SOS HARD PROBLEMS

The five Hard Problems are the broad research focus areas of SoS. These five were selected for their level of technical challenge, their potential operational significance, and potential benefit to research through the emphasis of scientific research methods. The five are not intended to be all inclusive of everything that needs to be done in cybersecurity but rather five specific areas that need scientific progress.



SCALABILITY AND COMPOSABILITY:

Develop methods to enable the construction of secure systems with known security properties from components with known security properties, without a requirement to fully re-analyze the constituent components.



POLICY-GOVERNED SECURE COLLABORATION:

Develop methods to express and enforce normative requirements and policies for handling data with differing usage or privacy needs among users in different authority domains.



SECURITY METRICS DRIVEN EVALUATION, DESIGN, DEVELOPMENT, AND DEPLOYMENT:

Develop security metrics and models capable of predicting whether or confirming that a given cyber system preserves a given set of security properties (deterministically or probabilistically) in a given context.



RESILIENT ARCHITECTURES:

Develop means to design and analyze system architectures that deliver required services in the face of compromised components.



UNDERSTANDING AND ACCOUNTING FOR HUMAN BEHAVIOR:

Develop models of human behavior (of both users and adversaries) that enable the design, modeling, and analysis of systems with specified security properties.

APPLYING THE SOS HARD PROBLEMS

Within SoS, Privacy Foundations and Cyber-Physical Systems (CPS) have growing cyber impact, and are unique in application. SoS's CPS research examines the Five Hard Problems in the context of CPS where the boundary between the cyber-domain and the physical world meet. SoS's Privacy research studies foundational privacy research challenges. Goals include a principled and methodological approach to evaluating privacy risk, and improving transparency.

SCIENCE OF SECURITY AND PRIVACY

SCIENCE OF SECURITY AND PRIVACY

SOS-VO.ORG

The **Science of Security & Privacy (SoS)** Initiative, sponsored by the **National Security Agency** Research Directorate , fosters a self-sustaining, open, and public security science research community to discover key cyber principles necessary to support improved security and privacy. This community is developing a body of scientific laws, testable explanations, predictions and confirmation or validation of predicted outcomes. The discipline of Science of Security and Privacy draws on bases from multiple disciplines including Computer Science, Engineering, Mathematics and Psychology. SoS is advancing the technical aspects of security along with an understanding the human elements involved.

Beginning in 2012, SoS has funded **Lablets** at leading universities. **Lablets** are multidisciplinary labs that are doing basic cybersecurity research and advancing the discipline of SoS. The initiative encourages the application of rigorous research methods through its **Annual Best Scientific Cybersecurity Paper Competition.** The competition awards the paper with the best scientific cybersecurity research contribution. To also promote rigorous research at the high school level, SoS started recognizing outstanding achievement in security science with a cash award at the **Intel International Science and Engineering Fair (ISEF)**. Research from the growing community is showcased annually at the **Hot Topics in the Science of Security (HotSoS) Symposium.** The **Science of Security Virtual Organization** was established to provide a focal point for security science related work, and a collaborative environment the community can use to further advance cybersecurity science. Since 2012, the community has had participation from more than 700 authors, in 27 countries, across 5 continents.

- Abu Dhabi
- Australia
- Belgium
- Brazil
- Canada
- China
- England
- France
- Germany
- Greece
- Iran
- Israel
- Italy
- Japan
- Netherlands
- New Zealand
- Norway
- Pakistan
- Poland
- Portugal
- Romania
- Singapore
- Spain
- Sweden
- Switzerland
- United States
- Wales

Science of Security

LABLETS

The SoS Initiative has funded foundational multidisciplinary research at leading universities, promoted the growth of the community doing relevant research, and supported the adoption of scientific research methods. They stimulate basic research, create scientific underpinnings for security, advocate for scientific rigor in security research, and create and broaden a Science of Security community and culture. With an emphasis on building a community, each Lablet create partnerships with other universities called Sub-Lablets. Science of Security researchers freely collaborate with researchers in other institutions worldwide.

The Lablets work on making scientific advances in the 5 Hard Problems including Privacy, and Cyber-Physical Systems (CPS).

A major goal of all the Lablets is the creation of a unified body of knowledge that can serve as the basis of a cybersecurity discipline, curriculum, and rigorous design methodologies. The results of the SoS Lablet research are extensively documented and widely distributed through the SoS Virtual Organization.

CURRENTLY FUNDED RESEARCH LABLETS

- Carnegie Mellon University (CMU)
- International Computer Science Institute (ICSI)
- North Carolina State University (NCSU)
- University of Illinois (UIUC)
- University of Kansas (KU)
- Vanderbilt University (VU)

QUARTERLY MEETINGS

Science of Security Lablet meetings are held in fall, winter, and summer. The initiative's annual conference HotSoS serves as the program's spring meeting. The location of the quarterly meetings rotates among the Lablet universities and NSA. The meetings are a mix of invited government and industry speakers, paper presentations, workshops, panel discussions, and Lablet research summaries. The quarterly meetings highlight advances in Lablet research; allows for collaboration among researchers from different Lablets and among government researchers and sponsors. Government and Industry participation are welcomed to provide perspective enhancing research focus, and increasing the community of interest.

HOTSOS

HOT TOPICS *in the* SCIENCE OF SECURITY *Symposium and Bootcamp (HotSoS)*

The Hot Topics in the Science of Security Symposium and Bootcamp (HotSoS) is the premier annual event of the Science of Security program. The goal of HotSoS is to bring together researchers, practitioners, and thought leaders from government, industry, and academia, and to provide a forum for dialogue centered upon the development and advancement of scientific foundations in cybersecurity. The technical emphasis of HotSoS is on scientific methods, data gathering and analysis, experimental approaches, mathematical models, and the interactions among those approaches to build a foundational science of security. The HotSoS vision is one of engaging and growing a community – including researchers and skilled practitioners from diverse disciplines – that is focused around the advancement of scientific methods as applied to cybersecurity.

http://hot-sos.com



BEST SCIENTIFIC CYBER-SECURITY PAPER COMPETITION

The Best Scientific Cybersecurity Paper Competition is sponsored by the NSA RD to promote rigorous research methods by identifying and highlighting excellence in science of security and privacy research. The competition accepts nominations from the public for refereed papers published in the previous year without geographic limitations. Nominated papers are evaluated by a panel of distinguished experts in cybersecurity. Winners are invited to NSA for recognition and to present their research.

http://sos-vo.org/papercompetition



HOTSOS BEST PAPER & POSTER AWARDS

The Best Paper and Poster Awards at HotSoS recognize cybersecurity research with scientific rigor, clarity of presentation, and global impact. These awards encourage scientists across multiple disciplines to address the fundamental problems of security in a principled manner.

intel ISEF

NSA RESEARCH DIRECTORATE AWARD AT ISEF

The Annual Intel International Science and Engineering Fair (ISEF) is the world's largest international pre-college science competition with approximately 1,800 high school students from more than 75 countries, regions, and territories. To qualify, students must first win coveted spots from regions or countries. The Science of Security and Privacy Initiative has sponsored a special Science of Security award at the ISEF to recognize outstanding scientific accomplishment in cybersecurity and to encourage future generations of students to pursue cybersecurity education, research and careers.



ISEF 2017 winners

SOS-VO.ORG

The Science of Security Virtual Organization (SoS-VO) was established to provide a focal point for information about ongoing activities related to cybersecurity science and as a repository for significant research results. It emphasizes community development, information sharing, and interaction among researchers in the field. The goal of the SoS-VO is to help establish and support true collaboration in advancing cybersecurity science. Now with over a thousand members, the SoS-VO enables those interested in cybersecurity science to survey current research, stay current on news in the field, find out about events related to cybersecurity, collaborate and share work, and access educational resources contributed by members. New members are encouraged and can join by signing up via the SoS-VO website at **http://sos-vo.org**





ANNUAL REPORT

The Science of Security and Privacy Annual Report details the progress of the activities in the Science of Security and Privacy research initiative. For more information about the activities associated with the SoS initiative, browse through the SoS Annual Report at **http://sos-vo.org/annualreport**