Call for Papers: Workshop on Cybersecurity State Awareness for Internet of Things (IoT)

The Federal Communications Commission in the United States is moving forward with a cybersecurity labeling program for consumer Internet of Things (IoT) products with similar programs emerging in Asia (e.g., Japan and Singapore). In Europe, cybersecurity of connected products is the focus of the Cyber Resilience Act. International attention to IoT cybersecurity is welcome, but guidelines and standards for cybersecurity must consider mitigations for some of IoT's unique risks. Troubleshooting, patch development, and digital forensics for IoT products require information about "cybersecurity state," which is data about the product or use of the product that helps identify or mitigate threats and vulnerabilities. Capturing this data via logging enables its active use, which can be as simple as pausing login attempts after a set number of failures and as complex as enterprise-level monitoring and response systems. To continue delivery of services, humans rely on in the physical world since IoT products can bridge the digital and physical domains, products may need to create or use information about cybersecurity state either manually or automatically to enable discovery, study, and mitigation of vulnerabilities. The introduction of artificial intelligence (AI) into IoT systems, particularly if related to decision making, amplifies the need for good cybersecurity state awareness to mitigate novel risks, such as entropic outputs from some AI technologies. Despite this, current IoT cybersecurity standards generally better reflect other cybersecurity concepts (e.g., delivery of software updates, protection of data at rest and in transit) than IoT cybersecurity state awareness, if this concept is addressed at all. This workshop will focus on current thought and research related to IoT cybersecurity state awareness with the goal of improving its standardization for IoT and incorporation in standardization efforts for IoT cybersecurity, including, but not limited to, topics such as:

- Risks faced by IoT potentially mitigated via cybersecurity state awareness
- Standardization of approaches to cybersecurity state awareness for IoT
- Novel tools and techniques for capturing or using cybersecurity state information for IoT
- Challenges capturing or using cybersecurity state information for IoT
- Challenges, opportunities, or other considerations for cybersecurity state awareness when combining IoT with other technologies such as artificial intelligence

Submissions will be judged based on their applicability to one or more of the topics above, the novelty of the work, and significance of the contribution. We solicit papers describing new research contributions in this area as well as case studies, work in progress, preliminary results, novel ideas, and position papers.

Papers should be at most six pages (excluding references) using the appropriate template format. Papers should be succinct but thorough in presenting the work. Typical papers will be 5-6 pages long (plus references), but papers can be shorter (e.g., 2-3 pages) if, for example, they present a novel idea with limited preliminary results or a position likely to drive a lively discussion. Shorter, more focused papers are encouraged and will be reviewed like any other paper. If you only need 2 or 4 pages (plus references) to clearly explain your work or idea, please submit a paper of that length. Reviewers will be instructed to assess the value of the talk to the workshop audience irrespective of the paper length; however, we stress again that the presentation should be sufficiently thorough for reviewers to make this evaluation. Submissions may be made via this Workshop's Editor's Assistant (EDAS) page.

Workshop papers will be made available to attendees prior to the workshop. Paper presentations will be approximately 10-12 minutes in length followed by 5 minutes of questions and answers. Presentations are expected to be made in-person; remote presentations may be accommodated for extenuating circumstances at the discretion of the workshop and conference organizers.

The deadline for submissions is August 4th, 2024, and authors will be notified of acceptance to the workshop by August 26th, 2024. Camera ready (i.e., final) versions of accepted papers must be submitted by September 13th, 2024.

This Workshop will occur at the 2024 IEEE World Forum on the Internet of Things, which is planned for November 10th-13th, 2024 in Ottawa, Ontario. Exact date and time of the Workshop will be determined closer to the conference.

You can find out more at our event page or by emailing iotsecurity@nist.gov