CS3STHLM 2021 Call For Participation

CS3STHLM is a conference focused on advancing the protection of critical infrastructure, industrial control systems and smart (but insecure) things. In 2021, we will run the CS3STHLM conference for the 8th time, and we plan to make it better than ever before.

At the time of writing this document we have no idea on how the pandemic will affect the event in October 2021 regarding physical meetings or not. So all information below is for an actual on-site conference, and needs to be altered if that type of event is not possible to arrange.

SUMMIT OVERVIEW

- One main stage with appx 16 speaker slots + two other stages used for parallel sessions, breakout sessions, interviews, panels, demos, lightning talks, work-in-progress, etc
- Extra conference rooms for up to 20 people that can be used for workshops, labs, demo etc
- Summit audience spans multiple business sectors, areas and industries and is a mix of management, policy makers, government employees, IT/OT staff, process engineers, security experts, vulnerability resear- chers, etc
- We prioritize real-world experiences and real-world solutions.
- We focus on providing all attendees with actionable takeaways
- More info on our web https://cs3sthlm.se , check videos from old conferences https://www.youtube.com/ cs3sthlm

IMPORTANT DATES

- Submission deadline for abstract – Mars 15, 2021
- Author notification – April 15, 2021
- Deadline of full presentation material – October 18, 2021
- Start of conference/expo/trainings – October 26-28, 2021

CS3STHLM 2021 Call For Participation

•

CS3STHLM 2021 THEME – SMARTER!

We have chosen **Smarter!** as the theme for the 2021 conference. And yes, we did choose that theme for last years conference as well, but then 2020 hit us like a ton of bricks and we had to change almost everything. So the theme never really came to use, and as sustainability is smart – let's reuse it!

There are many reasons for this selection: "Smart" is used to describe many current things in the cyber industry – such as "SmartGrid", "Smart Meters", "Smart Cities" and "smart vehicles". Smarter is also what the adversaries have become, finding more exotic vulnerabilities, and launching attacks built with increasing domain knowledge and sophistication. We, as pe- ople working in this profession, must be smarter, and we must design and implement smarter methods, tactics and solutions to be able to detect and protect against these attacks. At the same time, we cannot forget that we live in a complicated world where "stupid" still is a highly viable option: "Admin/admin" is still used as login combinations, end-of-life firewalls are still in use, old bugs are fore- verdays as updates are not done, as is negligence to separate sensitive infrastructure from the rest of the bu- siness. That being said, we will accept all types of submissions, no matter if they describe "smarter" or present the "stupid". The thing that matters is that all the conference participants will be **Smarter!** in the end of the day!

SUBMISSIONS

Submission should be sent via email to following adress: cfp@cs3sthlm.se

PLEASE NOTE - Submitted material:

• both for CFP and final material, must be in **ENGLISH**

• should use this form, and supply info in PDF, docx, or raw ASCII format •

• Submission **must be vendor-neutral, non-advertising material,** and it is for submissions to the conference 21-22 October. Logo is OK on first powerpoint slide, but no bio in presentation material. Bio - "who am I, where do I work, etc" will be displayed separately on large screens on stage

CS3STHLM 2021 Call For Participation

NON-EXHAUSTIVE LIST OF TOPICS OF INTEREST

Cyber security management, incident handling and response, forensic, security failures, research and experiences of attacks and attack methodology related to:

- Industrial Control Systems (ICS) and SCADA systems
- Operations Technology (OT), and the interactions/integrations between OT/IT
- Smart grid, smart cities, smart homes, smart meters, smart sensors
- Embedded systems, Industrial Internet of Things (IIoT)
- Safety Systems (SIS), ESD (emergency shutdown devices), High Security Devices
- Sensors, actuators, peripherals
- Critical Infrastructure
- Industrial Automation
- Building & Facility Automation
- Automotive, transport, air & space industry
- Chemical industry, Oil & Gas
- Medical devices and medical technology
- Robotics
- Nation state involvement in attacks, strategic conflicts targeting critical infrastructure, cyberwar
- Security assessments and penetration testing in ICS / SCADA / OT/ critical infrastructures / smart *
- Security and vulnerabilities in PLCs, RTUs, field devices, com infrastructure
- Safety-Security Interactions
- Threat intelligence and threat hunting
- Mitigation strategies and mitigation technologies
- Vulnerability research
- Hardware Security Solutions
- Success stories from asset owners, users, CSO's, CIO's, CEO's etc
- Failures, bad examples from asset owners, users, CSO's, CIO's, CEO's etc
- Human Factors Security
- Experiences on implementing standards IEC 62443, ISO 27019 or regulations (NIS directive, NERC CIP, etc)
- Experiences from designing and implementing security architectures, security zones, secure remote access
- Experiences from running or participating in cyber exercises
- Important lessons learned from failures or incidents
- Interesting ways of applying new technology (AI/ML, cloud, etc) to get better security
- Security and privacy
- Security patterns
- Security policies
- Security economics
- Non-technical security issues, e.g. social engineering, governance, security management, etc