCS publications portal at  
<http://mycs.computer.org>