Dagstuhl Seminar 22171: Digital Twins for Cyber-Physical Systems Security

April 24 – 29, 2022

Version 1.4

Organizers:
Mohammad Al Faruque (University of California, US) alfaruqu@uci.edu
Alvaro Cárdenas Mora (University of California – Santa Cruz, US) alacarde@ucsc.edu
Simin Nadjm-Tehrani (Linköping University, SE) simin.nadjm-tehrani@liu.se
Edgar Weippl (University of Vienna & SBA Research, AT) edgar.weippl@univie.ac.at

Collector:
Matthias Eckhart (University of Vienna & SBA Research, AT) meckhart@sba-research.org

1 Objectives and Topics of the Seminar

The aim of this Dagstuhl seminar is to investigate the benefits and challenges of implementing the digital-twin concept and other emerging technologies for the purpose of improving the security of cyber-physical systems (CPSs). Toward this end, we address pressing problems of creating, operating, and maintaining digital twins, and explore attractive security applications, such as intrusion detection. The developed concepts and methods will be a result of interdisciplinary work conducted by academics and industry professionals from the fields of computer science, automation engineering, and data science.

Expected Output The seminar is intended to serve as an interdisciplinary, open knowledge-sharing platform that connects researchers and facilitates scientific exchange. During the seminar, the participants will have the opportunity to work in groups on one of the seminar's topics. Ideally, the ideas generated during the breakout sessions will be refined by the group members after the seminar and published as a joint research work.

Research Topics To set the frame for this seminar, we identified three topics that will be covered in plenary sessions and breakout sessions. In each plenary session, lightning talks will be held that should motivate the collaborative work in the breakout sessions.

The main topics and motivating ideas are:

1. *Security-focused Digital Twins*:
   - Definition of the term *digital twin* in the security context and differences to other concepts, such as cyber ranges and information models
   - Emulations, simulations, and testbeds as key technologies and methods for digital-twin implementation
   - Relation between the concept of digital twins and smart manufacturing plants
   - Knowledge retrieval for digital-twin generation (in greenfield and brownfield settings)
   - State replication and synchronization (digital twin and physical counterpart)
   - Security applications
2. *Intrusion Detection*:
   - Physics-based IDSs
   - Behavior-based and anomaly-based IDSs

- Integrating process semantics into IDSs

3. *Proactive and Reactive Attack Response Mechanisms*:

   - Response strategies for control systems
   - Attack-resilient CPS architectures
   - Identification and assessment of countermeasures
   - Reconfiguration of CPSs

2 General Information

SARS-CoV-2 Prevention Measures The seminar takes place under strict hygiene and preventive measures. We expect that all participants have read and adhere to the protection and hygiene concept of Schloss Dagstuhl.[1] If you have additional questions regarding this concept, please send an e-mail to `service@dagstuhl.de`.

Collaborative Work Please follow the Dagstuhl Wiki[2] for further information, which can be accessed using your personal DOOR credentials. The findings of breakout sessions and other key results should be documented in our shared Google Drive directory.[3] Furthermore, note that we have setup a group on Signal[4] to facilitate communication among participants. You can join this group via the link[5] or by using the QR code shown in Figure 1.

Lightning Talks Please avoid conference-style talks, do not (only) propose solutions but allow your talk to raise open research questions. Leave enough time at the end of your talk for an open discussion. Furthermore, take the highly interdisciplinary setting of this seminar into account; try to avoid acronyms and technical jargon. We kindly ask you to upload your slides to the seminar materials website[6], which can be accessed using your personal DOOR credentials.

Figure 1: QR code to join the Signal group.

[1] `https://www.dagstuhl.de/program/planning-your-visit/sars-cov-2-prevention`

[2] `https://angelina.dagstuhl.de/guestWiki/index.php/22171`

[3] The link to the Google Drive directory can be found at the Dagstuhl Wiki.

[4] `https://signal.org/`

[5] `https://signal.group/#CjQKIIoCv8ylCTKZAequdR7IYl2ZMLDklr5stGesCtlOzOyPEhCYA48EAKSuAGajBQmryvsd`

[6] `https://materials.dagstuhl.de/index.php?semnr=22171`

3 Schedule

Monday, 25th April 2022

09:00 **Welcome Session**
Alvaro Cárdenas Mora, Simin Nadjm-Tehrani, Edgar Weippl

10:15 **Coffee Break**

10:30 **Session: Bridging the disciplinary gap**
A roadmap toward a digital-twin framework for cyber-physical systems security
Matthias Eckhart, Edgar Weippl
RICSel21: Attacks in a virtual power network
Simin Nadjm-Tehrani
Digital twins for CPS security
Alvaro Cárdenas Mora
Detection of cyber-physical attacks with IIoT data
Marina Krotofil

12:15 **Lunch**

13:30 **Breakout Session I: Brainstorming and discussion of open problems**
All participants

14:30 **Break**

14:45 **Breakout Session I: Brainstorming and formation of working groups**
All participants

15:30 **Short Coffee Break (Breakout Session I continues afterwards until 17:00)**

17:00 **Group discussion on the research topics of the working groups**
All participants

18:00 **Dinner**

Tuesday, 26th April 2022

09:00 **Lightning Talks I**
High-fidelity cyber and physical simulations of water distribution systems with DHALSIM
Nils Ole Tippenhauer
Building high fidelity replicas for CPS security research — Lessons from a testbeds program
Awais Rashid

10:00 **Coffee Break**

10:30 **Lightning Talks I**
Attack-resilient control using model- and data-based intrusion detection
Henrik Sandberg
Control-theoretical analysis of systems under CPU starvation attacks
Martina Maggio

12:15 **Lunch**

14:15 **Breakout Session II: Working groups**
All participants

15:30 **Short Coffee Break**

15:45 **Breakout Session II: Working groups**
All participants

17:00 **Reports from working groups**
Short presentation of initial ideas and general discussion
Group chairs

18:00 **Dinner**

Wednesday, 27th April 2022

09:00 **Lightning Talks II**
Securing cyber-physical systems with varying levels of autonomy
Miroslav Pajic

10:00 **Coffee Break**

10:30 **Lightning Talks II**
Integrated distributed SCADA security in power grids
Anne Remke
Towards semantically enhanced digital twins
Helge Janicke

12:15 **Lunch**

13:30 **Breakout Session V: Working groups**
All participants

15:30 **Break**

16:15 **Breakout Session V: Working groups**
All participants

18:00 **Dinner**

Thursday, 28th April 2022

09:00 **Session: Lightning Talks III**
Reverse engineering Siemens PLCs: Lessons learned for today and tomorrow
Ali Abbasi

10:00 **Coffee Break**

10:30 **Session: Lightning Talks III**
Modeling in the safety lifecycle of radiation monitoring systems at CERN
Katharina Ceesay-Seitz
Dataset availability and requirements for CPS security research
Magnus Almgren

12:15 **Lunch**

14:00 **Hiking trip or free time**

18:00 **Departing Reception**

Friday, 29th April 2022

09:00	**Presentations of results** *Group chairs*
10:45	**Coffee Break**
11:00	**Closing Session** Wrap-up, next steps, and feedback *Organizers*
12:15	**Lunch**
14:00	**Departure**