

6th Annual Winners

Submitted by Heather Lucas on Fri, 12/14/2018 - 2:07am

6th Annual Best Scientific Cybersecurity Paper Competition

[Winning Paper](#) | [Award Ceremony](#) | [Review Team](#)

The sixth NSA Competition for Best Scientific Cybersecurity Paper recognizes the best scientific cybersecurity paper published in 2017. Papers were nominated between January 1, 2017 through December 31, 2017 and 28 nominations were received. Only one paper was selected for recognition.

Winning Paper

The winner of the 6th Annual Best Scientific Cybersecurity Paper Competition is [How Shall We Play a Game? A Game-theoretical Model for Cyber-warfare Games](#) by Tiffany Bao, Yan Shoshitaishvili, Ruoyu Wang, Christopher Kruegel, Giovanni Vigna, and David Brumley. These researchers are from Carnegie Mellon University and University of California, Santa Barbara. This paper was originally accepted at 30th IEEE Computer Security Foundations Symposium (CSF '17).

The researchers endeavor to "identify the best strategy for the use of an identified zero-day vulnerability in a 'cyber-warfare' scenario where any action may reveal information to adversaries." They develop a game-theoretic model and the ability to quickly find optimal solutions to it. These strategies aid humans and computers in making decisions when dealing with previously unknown vulnerabilities in computer systems. This model accounts for both attack and defensive actions and imperfect information about the current status. Actions that can be taken include attacking by using this vulnerability, patching one's own systems, stockpiling for later, or taking no action. The model also develops steps for one to follow over time, such as patching one's own computers for a period and then later attacking.

The paper was selected because it exemplifies outstanding scientific research, is technically sound, and is well written. The authors develop a cyber-warfare strategy based on strong scientific methods and this new approach performs better than what was previously known. The reviewers particularly liked that the game theoretic model was reflective of the physical world with a realistic set of assumption and attributes, which is refreshing to see in game theory papers. The paper is noteworthy in the validation effort to test the effectiveness of the game theory strategy. They applied their game theory strategy to the to the 3rd place team at the [DARPA Cyber Grand Challenge](#). Validation of research with real world situations is important in science and helps build confidence in that results

apply to real-life situations. The attributes of this paper make it well deserving of winning the 6th Annual Best Scientific Cybersecurity Paper Competition.

The winning authors attended a special recognition ceremony at NSA in November.

The winning paper was selected from 28 nominations for papers published in 2017. The competition included two papers that addressed the philosophical question of 'what is a science of security?' The reviewers in the competition appreciate their work in helping to shape and mature the security discipline. As such, the authors are invited to further discuss their perspectives at the [Hot Topics in Science of Security \(HoTSoS\)](#) meeting in April 2019.

The first paper, [SoK: Science, Security and the Elusive Goal of Security as a Scientific Pursuit](#) by Cormac Herley and Paul van Oorschot, examines what has been done in Science of Security and puts it in context with historical science to offer observations and insights. They propose 11 constructive suggestions on how the discipline can improve and learn from the development of other disciplines. This paper was originally published in 2017 IEEE Symposium on Security and Privacy.

The second paper is [Practicing a Science of Security: A Philosophy of Science Perspective](#) by Jonathan Spring, Tyler Moore and David Pym; published at the 2017 New Security Paradigms Workshop. They examined purported serious obstacles to the practice of a science of security and found that they are either misguided or can be overcome.

Award Ceremony

On November 30, 2018, the Research Directorate at NSA hosted the 6th Annual Best Scientific Cybersecurity Paper Competition awards ceremony.

Review Team

NSA Competition Leads

- **Dr. Deborah Frincke** - Director of Research, NSA
- **Dr. Adam Tagert** - Science of Security, NSA Trusted Systems Research Group

Distinguished Expert Reviewers

- [Prof. L. Jean Camp](#) - Professor of Informatics at Indiana University
- [Dr. Robert Cunningham](#) - Secure Resilient Systems and Technology Group, Lincoln Laboratory
- [Dr. Whitfield Diffie](#) - Cybersecurity Advisor
- [Dr. Daniel Earl Greer Jr., Sc.D.](#) - Chief Information Security Officer at In-Q-Tel

- [John D. McLean](#) - Superintendent of the Naval Research Laboratory's Information Technology Division (ITD)
 - [Prof. Stefan Savage](#) - Department of Computer Science & Engineering at University of California San Diego
 - [Phil Venables](#) - Chief Information Risk Officer at Goldman Sachs
 - [David A. Wagner](#) - Assistant Professor in the Computer Science Division at the University of California, Berkeley
 - [Jeannette Wing](#) - Vice President, head of Microsoft Research International
-

About the Annual Paper Competition

The Best Scientific Cybersecurity Paper Competition is sponsored yearly by NSA's Research Directorate and reflects the Agency's desire to increase scientific rigor in the cybersecurity field. This competition was established to recognize current research that exemplifies the development of scientific rigor in cybersecurity research. SoS is a broad enterprise, involving both theoretical and empirical work across a diverse set of topics. While there can only be one best paper, no single paper can span the full breadth of SoS topics. Nevertheless, work in all facets of security science is both needed and encouraged.

Links
