Advancing the science of cybersecurity with a virtual organization

Frankie King, Heather Lucas, and Robert Meushaw

Origins

The National Science Foundation (NSF)’s Cyber-Physical Systems (CPS) program is a research initiative to support the development of systems that combine physical, computing, and communications components at very large scale and high complexity. Cyber-physical systems are not the traditional desktop computers, embedded/real-time systems, and sensor nets with which we are familiar today. They are characterized by cyber capabilities in all physical components, networking at multiple and extreme scales, high degrees of automation, dynamic reconfiguration and reorganization, and extreme requirements for dependability and reliability. Although cyber-physical systems are currently being planned and developed to support applications in numerous areas (e.g., the smart power grid, smart healthcare, and smart transportation), the scientific understanding and engineering tools needed to realize such systems with high-confidence reliability and dependability are lacking.

The CPS Virtual Organization (CPS VO), an offshoot of the CPS program, was envisioned as a tool to promote and support a broad spectrum of collaborative interactions among researchers to assist in solving complex, crosscutting problems requiring expertise from multiple domains. The CPS VO provides a web-based gathering place and clearinghouse for knowledge relevant to cyber-physical systems and to advance the theory, engineering, and operation of cyber-physical systems. A primary objective of the CPS VO is to overcome some of the major impediments to progress in complex systems science, such as the lack of integration and cross-fertilization of numerous traditionally isolated disciplines. The NSF intended the CPS VO to enable electronic community building and to provide a vehicle for sharing information among otherwise disparate researchers, students, educators, and industry practitioners within the growing cross-disciplinary field of cyber-physical systems.

Vanderbilt University was selected by NSF to develop and manage the CPS VO. It was built using DRUPAL, a widely used, free, and open-source content management system that provides the back end for at least two percent of all websites worldwide, including whitehouse.gov. The system is flexible and highly customizable, providing a rich set of capabilities for the CPS VO user community. The CPS VO was initially used to advertise the activities of the CPS program and to establish electronic forums for many of the common interest groups (e.g., medical, automotive, aviation, education, and architectures) within the national High Confidence Software and Systems Coordinating Group. The High Confidence Software and Systems Coordinating Group (HCSS CG) is part of the national Networking and Information Technology Research and Development (NITRD) Program. (For more information on NITRD, see www.nitrd.gov.)
Establishing a virtual organization for cybersecurity science

At a high level, NSF’s CPS program and the federal cyber-physical systems research portfolio can be seen as a broad research initiative intended to develop the scientific foundations for designing complex systems. Many of the activities associated with cyber-physical systems have focused on identifying the technical challenges associated with various types of complex systems. In late 2010, NITRD agencies, led by NSA and NSF, launched one such activity related to the science of dependable and secure cyber-physical systems. This effort culminated in the Workshop on Foundations of Dependable and Secure Cyber-Physical Systems, held as part of CPS Week 2011 in Chicago, Illinois. (For more information, see https://www.truststc.org/conferences/11/CPSWeek/program.htm).

The workshop focused on topics that addressed fundamental challenges of making cyber-physical systems secure, dependable, and trustworthy. Particular emphasis was placed on the control and verification challenges arising from the complex interdependencies among networked systems. Such systems are in widespread use today, controlling the operation of critical infrastructures such as power transmission, water distribution, transportation, healthcare, building automation, and process control. The combination of various factors—including the widespread use of commodity components, Internet connectivity, and the malicious intents of hackers and cybercriminals—have made these types of systems extremely vulnerable. Despite attempts to apply security-oriented design guidelines and policies, much remains to be done to achieve a scientifically grounded and principled design approach to security, trustworthiness, and dependability in these systems.

The 2011 workshop was a first formal attempt to foster collaboration among researchers from a variety of fields including control and systems theory, embedded systems, game theory, software verification and formal methods, and computer security. One important outcome of the workshop was the recognition that the science of cybersecurity was critical to the overall success of the CPS program and of the cyber-physical systems field. This recognition aligned with the vision that had been previously put forward by the NITRD HCSS CG co-chairs in a white paper to the Office of Science and Technology Policy (OSTP) titled “Winning the future with science and technology for 21st century smart systems.” Workshop recommendations went even further, recommending that a virtual organization dedicated to cybersecurity science be established within the CPS VO—the Science of Security Virtual Organization (SoS VO).

Growing interest in cybersecurity science

At the same time as the CPS program moved toward creating a distinct cybersecurity science group, a number of governmental initiatives in cybersecurity science began appearing from organizations across the broader cybersecurity community, including several outside of the US. Unfortunately, without the benefit of any centralized resource to help coordinate
their efforts, these activities developed in isolation. As information about these efforts became more widely available, it became clear that the SoS VO could serve an even more valuable role if it provided a focal point for all things cybersecurity science related. Together, through NSA leadership and sponsorship, Vanderbilt’s design goal for the CPS VO was augmented to provide a portal with a rich set of collaboration and sharing capabilities, leveraging and extending NSF’s investment to support an enhanced data repository and content management system. This coordinated effort served well the interest of both the CPS VO and SoS VO communities. While this approach was significantly more ambitious, it offered better opportunities for advancing work in both cyber-physical systems and cybersecurity science much more quickly and efficiently. The integrated approach and the resulting extended capabilities will benefit other cyber-physical systems special interest groups as they begin building their online communities.

Content is king, search is queen

From its inception, the CPS VO was intended to grow into an established research resource by offering a storehouse of information with a robust search capability to mine it efficiently. Achieving this goal meant that the virtual organization needed to attract a large user population and provide services that were valuable, engaging, and easy to use. These objectives were adopted as the guiding principles for all decisions made in augmenting support for the SoS VO. The target audience was expanded to include researchers, program managers, educators, funding agents, system designers, and students—almost anyone having an interest in cybersecurity science. Attracting such a broad group meant the SoS VO had to provide an extensive and useful assortment of information, accessible intuitively and efficiently—a very tall order. If the SoS VO is able to create an enduring engagement center for cybersecurity science, user-contributed content should generate value and further help to build a cybersecurity science community.

Evolving an SoS VO capability

After a careful assessment of the needs identified for the SoS VO, a plan was developed to roll out new capabilities in three basic areas. The first set of capabilities was geared toward establishing the SoS VO as a focal point for information about ongoing activities related to cybersecurity science and as a repository for significant research results. The second phase of development would place emphasis on community development, information sharing, and interaction among researchers in the field. The last, and most ambitious, set of capabilities envisioned for the SoS VO would help to establish and support true collaboration in advancing cybersecurity science. (See figure 1 for a screenshot of the SoS VO home page.)

SoS VO capability phases

- **Phase 1. Build a resource center.**
  Creating a centralized information resource on cybersecurity science activity is the first step planned for the SoS VO and is key to helping establish a community. An important goal of this phase involves identifying and collecting information about the disparate cybersecurity science work currently being performed. Providing descriptions and contact information for the organizations conducting and supporting cybersecurity science work is a priority, as well as advertising new program funding opportunities. For organizations currently producing reports related to cybersecurity science, the SoS VO intends to provide a centralized library for cataloging, analyzing, searching, and distributing information. A calendar of events related to cybersecurity science is a core capability of the SoS VO and will appear early with the ability to sync to users’ individual calendars.

- **Phase 2. Cultivate collaboration with virtual tools.**
  The second phase of planned SoS VO capabilities is intended to expand the reach of cybersecurity science information to a much broader community of users. One of the exciting features being developed will allow videos of research reviews to be viewed online in both real-time streaming and archived formats. This capability should permit users to become involved much more easily in reviews without the time and budget constraints of long distance travel. Discussion forums, blogs, content subscriptions, chat, wikis, and user profiles are being created to permit increased interaction among users and to promote simple forms of collaboration.
FIGURE 1. The Science of Security Virtual Organization (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 science; collaborate with others using chat, video conferencing, and forums; share work by uploading documents and creating wikis; and access educational resources contributed by members. Visit cps-vo.org/group/SoS to learn more.
Phase 3. Strengthen collaboration with social networking.

Ultimately, the capabilities delivered by the SoS VO, as well as the CPS VO, were conceived to promote community collaboration in order to advance science. The features deployed in the first phases of the SoS VO should help to create a broad community of users and establish a focal point for their interactions. But it is the last group of capabilities offered by the SoS VO that should enable the type of robust collaboration desired by blending elements of social networking with a rich set of communication and research tools. Some of the features currently being planned in this phase include:

» Research toolsets and datasets;
» On-demand video conferencing;
» Desktop sharing;
» Individual user space, dashboard, etc.;
» Interface personalization;
» Subscription services;
» Cybersecurity science-related newsfeeds;
» A multimedia library; and
» Open research support.

SoS VO rollout

The establishment of the SoS VO is founded on the beliefs that open collaboration can play a key role in advancing cybersecurity science and that the availability of a platform where researchers can share, collaborate, and learn is vital to building community. The structure and features of the SoS VO attempt to leverage popular features provided by social networking technology with rich domain-specific content to create a focal point for cybersecurity science research. The pilot version of the SoS VO has evolved dramatically in form and content since its inception in 2011, and it will continue to evolve as user feedback is received when it becomes operational and as the cybersecurity science community matures.

About the authors

Frankie D. King is the assistant director of the Annapolis Technical Coordination Project Office at Vanderbilt University’s Institute for Software Integrated Systems (VU-ISIS), where she is responsible for managing the coordination of collaborative research and development activities on the Cyber-Physical Systems Virtual Organization that are sponsored by federal agencies belonging to the Networking and Information Technology Research and Development (NITRD) Program. Before joining VU-ISIS, King served as the technical coordinator for the High Confidence Software and Systems Program Component Area at the National Coordination Office for the NITRD Program for nearly seven years. King has over 28 years of program development and management experience in domestic and international policy affairs where she has served in high-level capacities in the executive and legislative branches of the US government and the private sector. King received an MA from the University of Notre Dame and a BA from Fisk University, where she graduated summa cum laude.

Heather Lucas is a program director within the Trusted Systems Research Group at NSA and is the current program lead for NSA’s Science of Security Virtual Organization effort.

Robert Meushaw is the former technical director of NSA’s Information Assurance (IA) Research Laboratory. His current work focuses on developing new strategies and programs for the advancement of a science of cybersecurity. He retired from NSA in 2005 after 33 years of service, including over a decade of work in IA research. Meushaw’s career at NSA also included significant stints in both the Product Development Group and the Security Evaluation Group of the IA Directorate. In addition to his technical responsibilities, he served for six years as technical editor of NSA’s Tech Trend Notes and The Next Wave publications. Meushaw holds degrees in electrical engineering from Princeton University and the Johns Hopkins University.